LEARNING MADE EASY

Fortinet Special Edition

# Cybersecurity Mesh

for dummies®
A Wiley Brand

Quickly respond to threats

Work from a centralized platform

Easily integrate tools

Brought to you by

FORTINET

**Questions?** Möbius Partners is an IT solution provider specializing in networking and security. We can help! info@mobiuspartners.com

**Dan Sullivan**

# About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 595,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the https://www.fortinet.com/blog, or https://www.fortinet.com/fortiguard/labs.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Cybersecurity Mesh Architecture

Fortinet Special Edition

**by Dan Sullivan**

for dummies®
A Wiley Brand

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Cybersecurity Mesh Architecture For Dummies®, Fortinet Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2023 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Fortinet is a registered trademark of Fortinet, Inc. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-16164-5 (pbk); ISBN 978-1-394-16165-2 (ebk)

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Manager:** Jennifer Bingham
**Acquisitions Editor:** Ashely Coffey
**Editorial Manager:** Rev Mengle
**Business Development Representative:** Cynthia Tweed
**Content Refinement Specialist:** Saikarthick Kumarasamy

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Introduction

The cyber threat landscape is vast and always changing. It can seem like each new security solution brings new ways attackers can bypass your defenses. Security hardening tools, as well as the methods bad actors use to get around them, are part of a dynamic landscape that can be frustrating to navigate.

If there is one thing you take away from this book, it should be that a strong security posture today requires integration of and collaboration between the many deployed security solutions and tools. Modern technology stacks are widely distributed and hard to manage when separated into individual siloes, so integration, aggregation, and coordination are crucial to a successful security strategy.

Cybersecurity mesh architecture (CSMA) can be a great asset to large organizations. CSMA is a security architecture philosophy that champions tool integration and data aggregation to do just that. It also provides unified threat intelligence and AI-supported automation to achieve a dynamic security posture that can respond faster than attackers.

## Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless! Mainly, that you're a chief information officer (CIO), chief information security officer (CISO), vice president, architect, engineer, SOC professional, threat hunter, endpoint security manager, or administrator working on an enterprise security, networking, or infrastructure team. As such, this book is written primarily for technical readers with at least a basic understanding of security and networking technologies and challenges.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and when you finish reading it, you'll have more trust in your knowledge of CSMA.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Icons Used in This Book

Throughout this book, you will see special icons to call attention to important information. Here's what to expect.

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with birthdays and anniversaries!

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — you'll appreciate these useful nuggets of information and helpful advice.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

# Beyond the Book

There's only so much space in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fortinet.com`.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Challenges facing cybersecurity experts today
- Siloed security systems and threat readiness
- How attackers take advantage of siloed systems

# Chapter 1
# The Dynamic Challenges of Cybersecurity

This chapter looks at the primary concerns of cybersecurity overall, and how they have shaped common security philosophies seen in organizations today.

## The Core of Cybersecurity

At the end of the day, cybersecurity is mostly about data. How is it stored? Who has read access? Who has write access? How is it moved? These types of questions about your data make up the majority of the cybersecurity core. As long as there have been IT systems, there have been attackers and security personnel working to prevent them from accessing internal resources.

REMEMBER

Data becomes almost useless once it loses integrity. Unless there is a way to restore compromised data to a previous undamaged state, organizations might spend large amounts of money and time repairing and regathering the lost data. Protecting the integrity of your data is one of the most important aspects of a comprehensive security system and should be at the front of your mind when looking for any security solution.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Another crucial part of a hardened security ecosystem is proper access controls. While appropriate access permissions prevent unauthorized people from accessing sensitive information or resources, access controls also play an important role in monitoring and logging an entire IT ecosystem.

Finally, availability, not just of data but of services and tools, is critical to the day-to-day functioning of an organization. Malware packages, as well as DDoS and other network-based threats, can shut down entire IT systems for days, or longer, if not swiftly remediated.

# The Basics of a Security Ecosystem

Every organization has different security needs, business goals, staffing limitations, and more, but there are some common challenges every security system should address to be suitable for the modern threat landscape.

## Who has access?

Access controls and identity management are more than just a way to distribute digital ID badges. Identity and access management allows administrators and managers to think about and organize teams in a security-centric way.

Data access is not static, however. Roles change, personnel move positions, and business needs and goals shift over time. Data access permissions should reflect the dynamic nature of organizational goals. This means access should change and be updated along with any project completions or position changes.

TIP

When a project wraps up, administrators — or others in charge of identity and access management — should check if any permissions need to change.

Keeping access and identity management up to date isn't just a security issue because staff who have no need to view or edit certain tables shouldn't have access to them. Keeping up with role changes and project goals in terms of access controls also aids in proper monitoring and logging, which can have larger security consequences.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Well-managed access controls both prevent unauthorized access to sensitive data and help SecOps teams monitor broader security concerns.

Each portion of an organization's security system is connected to the others. While many security solutions attempt to treat a single problem as existing in a vacuum, it simply isn't true with the complex IT systems of today.

## How do distant resources communicate securely?

Network security is another concern for appropriately securing internal resources. On-premises servers, cloud resources and tools, at-home and edge devices all need to be connected over a network for a modern organization to function. Securing these geographically separate resources is the center of network security.

Cloud applications and workloads, on-premises computers, laptops, corporate tablets, and phones all make up the attack surface. The attack surface is every item that could act as an entry point into your internal systems or give access to proprietary information. With the push to work from home, the attack surface has expanded and continues to grow quickly.

TIP

Email phishing scams are more popular than ever. The increasing number of staff working from home means personal electronic devices are more likely to be the targets of corporate-targeting attacks.

A broad attack surface means more opportunities for bad actors to attack an organization's systems. Each laptop used for business-related work, connected to a home network, is an access point into internal resources. Network security not only involves VPNs and access keys for access reasons, but also, like identity management, promotes comprehensive monitoring and logging to increase the overall security of an organization.

WARNING

Unsecured communications also leave an organization vulnerable to attacks that halt availability to services and resources. Today, enterprises depend on IT systems for even the most basic day-to-day functions. Losing network communication or access to internal or external systems could mean your entire organization coming to a stop.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# One Problem, One Solution

In the past, cybersecurity measures have targeted single elements of the security landscape, creating siloed systems. This method of securing IT systems involves pinpointing a problem area, such as the need for a firewall, and using a single solution to fill the one defense gap. This creates a silo, meaning an organization's IT systems will be split into branches of separated visibility and functionality.

Take access control solutions as an example. Identity and access (IAM) solutions often incorporate access controls, authorization and permission settings, and sometimes, authentication tools. These are all critical cybersecurity tools and are present in any comprehensive security ecosystem. However, IAM is just a part of the entire security problem.

Similarly, network security tools, like perimeter defense solutions, traffic flow monitoring, intrusion detection, and DDoS protection, only cover a section of an organization's security needs.

Here is a quick list of some other types of security solutions that often lead to a siloed infrastructure:

- Encryption solutions (at rest and in transit)
- Web application security solutions
- Threat intelligence tools
- Data loss prevention services and solutions

The philosophy of "one problem, one solution" is outdated when it comes to cybersecurity. There are modern tools like cybersecurity meshes that can help to integrate previously disparate security systems into a single unified system that can benefit from the strengths, and reduce the weaknesses, of each individual component.

# The Problem with the Silo

The simple answer to why security silos no longer work is that security ecosystems have gotten too complex. Cloud technologies, at-home workers, on-premises resources, and edge devices all



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

add up to an intricate web of security risks and, using the silo philosophy, might seem ready for one problem, one solution security tools. But the lack of visibility and control is simply too damaging to a cybersecurity ecosystem considering today's threat landscape.

Each siloed system has to be a part of the larger security picture. Network security tools, IAM solutions, and endpoint security should all be visible and manageable in a centralized place. Modern threats have ways of countering or avoiding single point security controls and a comprehensive view of your security environment is a must to detect today's attacks.

Consider how attackers can avoid detection when operating in an enterprise with siloed security tools. For starters, an attacker might use a trusted platform, like a penetration tool to install malware or create communication channel between a trusted server and a malicious server. Next, the attacker exfiltrates data using the communication channel to the malicious server. Assuming the trusted server regularly sends data to external servers, this kind of data transfer will not seem unusual. What is missed is the fact that penetration testing may set up communication channels for the duration of a test but not keep the channel open for long periods of time. By using siloed security information systems, we are not able to see connections between events that would look suspicious and prompt further investigation.

Simply put, piecemeal security systems are too slow. Response times can suffer due to confusion and disorganized tools required for remediation and detection, siloed systems are often difficult to scale, and the possibility of human error is much higher than when using an integrated security solution.

REMEMBER

Human error is an especially important consideration when talking about siloed security systems. Alert fatigue is a plague on security teams and can lead to serious lapses in threat preparedness.

## Modern solutions

The last decade has seen the security market answer the call for integrated solutions. Some early examples of tools that aimed to simplify security operations were security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions. Although SIEM and SOAR can be



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

useful solutions, and were important steps forward in IT security when they came into common use, by themselves they are not sufficient to defend against modern threats.

SIEM solutions primarily gather and analyze security alerts. With so many security tools sending a variety of alerts to security staff, SIEM provides an important service in streamlining alerting and logging requirements, especially for restrictive industries such as health care and finance. However, it is usually not streamlined enough. Alert fatigue can happen when overworked security professionals are bombarded with security events, eventually leading to them ignoring or missing important alerts. Moreover, SIEM is a data intake tool, meaning that it ingests data to provide some degree of aggregated insight but does not deliver actionable outputs or automation to enable timely response to threats.

Similarly, SOAR solutions were a boon to enterprise security, but have been surpassed by other security solutions recently. SOAR platforms often incorporate detection tools into their system to leverage machine learning and automation functions that facilitate faster detection and response times. Obviously, SOAR can be a powerful tool in most cybersecurity ecosystems, but the complexity and visibility requirements of modern systems has surpassed SOAR's capability to effectively orchestrate security for a large organization.

One of the most recent innovations in the cybersecurity space is the cybersecurity mesh architecture. Cybersecurity meshes are systems designed to incorporate disparate parts of a large security ecosystem, make them more manageable and scalable, and facilitate collaboration and coordination between solutions and tools. The result is faster identification and automated responses to threats.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- What are distributed systems?
- Why are they so hard to secure?
- The human element has a big impact on cybersecurity needs

# Chapter 2
# Understanding Today's Security Challenges

The modern cybersecurity landscape is complex, varied, and dynamic. New threat types emerge every year, white hats and other security professionals find new ways to secure sensitive data while attackers are on the lookout for new ways to get around those defenses. There are smart, determined people on both sides innovating to find the next big security loophole.

One of the most important security developments of the past decade is the expansion of the attack surface. Every element of an IT ecosystem — each database, personal computer, and network port — is a potential doorway into an organization's internal systems.

This chapter discusses the nature of these widely distributed systems, how their expansiveness impacts cybersecurity, and even covers how humans can contribute to today's security challenges.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Complex Systems and Operations

The increasing breadth of a modern enterprise scale infrastructure presents new and unique hurdles to cybersecurity operations. The growing number of edge devices, hybrid cloud systems, employees that work from home, and more add up to a large, intricate attack surface that only the most modern security tools are equipped to handle.

## Distributed systems

Almost all large organizations have to face the effects of highly distributed IT systems, and there is not a one-size-fits-all solution. Each organization has specific business and operational needs that have to be met, unique ecosystems that have to be hardened, and varying resources available to commit to SecOps.

However, there are some common ways enterprises distribute their systems. While the particulars of these distributions will depend on your specific needs, here are some of the most frequent ways an attack surface expands:

- Multiple corporate campuses
- Branch offices
- Multiple public clouds
- Edge computing
- IoT devices

REMEMBER

Large organizations will likely manage some combination of these resources, or even all five of those listed. Furthermore, the administrative complexities of these resources compound each other.

For instance, say your business operations are spread across several offices. Each device, network, and on-premises computing resource or data base would need to be secured. Given the advantages of cloud technologies, it's likely public clouds would play a large part in day-to-day operations. For each office, communications between public clouds and on-premises devices and applications would need to be secured, visibility and policy enforcement requirements would increase, and most likely, the volume of data



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

and logs to sift through would increase. All that activity could lead to detection and response times taking a big hit.

## Challenges of highly distributed systems

The main challenges of maintaining a hardened distributed ecosystem can be split into three overarching problems:

- Distributed systems are porous.
- Distributed systems can be opaque.
- Distributed systems are difficult to manage.

What does that mean? First, highly distributed systems are porous because the various systems need to communicate with one another. From a security standpoint, this encompasses both network communication requirements and user or device authentication.

Both authentication events and opened networks have to be monitored. Edge computing, remote offices, and other external devices all need access to company networks and systems. This means opening the door for communication that should get in, and maybe some that shouldn't if you aren't careful.

Authentication presents a similar problem. Each user or device attempting to access a network is a potential security incident. User devices are particularly vulnerable to becoming carriers of malicious code given the rise in phishing attacks. Legitimate users can be hijacked by attacker code, not only from phishing threats, but compromised web applications that inject malicious code into user devices.

One of the biggest security concerns right now is public clouds. According to the Fortinet 2022 Cloud Security Report, 75 percent of respondent organizations are either very concerned or extremely concerned about cloud security, which is a lot! Public cloud adoption leads to an increase in configuration and management overhead, new authentication challenges, and increased network monitoring requirements.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WARNING

The Fortinet report also found that 62 percent of organizations thought cloud misconfiguration was the top security threat when it comes to public clouds.

## Lack of visibility

Traffic and general activity monitoring are key pain points for security professionals, as they are the ones most often on the front lines trying to sort through a web of interconnected systems to find a threat's source.

Any highly distributed system is, by definition, made up of many applications, servers, and services. This large number of components makes the ecosystem difficult to monitor, not only because it's simply a lot of individual elements to keep an eye on, but log overload and complexity of communication make it hard to see what's actually going on.

There are many modern security tools that make generating log and monitoring data easy, but analyzing that data is another story. The first problem is simply the volume of data generated with SIEM and other solutions. Truly threatening events can get lost in the haystack of alerts, unusual usage patterns can go unnoticed due to the overwhelming amount of monitoring data, and security professionals suffer from burnout trying to sort through the deluge of information.

TIP

Lots of log data isn't always a bad thing! Many organizations require extensive log collections for audit or industry regulation purposes. Visibility is the real issue, not the number of alerts.

