LEARNING MADE EASY

Palo Alto Networks Special Edition

Attack Surface Management

for dummies®
A Wiley Brand

Discover active attack surface management

Accelerate investigation and response

Gain immediate visibility against vulnerabilities

Brought to you by

CORTEX XPANSE™
BY PALO ALTO NETWORKS

Lawrence Miller

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2022), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

Attack Surface Management

Palo Alto Networks Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Attack Surface Management For Dummies®, Palo Alto Networks Special Edition

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

ISBN 978-1-394-18314-2 (pbk); ISBN 978-1-394-18315-9 (ebk)

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.

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Client Account Manager: Cynthia Tweed
Production Editor: Mohammed Zafar

Table of Contents

Introduction

The enterprise attack surface is more complex and difficult to manage than ever. Securing and managing a hybrid IT environment — composed of on-premises data centers, cloud infrastructure, critical supplier networks, and remote employee workstations — can be nearly impossible without full visibility into your entire attack surface. Modern organizations need a better way to manage their attack surfaces.

About This Book

Attack Surface Management For Dummies, Palo Alto Networks Special Edition, consists of six chapters that explore the following:

- The modern threat landscape, security challenges, and limitations of existing technologies and approaches (Chapter 1)
- What attack surface management is all about (Chapter 2)
- How to prevent cyberattacks with attack surface management (Chapter 3)
- Common attack surface management use cases (Chapter 4)
- How to automate attack surface management with Cortex Xpanse (Chapter 5)
- Must-have capabilities and features to look for in an attack surface management solution (Chapter 6)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

There's also a helpful glossary in case you get stumped by any terms or acronyms used in this book.

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless.

Mainly, I assume that you're a decision-maker or a security practitioner and you're looking for a better way to manage your enterprise attack surface. Whether you're a chief information security officer (CISO), an IT manager, or a security engineer, this book will help you understand how to effectively address the challenges of a greatly expanded attack surface and an increasingly hostile threat landscape.

Icons Used in This Book

Throughout this book, I occasionally use 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.

TIP

Tips are appreciated, but never expected, and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice.

Beyond the Book

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

IN THIS CHAPTER

- Recognizing risk in your attack surface
- Facing visibility and staff challenges
- Understanding limitations in existing technologies and processes

Chapter 1
The Current State of Attack Surface Management

In this chapter, you explore the modern threat landscape and how the growing enterprise attack surface has created a target-rich environment for threat actors. You also learn about the challenges of having too many assets and too few resources, limited visibility, and ineffective tools and processes for attack surface management (ASM).

Surveying the Modern Threat Landscape

Threat actors are constantly looking for ways to attack organizations. They actively look for exposures on websites, servers in the cloud, and other Internet-connected systems and services that have been forgotten about or have little to no protection. Organizations need to understand their attack surface and all the ways it's exposed and vulnerable to attack, and prioritize activities that can help make that attack surface smaller and more secure.

WARNING

The potential damage to your attack surface is real and substantial. Consider the following examples:

- Security researchers recently found 1.2 billion records with individuals' personal data aggregated by People Data Labs on an exposed Elasticsearch server.
- MoviePass exposed credit card information for thousands of customers on a server open to the Internet that was unencrypted and not password protected.
- Hackers compromised a reservation database for Marriott's Starwood division and accessed the data of 383 million guests.
- A database managed by the Indian government was left open to the Internet without a password, exposing the medical records of more than 12.5 million pregnant women.
- A brute-force attack on an exposed Remote Desktop Protocol (RDP) server from Labcorp resulted in 7,000 systems and 1,900 servers infected.

With so many attack vectors and limited resources to defend them, it's critical that organizations understand where the critical entry points are and how they can prioritize attack surface reduction in an automated way.

Too Many Assets, Too Little Visibility and Staff

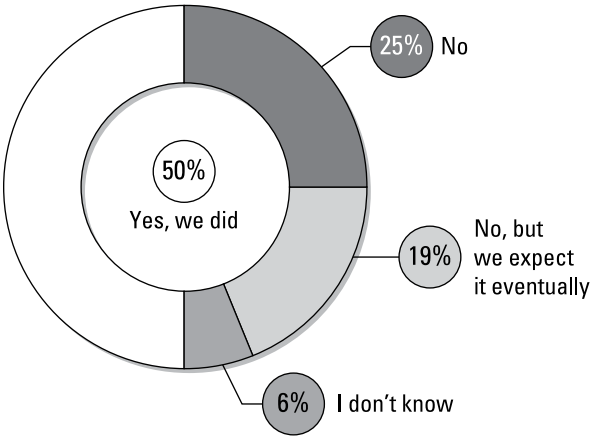
Modern enterprises have more complex and difficult-to-manage attack surfaces than ever before. Whether you're working to secure an on-premises network, unknown cloud infrastructure, critical supplier networks, or remote employee workstations, it can be nearly impossible to get visibility into and manage your entire external attack surface.