Siloed security solutions also cause data integration to be a challenge. The large volume of logs and monitoring information will arrive from different tools and artificially separated regions of your ecosystem, meaning that analysis is delayed to properly integrate that data so it can be leveraged.

Speaking of speed, IT security pros don't have the luxury of working at a leisurely pace when a threat event occurs. Time to detect is a crucial metric in assessing the effectiveness of your organization's attack readiness, and for good reason. The longer a bad actor has access to internal systems, the more damage they can do and the more money and time it will cost an organization.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TECHNICAL STUFF

Mean time to detect (MTTD) and mean time to remediate (MTTR) are important metrics to look at when assessing the effectiveness of your security systems. SecOps tools and practices will change over time to meet new threats, but these metrics should follow a downward slope as time goes on.

In the end, visibility isn't just a matter of knowing an attack is occurring. It is about finding and properly understanding a threat. Context matters. For example, a network security alert might point to a vulnerable port, but closing that port might not be the whole solution. Why was the network compromised in the first place?

Perhaps an edge device had been infected with malicious code and this was the real culprit, but without comprehensive visibility, security staff might not have all the information needed to identify the compromised device, such as data that shows unusual activity coming from that device. Modern IT ecosystems are large and interconnected, so visibility is about seeing both the big and the small pictures.

## Policy and control management difficulties

It's no secret that modern security controls require well defined and crafted policies to properly function. In fact, according to the Fortinet 2022 Cloud Security Report, cloud configuration was the top security concern for most organizations, with insecure APIs and data exfiltration running just behind.

Policy consistency is difficult to maintain across highly distributed systems. Across all the tools, solutions, and resources there will be many policy control requirements, each with different idiosyncrasies and upkeep needs. Again, this is the result of security siloes.

Furthermore, policy control needs will likely drift over time, requiring reassessment by administrators, business leaders, and security pros. Each siloed system will drift at a unique pace depending on operational requirements and the changing threat landscape. Some organizations opt to make controls easier to change, but this can have serious security implications.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Regardless of your SecOps philosophies and methods, staying agile and having the capability to adapt to new security threats is a must. New threats emerge every day, attack patterns change, and security teams should be able to change strategies to meet these new attacks.

Taking a soft approach to policy control can cause policies to overlap, which can have unintended negative consequences, such as producing redundant or false alerts. Simply put, any "quick fix" solution to the complex problems presented by siloed security systems is likely to create new vulnerabilities in an organization's IT ecosystem.

# The Human Element

There are two main issues when it comes to forming a cohesive, efficient security team: lack of experienced security pros and expertise siloes.

## The skills gap

First up, many security teams are having a hard time finding new talent and, over the past several years, the hiring market for cybersecurity pros has become increasingly competitive. There are a few reasons this is happening.

One primary driver of the security expert drought is that the demand for cybersecurity skills is outpacing the supply. Security threats are increasing in complexity and number, and organizations find themselves requiring larger and larger SecOps teams. Yet, at the same time, organizations are driving toward greater digital acceleration of their business which results in an ever-growing deployment footprint, particularly in the cloud. Another driver is that even if a business does put together a pool of potential security hires, the desired expertise among those chosen is lacking.

It is becoming more difficult to acquire necessary security skills that organizations are looking for. It takes time to develop true expertise, and with how fast security technology and the threats working against them develop, how can someone actually attain the expertise required by an enterprise SecOps team?



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Of course, there are highly skilled security experts out there. There just aren't enough of them to fill the many high-skill security roles needed in modern enterprises. Unfortunately, there's also another issue.

## Expertise siloes

The second half of the larger personnel problem is expertise siloes. This is yet another hurdle brought on by security ecosystem siloes. Splitting networking, endpoint, and database security between different teams, each with different area-specific experts, often means that security staff itself is siloed!

With this SecOps staffing method, vital security knowledge is spread throughout an organization rather than centralized in a unified security operations body where experts can easily work together to solve problems. An expert in data loss prevention may be on one team, while an authentication expert is on another. If data exfiltration from an on-premises database occurs, both are needed to analyze and remediate the situation, and yet they are separated and might not even be used to working with one another.

Again, the complexity of distributed systems requires integration of many, if not all, elements of the ecosystem: system controls, security staff expertise, management and analysis tools, and more. Luckily, there are solutions to the various challenges that come with wide IT systems, such as cybersecurity meshes.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Overview of the security challenges CSMA aims to tackle
- Basic overview of security meshes
- Primary benefits of using a security mesh

# Chapter 3
# The Need for Cybersecurity Meshes

Cybersecurity innovations are not just found in new tools and technologies, but in organizational and architectural philosophies as well. Event detection and logging, analysis tools, and playbook management solutions have all come a long way in the last decade, but the complexity and wide distribution of today's attack surface calls for a more integrated approach to security.

This chapter discusses some of the specific challenges that have brought about new cybersecurity mesh architecture (CSMA) platforms, what those platforms actually do, and explains the primary benefits of using CSMAs.

## Why Do You Need Cybersecurity Meshes?

Modern cybersecurity tools are powerful, but complex. Security information and event management (SIEM) tools, endpoint detection and response (EDR), network detection and response (NDR), and many more have been boons to security operations teams. Each of these advanced tools add an important piece to the



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

larger cybersecurity puzzle. However, there is one problem that most of these tools have in common: They generate a lot of data and alerts.

## Too much data

So many modern business processes rely on fast and accurate data collection and processing. Security is no different. But there can be too much of a good thing. Data overload can be a serious issue for security teams. They can become overwhelmed with alerts, miss important events, ignore events due to alert fatigue, or simply not have enough time to process and leverage all the data their security tools are generating.

SIEM solutions, along with most detection-oriented tools, produce massive amounts of event data. They're powerful tools and are required for deep, accurate monitoring of their respective systems. All this data, however, is dead weight without a security infrastructure that can support fast aggregation and integration. Plus, with all this data, the signal-to-noise ratio matters greatly for security teams to be effective.

Unfortunately, enterprises don't have the option to scale down security data collection. Agile, cutting-edge operations often require continuously shifting and adding to their attack surfaces with new endpoint and edge devices, cloud computing resources, and more.

## Analysis challenges

Sorting through the sheer amount of data isn't the only issue presented by the large volumes created by modern security tools. This data also needs to be analyzed and leveraged to get value out of your extensive suite of security solutions.

One of the first, and most difficult, challenges is integrating data from multiple source systems. For example, network logs and application logs both hold valuable information but they are often tracked separately. A security analyst might notice anomalous data in network logs and wonder about the implications for those anomalies. The data is at the network level and does not give insights into unusual activities that may be going on at the application level. To understand that, the analyst would have to



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

switch to another tool to start analyzing application logs. At this point the process of correlating data from network and applications logs can be slow, tedious, and error prone.

REMEMBER

Even when data is integrated, analysis can be difficult. Integrated data solves some problems for analysts but it extends the common problem of having too much data to work with effectively without proper tools. Analysts need to be able to filter data to focus on time periods or infrastructure of particular interest. Once their data is narrowed, they will often want to consider aggregating data along a variety of dimensions, such as time, resource type, log severity level, and so on. Ad hoc query tools that work across integrated data sets are needed to address this problem.

## Security happens in real time

Mean time to detect (MTTD) and mean time to remediate (MTTR) are two of the best ways to assess your organization on its overall cybersecurity performance. Quick detection of a threat means security teams can begin finding the source of an attack and halt the intrusion before serious damage is done. All of this happens in real time, however, so security teams must have access to tools that allow them to get the job done efficiently.

WARNING

If there is a breach of your defenses and an attacker can inject malicious code into a system and execute that code, the damage they do will be at the speed of the machines. Humans can't be expected to manually respond at anywhere close to what is needed to block such attacks. The best outcome when such attempts occur is to block them completely, the second-best thing is to detect the event quickly and respond quickly.

Responses to security incidents vary depending on the type of incident. If malicious code is detected in the traffic from a known IP address, that address can be blocked. If a process running on a database server is exfiltrating large amounts of data, that process can be terminated. Now, these examples are oversimplifying the actual response, which might include collecting data on the attack or possibly monitoring the process of the attack to collect more information about the attacker's methods. The important point is that whatever our response is, whether it is to block or allow it to continue and observe, that response needs to happen in as close to real time as possible.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# What Is a Cybersecurity Mesh?

While there will be more detail about what components make up a security mesh later, for now let's quickly go over the basics.

As defined by Gartner in their 2021 Top Strategic Trends for 2022: Cybersecurity Mesh report, a CSMA platform is "a composable and scalable approach to extending security controls, even to widely distributed assets." Additionally, a security mesh should be compatible with "modular" approaches to IT infrastructure, such as with multi-cloud or hybrid cloud systems.

A CSMA platform groups existing security and analysis tools into layers, with each layer able to interact with those above and below it. This forms a web of functionality, allowing complex distributed systems to communicate with and benefit from one another. All of this then feeds into centralized dashboards and controls that streamline security operations.

# Cybersecurity Mesh Benefits

Cybersecurity meshes start from a simple idea: If you can reduce the time needed to collect and organize security data, then you can spend more time planning for and responding to threats. A platform that enables just this would be a great asset to any enterprise's IT operations, but cybersecurity meshes can go further by increasing security ecosystem visibility, reducing operational complexity, and increasing security intelligence sharing across an organization.

## Boosting visibility

As discussed in Chapter 2, visibility is about seeing and understanding the many parts of a distributed security infrastructure. CSMA's integration-centric approach to IT systems increases visibility by aggregating security data and centralizing detection tool information. In turn, this aggregation allows security teams to discern patterns more easily in their data.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cybersecurity meshes integrate with existing data collection and threat detection tools by gathering the outputs of these systems for further processing and analysis. Whether they are firewalls, identity and access management tools, or endpoint protection solutions, a properly implemented mesh can gather data from each of them so that security teams can gain valuable threat intelligence.

A second boost in visibility is a bit more subtle. Identifying patterns in aggregated security data is a powerful way to pinpoint well-hidden attacks. With a distributed system generating security data across an array of devices and tools, it can be difficult to make connections between events. For instance, a small increase in compute resource usage on a cloud server might seem normal out of context, but when combined with an IAM incident and network event, the cloud security issue is clearer.

Again, merely seeing the data from each security solution is not enough. A hardened security infrastructure allows security teams to better understand the connections between elements.

## Reducing complexity

In the case of cybersecurity, increased data aggregation usually goes hand-in-hand with a reduction in overall complexity. Siloed security resources are difficult to manage, as each section of an organization's security ecosystem will have different operational upkeep needs, and this kind of structure can separate experts that should be communicating with one another.

CSMA reduces complexity by integrating siloed security systems into a centrally observable and controllable operations dashboard. This kind of operational change lets SecOps staff respond to security incidents more quickly and efficiently. When suspicious activity is detected and communicated to staff through the mesh architecture in an aggregated and integrated way, they are then able to prioritize events more accurately. More information, and more centralized controls, enable staff to exercise their security expertise by streamlining security data collection and analysis.

## Intelligence sharing

Speaking of the importance of staff expertise, CSMAs also support more comprehensive threat intelligence and intelligence



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

sharing across an entire security ecosystem and SecOps division. Siloed security tools and devices are problematic on their own, but expertise siloes promote wasting one of the most valuable resources a large organization has: an expert's time and energy.

A well implemented CSMA provides a unified view of the security ecosystem and allows experts to communicate with one another more easily and freely by removing silo barriers. They no longer have to "stay in their lane" because their lane is now the entire security ecosystem. Once again, well integrated data from across an enterprise increases communication and cooperation between all of an organization's resources, including security experts. When security experts can do their job more efficiently and effectively, they can accomplish more with less!

Cybersecurity meshes also enable intelligence sharing between different security tools, including those spread across on-premises and multiple clouds. By streamlining security data collection, a cybersecurity mesh can feed this aggregated data into a threat-intelligence layer. A CSMA would offer analytics aggregation, machine learning-driven security tools, risk scoring, and other analysis tools in this layer. This layer, in turn, can feed into policy making and orchestration tools, visualizations, and more.

## Automation

Attacks are progressive and well-coordinated. They also mask their actions and intents by morphing and adapting their sequence of events to make it more difficult to detect the attack. Security professionals are working against the clock and can't respond to AI-based attacks in time without AI-powered automation. That automation has to operate across the security ecosystem to effectively address the risks posed by weaponized AI.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Covering the three basic layers of a mesh architecture
- How each layer contributes to a hardened security stance
- How the Fortinet Security Fabric fits in

# Chapter 4
# Critical Elements of a Cybersecurity Mesh Platform

While a security mesh architecture is more of a philosophy than a single security solution, there are common elements that should be present in any cybersecurity mesh architecture (CSMA). While the components that make up the foundation of the mesh, such as existing security tools or analysis solutions, might be different in each instance, how these elements are brought together to create an integrated security ecosystem has a basic structure.

This chapter discusses the three layers of any CSMA, how each of those layers interacts with the others, how this architecture contributes to a strong security posture, and how CSMAs, such as the Fortinet Security Fabric, try to bring these elements together.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# The Three Layers of a Cybersecurity Mesh

The three layers of a cybersecurity mesh are integration of data, broad security intelligence, and automated response based on policies and centralized management. A cybersecurity mesh also has three characteristics that span layers: they are composable, distributed, and support collaboration. These three layers and the common characteristics shared among layers are the keys to enabling the benefits of a security mesh.

REMEMBER

Additionally, a successful CSMA depends on quality security solutions, such as NGFW, SEG, WAAP, and EPP security systems. Each of these generate important security data that will be aggregated and analyzed later in higher layers of the architecture. But how does it get there?

## Data integration

The first layer works to incorporate the disparate sources of data across your security systems into a single line of communication. Not only does this set up the data for easier analysis and intelligence mining down the road, it also enables these security products to talk to one another, increasing each component's flexibility and effectiveness.

For example, an identity and access management (IAM) tool might send out alerts only when improper access attempts are made, or accounts are incorrectly created. These are important tasks, but there may be weakness in this tool that can only be made up for with the help of other security systems. With a CSMA, a cloud monitoring tool might be able to correlate unusual cloud compute resource access with a high privilege account, and then question the IAM tool for more information about that account.

A CSMA's data integration layer is more than just an aggregation pathway. It empowers previously siloed systems to more effectively work for SecOps teams by making more complex event correlations.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Broad security intelligence

The next layer in a CSMA is focused on security data analysis and threat intelligence. This layer processes the aggregated security tool data and processes it so that security pros can make informed policy and management decisions. It also provides a centralized analytical space for improving the threat analysis capabilities of your entire security intelligence system.

Many modern security analytics platforms incorporate machine learning, or sometimes deep learning, techniques to increase security intelligence gains and efficiency. These are technologies like EDR, NDR, UEBA and more. Centralized access to your analytic tools combined with consistent, automated data aggregation increase the value of machine learning (ML)-driven tools further by slightly reducing the operational overhead, such as data processing, that is required to fully leverage them. In fact, management and operational simplicity is a great strength of CSMA.

## Automated operations

The third layer aims to streamline policy, posture, and playbook management. The previous two layers that focused on integration and analysis aren't too useful if you can't control how they work. The management layer enables security staff to set policies that determine how and when alerts happen, how their analytics tools process data, and security goals.

Again, centralization and integration are what CSMA is bringing to the table. It allows SecOps management to set policies for any security component connected to the security mesh. IAM controls, zero trust system policies, and SIEM logs can all be configured from one location. Similarly, event playbooks can be set for each integrated security system, and even incorporate several systems for more complex and comprehensive defense responses.

## Centralized operations

The CSMA takes everything under it and utilizes dashboards, operations controls, and visualization tools to bring it all together. The operations dashboard concentrates on the operational aspects of cybersecurity. A full cybersecurity mesh operations dashboard is built over time and should encompass tools for event investigations, event reporting, and various visualization tools. Because



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

meshes promote such comprehensive security data aggregation, risk score visualizations of the entire security stack can also be generated using visualization tools in the layer.

# A Unifying Architecture

The Fortinet Security Fabric is a cybersecurity mesh platform that encompasses a wide range of integrated security capabilities across a broad ecosystem and utilizes artificial intelligence (AI)-powered automation to improve security postures even in the face of complex modern threats. Fortinet has worked hard to incorporate the three core layers of the cybersecurity mesh philosophy to bring organizations a comprehensive security platform that fits a range of infrastructure and deployment styles.

This section discusses how Fortinet employs the central philosophies of cybersecurity meshes to increase any organization's security posture.

## Broad

A well implemented cybersecurity mesh needs a base of observation and analysis tools to collect and process security data across the entire IT ecosystem. CSMA only works if there is enough data to confidently abstract the operations of each endpoint, network, and cloud security solution. This means there must be a broad range of high-quality security systems in place to support the higher layers of the security mesh.

Fortinet provides businesses with a suite of security solutions that cover an array of IT security needs. Network security, zero trust access, and cloud security solutions are all available through the Fortinet portfolio and each component has powerful communication capabilities that allow them to integrate into the larger security ecosystem.

The Fortinet Security Fabric also supports an open ecosystem that can incorporate over 500 third-party vendors and technologies. This not only allows many existing security systems to stay in place during the mesh adoption process and lowers the barrier to entry but also provides organizations with the flexibility to deploy



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

solutions that fit their needs while still benefitting from all the advantages that a cybersecurity mesh platform brings.

## Integrated

Speaking of incorporating distinct security systems, the Fortinet Security Fabric is bolstered by a centralized operations center, the Fabric Management Center, which supports both SOC and NOC use cases. The Fabric Management Center includes a suite of integrated analysis and response solutions that help pull together the many elements of distributed IT systems. FortiSIEM, FortiSOAR, and FortiEDR are solutions that all fall under this umbrella, and each integrates with the security ecosystem to provide threat intelligence quickly and efficiently to security teams.

For instance, one of the security data integration and operation tools is FortiAnalyzer. It's a solution that wears many hats, from log management and reporting to data analytics and incident response. There are even automation features built into FortiAnalyzer that streamline playbook implementation and incident response.

REMEMBER

A mesh architecture is built over time, not overnight. As you can tell, there are many services and features that go into a CSMA and each part of the ecosystem can be added or tweaked over time to fit your changing needs.

What makes platforms like this work is the underlying network of interconnected systems, whether provided by Fortinet or a third-party vendor. Integration is key to achieving this goal, and the Fortinet portfolio of security solutions, along with the third-party partner support, allows organizations to choose how they unify their security architecture and delivers reduced management complexity while enhancing shared threat intelligence.

## Automation — Accelerating Security from Detection to Response

Once everything in the infrastructure is working together as an ecosystem, it's time to start automating. Security infrastructure automation is easy to do in pockets — such as with security orchestration automation and response (SOAR) solutions that can automate playbooks. Many organizations already have some kind of automated detection, prevention, or threat hunting. But to



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

actually defend against a real-world coordinated cyberattack, you require end-to-end automation — all the way from prevention to remediation.

The Fortinet Security Fabric aims to decrease operational overhead while increasing security team effectiveness, and one of the best ways to do that is through automation. AI-driven security uses self-healing networks for rapid and effective responses to security issues.

Beyond automation, an effective cybersecurity mesh platform must actually enable effective security. Effective security in itself needs to start with best-in-class real-time security intelligence such as FortiGuard security services, which is a part of the Fortinet Security Fabric. This allows organizations to better monitor, identify, and stop threats like ransomware, phishing, and other common and advanced attacks. Modern device fleets can be complex and highly distributed, so FortiGuard delivers capabilities to protect and monitor IoT and edge devices, along with virtual patching capabilities.

TIP

FortiGuard also delivers application security and internal system content security. For example, the Fortinet Security Fabric incorporates enhanced data enrichment using threat intelligence from multiple threat intelligent analysts and products.

Policies for all of these services can be set from a centralized location and, when an attack occurs, are executed quickly and consistently. Automated attacks are commonplace at this point, and organizations will benefit from tools that can match those threats in speed and efficiency.

TIP

Many vendors claim their products include AI and ML capabilities to enhance automation. But AI and ML are only as good as the data they're trained on — and the people who train them. Be mindful when investing in new technologies. Make sure the automation is trustworthy.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Securing work-from-home environments
- Cloud security
- Securing operational technology (OT)

# Chapter 5
# Putting a Cybersecurity Mesh Platform into Practice

A cybersecurity mesh is a comprehensive approach to protecting your information assets and infrastructure so it should come as no surprise that it works in a wide array of situations. This chapter examines three very different use cases: work-from-home environments, cloud environments, and operational technologies environments. Each of these use cases has distinct security challenges.

Despite the variation among these use cases, cybersecurity mesh can significantly contribute to the improved security of each of these environments.

## Securing Work-from-Home Environments

Many organizations have taken advantage of the fact that their employees worked in offices and on devices that the organization controlled. That changed radically during the COVID-19 pandemic. Businesses and other organizations were thrust into an



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

unusual set of circumstances that demanded radically new ways of working. Many turned to remote work for employees who did not have to be in specific location for their roles.

Cybersecurity mesh approaches for securing work from home environments encompass three key factors: employing zero-trust access, using endpoint detection and response, and implementing home network security best practice.

## Zero-trust network access

Remote access to centralized networks and infrastructure is not new. People who work in remote offices or spend a lot of time on the road have probably used virtual private networks (VPNs) to access enterprise networks. The idea behind a VPN is that you can limit access to infrastructure and systems based on a user's network connection. If someone is on the secure network, they're presumably allowed to use the systems. This line of reasoning fits well if there is strong physical security protecting access to buildings that house your systems and only people in those buildings have access to those systems. As soon as you allow a remote worker to access those systems, this security control fails.

VPNs are used to extend the logical network to remote locations. Communications between endpoints and the central network are encrypted to prevent others on the network from knowing what is being communicated. This level of security is no longer sufficient. An employee may have a legitimate reason to use a VPN to access a corporate resource but they may not have a reason to access many other resources. A lost or stolen laptop configured for remote access could look like a legitimate use case to the VPN when in fact, the device is being used to steal confidential data from the network.

A better approach is to follow a zero-trust network access approach. In this model, you don't trust users because they have access to a VPN. Instead, both users and devices must be authenticated. Now instead of just needing to gain access to a VPN, an attacker would need to have a device that was allowed access to enterprise infrastructure and they would have to somehow find a way to pass authentication and authorization checks.

## Endpoint detection and response

Remote work means devices that are accessing your infrastructure and systems are remote as well. These devices are used from



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

home, coffee shops, planes, and anywhere else a Wi-Fi connection is available. It is not uncommon to work from a publicly accessible network. Attackers could find ways to use those networks to attack other devices on the network. They could even spoof users into connecting to a network that looks legitimate but is controlled by attackers.

TIP

Cybersecurity mesh can help ensure endpoints are configured and monitored to detect attacks on laptops and other endpoints. The threat landscape is constantly changing so it is important to keep endpoint protection up to date. Comprehensive endpoint detection and response services are essential to block and remediate attacks. These include potentially costly ransomware attacks as well as unauthorized changes to devices.

### Home network security

Getting info security right is difficult even for security professionals so it's no surprise that a typical user of a home network may not be running a secure network. Home networks are usually secured using wireless routers that are shared among users. These may be configured with weak administrator passwords or may have older software with known vulnerabilities that could be exploited by an attacker.

TIP

By using a cybersecurity mesh, you can extend enterprise security to networking devices in the home. This provides the organization with visibility into the state of home networks used for work. It also provides control over the extended business network. At the same time, employees have more visibility and control over their own private personal network. Additionally, a cybersecurity mesh can help reduce the number of deployed tools and vendors required to achieve a complete solution, which ultimately reduces complexity and simplifies security operations.

## Cloud Security

Cloud security is an emerging area of concern for enterprises. Cloud computing offers significant advantages for many workloads and enterprises are rapidly adapting to use these new technologies. Of course, as with any new technology, comes new ways of doing things — including developing and managing software. To help understand some of the distinct security challenges of



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cloud computing, it can be helpful to review some characteristics of applications designed specifically for the cloud.

## Characteristics of cloud native applications

Applications that run in clouds often use a different deployment model than applications have traditionally used in on-premises systems. Virtual machines and physical servers are widely used for deploying on-premises applications, but cloud platforms are optimized for using containers. Containers use fewer resources than virtual machines and so a single server can effectively run more applications when they run in containers than in virtual machines.

As the number of containers in operation grows, so do the management challenges. There are challenges to deploying containers so that servers are used efficiently. There are challenges to ensuring containers are secured consistently. There are also challenges with monitoring and ensuring containers are running as expected. If a container fails, an application or other service may be unavailable until a replacement container is brought online. These and other operational challenges of large-scale deployment of containers are well addressed by Kubernetes.

Kubernetes is a platform for dynamically orchestrating large-scale container deployments. This is especially useful when developing applications using microservices architectures. In these architectures, complex systems are decomposed into small function units or services that operate independently. Each of these microservices can be deployed in their own containers and this allows system administrators to update and manage microservices without disrupting other services.

## Security challenges and requirements

When operating in the cloud, it is important to address common security and operational issues. For example, the OWASP Top Ten list identifies some of the most important security for web applications. The list has changed over time and now includes:

- Broken access controls
- Cryptographic failures



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgeries

Cybersecurity mesh can help with many of these.

Another challenge with cloud is that organizations frequently need to deploy their applications across multiple clouds, including hybrid clouds where on-premises deployments such as a data center are leveraged simultaneously alongside cloud instances. While this is great for organizations to achieve digital acceleration, it can create a headache for security and cloud operations teams who need to manage across all these cloud instances. A security mesh can help simplify things by enabling a consolidated single point of view across all these clouds and eliminate visibility gaps.

TIP

In addition, you can use cybersecurity mesh to help implement predefined policies that implement best practices. Policies are defined consistently and continuously by automated processes and this reduces the chance of human error. Cybersecurity mesh also incorporates transparent, comprehensive logging and monitoring. In addition, security meshes can scale up and down as needed based on demand.

## Securing Operational Technology

In addition, the kinds of security challenges faced in remote work environments and in the cloud, operational technology (OT) has a distinct set of challenges that once again can be addressed by security mesh.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Overview of operational technology

Operational technology has at its core, a collection of industrial controls systems (ICS). This can be a diverse array of sensors, monitors, actuators, and other technologies used in industrial settings.

The characteristics of these systems is somewhat different than a typical back-office application. They can generate large volumes of data and do so continuously. There may be implicit trust between components since it is assumed if a component is accessible then it must be part of the same ICS. When an ICS is isolated from other systems, this may be a reasonable assumption. As soon as ICS devices become accessible through network traffic, and over the internet in particular, you no longer have the security benefits of isolation.

## Operational technology security practices

Cybersecurity mesh can help with good OT security practices. These include identifying assets and classifying them. It is particularly important to prioritize the value of different types of OT assets. Some will be more important to your business than others. Knowing which are the most important and securing those should be a top priority.

TIP

You will also want to be able to analyze traffic along with threats and vulnerabilities. This is similar to the needs of devices on-premises, in remote work locations, or in the cloud. In all these cases, security mesh can help significantly reduce the overall risk to your infrastructure and services.

It is important to secure both wired and wireless access. Some OT technologies may require wired network access, especially in environments with significant interference to Wi-Fi signals. Regardless of whether OT devices use wired or wireless network connections, end to end communications should be secured. Similar to prior two examples, a cybersecurity mesh can help reduce the number of tools required to achieve optimal results and security.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Looking at the past
- The changing landscape
- Modern security systems

# Chapter 6
# Putting It All Together

Cybersecurity mesh architectures (CSMAs) provide a powerful framework for security infrastructure. Modern threats are sophisticated and constantly evolving, but there are many cutting-edge security tools rising to meet that challenge. CSMA is one of them and aims to integrate an increasingly wide deployment of company resources and applications.

Looking back to the successful security tools from the last decade is no longer an option. There are too many attack strategies built to infiltrate the highly distributed system so common today. A hardened IT infrastructure doesn't only need powerful tools, though. SecOps teams need to be ready to face new challenges and adapt to the changing state of cybersecurity.

This chapter discusses what to expect when adopting a mesh architecture and how to prepare for the future of cybersecurity.

## What Worked Before Doesn't Work Today

Piecemeal security solutions were a solid way to deal with cybersecurity concerns for a long time. Organizations could throw together some endpoint, network, cloud, and email security and call it a day. Unfortunately, that's no longer the case. Operational



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

needs have pushed IT infrastructures into increasingly complex states. IoT fleets, multiple corporate user devices per employee, hybrid cloud deployments, and geographically separated offices all contribute to the trend of widely distributed company resources.

REMEMBER

Organizations must stay effective and competitive, which means there is rarely a way to roll back distributed resources. There are too many benefits to these technologies, not to mention the hiring flexibility granted by tools that support working from home. IoT devices and cloud technologies add so much value to operations, and innovations are pushing them forward faster than ever.