REMEMBER

An attack surface is like shifting sand. Between multicloud environments, private clouds, and public clouds; inheriting assets via mergers and acquisitions (M&A); and access from supply chain partners and remote workers, it's impossible for IT to manually keep track of all the organization's assets and the people responsible for them.

Unfortunately, even as the enterprise attack surface is growing exponentially and constantly evolving, organizations find themselves struggling to attract and retain experienced cybersecurity professionals. The Information Systems Audit and Control Association (ISACA) estimates that almost two-thirds of enterprise security teams are understaffed, and more than half have open positions. The International Information System Security Certification Consortium (ISC)[2] estimated the global shortage of cybersecurity professionals to be 2.72 million in 2021.

Despite these challenges, security teams must know where the critical entry points are across the entire enterprise attack surface. They must proactively reduce and protect the attack surface in a smart, data-driven manner. More than half of all companies participating in a recent survey by MIT Technology Review Insights and Palo Alto Networks had experienced a cyberattack originating on an unknown, unmanaged, or poorly managed digital asset (see Figure 1-1). Without a full inventory of their digital assets — from laptops to cloud resources — companies struggle to identify and remediate their exposure to cyberattacks.



Source: MIT Technology Review Insights 2021 survey of 728 global executives and decision-makers

FIGURE 1-1: More than half of survey respondents experienced a cybersecurity attack on an unknown or unmanaged digital asset.

REMEMBER

The key to a successful cybersecurity strategy is knowing what you need to protect.

WHAT DOES A SOC TEAM DO?

A security operations center (SOC) team is comprised of cybersecurity analysts working together to monitor enterprise systems; defend against security breaches; and identify, investigate, and mitigate cybersecurity threats. SOC teams streamline the security incident handling process with analysts performing key functions based on their experience level. A typical SOC structure consists of three tiers:

- **Tier 1 — Triage:** This is where security analysts typically spend most of their time. Tier 1 analysts are typically the least experienced analysts, and their primary function is to monitor event logs for suspicious activity. When they think something needs further investigation, they gather as much information as they can and escalate the incident to Tier 2.
- **Tier 2 — Investigation:** Tier 2 analysts dig deeper into suspicious activity to determine the nature of a threat and the extent to which it has penetrated the infrastructure. These analysts then coordinate a response to remediate the issue. This is a higher-impact activity that generally requires more experienced analysts.
- **Tier 3 — Threat hunting:** The most experienced analysts support complex incident response and spend any remaining time looking through forensic and telemetry data for threats that detection software may not have identified as suspicious. The average company spends the least time on threat-hunting activities because Tier 1 and Tier 2 consume most analyst resources.

Recognizing the Limitations of Traditional Approaches

Traditional security tools and approaches to ASM are imprecise and incomplete. These tools and approaches — discussed in the following sections — typically don't do an adequate job of finding both known and unknown assets. These tools and approaches also don't perform asset discoveries frequently enough to maintain a complete and accurate picture of the rapidly changing and growing attack surface, particularly when compared to the tools and approaches used by attackers (see Figure 1-2).

Your organization should find and fix your risks before your attackers can exploit them.

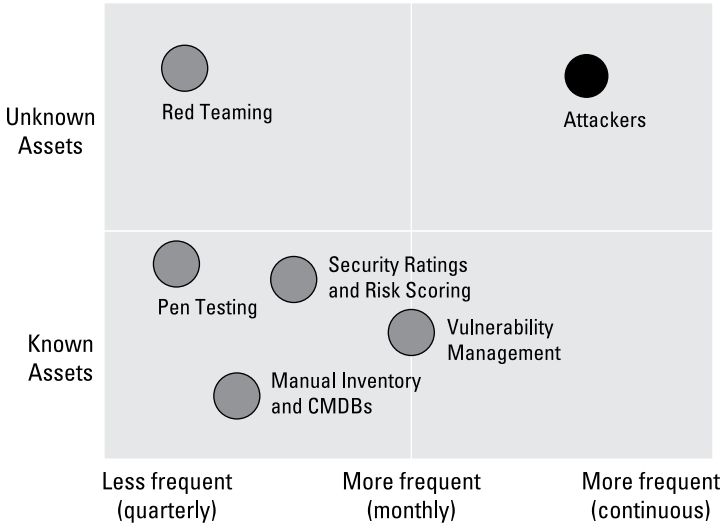


FIGURE 1-2: Attackers have the upper hand compared to traditional technologies and approaches for ASM.

Security ratings and risk scoring

Security ratings attempt to quantify the cyber risk in an organization by correlating various external data about that organization. A security rating also allows for comparison between organizations, assigning the significance of various factors based on the company- or sector-specific knowledge and measuring changes in the external data as a proxy for the organization's cybersecurity posture.