## The problem with best of breed solutions

Names can be deceiving, and best-of-breed security solutions are one such example. While it sounds like finding the best security tool for each component of your IT infrastructure is the best course of action, this method of securing your ecosystem misses the most critical points of modern IT security.

Mid- to large-sized organizations often have resources spread across many geographical locations and technologies, meaning the most pressing issue is not how to secure each piece of the infrastructure, but how to secure all of them effectively and simultaneously. Best-of-breed technologies are, in fact, excellent answers to specific security concerns, but that simply isn't how modern IT ecosystems are put together.

Networks, endpoints, edge devices, and cloud resources don't exist in a vacuum. Many of these components depend on one another to properly function — securing them involves looking at all of them in an aggregated way. Even cutting-edge firewalls might get breached, meaning there has to be a way to quickly see other areas where an attack might show itself.

REMEMBER

Siloed security solutions often have limited capability to communicate with one another. This limits their detection capabilities as well as the potential for automated responses and policies set by security staff.

Security siloes worked better when IT infrastructure was simpler, with fewer components and a more centralized location. Now, the high complexity and high distribution of infrastructure prohibits an effective silo configuration. Not only are tools and attack



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

surfaces less visible to security staff, but the staff themselves can become separated from one another, missing out on the benefits of routinely interacting with other experts. An organization's SecOps teams are always its greatest security resource, and SecOps staff will work more effectively when able to freely communicate with one another.

Additionally, the security landscape is constantly shifting, meaning any defense posture will need to change with it. This kind of flexibility greatly benefits from security staff working on centralized problems where wide and deep security system controls can enable them to adapt to new threats. This brings us to our next point: the importance of a unified architecture.

## Unification is the answer

The past decade has seen the development of several security solutions that aim to unify security infrastructure, such as SOAR. While they are powerful solutions that have added value to many organizations, they are missing a larger philosophical foundation that promotes integration and aggregation of security data.

TIP

Unified visibility and functionality are crucial to a successful security ecosystem now. Attackers are very aware of the broad attack surface that many organizations have, and they know how to exploit gaps in awareness. A CSMA is designed to combat this by making security tool's data generation centrally visible.

Similarly, automation has not just been a boon to business and IT operations. Cyberattackers are also utilizing automated tools to quickly move through infiltrated systems. Centralized security controls and automation tools are the most straightforward ways to combat these evolving threats. Human experts should be saved for complex problem solving, when possible, not shutting network ports to stop a threat.

TIP

Lack of security talent is already a pressing issue. Looking for ways to leverage the experts already on hand is a great way to increase security posture.

Security automation and easy-to-use policy management tools are made possible under a unified security architecture. With all the important security components visible and controllable in one place, SecOps teams can configure, observe, and reassess quickly.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# The Modern Security Landscape Is Dynamic

The security landscape has become a fast-paced back and forth between attackers and IT security professionals. Attack types fall in and out of fashion, new threats are developed, and security experts change configurations and innovate on new defense methods to meet the challenge.

## The expanding attack surface

The last two years have seen a massive shift in how work is done with the push to work from home. More people than ever are taking home corporate devices, connecting them to home networks, and are more susceptible to end device attacks than when staff were working from an office.

Shared workspaces provide a small but significant security blanket by facilitating simple questions such as, "Have you seen this email?" One quick exchange later and that email is flagged as a phishing scam. Working from home has increased many types of endpoint-targeting attacks, and phishing is just one example.

SecOps teams need comprehensive visibility to see how and when attacks happen, especially threats with difficult to identify sources, such as those emanating from an endpoint. The broader an attack surface becomes, the harder it is to pinpoint the source of an attack.

REMEMBER

Just because an attack was noticed through a network detection doesn't mean that's the only place it's been or the source of the breach.

The highly distributed nature of modern IT systems also makes investigation and analysis more difficult. While a threat might be noticed as it exfiltrates data from a database, that is likely just the tip of the iceberg. A siloed security system would have difficulty finding the source of the problem, not to mention other potential points of infiltration.

Additionally, once a threat is detected and remediated, threat analysis begins. Security teams can extract a lot of knowledge



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

about weak points in their own security systems while analyzing threats, but lacking visibility can hinder investigations. The complexity of modern systems requires easily accessible tools to conduct thorough post-attack analysis, and a unified security architecture is often the best way to do that.

## Cloud adoption challenges

Over the past ten years, it seems like there's always someone saying, "Cloud adoption is growing fast." Well, it's still true. According to the Fortinet 2022 Cloud Security Report, 58 percent of responding organizations estimated that more than 50 percent of their workloads would be run in the cloud within the next 12 to 18 months. And 39 percent said that more than 50 percent of workloads already happen in the cloud.

With so many benefits to utilizing cloud technologies, it's easy to see why so much work is moving to the cloud. But many organizations still have serious security concerns when it comes to cloud adoption. As part of the Fortinet report, security pros were asked what unforeseen roadblocks they found while adopting cloud technologies. 49 percent said a lack of visibility, and 42 percent said there weren't enough security controls.

Cloud adoption adds a layer of complexity to an already complex infrastructure. New tools, new points of entry for attackers, and administrative or engineering staff unfamiliar with the new technologies all add up to increased security risk. On top of that, many cloud solutions come with a lack of visibility and control that is clear to any cybersecurity expert. This problem is further compounded by the fact that many organizations operate in a hybrid and multi-cloud world where technologies can differ greatly across each point of deployment. Many workloads are counting on a secured cloud environment, and that number is only growing. Cybersecurity meshes are architectural methods of meeting cloud security challenges by pulling security data from the wide array of security resources and centralizing security controls to increase ease of use. Integration and aggregation are important aspects of future-facing security tools, and security meshes are a flexible way to start fostering that kind of security ecosystem.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Looking Toward the Future

Truly modern security systems are more than just sets of tools to meet today's cybersecurity threats. They are collections of methods and solutions that meet those threats, while allowing for flexibility in the fact of the ever-changing security landscape. CSMA enables the creation and maintenance of dynamic security systems, while also adding powerful integration and aggregation capabilities that promote a strong security posture.

In this final section, let's review some of the key points of cybersecurity meshes that make it a strong modern option for hardening your organization's resources against both old and new attacks.

## The importance of integration

Infrastructure and data visibility are among the most important aspects of a strong security ecosystem. They help to prevent attackers from slipping by unnoticed through exploiting a single weak point by combining security resources into a centralized pool. Cybersecurity meshes like the Fortinet Security Fabric accomplish this by creating connections between previously siloed tools and aggregating security data for easier observability and analysis.

TIP

Learning from past cyberattacks is a great way to improve the weaknesses of your security system, and this is made possible only through comprehensive data collection. By integrating data sources, SecOps investigators can quickly gather and analyze post-incident information and get to the important problem solving that their expertise enables.

Similarly, being able to observe activity across your systems in an aggregated way, with updates in near real time, increases detection and response speed. Attacks are likely to occasionally get through and giving security teams the most efficient tools for the job is the best way to combat fast-moving attacks.

TIP

The Fortinet Cloud Security Report also found that 47 percent of organizations thought that loss of visibility and control was the biggest challenge in maintaining and securing a multi-cloud environment.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Comprehensive scope

Observing security data doesn't do much good if you can't do anything with it, so another critical part of a flexible and efficient security ecosystem is powerful control capabilities. A CSMA aims to centralize as many security controls as possible by utilizing the aggregated data to create comprehensive dashboards and control consoles.

Reporting, investigation, and alerting all benefit from a single point of access. Each is made faster and easier for SecOps staff with a mesh such as the Fortinet Security Fabric, bringing together controls and visualization tools. Taking a CSMA philosophy often means not only integrating security data, but also the controls and management tools needed to operate SecOps resources.

Policy management and orchestration are also often centralized in a CSMA. Because security tool functionality has been integrated, policies can be set across ranges of solutions, not just one by one. Playbook creation and management can also utilize system integration by having access to more parts of the ecosystem.

## Automation is key

Security task automation becomes much more powerful when solutions are integrated into a central control system. Many cybercriminals are utilizing automation to quickly move through breached systems and carry out complex attacks on internal resources. Automated defense tools are important in the current landscape and will become even more critical over the next decade.

Cybersecurity meshes allow for a range of automated tasks and a lot of flexibility when tweaking automated processes. For instance, the Fortinet Security Fabric includes support for many configuration automation opportunities. Through the central controls, security staff can schedule device configuration tasks while also tracking the people who set up those changes. Triggers can be set to backup or update devices as well, freeing up the time of SecOps personnel.

While there are other security solutions out there that enable task automation and leverage machine learning and AI, a mesh architecture is built with tool integration as a core tenet which allows for more dynamic configurations and policies.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Chapter 7
# Ten Things to Remember about CSMA

Cybersecurity mesh is an architectural and philosophical change that will be an asset to your business for many years to come. Here are ten easily digestible bits of information that will help you get on the road to incorporating cybersecurity mesh.

## Inventory Existing Technologies

Before SecOps can determine how to integrate their security system, there should be investigation into how your security system already operates. Identify weak points, inadequate tools, and potential points of failure in the future to prepare for the transition into a cybersecurity mesh architecture.

## Prioritize Risks and Vulnerabilities

A big part of any technology adoption process is assessing risks and potential vulnerabilities. New technologies can add a lot of value to an organization's operations, but thoroughly assessing possible problems might cause business leaders to reconsider



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

parts of the adoption plan. Before implementing new security solutions, think like an attacker. External attack surface management tools (EASM) and other methods of switching perspective can help identify and prioritize vulnerable areas.

Identified vulnerabilities should also be prioritized. Adopting a new security architecture takes time, so SecOps needs to answer the question, "What are the most important security weak points that we need to cover?" This will give the adoption process direction.

TIP

Technological problems might not be the only thing holding back your security posture. Take a look at organizational and managerial issues that might be affecting security performance. Are teams structured correctly? Are there clear lines of communication between teams? Do hiring policies have to be updated to compensate for security talent issues? Take a look at the human element as well as the technological one while adopting any new security technology.

## Implement Best Practices

Even though there are many strong security tools ready to deploy, and architectural advancements like CSMA provide a strong foundation for building up your defenses, best practices are still an important aspect of any security ecosystem. Following standard guidelines, such as the principle of least privilege and integrating any tool or resource that can be integrated, are necessary to fully securing your resources. Best practices might also change over time, so make sure to reassess policies regularly.

## Identify Security Control Silos

The first step to adopting a cybersecurity mesh is pinpointing security silos. Silos damage the overall readiness of any security system by locking useful data in separate boxes. This means security pros can't access or intelligently control their tools, or set proactive policies, because they don't have a clear, easily accessible view of the security ecosystem. Additionally, security controls placed closer to the systems they govern decrease detection and response times so moving controls closer to assets is an important part of breaking down siloes.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Centralize Threat Intelligence and Analytics

Promoting unified security systems leads to lower detection and response times, as well as more effective intelligence gathering and analytics. A security mesh centralizes security system information, making threat analysis more efficient. This speeds up response plan development and leads to a richer understanding of the cybersecurity landscape.

## Move at Machine Speed

Recent developments in machine learning (ML) and artificial intelligence (AI) have opened the door for many security-related ML applications. The key to this point is trusting the ML and automation capabilities of the tools you use. Always vet ML and AI tool providers to make sure they are providing comprehensive and effective products.

## Automate Your Security Stack

Automation is a great way to streamline security operations, and adopting a unified security ecosystem like a CSMA enables some powerful automation uses. Define policies, create playbooks, and automate as many tasks as possible. Device updates, basic analysis tasks, and much more can all be automated to save the time of busy security pros. Additionally, automating threat responses leaves more time for evaluation tasks and automatic threat analysis means security intelligence can be generated quickly.

## Identify Skill Gaps

It is difficult to find security talent right now and this can lead to problematic hiring and team assignment practices. Modern security tools encompass a wide range of resources and attack surfaces, from endpoint and edge devices to cloud assets and applications. Skill with these technologies varies widely, and this



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

skill gap is only widening. Pinpoint where your security teams lack the most so you can shore up any security deficiencies.

TIP

Using a unified architecture can simplify many security processes and narrow skill deficiencies by pushing new security tasks into more familiar territory to help remedy security skill shortages. For more serious staff skill gaps, seek outside training or skill outsourcing.

## Partner with Industry Experts

No one person can know everything there is to know about cybersecurity. Similarly, no one organization can possess all the expertise necessary to maximize its security posture. Reach out to industry experts like those at Fortinet to talk about security concerns, potential attack surface vulnerabilities, and more. Security training often covers a variety of skills, such as incident response and best practice training.

TIP

Expertise is the best tool for defending your resources from attackers, and security-focused organizations like Fortinet often have access to specialized professionals you won't find in an average security team.

## Monitor, Assess, Improve

New types of threats show up every year, so prepare to change your security methods and the components of your toolbox when necessary. Each attack that does occur is also an opportunity to evaluate current policies and playbooks and is a great way to find points of improvement for your security systems.

Security technologies and defensive techniques are also on the move, so keep up with the latest industry practices to make sure your threat readiness is up to par with current potential attacks. This is another reason flexible security architecture is key to responding to any shape the threat landscape takes. Adopting a cybersecurity mesh is a journey, not a destination. Make regular assessments of your security architecture to improve on it and adapt to present threats by increasing integration and automation.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The Fortinet Security Fabric is the highest-performing cybersecurity mesh platform. Delivering broad, integrated, automated cybersecurity capabilities supported by a large, open ecosystem, makes cybersecurity mesh architectures a reality. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities. **Learn more at fortinet.com**

Copyright © 2022 Fortinet, Inc. All Rights Reserved.

FORTINET®

## Find out more about cybersecurity mesh

Cybersecurity mesh architecture (CSMA) can be a great asset to large organizations. CSMA is a security architecture philosophy that champions tool integration and data aggregation. It also provides unified threat intelligence and AI-supported automation to achieve a dynamic security posture that can respond faster than attackers. Cybersecurity meshes can help to integrate previously disparate security systems into a single unified system that can benefit from the strengths, and reduce the weaknesses, of each individual component.

## Inside...

- A basic overview of cybersecurity meshes
- The three basic layers of a mesh architecture
- Securing different environments
- Tips for adopting cybersecurity mesh technology
- Challenges facing cybersecurity experts today

FORTINET

**Dan Sullivan** is an enterprise architect specializing in data architecture, analytics, data mining, statistics, and computational biology. He has extensive writing experience in topics including cloud computing, big data, Hadoop, and security.

**Go to Dummies.com™**
**for videos, step-by-step photos, how-to articles, or to shop!**

ISBN: 978-1-394-16164-5
Not For Resale

for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.

# About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 595,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the https://www.fortinet.com/blog, or https://www.fortinet.com/fortiguard/labs.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Cybersecurity Mesh Architecture

Fortinet Special Edition

**by Dan Sullivan**

for dummies®
A Wiley Brand

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Cybersecurity Mesh Architecture For Dummies®, Fortinet Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2023 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Fortinet is a registered trademark of Fortinet, Inc. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-16164-5 (pbk); ISBN 978-1-394-16165-2 (ebk)

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Manager:** Jennifer Bingham
**Acquisitions Editor:** Ashely Coffey
**Editorial Manager:** Rev Mengle
**Business Development Representative:** Cynthia Tweed
**Content Refinement Specialist:** Saikarthick Kumarasamy

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Introduction

The cyber threat landscape is vast and always changing. It can seem like each new security solution brings new ways attackers can bypass your defenses. Security hardening tools, as well as the methods bad actors use to get around them, are part of a dynamic landscape that can be frustrating to navigate.

If there is one thing you take away from this book, it should be that a strong security posture today requires integration of and collaboration between the many deployed security solutions and tools. Modern technology stacks are widely distributed and hard to manage when separated into individual siloes, so integration, aggregation, and coordination are crucial to a successful security strategy.

Cybersecurity mesh architecture (CSMA) can be a great asset to large organizations. CSMA is a security architecture philosophy that champions tool integration and data aggregation to do just that. It also provides unified threat intelligence and AI-supported automation to achieve a dynamic security posture that can respond faster than attackers.

## Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless! Mainly, that you're a chief information officer (CIO), chief information security officer (CISO), vice president, architect, engineer, SOC professional, threat hunter, endpoint security manager, or administrator working on an enterprise security, networking, or infrastructure team. As such, this book is written primarily for technical readers with at least a basic understanding of security and networking technologies and challenges.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and when you finish reading it, you'll have more trust in your knowledge of CSMA.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Icons Used in This Book

Throughout this book, you will see special icons to call attention to important information. Here's what to expect.

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with birthdays and anniversaries!

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — you'll appreciate these useful nuggets of information and helpful advice.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

# Beyond the Book

There's only so much space in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fortinet.com`.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Challenges facing cybersecurity experts today
- Siloed security systems and threat readiness
- How attackers take advantage of siloed systems

# Chapter 1
# The Dynamic Challenges of Cybersecurity

This chapter looks at the primary concerns of cybersecurity overall, and how they have shaped common security philosophies seen in organizations today.

## The Core of Cybersecurity

At the end of the day, cybersecurity is mostly about data. How is it stored? Who has read access? Who has write access? How is it moved? These types of questions about your data make up the majority of the cybersecurity core. As long as there have been IT systems, there have been attackers and security personnel working to prevent them from accessing internal resources.

REMEMBER

Data becomes almost useless once it loses integrity. Unless there is a way to restore compromised data to a previous undamaged state, organizations might spend large amounts of money and time repairing and regathering the lost data. Protecting the integrity of your data is one of the most important aspects of a comprehensive security system and should be at the front of your mind when looking for any security solution.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Another crucial part of a hardened security ecosystem is proper access controls. While appropriate access permissions prevent unauthorized people from accessing sensitive information or resources, access controls also play an important role in monitoring and logging an entire IT ecosystem.

Finally, availability, not just of data but of services and tools, is critical to the day-to-day functioning of an organization. Malware packages, as well as DDoS and other network-based threats, can shut down entire IT systems for days, or longer, if not swiftly remediated.

# The Basics of a Security Ecosystem

Every organization has different security needs, business goals, staffing limitations, and more, but there are some common challenges every security system should address to be suitable for the modern threat landscape.

## Who has access?

Access controls and identity management are more than just a way to distribute digital ID badges. Identity and access management allows administrators and managers to think about and organize teams in a security-centric way.

Data access is not static, however. Roles change, personnel move positions, and business needs and goals shift over time. Data access permissions should reflect the dynamic nature of organizational goals. This means access should change and be updated along with any project completions or position changes.

TIP

When a project wraps up, administrators — or others in charge of identity and access management — should check if any permissions need to change.

Keeping access and identity management up to date isn't just a security issue because staff who have no need to view or edit certain tables shouldn't have access to them. Keeping up with role changes and project goals in terms of access controls also aids in proper monitoring and logging, which can have larger security consequences.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Well-managed access controls both prevent unauthorized access to sensitive data and help SecOps teams monitor broader security concerns.

Each portion of an organization's security system is connected to the others. While many security solutions attempt to treat a single problem as existing in a vacuum, it simply isn't true with the complex IT systems of today.

## How do distant resources communicate securely?

Network security is another concern for appropriately securing internal resources. On-premises servers, cloud resources and tools, at-home and edge devices all need to be connected over a network for a modern organization to function. Securing these geographically separate resources is the center of network security.

Cloud applications and workloads, on-premises computers, laptops, corporate tablets, and phones all make up the attack surface. The attack surface is every item that could act as an entry point into your internal systems or give access to proprietary information. With the push to work from home, the attack surface has expanded and continues to grow quickly.

TIP

Email phishing scams are more popular than ever. The increasing number of staff working from home means personal electronic devices are more likely to be the targets of corporate-targeting attacks.

A broad attack surface means more opportunities for bad actors to attack an organization's systems. Each laptop used for business-related work, connected to a home network, is an access point into internal resources. Network security not only involves VPNs and access keys for access reasons, but also, like identity management, promotes comprehensive monitoring and logging to increase the overall security of an organization.

WARNING

Unsecured communications also leave an organization vulnerable to attacks that halt availability to services and resources. Today, enterprises depend on IT systems for even the most basic day-to-day functions. Losing network communication or access to internal or external systems could mean your entire organization coming to a stop.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# One Problem, One Solution

In the past, cybersecurity measures have targeted single elements of the security landscape, creating siloed systems. This method of securing IT systems involves pinpointing a problem area, such as the need for a firewall, and using a single solution to fill the one defense gap. This creates a silo, meaning an organization's IT systems will be split into branches of separated visibility and functionality.

Take access control solutions as an example. Identity and access (IAM) solutions often incorporate access controls, authorization and permission settings, and sometimes, authentication tools. These are all critical cybersecurity tools and are present in any comprehensive security ecosystem. However, IAM is just a part of the entire security problem.

Similarly, network security tools, like perimeter defense solutions, traffic flow monitoring, intrusion detection, and DDoS protection, only cover a section of an organization's security needs.

Here is a quick list of some other types of security solutions that often lead to a siloed infrastructure:

- Encryption solutions (at rest and in transit)
- Web application security solutions
- Threat intelligence tools
- Data loss prevention services and solutions

The philosophy of "one problem, one solution" is outdated when it comes to cybersecurity. There are modern tools like cybersecurity meshes that can help to integrate previously disparate security systems into a single unified system that can benefit from the strengths, and reduce the weaknesses, of each individual component.

# The Problem with the Silo

The simple answer to why security silos no longer work is that security ecosystems have gotten too complex. Cloud technologies, at-home workers, on-premises resources, and edge devices all



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

add up to an intricate web of security risks and, using the silo philosophy, might seem ready for one problem, one solution security tools. But the lack of visibility and control is simply too damaging to a cybersecurity ecosystem considering today's threat landscape.

Each siloed system has to be a part of the larger security picture. Network security tools, IAM solutions, and endpoint security should all be visible and manageable in a centralized place. Modern threats have ways of countering or avoiding single point security controls and a comprehensive view of your security environment is a must to detect today's attacks.

Consider how attackers can avoid detection when operating in an enterprise with siloed security tools. For starters, an attacker might use a trusted platform, like a penetration tool to install malware or create communication channel between a trusted server and a malicious server. Next, the attacker exfiltrates data using the communication channel to the malicious server. Assuming the trusted server regularly sends data to external servers, this kind of data transfer will not seem unusual. What is missed is the fact that penetration testing may set up communication channels for the duration of a test but not keep the channel open for long periods of time. By using siloed security information systems, we are not able to see connections between events that would look suspicious and prompt further investigation.

Simply put, piecemeal security systems are too slow. Response times can suffer due to confusion and disorganized tools required for remediation and detection, siloed systems are often difficult to scale, and the possibility of human error is much higher than when using an integrated security solution.

REMEMBER

Human error is an especially important consideration when talking about siloed security systems. Alert fatigue is a plague on security teams and can lead to serious lapses in threat preparedness.

## Modern solutions

The last decade has seen the security market answer the call for integrated solutions. Some early examples of tools that aimed to simplify security operations were security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions. Although SIEM and SOAR can be



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

useful solutions, and were important steps forward in IT security when they came into common use, by themselves they are not sufficient to defend against modern threats.

SIEM solutions primarily gather and analyze security alerts. With so many security tools sending a variety of alerts to security staff, SIEM provides an important service in streamlining alerting and logging requirements, especially for restrictive industries such as health care and finance. However, it is usually not streamlined enough. Alert fatigue can happen when overworked security professionals are bombarded with security events, eventually leading to them ignoring or missing important alerts. Moreover, SIEM is a data intake tool, meaning that it ingests data to provide some degree of aggregated insight but does not deliver actionable outputs or automation to enable timely response to threats.

Similarly, SOAR solutions were a boon to enterprise security, but have been surpassed by other security solutions recently. SOAR platforms often incorporate detection tools into their system to leverage machine learning and automation functions that facilitate faster detection and response times. Obviously, SOAR can be a powerful tool in most cybersecurity ecosystems, but the complexity and visibility requirements of modern systems has surpassed SOAR's capability to effectively orchestrate security for a large organization.

One of the most recent innovations in the cybersecurity space is the cybersecurity mesh architecture. Cybersecurity meshes are systems designed to incorporate disparate parts of a large security ecosystem, make them more manageable and scalable, and facilitate collaboration and coordination between solutions and tools. The result is faster identification and automated responses to threats.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- What are distributed systems?
- Why are they so hard to secure?
- The human element has a big impact on cybersecurity needs

# Chapter 2
# Understanding Today's Security Challenges

The modern cybersecurity landscape is complex, varied, and dynamic. New threat types emerge every year, white hats and other security professionals find new ways to secure sensitive data while attackers are on the lookout for new ways to get around those defenses. There are smart, determined people on both sides innovating to find the next big security loophole.

One of the most important security developments of the past decade is the expansion of the attack surface. Every element of an IT ecosystem — each database, personal computer, and network port — is a potential doorway into an organization's internal systems.

This chapter discusses the nature of these widely distributed systems, how their expansiveness impacts cybersecurity, and even covers how humans can contribute to today's security challenges.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Complex Systems and Operations

The increasing breadth of a modern enterprise scale infrastructure presents new and unique hurdles to cybersecurity operations. The growing number of edge devices, hybrid cloud systems, employees that work from home, and more add up to a large, intricate attack surface that only the most modern security tools are equipped to handle.

## Distributed systems

Almost all large organizations have to face the effects of highly distributed IT systems, and there is not a one-size-fits-all solution. Each organization has specific business and operational needs that have to be met, unique ecosystems that have to be hardened, and varying resources available to commit to SecOps.

However, there are some common ways enterprises distribute their systems. While the particulars of these distributions will depend on your specific needs, here are some of the most frequent ways an attack surface expands:

- Multiple corporate campuses
- Branch offices
- Multiple public clouds
- Edge computing
- IoT devices

REMEMBER

Large organizations will likely manage some combination of these resources, or even all five of those listed. Furthermore, the administrative complexities of these resources compound each other.

For instance, say your business operations are spread across several offices. Each device, network, and on-premises computing resource or data base would need to be secured. Given the advantages of cloud technologies, it's likely public clouds would play a large part in day-to-day operations. For each office, communications between public clouds and on-premises devices and applications would need to be secured, visibility and policy enforcement requirements would increase, and most likely, the volume of data



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

and logs to sift through would increase. All that activity could lead to detection and response times taking a big hit.

## Challenges of highly distributed systems

The main challenges of maintaining a hardened distributed ecosystem can be split into three overarching problems:

- Distributed systems are porous.
- Distributed systems can be opaque.
- Distributed systems are difficult to manage.

What does that mean? First, highly distributed systems are porous because the various systems need to communicate with one another. From a security standpoint, this encompasses both network communication requirements and user or device authentication.

Both authentication events and opened networks have to be monitored. Edge computing, remote offices, and other external devices all need access to company networks and systems. This means opening the door for communication that should get in, and maybe some that shouldn't if you aren't careful.

Authentication presents a similar problem. Each user or device attempting to access a network is a potential security incident. User devices are particularly vulnerable to becoming carriers of malicious code given the rise in phishing attacks. Legitimate users can be hijacked by attacker code, not only from phishing threats, but compromised web applications that inject malicious code into user devices.

One of the biggest security concerns right now is public clouds. According to the Fortinet 2022 Cloud Security Report, 75 percent of respondent organizations are either very concerned or extremely concerned about cloud security, which is a lot! Public cloud adoption leads to an increase in configuration and management overhead, new authentication challenges, and increased network monitoring requirements.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WARNING

The Fortinet report also found that 62 percent of organizations thought cloud misconfiguration was the top security threat when it comes to public clouds.

## Lack of visibility

Traffic and general activity monitoring are key pain points for security professionals, as they are the ones most often on the front lines trying to sort through a web of interconnected systems to find a threat's source.

Any highly distributed system is, by definition, made up of many applications, servers, and services. This large number of components makes the ecosystem difficult to monitor, not only because it's simply a lot of individual elements to keep an eye on, but log overload and complexity of communication make it hard to see what's actually going on.

There are many modern security tools that make generating log and monitoring data easy, but analyzing that data is another story. The first problem is simply the volume of data generated with SIEM and other solutions. Truly threatening events can get lost in the haystack of alerts, unusual usage patterns can go unnoticed due to the overwhelming amount of monitoring data, and security professionals suffer from burnout trying to sort through the deluge of information.

TIP

Lots of log data isn't always a bad thing! Many organizations require extensive log collections for audit or industry regulation purposes. Visibility is the real issue, not the number of alerts.

Siloed security solutions also cause data integration to be a challenge. The large volume of logs and monitoring information will arrive from different tools and artificially separated regions of your ecosystem, meaning that analysis is delayed to properly integrate that data so it can be leveraged.