Unfortunately, security ratings are simply the output of a subjectively weighted function. Security ratings provide a risk score derived from data that can be gathered independently and are often based on an incomplete list of assets. The basic idea behind security ratings is that if an organization has abysmal external security (for example, lots of expired certificates and unpatched vulnerabilities on public-facing systems), then the inside of its enterprise network is also probably a mess.

REMEMBER

Security ratings and risk scores offer only a snapshot in time, making them less accurate in rapidly changing networks. They don't find assets or mitigate risks directly.

Vulnerability management

Many organizations rely on vulnerability scanners to identify their attack surface. However, this approach falls short because it

requires an asset list to perform scans, which misses the unknown assets that attackers use to gain access and exploit an organization.

Additionally, the process of vulnerability management within security teams is flawed. Like antivirus systems, vulnerability scanners rely on a database of known vulnerabilities — making them only as good as the latest update. This means you wait hours or days for an updated vulnerability profile, which consequently translates to a longer overall patching process that takes days. Worse, vulnerability scanners query only known devices to see what's exposed.

Red teaming and penetration testing

For assets that enterprises don't know about, third-party vendors may perform quarterly penetration tests or red teaming to partially enumerate assets and test infrastructure. Typically, discovery of assets happens just once per quarter and uses a patchwork of scripts and programs the penetration testers have put together to find some of the infrastructure that is potentially vulnerable. The periodic nature of penetration tests make them an incomplete solution against attackers who are actively scanning for exposures.

These issues, coupled with a rapid shift to multicloud and cloud-native ephemeral systems and microservices on the scale of hours and minutes, results in enterprise security teams significantly lagging behind attackers in not only having an inventory of assets but also knowing if those assets are vulnerable.

Manual inventory and CMDBs

Sadly, many organizations still keep track of known assets using spreadsheets and emails, which are extremely labor intensive and error prone. Even when tracked in a configuration management database (CMDB) that is integrated with other tools and ingests asset information, the manual efforts required can overwhelm smaller organizations, and the challenge of discovering unknown assets remains. Establishing the CMDB as a single source of truth requires tedious and error-prone manual efforts to:

- Keep the database information current.
- Eliminate duplicate or erroneous information.
- Ensure complete asset information.

IN THIS CHAPTER

- Identifying your attack surface and prioritizing risk
- Investigating and responding to threats faster
- Raising the bar on security effectiveness
- Being proactive in security operations

Chapter 2
Defining Attack Surface Management

Attack surface management (ASM) performs several critical functions to give a security operations center (SOC) the visibility needed to ensure security across an organization. It provides a complete, up-to-date inventory of all assets (both known and unknown), continuously finds potential vulnerabilities, and offers risk prioritization. In this chapter, you learn about the key capabilities and benefits that define a complete ASM solution.

Providing Continuous Visibility and Prioritization

ASM is the process of continuously identifying, monitoring, and managing all Internet-connected assets, both internal and external, for potential attack vectors, exposures, and risks.

ASM is based on the understanding that you can't secure what you don't know about. As such, the key is to ensure your organization has a comprehensive and continuously updated inventory of all Internet-facing assets and the risks associated with them.

Being able to create a complete system of record like this requires a new line of thinking. Network perimeters are a thing of the past, so the traditional view of an organization's attack surface no longer applies. A modern attack surface is made up of any Internet-facing asset, whether in the cloud, on premises, or colocated in multiple places.

WARNING

Between multicloud, private and public clouds, inheriting assets via mergers and acquisitions (M&A), and access from supply chain partners and remote workers, it's impossible for IT experts to keep track of all assets and the people responsible for them via manual methods.

Traditionally, asset inventories have been generated with slow, manual, and infrequent processes. Unfortunately, modern infrastructure, especially in the cloud, can change in an instant. All it takes for a new cloud instance to be created outside of security processes is an employee with a credit card.

Additionally, the quality of data in an asset inventory directly impacts the efficacy of all security processes. Vulnerability scanners that only check known assets mean unknown assets can't be secured. These unknown assets are a direct threat. Modern enterprise networks have evolved and become highly dynamic, connecting on-premises data centers, headquarters, branch locations, private and public clouds, remote workers, and other environments.

REMEMBER

As an organization's digital footprint increases, so does its accidentally exposed threat exposure. Maintaining asset inventory is fundamental to any robust cybersecurity program, but a prioritization and mitigation platform ensures that your ASM program is complete.

Accelerating Investigation and Response

Threat actors are opportunistic predators, constantly searching for vulnerable assets to attack in a target environment. Unfortunately, these threat actors are much faster at finding targets of opportunity than enterprise defenders are at finding and securing those assets.