Speaking of speed, IT security pros don't have the luxury of working at a leisurely pace when a threat event occurs. Time to detect is a crucial metric in assessing the effectiveness of your organization's attack readiness, and for good reason. The longer a bad actor has access to internal systems, the more damage they can do and the more money and time it will cost an organization.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TECHNICAL STUFF

Mean time to detect (MTTD) and mean time to remediate (MTTR) are important metrics to look at when assessing the effectiveness of your security systems. SecOps tools and practices will change over time to meet new threats, but these metrics should follow a downward slope as time goes on.

In the end, visibility isn't just a matter of knowing an attack is occurring. It is about finding and properly understanding a threat. Context matters. For example, a network security alert might point to a vulnerable port, but closing that port might not be the whole solution. Why was the network compromised in the first place?

Perhaps an edge device had been infected with malicious code and this was the real culprit, but without comprehensive visibility, security staff might not have all the information needed to identify the compromised device, such as data that shows unusual activity coming from that device. Modern IT ecosystems are large and interconnected, so visibility is about seeing both the big and the small pictures.

## Policy and control management difficulties

It's no secret that modern security controls require well defined and crafted policies to properly function. In fact, according to the Fortinet 2022 Cloud Security Report, cloud configuration was the top security concern for most organizations, with insecure APIs and data exfiltration running just behind.

Policy consistency is difficult to maintain across highly distributed systems. Across all the tools, solutions, and resources there will be many policy control requirements, each with different idiosyncrasies and upkeep needs. Again, this is the result of security siloes.

Furthermore, policy control needs will likely drift over time, requiring reassessment by administrators, business leaders, and security pros. Each siloed system will drift at a unique pace depending on operational requirements and the changing threat landscape. Some organizations opt to make controls easier to change, but this can have serious security implications.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Regardless of your SecOps philosophies and methods, staying agile and having the capability to adapt to new security threats is a must. New threats emerge every day, attack patterns change, and security teams should be able to change strategies to meet these new attacks.

Taking a soft approach to policy control can cause policies to overlap, which can have unintended negative consequences, such as producing redundant or false alerts. Simply put, any "quick fix" solution to the complex problems presented by siloed security systems is likely to create new vulnerabilities in an organization's IT ecosystem.

# The Human Element

There are two main issues when it comes to forming a cohesive, efficient security team: lack of experienced security pros and expertise siloes.

## The skills gap

First up, many security teams are having a hard time finding new talent and, over the past several years, the hiring market for cybersecurity pros has become increasingly competitive. There are a few reasons this is happening.

One primary driver of the security expert drought is that the demand for cybersecurity skills is outpacing the supply. Security threats are increasing in complexity and number, and organizations find themselves requiring larger and larger SecOps teams. Yet, at the same time, organizations are driving toward greater digital acceleration of their business which results in an ever-growing deployment footprint, particularly in the cloud. Another driver is that even if a business does put together a pool of potential security hires, the desired expertise among those chosen is lacking.

It is becoming more difficult to acquire necessary security skills that organizations are looking for. It takes time to develop true expertise, and with how fast security technology and the threats working against them develop, how can someone actually attain the expertise required by an enterprise SecOps team?



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Of course, there are highly skilled security experts out there. There just aren't enough of them to fill the many high-skill security roles needed in modern enterprises. Unfortunately, there's also another issue.

## Expertise siloes

The second half of the larger personnel problem is expertise siloes. This is yet another hurdle brought on by security ecosystem siloes. Splitting networking, endpoint, and database security between different teams, each with different area-specific experts, often means that security staff itself is siloed!

With this SecOps staffing method, vital security knowledge is spread throughout an organization rather than centralized in a unified security operations body where experts can easily work together to solve problems. An expert in data loss prevention may be on one team, while an authentication expert is on another. If data exfiltration from an on-premises database occurs, both are needed to analyze and remediate the situation, and yet they are separated and might not even be used to working with one another.

Again, the complexity of distributed systems requires integration of many, if not all, elements of the ecosystem: system controls, security staff expertise, management and analysis tools, and more. Luckily, there are solutions to the various challenges that come with wide IT systems, such as cybersecurity meshes.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Overview of the security challenges CSMA aims to tackle
- Basic overview of security meshes
- Primary benefits of using a security mesh

# Chapter 3
# The Need for Cybersecurity Meshes

Cybersecurity innovations are not just found in new tools and technologies, but in organizational and architectural philosophies as well. Event detection and logging, analysis tools, and playbook management solutions have all come a long way in the last decade, but the complexity and wide distribution of today's attack surface calls for a more integrated approach to security.

This chapter discusses some of the specific challenges that have brought about new cybersecurity mesh architecture (CSMA) platforms, what those platforms actually do, and explains the primary benefits of using CSMAs.

## Why Do You Need Cybersecurity Meshes?

Modern cybersecurity tools are powerful, but complex. Security information and event management (SIEM) tools, endpoint detection and response (EDR), network detection and response (NDR), and many more have been boons to security operations teams. Each of these advanced tools add an important piece to the



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

larger cybersecurity puzzle. However, there is one problem that most of these tools have in common: They generate a lot of data and alerts.

## Too much data

So many modern business processes rely on fast and accurate data collection and processing. Security is no different. But there can be too much of a good thing. Data overload can be a serious issue for security teams. They can become overwhelmed with alerts, miss important events, ignore events due to alert fatigue, or simply not have enough time to process and leverage all the data their security tools are generating.

SIEM solutions, along with most detection-oriented tools, produce massive amounts of event data. They're powerful tools and are required for deep, accurate monitoring of their respective systems. All this data, however, is dead weight without a security infrastructure that can support fast aggregation and integration. Plus, with all this data, the signal-to-noise ratio matters greatly for security teams to be effective.

Unfortunately, enterprises don't have the option to scale down security data collection. Agile, cutting-edge operations often require continuously shifting and adding to their attack surfaces with new endpoint and edge devices, cloud computing resources, and more.

## Analysis challenges

Sorting through the sheer amount of data isn't the only issue presented by the large volumes created by modern security tools. This data also needs to be analyzed and leveraged to get value out of your extensive suite of security solutions.

One of the first, and most difficult, challenges is integrating data from multiple source systems. For example, network logs and application logs both hold valuable information but they are often tracked separately. A security analyst might notice anomalous data in network logs and wonder about the implications for those anomalies. The data is at the network level and does not give insights into unusual activities that may be going on at the application level. To understand that, the analyst would have to



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

switch to another tool to start analyzing application logs. At this point the process of correlating data from network and applications logs can be slow, tedious, and error prone.

REMEMBER

Even when data is integrated, analysis can be difficult. Integrated data solves some problems for analysts but it extends the common problem of having too much data to work with effectively without proper tools. Analysts need to be able to filter data to focus on time periods or infrastructure of particular interest. Once their data is narrowed, they will often want to consider aggregating data along a variety of dimensions, such as time, resource type, log severity level, and so on. Ad hoc query tools that work across integrated data sets are needed to address this problem.

## Security happens in real time

Mean time to detect (MTTD) and mean time to remediate (MTTR) are two of the best ways to assess your organization on its overall cybersecurity performance. Quick detection of a threat means security teams can begin finding the source of an attack and halt the intrusion before serious damage is done. All of this happens in real time, however, so security teams must have access to tools that allow them to get the job done efficiently.

WARNING

If there is a breach of your defenses and an attacker can inject malicious code into a system and execute that code, the damage they do will be at the speed of the machines. Humans can't be expected to manually respond at anywhere close to what is needed to block such attacks. The best outcome when such attempts occur is to block them completely, the second-best thing is to detect the event quickly and respond quickly.

Responses to security incidents vary depending on the type of incident. If malicious code is detected in the traffic from a known IP address, that address can be blocked. If a process running on a database server is exfiltrating large amounts of data, that process can be terminated. Now, these examples are oversimplifying the actual response, which might include collecting data on the attack or possibly monitoring the process of the attack to collect more information about the attacker's methods. The important point is that whatever our response is, whether it is to block or allow it to continue and observe, that response needs to happen in as close to real time as possible.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# What Is a Cybersecurity Mesh?

While there will be more detail about what components make up a security mesh later, for now let's quickly go over the basics.

As defined by Gartner in their 2021 Top Strategic Trends for 2022: Cybersecurity Mesh report, a CSMA platform is "a composable and scalable approach to extending security controls, even to widely distributed assets." Additionally, a security mesh should be compatible with "modular" approaches to IT infrastructure, such as with multi-cloud or hybrid cloud systems.

A CSMA platform groups existing security and analysis tools into layers, with each layer able to interact with those above and below it. This forms a web of functionality, allowing complex distributed systems to communicate with and benefit from one another. All of this then feeds into centralized dashboards and controls that streamline security operations.

# Cybersecurity Mesh Benefits

Cybersecurity meshes start from a simple idea: If you can reduce the time needed to collect and organize security data, then you can spend more time planning for and responding to threats. A platform that enables just this would be a great asset to any enterprise's IT operations, but cybersecurity meshes can go further by increasing security ecosystem visibility, reducing operational complexity, and increasing security intelligence sharing across an organization.

## Boosting visibility

As discussed in Chapter 2, visibility is about seeing and understanding the many parts of a distributed security infrastructure. CSMA's integration-centric approach to IT systems increases visibility by aggregating security data and centralizing detection tool information. In turn, this aggregation allows security teams to discern patterns more easily in their data.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cybersecurity meshes integrate with existing data collection and threat detection tools by gathering the outputs of these systems for further processing and analysis. Whether they are firewalls, identity and access management tools, or endpoint protection solutions, a properly implemented mesh can gather data from each of them so that security teams can gain valuable threat intelligence.

A second boost in visibility is a bit more subtle. Identifying patterns in aggregated security data is a powerful way to pinpoint well-hidden attacks. With a distributed system generating security data across an array of devices and tools, it can be difficult to make connections between events. For instance, a small increase in compute resource usage on a cloud server might seem normal out of context, but when combined with an IAM incident and network event, the cloud security issue is clearer.

Again, merely seeing the data from each security solution is not enough. A hardened security infrastructure allows security teams to better understand the connections between elements.

## Reducing complexity

In the case of cybersecurity, increased data aggregation usually goes hand-in-hand with a reduction in overall complexity. Siloed security resources are difficult to manage, as each section of an organization's security ecosystem will have different operational upkeep needs, and this kind of structure can separate experts that should be communicating with one another.

CSMA reduces complexity by integrating siloed security systems into a centrally observable and controllable operations dashboard. This kind of operational change lets SecOps staff respond to security incidents more quickly and efficiently. When suspicious activity is detected and communicated to staff through the mesh architecture in an aggregated and integrated way, they are then able to prioritize events more accurately. More information, and more centralized controls, enable staff to exercise their security expertise by streamlining security data collection and analysis.

## Intelligence sharing

Speaking of the importance of staff expertise, CSMAs also support more comprehensive threat intelligence and intelligence



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

sharing across an entire security ecosystem and SecOps division. Siloed security tools and devices are problematic on their own, but expertise siloes promote wasting one of the most valuable resources a large organization has: an expert's time and energy.

A well implemented CSMA provides a unified view of the security ecosystem and allows experts to communicate with one another more easily and freely by removing silo barriers. They no longer have to "stay in their lane" because their lane is now the entire security ecosystem. Once again, well integrated data from across an enterprise increases communication and cooperation between all of an organization's resources, including security experts. When security experts can do their job more efficiently and effectively, they can accomplish more with less!

Cybersecurity meshes also enable intelligence sharing between different security tools, including those spread across on-premises and multiple clouds. By streamlining security data collection, a cybersecurity mesh can feed this aggregated data into a threat-intelligence layer. A CSMA would offer analytics aggregation, machine learning-driven security tools, risk scoring, and other analysis tools in this layer. This layer, in turn, can feed into policy making and orchestration tools, visualizations, and more.

## Automation

Attacks are progressive and well-coordinated. They also mask their actions and intents by morphing and adapting their sequence of events to make it more difficult to detect the attack. Security professionals are working against the clock and can't respond to AI-based attacks in time without AI-powered automation. That automation has to operate across the security ecosystem to effectively address the risks posed by weaponized AI.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Covering the three basic layers of a mesh architecture
- How each layer contributes to a hardened security stance
- How the Fortinet Security Fabric fits in

# Chapter 4
# Critical Elements of a Cybersecurity Mesh Platform

While a security mesh architecture is more of a philosophy than a single security solution, there are common elements that should be present in any cybersecurity mesh architecture (CSMA). While the components that make up the foundation of the mesh, such as existing security tools or analysis solutions, might be different in each instance, how these elements are brought together to create an integrated security ecosystem has a basic structure.

This chapter discusses the three layers of any CSMA, how each of those layers interacts with the others, how this architecture contributes to a strong security posture, and how CSMAs, such as the Fortinet Security Fabric, try to bring these elements together.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# The Three Layers of a Cybersecurity Mesh

The three layers of a cybersecurity mesh are integration of data, broad security intelligence, and automated response based on policies and centralized management. A cybersecurity mesh also has three characteristics that span layers: they are composable, distributed, and support collaboration. These three layers and the common characteristics shared among layers are the keys to enabling the benefits of a security mesh.

REMEMBER

Additionally, a successful CSMA depends on quality security solutions, such as NGFW, SEG, WAAP, and EPP security systems. Each of these generate important security data that will be aggregated and analyzed later in higher layers of the architecture. But how does it get there?

## Data integration

The first layer works to incorporate the disparate sources of data across your security systems into a single line of communication. Not only does this set up the data for easier analysis and intelligence mining down the road, it also enables these security products to talk to one another, increasing each component's flexibility and effectiveness.

For example, an identity and access management (IAM) tool might send out alerts only when improper access attempts are made, or accounts are incorrectly created. These are important tasks, but there may be weakness in this tool that can only be made up for with the help of other security systems. With a CSMA, a cloud monitoring tool might be able to correlate unusual cloud compute resource access with a high privilege account, and then question the IAM tool for more information about that account.

A CSMA's data integration layer is more than just an aggregation pathway. It empowers previously siloed systems to more effectively work for SecOps teams by making more complex event correlations.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Broad security intelligence

The next layer in a CSMA is focused on security data analysis and threat intelligence. This layer processes the aggregated security tool data and processes it so that security pros can make informed policy and management decisions. It also provides a centralized analytical space for improving the threat analysis capabilities of your entire security intelligence system.

Many modern security analytics platforms incorporate machine learning, or sometimes deep learning, techniques to increase security intelligence gains and efficiency. These are technologies like EDR, NDR, UEBA and more. Centralized access to your analytic tools combined with consistent, automated data aggregation increase the value of machine learning (ML)-driven tools further by slightly reducing the operational overhead, such as data processing, that is required to fully leverage them. In fact, management and operational simplicity is a great strength of CSMA.

## Automated operations

The third layer aims to streamline policy, posture, and playbook management. The previous two layers that focused on integration and analysis aren't too useful if you can't control how they work. The management layer enables security staff to set policies that determine how and when alerts happen, how their analytics tools process data, and security goals.

Again, centralization and integration are what CSMA is bringing to the table. It allows SecOps management to set policies for any security component connected to the security mesh. IAM controls, zero trust system policies, and SIEM logs can all be configured from one location. Similarly, event playbooks can be set for each integrated security system, and even incorporate several systems for more complex and comprehensive defense responses.

## Centralized operations

The CSMA takes everything under it and utilizes dashboards, operations controls, and visualization tools to bring it all together. The operations dashboard concentrates on the operational aspects of cybersecurity. A full cybersecurity mesh operations dashboard is built over time and should encompass tools for event investigations, event reporting, and various visualization tools. Because



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

meshes promote such comprehensive security data aggregation, risk score visualizations of the entire security stack can also be generated using visualization tools in the layer.

# A Unifying Architecture

The Fortinet Security Fabric is a cybersecurity mesh platform that encompasses a wide range of integrated security capabilities across a broad ecosystem and utilizes artificial intelligence (AI)-powered automation to improve security postures even in the face of complex modern threats. Fortinet has worked hard to incorporate the three core layers of the cybersecurity mesh philosophy to bring organizations a comprehensive security platform that fits a range of infrastructure and deployment styles.

This section discusses how Fortinet employs the central philosophies of cybersecurity meshes to increase any organization's security posture.

## Broad

A well implemented cybersecurity mesh needs a base of observation and analysis tools to collect and process security data across the entire IT ecosystem. CSMA only works if there is enough data to confidently abstract the operations of each endpoint, network, and cloud security solution. This means there must be a broad range of high-quality security systems in place to support the higher layers of the security mesh.

Fortinet provides businesses with a suite of security solutions that cover an array of IT security needs. Network security, zero trust access, and cloud security solutions are all available through the Fortinet portfolio and each component has powerful communication capabilities that allow them to integrate into the larger security ecosystem.

The Fortinet Security Fabric also supports an open ecosystem that can incorporate over 500 third-party vendors and technologies. This not only allows many existing security systems to stay in place during the mesh adoption process and lowers the barrier to entry but also provides organizations with the flexibility to deploy



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

solutions that fit their needs while still benefitting from all the advantages that a cybersecurity mesh platform brings.

## Integrated

Speaking of incorporating distinct security systems, the Fortinet Security Fabric is bolstered by a centralized operations center, the Fabric Management Center, which supports both SOC and NOC use cases. The Fabric Management Center includes a suite of integrated analysis and response solutions that help pull together the many elements of distributed IT systems. FortiSIEM, FortiSOAR, and FortiEDR are solutions that all fall under this umbrella, and each integrates with the security ecosystem to provide threat intelligence quickly and efficiently to security teams.

For instance, one of the security data integration and operation tools is FortiAnalyzer. It's a solution that wears many hats, from log management and reporting to data analytics and incident response. There are even automation features built into FortiAnalyzer that streamline playbook implementation and incident response.

REMEMBER

A mesh architecture is built over time, not overnight. As you can tell, there are many services and features that go into a CSMA and each part of the ecosystem can be added or tweaked over time to fit your changing needs.

What makes platforms like this work is the underlying network of interconnected systems, whether provided by Fortinet or a third-party vendor. Integration is key to achieving this goal, and the Fortinet portfolio of security solutions, along with the third-party partner support, allows organizations to choose how they unify their security architecture and delivers reduced management complexity while enhancing shared threat intelligence.

## Automation — Accelerating Security from Detection to Response

Once everything in the infrastructure is working together as an ecosystem, it's time to start automating. Security infrastructure automation is easy to do in pockets — such as with security orchestration automation and response (SOAR) solutions that can automate playbooks. Many organizations already have some kind of automated detection, prevention, or threat hunting. But to



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

actually defend against a real-world coordinated cyberattack, you require end-to-end automation — all the way from prevention to remediation.

The Fortinet Security Fabric aims to decrease operational overhead while increasing security team effectiveness, and one of the best ways to do that is through automation. AI-driven security uses self-healing networks for rapid and effective responses to security issues.

Beyond automation, an effective cybersecurity mesh platform must actually enable effective security. Effective security in itself needs to start with best-in-class real-time security intelligence such as FortiGuard security services, which is a part of the Fortinet Security Fabric. This allows organizations to better monitor, identify, and stop threats like ransomware, phishing, and other common and advanced attacks. Modern device fleets can be complex and highly distributed, so FortiGuard delivers capabilities to protect and monitor IoT and edge devices, along with virtual patching capabilities.

TIP

FortiGuard also delivers application security and internal system content security. For example, the Fortinet Security Fabric incorporates enhanced data enrichment using threat intelligence from multiple threat intelligent analysts and products.

Policies for all of these services can be set from a centralized location and, when an attack occurs, are executed quickly and consistently. Automated attacks are commonplace at this point, and organizations will benefit from tools that can match those threats in speed and efficiency.

TIP

Many vendors claim their products include AI and ML capabilities to enhance automation. But AI and ML are only as good as the data they're trained on — and the people who train them. Be mindful when investing in new technologies. Make sure the automation is trustworthy.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Securing work-from-home environments
- Cloud security
- Securing operational technology (OT)

# Chapter 5
# Putting a Cybersecurity Mesh Platform into Practice

A cybersecurity mesh is a comprehensive approach to protecting your information assets and infrastructure so it should come as no surprise that it works in a wide array of situations. This chapter examines three very different use cases: work-from-home environments, cloud environments, and operational technologies environments. Each of these use cases has distinct security challenges.

Despite the variation among these use cases, cybersecurity mesh can significantly contribute to the improved security of each of these environments.

## Securing Work-from-Home Environments

Many organizations have taken advantage of the fact that their employees worked in offices and on devices that the organization controlled. That changed radically during the COVID-19 pandemic. Businesses and other organizations were thrust into an



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

unusual set of circumstances that demanded radically new ways of working. Many turned to remote work for employees who did not have to be in specific location for their roles.

Cybersecurity mesh approaches for securing work from home environments encompass three key factors: employing zero-trust access, using endpoint detection and response, and implementing home network security best practice.

## Zero-trust network access

Remote access to centralized networks and infrastructure is not new. People who work in remote offices or spend a lot of time on the road have probably used virtual private networks (VPNs) to access enterprise networks. The idea behind a VPN is that you can limit access to infrastructure and systems based on a user's network connection. If someone is on the secure network, they're presumably allowed to use the systems. This line of reasoning fits well if there is strong physical security protecting access to buildings that house your systems and only people in those buildings have access to those systems. As soon as you allow a remote worker to access those systems, this security control fails.

VPNs are used to extend the logical network to remote locations. Communications between endpoints and the central network are encrypted to prevent others on the network from knowing what is being communicated. This level of security is no longer sufficient. An employee may have a legitimate reason to use a VPN to access a corporate resource but they may not have a reason to access many other resources. A lost or stolen laptop configured for remote access could look like a legitimate use case to the VPN when in fact, the device is being used to steal confidential data from the network.

A better approach is to follow a zero-trust network access approach. In this model, you don't trust users because they have access to a VPN. Instead, both users and devices must be authenticated. Now instead of just needing to gain access to a VPN, an attacker would need to have a device that was allowed access to enterprise infrastructure and they would have to somehow find a way to pass authentication and authorization checks.

## Endpoint detection and response

Remote work means devices that are accessing your infrastructure and systems are remote as well. These devices are used from



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

home, coffee shops, planes, and anywhere else a Wi-Fi connection is available. It is not uncommon to work from a publicly accessible network. Attackers could find ways to use those networks to attack other devices on the network. They could even spoof users into connecting to a network that looks legitimate but is controlled by attackers.

TIP

Cybersecurity mesh can help ensure endpoints are configured and monitored to detect attacks on laptops and other endpoints. The threat landscape is constantly changing so it is important to keep endpoint protection up to date. Comprehensive endpoint detection and response services are essential to block and remediate attacks. These include potentially costly ransomware attacks as well as unauthorized changes to devices.

### Home network security

Getting info security right is difficult even for security professionals so it's no surprise that a typical user of a home network may not be running a secure network. Home networks are usually secured using wireless routers that are shared among users. These may be configured with weak administrator passwords or may have older software with known vulnerabilities that could be exploited by an attacker.

TIP

By using a cybersecurity mesh, you can extend enterprise security to networking devices in the home. This provides the organization with visibility into the state of home networks used for work. It also provides control over the extended business network. At the same time, employees have more visibility and control over their own private personal network. Additionally, a cybersecurity mesh can help reduce the number of deployed tools and vendors required to achieve a complete solution, which ultimately reduces complexity and simplifies security operations.

## Cloud Security

Cloud security is an emerging area of concern for enterprises. Cloud computing offers significant advantages for many workloads and enterprises are rapidly adapting to use these new technologies. Of course, as with any new technology, comes new ways of doing things — including developing and managing software. To help understand some of the distinct security challenges of



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cloud computing, it can be helpful to review some characteristics of applications designed specifically for the cloud.

## Characteristics of cloud native applications

Applications that run in clouds often use a different deployment model than applications have traditionally used in on-premises systems. Virtual machines and physical servers are widely used for deploying on-premises applications, but cloud platforms are optimized for using containers. Containers use fewer resources than virtual machines and so a single server can effectively run more applications when they run in containers than in virtual machines.

As the number of containers in operation grows, so do the management challenges. There are challenges to deploying containers so that servers are used efficiently. There are challenges to ensuring containers are secured consistently. There are also challenges with monitoring and ensuring containers are running as expected. If a container fails, an application or other service may be unavailable until a replacement container is brought online. These and other operational challenges of large-scale deployment of containers are well addressed by Kubernetes.

Kubernetes is a platform for dynamically orchestrating large-scale container deployments. This is especially useful when developing applications using microservices architectures. In these architectures, complex systems are decomposed into small function units or services that operate independently. Each of these microservices can be deployed in their own containers and this allows system administrators to update and manage microservices without disrupting other services.

## Security challenges and requirements

When operating in the cloud, it is important to address common security and operational issues. For example, the OWASP Top Ten list identifies some of the most important security for web applications. The list has changed over time and now includes:

- Broken access controls
- Cryptographic failures



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgeries

Cybersecurity mesh can help with many of these.

Another challenge with cloud is that organizations frequently need to deploy their applications across multiple clouds, including hybrid clouds where on-premises deployments such as a data center are leveraged simultaneously alongside cloud instances. While this is great for organizations to achieve digital acceleration, it can create a headache for security and cloud operations teams who need to manage across all these cloud instances. A security mesh can help simplify things by enabling a consolidated single point of view across all these clouds and eliminate visibility gaps.

TIP

In addition, you can use cybersecurity mesh to help implement predefined policies that implement best practices. Policies are defined consistently and continuously by automated processes and this reduces the chance of human error. Cybersecurity mesh also incorporates transparent, comprehensive logging and monitoring. In addition, security meshes can scale up and down as needed based on demand.

## Securing Operational Technology

In addition, the kinds of security challenges faced in remote work environments and in the cloud, operational technology (OT) has a distinct set of challenges that once again can be addressed by security mesh.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Overview of operational technology

Operational technology has at its core, a collection of industrial controls systems (ICS). This can be a diverse array of sensors, monitors, actuators, and other technologies used in industrial settings.

The characteristics of these systems is somewhat different than a typical back-office application. They can generate large volumes of data and do so continuously. There may be implicit trust between components since it is assumed if a component is accessible then it must be part of the same ICS. When an ICS is isolated from other systems, this may be a reasonable assumption. As soon as ICS devices become accessible through network traffic, and over the internet in particular, you no longer have the security benefits of isolation.

## Operational technology security practices

Cybersecurity mesh can help with good OT security practices. These include identifying assets and classifying them. It is particularly important to prioritize the value of different types of OT assets. Some will be more important to your business than others. Knowing which are the most important and securing those should be a top priority.

TIP

You will also want to be able to analyze traffic along with threats and vulnerabilities. This is similar to the needs of devices on-premises, in remote work locations, or in the cloud. In all these cases, security mesh can help significantly reduce the overall risk to your infrastructure and services.

It is important to secure both wired and wireless access. Some OT technologies may require wired network access, especially in environments with significant interference to Wi-Fi signals. Regardless of whether OT devices use wired or wireless network connections, end to end communications should be secured. Similar to prior two examples, a cybersecurity mesh can help reduce the number of tools required to achieve optimal results and security.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Looking at the past
- The changing landscape
- Modern security systems

# Chapter 6
# Putting It All Together

Cybersecurity mesh architectures (CSMAs) provide a powerful framework for security infrastructure. Modern threats are sophisticated and constantly evolving, but there are many cutting-edge security tools rising to meet that challenge. CSMA is one of them and aims to integrate an increasingly wide deployment of company resources and applications.

Looking back to the successful security tools from the last decade is no longer an option. There are too many attack strategies built to infiltrate the highly distributed system so common today. A hardened IT infrastructure doesn't only need powerful tools, though. SecOps teams need to be ready to face new challenges and adapt to the changing state of cybersecurity.

This chapter discusses what to expect when adopting a mesh architecture and how to prepare for the future of cybersecurity.

## What Worked Before Doesn't Work Today

Piecemeal security solutions were a solid way to deal with cybersecurity concerns for a long time. Organizations could throw together some endpoint, network, cloud, and email security and call it a day. Unfortunately, that's no longer the case. Operational



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

needs have pushed IT infrastructures into increasingly complex states. IoT fleets, multiple corporate user devices per employee, hybrid cloud deployments, and geographically separated offices all contribute to the trend of widely distributed company resources.

REMEMBER

Organizations must stay effective and competitive, which means there is rarely a way to roll back distributed resources. There are too many benefits to these technologies, not to mention the hiring flexibility granted by tools that support working from home. IoT devices and cloud technologies add so much value to operations, and innovations are pushing them forward faster than ever.

## The problem with best of breed solutions

Names can be deceiving, and best-of-breed security solutions are one such example. While it sounds like finding the best security tool for each component of your IT infrastructure is the best course of action, this method of securing your ecosystem misses the most critical points of modern IT security.