The Palo Alto Networks Cortex Xpanse research team continuously monitors the global attack surface to better understand how

much of an edge adversaries have in detecting systems that are vulnerable to attack.

Most threat actor scans observed during the first three months of 2021 began within 15 to 60 minutes of a common vulnerabilities and exposures (CVEs) announcement. But, in some cases, they were much faster. On March 2, 2021, threat actors started scanning for vulnerable Exchange Server systems within five minutes of Microsoft's disclosure of three zero-day vulnerabilities.

WARNING

It used to take weeks or months to scan the entire Internet, but today it takes less than 45 minutes to scan every public-facing Internet Protocol (IP) address in the IPv4 space. Xpanse research shows that enterprises experience, on average, two new serious exposures per day — or one every 12 hours.

Enterprises tend to be slow to react due to three primary reasons:

- The attack surface is growing exponentially as more enterprises migrate to the public cloud and adopt hybrid, work-from-home/work-from-anywhere models.
- Vulnerability scanners depend on timely CVE database updates, which only query known assets.
- With the exception of red teaming, which may not be comprehensive enough, periodic penetration testing and various approaches to verify asset inventories focus on known assets — leaving unknown assets and their associated vulnerabilities unknown.

Xpanse research found that 90 percent of observed exposures occurred in the cloud. The cloud is inherently connected to the Internet, and it's surprisingly easy for new publicly accessible cloud deployments to spin up outside of normal IT processes, which means they often use insufficient default security settings and may even be forgotten.

Asset leak is likely inevitable when an expanding cloud attack surface is combined with more traditional factors that bypass change control such as M&As, supply chain, and the Internet of Things (IoT). But that doesn't mean enterprises should accept the risk. Tracking an ever-changing infrastructure landscape is an almost impossible task for humans and requires an automated approach, both to discover unknown assets and to ensure they're secure.

Improving Security Effectiveness

Protecting your attack surface should start with a data-driven approach. Lots of information exists detailing how threat actors search for vulnerable systems across the Internet. The most important takeaway is that, although the Internet is a large place, it's actually very small from an attacker's perspective. In less than an hour, a threat actor can have a list of every exposed system of a given type across the entire Internet.

Some of the most common exposures are also the simplest to exploit. Attackers don't need zero-day exploits when insecure systems are left open to the public. Prioritizing the following exposures can go a long way toward improving security effectiveness across your attack surface:

- **Remote Desktop Protocol (RDP):** RDP allows users to remotely connect to and control a computer. It provides a screen share that makes it look as if you're sitting in front of another computer's monitor. RDP exposures can be difficult for organizations to detect on their own because they frequently occur when IT assets are misconfigured and outside of core networks that are regularly monitored by IT staff, such as when employees work remotely or when DevOps teams deploy virtual machine instances in the public cloud. Organizations can protect themselves with several layered controls:
  - Don't permit RDP to be public facing. Block at the port/protocol level via the machine build and the end-point firewall.
  - Enforce login attempt lockouts.
  - Use multifactor authentication (MFA), even for user workstations.
- **Telnet:** Telnet is an unencrypted remote access protocol. It's sort of like RDP without the desktop interface, using terminal commands instead. Telnet is an extremely old protocol that has no real requirement to be used today. To protect your organization from risks associated with Telnet, do the following:
  - Never allow Telnet (or any other unencrypted remote access service) to be reachable from the public Internet.

- If a legacy Telnet service must be run, make it accessible only on a segmented internal network and require strong authentication from other devices to connect to that network.
- Because Telnet is frequently associated with legacy systems, don't limit discovery and detection efforts only to networks where normal day-to-day IT operations occur. Include them on lesser-known parts of your network, such as equipment provided by your Internet service provider (ISP) for your regional offices. Systems like these are often overlooked in asset management systems, and they frequently contain misconfigurations, making them ideal targets for threat actors to gain access to your network.

» **Exposed databases:** Securing databases has always been notoriously difficult, which makes them a huge target for threat actors. Instead of needing to breach a network and find data, database servers prepackage all the valuable data for attackers. The public cloud makes it easy for a developer (or practically anyone within your organization) to quickly spin up a database in IP space that isn't owned or monitored by your organization. To protect your organization from risks associated with exposed databases, do the following:

- Never have database servers accessible from the public Internet — even allowing queries over the Internet is risky.
- Implement a robust discovery program looking for SQL databases such as Elasticsearch, Memcached, MongoDB, MSSQL, MySQL, and Postgres.

» **Exposed engineering systems:** Exposed engineering systems can pose many risks. Development, staging, and quality assurance (QA) environments are often exposed briefly for testing and are supposed to be taken offline after a few hours. They often aren't included in vulnerability scanning or patch management because they're assumed to be carefully managed. However, these assets are often forgotten and then end up persisting for months or even years. Because they aren't actively monitored or managed, they may become vulnerable as new exploits are released. In addition, these systems are usually not provisioned or configured to production security standards in the first place,

and they may contain sensitive data that was only intended for testing and integration purposes but was then accidentally left on the machines, putting that data at risk of compromise. To protect your organization, do the following:

- Perform routine discovery and monitoring of everything your organization has connected to the Internet.
- Take an outside-in view — just like an attacker does — to uncover systems that look normal from the inside but look like a big bull's-eye from the outside.
- Deploy test, development, and staging environments behind a firewall and only expose them for brief testing periods when required.

» **Certificate issues:** Certificate health is one of the basic tenets of good cyber hygiene. Despite this, certificate issues remain incredibly common across large and small organizations. Certificates that are expired or self-signed or that use a deprecated signature algorithm provide a road map for attackers to find unmonitored and potentially unprotected systems. To protect your organization from risks associated with certificate issues, do the following:

- Proactively identify certificates that are expired, self-signed, and/or use deprecated algorithms.
- Never use unhealthy certificates on business-critical systems. These systems often can't be easily accessed by users anyway because of browser warnings about an unhealthy or unsafe certificate, so consider taking these systems offline.

A FEW WORDS ABOUT HYGIENE

While I'm on the topic of hygiene (cyber, not personal), let's quickly review the importance of good cyber hygiene.

Cyber hygiene represents the conditions and practices that are conducive to good IT health. In other words, cyber hygiene is what you do, or should be doing, on an ongoing basis to ensure that your systems and services are safe, reliable, and available.

Organizations need a cyber hygiene program to ensure business continuity and lay the foundation for other critical IT and security initiatives such as attack surface area reduction and cloud governance.

An effective cyber hygiene strategy encompasses your:

- **Asset inventory:** The systems, devices, software, and services that comprise your network
- **People:** The individuals who make up your organization and their credentials and access
- **Processes:** The structured work to manage components of the IT hygiene program
- **Exposures and (mis)configurations:** The way technology creates threat vectors that could be abused by bad actors
- **Policies:** The agreed-upon ways that processes must be mapped and carried out

REMEMBER

Attack surfaces are constantly evolving, and cloud infrastructure is constantly changing. Organizations need an ASM plan that includes the following:

- Generating an automated and continuously updated single source of truth for all Internet-connected assets
- Decommissioning or isolating assets that don't need to be Internet-facing to reduce your attack surface
- Discovering and identifying account owners for all previously known and unknown assets
- Finding all exposures — vulnerabilities, expired certificates, unsecured remote access protocols, and so on
- Automating risk remediation and reporting with a quality security orchestration, automation, and response (SOAR) platform
- Continuously monitoring, discovering, evaluating, and mitigating risks as the attack surface changes

Developing Proactive Security Operations

Cybersecurity practitioners have a hard enough job without spending unnecessary time and energy on processes that can be automated. So, perhaps the most obvious value of ASM is as the first step in transitioning a SOC from being reactive to being proactive and saving time and money in the process.

ASM helps make your SOC more efficient, reducing human effort to inventory assets, evaluate risks, and investigate stakeholder information, as well as eliminating the need for point-in-time analysis programs. A major concern for chief information security officers (CISOs) is the downtime and remediation associated with ransomware in particular and data breaches more generally. ASM can be incredibly valuable in reducing the costs associated with cyberattacks by helping discover exposures, prioritize risk management, and ensure risks are remediated before they can be exploited.

FRIEND OR FAUX? DEFINING TRUE ASM

Identifying and managing an attack surface is no easy task for security teams. Dealing with multiple cloud vendors, an increasingly remote workforce, supply chain vendors, third-party partners, and numerous security flaws inherited through M&A is just another day in the life of a security analyst.

Adding to the complexity are assets available on premises, in the cloud, or colocated. Attack surfaces are changing fast, making it essential to be able to find and remediate issues before threat actors discover them.

However, not all ASM solutions are created the same or provide value in the same ways. Organizations must ensure the tools and services used have the capabilities to address the most important use cases that apply to their business.

Three main capabilities support ASM:

- **External attack surface management (EASM)** is the process and technology that identifies and manages threats discovered in Internet-facing assets using independent external scans of an organization's attack surface. This method of discovery can continuously monitor servers, public cloud instances, expired certificates, and third-party partner software code vulnerabilities on all Internet-connected assets that could be exposed to adversaries. EASM excels at supporting security processes like vulnerability management, penetration testing, and threat hunting.
- **Cyber asset attack surface management (CAASM)** is an emerging technology that enables organizations to see all assets (internal and external) regardless of where they're located. However, because it relies on application programming interface (API) integrations with existing tools, visibility can be limited by existing inventory data, and the value of CAASM is primarily in keeping track of internal assets only.
- **Digital risk protection service (DRPS)** is a managed service that provides visibility into open-source assets, such as social media and deep web sources. This means it will primarily be useful for performing risk assessments and brand protection, but it won't be able to provide an inventory of assets managed by your organization.