Mid- to large-sized organizations often have resources spread across many geographical locations and technologies, meaning the most pressing issue is not how to secure each piece of the infrastructure, but how to secure all of them effectively and simultaneously. Best-of-breed technologies are, in fact, excellent answers to specific security concerns, but that simply isn't how modern IT ecosystems are put together.

Networks, endpoints, edge devices, and cloud resources don't exist in a vacuum. Many of these components depend on one another to properly function — securing them involves looking at all of them in an aggregated way. Even cutting-edge firewalls might get breached, meaning there has to be a way to quickly see other areas where an attack might show itself.

REMEMBER

Siloed security solutions often have limited capability to communicate with one another. This limits their detection capabilities as well as the potential for automated responses and policies set by security staff.

Security siloes worked better when IT infrastructure was simpler, with fewer components and a more centralized location. Now, the high complexity and high distribution of infrastructure prohibits an effective silo configuration. Not only are tools and attack



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

surfaces less visible to security staff, but the staff themselves can become separated from one another, missing out on the benefits of routinely interacting with other experts. An organization's SecOps teams are always its greatest security resource, and SecOps staff will work more effectively when able to freely communicate with one another.

Additionally, the security landscape is constantly shifting, meaning any defense posture will need to change with it. This kind of flexibility greatly benefits from security staff working on centralized problems where wide and deep security system controls can enable them to adapt to new threats. This brings us to our next point: the importance of a unified architecture.

## Unification is the answer

The past decade has seen the development of several security solutions that aim to unify security infrastructure, such as SOAR. While they are powerful solutions that have added value to many organizations, they are missing a larger philosophical foundation that promotes integration and aggregation of security data.

TIP

Unified visibility and functionality are crucial to a successful security ecosystem now. Attackers are very aware of the broad attack surface that many organizations have, and they know how to exploit gaps in awareness. A CSMA is designed to combat this by making security tool's data generation centrally visible.

Similarly, automation has not just been a boon to business and IT operations. Cyberattackers are also utilizing automated tools to quickly move through infiltrated systems. Centralized security controls and automation tools are the most straightforward ways to combat these evolving threats. Human experts should be saved for complex problem solving, when possible, not shutting network ports to stop a threat.

TIP

Lack of security talent is already a pressing issue. Looking for ways to leverage the experts already on hand is a great way to increase security posture.

Security automation and easy-to-use policy management tools are made possible under a unified security architecture. With all the important security components visible and controllable in one place, SecOps teams can configure, observe, and reassess quickly.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# The Modern Security Landscape Is Dynamic

The security landscape has become a fast-paced back and forth between attackers and IT security professionals. Attack types fall in and out of fashion, new threats are developed, and security experts change configurations and innovate on new defense methods to meet the challenge.

## The expanding attack surface

The last two years have seen a massive shift in how work is done with the push to work from home. More people than ever are taking home corporate devices, connecting them to home networks, and are more susceptible to end device attacks than when staff were working from an office.

Shared workspaces provide a small but significant security blanket by facilitating simple questions such as, "Have you seen this email?" One quick exchange later and that email is flagged as a phishing scam. Working from home has increased many types of endpoint-targeting attacks, and phishing is just one example.

SecOps teams need comprehensive visibility to see how and when attacks happen, especially threats with difficult to identify sources, such as those emanating from an endpoint. The broader an attack surface becomes, the harder it is to pinpoint the source of an attack.

REMEMBER

Just because an attack was noticed through a network detection doesn't mean that's the only place it's been or the source of the breach.

The highly distributed nature of modern IT systems also makes investigation and analysis more difficult. While a threat might be noticed as it exfiltrates data from a database, that is likely just the tip of the iceberg. A siloed security system would have difficulty finding the source of the problem, not to mention other potential points of infiltration.

Additionally, once a threat is detected and remediated, threat analysis begins. Security teams can extract a lot of knowledge



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

about weak points in their own security systems while analyzing threats, but lacking visibility can hinder investigations. The complexity of modern systems requires easily accessible tools to conduct thorough post-attack analysis, and a unified security architecture is often the best way to do that.

## Cloud adoption challenges

Over the past ten years, it seems like there's always someone saying, "Cloud adoption is growing fast." Well, it's still true. According to the Fortinet 2022 Cloud Security Report, 58 percent of responding organizations estimated that more than 50 percent of their workloads would be run in the cloud within the next 12 to 18 months. And 39 percent said that more than 50 percent of workloads already happen in the cloud.

With so many benefits to utilizing cloud technologies, it's easy to see why so much work is moving to the cloud. But many organizations still have serious security concerns when it comes to cloud adoption. As part of the Fortinet report, security pros were asked what unforeseen roadblocks they found while adopting cloud technologies. 49 percent said a lack of visibility, and 42 percent said there weren't enough security controls.

Cloud adoption adds a layer of complexity to an already complex infrastructure. New tools, new points of entry for attackers, and administrative or engineering staff unfamiliar with the new technologies all add up to increased security risk. On top of that, many cloud solutions come with a lack of visibility and control that is clear to any cybersecurity expert. This problem is further compounded by the fact that many organizations operate in a hybrid and multi-cloud world where technologies can differ greatly across each point of deployment. Many workloads are counting on a secured cloud environment, and that number is only growing. Cybersecurity meshes are architectural methods of meeting cloud security challenges by pulling security data from the wide array of security resources and centralizing security controls to increase ease of use. Integration and aggregation are important aspects of future-facing security tools, and security meshes are a flexible way to start fostering that kind of security ecosystem.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Looking Toward the Future

Truly modern security systems are more than just sets of tools to meet today's cybersecurity threats. They are collections of methods and solutions that meet those threats, while allowing for flexibility in the fact of the ever-changing security landscape. CSMA enables the creation and maintenance of dynamic security systems, while also adding powerful integration and aggregation capabilities that promote a strong security posture.

In this final section, let's review some of the key points of cybersecurity meshes that make it a strong modern option for hardening your organization's resources against both old and new attacks.

## The importance of integration

Infrastructure and data visibility are among the most important aspects of a strong security ecosystem. They help to prevent attackers from slipping by unnoticed through exploiting a single weak point by combining security resources into a centralized pool. Cybersecurity meshes like the Fortinet Security Fabric accomplish this by creating connections between previously siloed tools and aggregating security data for easier observability and analysis.

TIP

Learning from past cyberattacks is a great way to improve the weaknesses of your security system, and this is made possible only through comprehensive data collection. By integrating data sources, SecOps investigators can quickly gather and analyze post-incident information and get to the important problem solving that their expertise enables.

Similarly, being able to observe activity across your systems in an aggregated way, with updates in near real time, increases detection and response speed. Attacks are likely to occasionally get through and giving security teams the most efficient tools for the job is the best way to combat fast-moving attacks.

TIP

The Fortinet Cloud Security Report also found that 47 percent of organizations thought that loss of visibility and control was the biggest challenge in maintaining and securing a multi-cloud environment.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Comprehensive scope

Observing security data doesn't do much good if you can't do anything with it, so another critical part of a flexible and efficient security ecosystem is powerful control capabilities. A CSMA aims to centralize as many security controls as possible by utilizing the aggregated data to create comprehensive dashboards and control consoles.

Reporting, investigation, and alerting all benefit from a single point of access. Each is made faster and easier for SecOps staff with a mesh such as the Fortinet Security Fabric, bringing together controls and visualization tools. Taking a CSMA philosophy often means not only integrating security data, but also the controls and management tools needed to operate SecOps resources.

Policy management and orchestration are also often centralized in a CSMA. Because security tool functionality has been integrated, policies can be set across ranges of solutions, not just one by one. Playbook creation and management can also utilize system integration by having access to more parts of the ecosystem.

## Automation is key

Security task automation becomes much more powerful when solutions are integrated into a central control system. Many cybercriminals are utilizing automation to quickly move through breached systems and carry out complex attacks on internal resources. Automated defense tools are important in the current landscape and will become even more critical over the next decade.

Cybersecurity meshes allow for a range of automated tasks and a lot of flexibility when tweaking automated processes. For instance, the Fortinet Security Fabric includes support for many configuration automation opportunities. Through the central controls, security staff can schedule device configuration tasks while also tracking the people who set up those changes. Triggers can be set to backup or update devices as well, freeing up the time of SecOps personnel.

While there are other security solutions out there that enable task automation and leverage machine learning and AI, a mesh architecture is built with tool integration as a core tenet which allows for more dynamic configurations and policies.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Chapter 7
# Ten Things to Remember about CSMA

Cybersecurity mesh is an architectural and philosophical change that will be an asset to your business for many years to come. Here are ten easily digestible bits of information that will help you get on the road to incorporating cybersecurity mesh.

## Inventory Existing Technologies

Before SecOps can determine how to integrate their security system, there should be investigation into how your security system already operates. Identify weak points, inadequate tools, and potential points of failure in the future to prepare for the transition into a cybersecurity mesh architecture.

## Prioritize Risks and Vulnerabilities

A big part of any technology adoption process is assessing risks and potential vulnerabilities. New technologies can add a lot of value to an organization's operations, but thoroughly assessing possible problems might cause business leaders to reconsider



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

parts of the adoption plan. Before implementing new security solutions, think like an attacker. External attack surface management tools (EASM) and other methods of switching perspective can help identify and prioritize vulnerable areas.

Identified vulnerabilities should also be prioritized. Adopting a new security architecture takes time, so SecOps needs to answer the question, "What are the most important security weak points that we need to cover?" This will give the adoption process direction.

TIP

Technological problems might not be the only thing holding back your security posture. Take a look at organizational and managerial issues that might be affecting security performance. Are teams structured correctly? Are there clear lines of communication between teams? Do hiring policies have to be updated to compensate for security talent issues? Take a look at the human element as well as the technological one while adopting any new security technology.

## Implement Best Practices

Even though there are many strong security tools ready to deploy, and architectural advancements like CSMA provide a strong foundation for building up your defenses, best practices are still an important aspect of any security ecosystem. Following standard guidelines, such as the principle of least privilege and integrating any tool or resource that can be integrated, are necessary to fully securing your resources. Best practices might also change over time, so make sure to reassess policies regularly.

## Identify Security Control Silos

The first step to adopting a cybersecurity mesh is pinpointing security silos. Silos damage the overall readiness of any security system by locking useful data in separate boxes. This means security pros can't access or intelligently control their tools, or set proactive policies, because they don't have a clear, easily accessible view of the security ecosystem. Additionally, security controls placed closer to the systems they govern decrease detection and response times so moving controls closer to assets is an important part of breaking down siloes.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Centralize Threat Intelligence and Analytics

Promoting unified security systems leads to lower detection and response times, as well as more effective intelligence gathering and analytics. A security mesh centralizes security system information, making threat analysis more efficient. This speeds up response plan development and leads to a richer understanding of the cybersecurity landscape.

## Move at Machine Speed

Recent developments in machine learning (ML) and artificial intelligence (AI) have opened the door for many security-related ML applications. The key to this point is trusting the ML and automation capabilities of the tools you use. Always vet ML and AI tool providers to make sure they are providing comprehensive and effective products.

## Automate Your Security Stack

Automation is a great way to streamline security operations, and adopting a unified security ecosystem like a CSMA enables some powerful automation uses. Define policies, create playbooks, and automate as many tasks as possible. Device updates, basic analysis tasks, and much more can all be automated to save the time of busy security pros. Additionally, automating threat responses leaves more time for evaluation tasks and automatic threat analysis means security intelligence can be generated quickly.

## Identify Skill Gaps

It is difficult to find security talent right now and this can lead to problematic hiring and team assignment practices. Modern security tools encompass a wide range of resources and attack surfaces, from endpoint and edge devices to cloud assets and applications. Skill with these technologies varies widely, and this



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

skill gap is only widening. Pinpoint where your security teams lack the most so you can shore up any security deficiencies.

TIP

Using a unified architecture can simplify many security processes and narrow skill deficiencies by pushing new security tasks into more familiar territory to help remedy security skill shortages. For more serious staff skill gaps, seek outside training or skill outsourcing.

## Partner with Industry Experts

No one person can know everything there is to know about cybersecurity. Similarly, no one organization can possess all the expertise necessary to maximize its security posture. Reach out to industry experts like those at Fortinet to talk about security concerns, potential attack surface vulnerabilities, and more. Security training often covers a variety of skills, such as incident response and best practice training.

TIP

Expertise is the best tool for defending your resources from attackers, and security-focused organizations like Fortinet often have access to specialized professionals you won't find in an average security team.

## Monitor, Assess, Improve

New types of threats show up every year, so prepare to change your security methods and the components of your toolbox when necessary. Each attack that does occur is also an opportunity to evaluate current policies and playbooks and is a great way to find points of improvement for your security systems.

Security technologies and defensive techniques are also on the move, so keep up with the latest industry practices to make sure your threat readiness is up to par with current potential attacks. This is another reason flexible security architecture is key to responding to any shape the threat landscape takes. Adopting a cybersecurity mesh is a journey, not a destination. Make regular assessments of your security architecture to improve on it and adapt to present threats by increasing integration and automation.



These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The Fortinet Security Fabric is the highest-performing cybersecurity mesh platform. Delivering broad, integrated, automated cybersecurity capabilities supported by a large, open ecosystem, makes cybersecurity mesh architectures a reality. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities. **Learn more at fortinet.com**

Copyright © 2022 Fortinet, Inc. All Rights Reserved.

FORTINET®

Check out Möbius Partners Technical Expert Series on CSMA at mobiuspartners.com/csma

## Find out more about cybersecurity mesh

Cybersecurity mesh architecture (CSMA) can be a great asset to large organizations. CSMA is a security architecture philosophy that champions tool integration and data aggregation. It also provides unified threat intelligence and AI-supported automation to achieve a dynamic security posture that can respond faster than attackers. Cybersecurity meshes can help to integrate previously disparate security systems into a single unified system that can benefit from the strengths, and reduce the weaknesses, of each individual component.

## Inside...

- A basic overview of cybersecurity meshes
- The three basic layers of a mesh architecture
- Securing different environments
- Tips for adopting cybersecurity mesh technology
- Challenges facing cybersecurity experts today

FORTINET

**Dan Sullivan** is an enterprise architect specializing in data architecture, analytics, data mining, statistics, and computational biology. He has extensive writing experience in topics including cloud computing, big data, Hadoop, and security.

**Go to Dummies.com™**
**for videos, step-by-step photos, how-to articles, or to shop!**

ISBN: 978-1-394-16164-5
Not For Resale

for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.