Looking at the strengths and weaknesses of each solution, it becomes clear that organizations looking to boost overall security operations likely want to choose EASM as the main piece of an ASM program. EASM is the only option that provides a true source of record of all Internet-connected assets to help in performing vulnerability management, penetration testing, cloud security and governance, and assessing the security of subsidiaries and third-party partners.

IN THIS CHAPTER

- Discovering vulnerabilities across the global attack surface
- Identifying the most common attack surface exposures
- Implementing best practices for attack surface management
- Scaling your security operations center

Chapter 3
Preventing Common Attacks with Attack Surface Management

In this chapter, you learn about the rapidly growing global attack surface, the top attack surface exposures, best practices in attack surface management (ASM), and how to scale your security operations center (SOC) for effective ASM.

An Overview of the Global Attack Surface

It used to take weeks to scan the entire Internet and required a room full of supercomputers running 24/7. So, Internet scanning was largely the realm of well-funded nation-state threat actors, and identifying every device on the Internet in a reasonable amount of time required illegal methods (for example, building your own botnet).

Everything changed in 2013. New algorithms allowed global Internet scanning at a rate 1,500 times faster than previous methods. Today, it takes less than 45 minutes to communicate with every

public-facing IPv4 address (that's 4.3 billion Internet Protocol [IP] addresses) on the Internet. Several important technological advances have accelerated the speed of Internet scanning:

- **Computing and infrastructure costs dropped.** With the rise of cloud computing, a major barrier to entry for Internet scanning — that is, the cost of computing and infrastructure — disappeared with the ease and relatively negligible cost of spinning up cloud infrastructure.
- **Algorithms randomized the IP addresses scanned.** Scanning IP addresses sequentially can look like a distributed denial-of-service (DDoS) attack because traditional on-premises IP addresses are assigned to organizations in blocks. New scanning techniques used an algorithm that randomized the order of IP addresses scanned. This approach also allowed for the use of distributed scanning architectures and reduced computing resources needed because tracking the order of scanning targets was no longer necessary.
- **Packet lag parallelized the handshake process.** When two devices on the Internet communicate, there is always some delay as packets of information travel through the system. On a global scale, this lag adds up fast. New ways to keep track of connections allowed scanners to send more packets at once, effectively bundling the delay time into one brief waiting period. This made bulk scanning of millions of devices almost as fast as making a single connection to just one of those devices.

Thus, enterprises must be proactive in identifying and managing their unique attack surfaces. Digital transformation initiatives have turned enterprises inside out, often creating numerous backdoors into their network in the form of abandoned, rogue, or misconfigured assets. The advancements in scanning technology make these backdoors easier to find and have fundamentally changed how we need to think about the Internet and the global attack surface.

In the past, the majority of IT infrastructure lived on premises, and IT and security teams had a pretty good (though not great) idea of their attack surface. Today, far more assets are deployed in the public cloud and remote work environments — particularly with the adoption of work-from-home models. Many cloud resources are ephemeral — sometimes existing only for a few

seconds or minutes — leading to network sprawl and making it difficult, if not impossible, for SOCs to understand how their networks are configured. Mergers and acquisitions (M&As), supply chain and third-party networks, and the Internet of Things (IoT) add more complexity to the growing challenge of ASM.

Top Ten Attack Surface Exposures

The ASM Top 10 serves as a guide to help security teams identify attack surface exposures ranked on potential risk posed to enterprises. The list is rank-ordered based on two main tenets:

- Certain things should never be on the Internet because, if exploited, attackers can move laterally or expose sensitive business processes and data. These include
  - Inherently bad protocols
  - Exposures that relate to the control plane of your network
- Older assets that were secure in the past may have since become vulnerable.

The ASM Top 10 is as follows:

- **Remote access services** (for example, Remote Desktop Protocol [RDP] and virtual private networks [VPNs])
- **Insecure file sharing/exchange services** (for example, Server Message Block [SMB] and NetBIOS)
- **Unpatched systems** vulnerable to public exploits and end-of-life (EOL) systems
- **IT admin system portals** (for example, Cisco Security Manager and Kubernetes)
- **Sensitive business operation applications** (for example, Grafana and Jenkins)
- **Unencrypted logins and text protocols** (for example, Telnet, Simple Mail Transfer Protocol [SMTP], and File Transfer Protocol [FTP])
- **Directly exposed IoT devices** (for example, building control systems and Modbus servers)

- **Weak and insecure/deprecated cryptography** (for example, expired and self-signed certificates)
- **Exposed development infrastructure** (for example, Grafana and Kubernetes)
- **Insecure or abandoned marketing portals** (for example, Adobe Experience Manager [AEM] and Adobe Flash)

TIP

Learn more about the ASM Top 10 at `www.asmtop10.com`.

Best Practices in Attack Surface Management

Modern enterprise attack surfaces are highly dynamic. Without a complete picture of your attack surface that is continuously updated, persistent exposures and unmanaged assets put your organization at risk.

TIP

It's a well-known security axiom that you can't protect what you don't know about. Therefore, it's no accident that the Center for Internet Security (CIS) Critical Security Controls and U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework both start with asset management:

- **Inventory and control of enterprise assets (CIS 1):** "Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments. . .."
- **Inventory and control of software assets (CIS 2):** "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."
- **Identify – Asset Management (NIST ID.AM):** "The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and

managed consistent with their relative importance to organizational objectives and the organization's risk strategy."

Attackers thrive on the complexity and ever-changing nature of attack surfaces. Security teams need to have the same view as their adversaries to effectively identify and prioritize risks across the enterprise attack surface.

Although metrics like mean time to detect (MTTD) and mean time to respond (MTTR) are essential after a breach has occurred, security teams should also be focused on doing all they can to prevent breaches before they happen. This means putting more stake in mean time to inventory (MTTI) because it's impossible to secure unknown assets and unknown exposures.

WARNING

Organizations typically use metrics such as dwell time, MTTD, or MTTR to gauge cybersecurity effectiveness. However, these metrics are inherently reactive in nature and focus only on known assets.

MTTI measures the time required for organizations to perform a full external asset inventory that assigns ownership to drive classification and protection based on value. MTTI becomes especially critical following common vulnerabilities and exposures (CVEs) announcements as attackers often begin scanning for vulnerable services immediately after the disclosure of a new CVE. If proof-of-concept code or a known exploit is published, threat actor activity accelerates rapidly. Unfortunately, threat actor scanning in the wake of these events occurs well before most organizations have completed their own first pass of an inventory scan.

Beyond measuring MTTI, organizations should take the following steps to manage their growing attack surfaces proactively and effectively:

- Generate an automated and continuously updated single source of truth for all Internet-connected assets.
- Decommission or isolate assets that don't need to be Internet-facing to reduce your attack surface.
- Discover and identify system owners for all previously known and unknown assets.

- Find all exposures — vulnerabilities, expired certificates, unsecured remote access protocols, and so on.
- Automate risk remediation and reporting with a quality security orchestration, automation, and response (SOAR) platform.
- Continue to monitor, discover, evaluate, and mitigate risks as the attack surface changes.

REMEMBER

A strong foundation of continuous discovery and monitoring ensures you can keep up with modern, dynamic attack surfaces in order to find, prioritize, and mitigate exposures as they arise.

Scaling Your SOC with Attack Surface Management

Many enterprise SOC teams today are relegated to using manual checklists — playbooks — to determine which alerts require attention and how to respond. There is little automation or intelligence in these playbooks but plenty of inefficiency.

This means that SOC analysts must review each alert, correlate the alert with an asset in a static inventory, find the playbook for that corresponding alert, and manually execute the steps to investigate and remediate the alert. The playbook may have dozens of sequential steps that take many painstaking hours to perform. In the interim, a backlog of potentially hundreds of new alerts is quickly growing.

This operating model is inefficient, it doesn't scale, and it doesn't work in today's threat environment. Instead, organizations need to implement the following key principles to scale their SOCs and improve their security efficacy:

- **Interoperability:** Your SOC should be using tools and solutions — including ASM — that are designed to work together. This is a critical first step to enabling automation.
- **Automation:** All the important actions performed by your SOC must be automated instead of relying extensively or solely on manual intervention. Playbooks are now automated, running 24/7/365, and are triggered to handle the

steps essential to prevent, detect, and remediate potential threats. Searching for indicators of compromise (IoCs), isolating users and systems, performing forensics, and completing remediation tasks should all take place automatically — in minutes or even seconds.

- **Collaboration:** Your SOC strategy should promote collaboration across your entire organization. If your credit card company detects suspicious activity, it typically texts you and asks you to validate via a yes/no question. The same should take place for potential security events. A text can be automatically generated by your SOC to ask a user if they logged into the network from Russia at 3 a.m. If the answer is no, an automated remediation playbook can be triggered. Now, instead of having a physical SOC with perhaps ten engineers, you have a virtual SOC composed of everyone in the company — perhaps thousands of people. Collaboration is an exceptional force multiplier in re-architecting your SOC and securing your company.

AN ATTACK EXAMPLE: RDP, THE "RANSOMWARE DELIVERY PROTOCOL"

Remote Desktop Protocol (RDP) is a popular technology for connecting to remote systems, and there are millions of computers with publicly exposed RDP ports, making RDP a top threat vector for threat actors and representing 25 percent of all security issues, according to research by Palo Alto Networks.

Having a workstation with RDP exposed on the public Internet is the equivalent of leaving a laptop open to its login screen sitting on the street, where anyone can repeatedly try to log in by guessing the username and password. Most organizations think that they're blocking RDP across their networks and devices, but RDP instances for organizations — including a majority of the Fortune 100 — are regularly found on the public Internet.

The most common attack against RDP starts out with a brute-force password-guessing attempt. If the password isn't complex enough or

(continued)

(continued)

if there aren't lockout attempts, then attackers will eventually compromise a device. When this happens, ransomware is typically installed, which can spread throughout the organization, causing significant business interruption incidents. Data is encrypted or destroyed, leaving organizations with a crippled network caused by an unknown exposure that occurred in IP space that they weren't monitoring.

Today, many cybercriminal groups specialize in scanning the Internet for RDP endpoints, and then carrying out brute-force attacks against these systems to obtain their credentials. Systems that use weak username and password combinations are easily compromised, and the credentials are then sold in "RDP shops" on the dark web.

RDP is particularly troublesome because it's a top vector for ransomware. The Palo Alto Networks Unit 42 incident response team has seen constant RDP scanning for port 3389 — reserved for RDP — in its investigations, followed by brute-forcing credentials or basic credential-cracking tools. Worse, in the remote work environment, connecting from a personal device means it's out of the security team's control. This gap means most companies don't have the right controls, and without visibility, attackers have the luxury of time to find and exploit RDP.

RDP is typically plagued by a number of security issues, including the following:

- Weak passwords that are vulnerable to brute-force and dictionary attacks
- Outdated versions of RDP that may use Credential Security Support Provider (CredSSP), thus enabling a potential man-in-the-middle attack
- Allowing unrestricted access to the default RDP port (TCP 3389)
- Allowing unlimited login attempts to a user account

IN THIS CHAPTER

- Keeping pace with attackers when new vulnerabilities are published
- Bolstering vulnerability management in the cloud
- Leveraging automation for attack surface management
- Discovering risk in your extended attack surface ecosystem

Chapter 4
Exploring Attack Surface Management Use Cases

In this chapter, you learn about several common attack surface management (ASM) use cases, including immediately identifying common vulnerabilities and exposures (CVEs) across your attack surface, addressing vulnerability management challenges in the cloud, automating ASM, and discovering risk in mergers and acquisitions (M&As) and across your supply chain.

Gaining Immediate Visibility Against Common Vulnerabilities and Exposures

Every time a new security vulnerability surfaces, a frenzied race kicks off between attackers scanning the Internet to identify vulnerable systems and defenders scrambling to implement patches and other mitigations to protect their networks. Today, it takes only 45 minutes for threat actors to scan the entire Internet for vulnerabilities, and within 15 minutes of a CVE disclosure, attackers are on the prowl for potential targets.

A CVE PRIMER

The CVE program maintains a list of publicly disclosed security flaws in computer hardware and software. Security advisories issued by various vendors and researchers typically reference one or more CVEs. The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) funds the CVE program, which is overseen by the MITRE corporation.

CVE identifiers are assigned by a CVE Numbering Authority (CNA). CNAs include various IT hardware and software vendors, security companies, and research organizations, as well as the MITRE corporation itself.

CVEs help IT and security teams to uniquely identify vulnerabilities that may exist in their attack surface. Thousands of CVEs are published annually and, as of November 2022, there were more than 189,000 CVE records.

To learn more about CVEs, go to `https://cve.mitre.org`.

To successfully protect the enterprise attack surface against unrelenting threat actors scanning the Internet for new targets of opportunity, defenders must ensure their mean time to inventory (MTTI) — the time it takes to inventory all known and unknown vulnerable assets — is faster than the MTTI for attackers.

This starts with scanning the entirety of IPv4 space for assets connected to an organization's network and determining which ones need patching or have insecure remote access implementations, exposed databases, or other risks. When a previously unknown asset is found, the notification should be automatically routed to the IT team or individual responsible for securing that asset.

ASM processes should also focus on reducing a vulnerability manager's workload by helping to highlight the most pressing risks and exposures and efficiently handling alerts. ASM combined with security orchestration, automation, and response (SOAR) can be invaluable in automatically attributing a previously unknown asset and routing the alert to the relevant stakeholders for remediation.

Improving Cloud Vulnerability Management

Today, most organizations have built, or are building, substantial cloud footprints. Application developers, marketing teams, and other non-IT functions are routinely creating (and abandoning) assets in the cloud. Many of these unknown and unauthorized cloud assets are in ephemeral Internet Protocol (IP) space, making it even harder for organizations to get a holistic view of their cloud footprint for security and infrastructure management.

As cloud adoption increases, new challenges for IT and security teams emerge that current tools fail to address. Securing known assets can be challenging in itself, but it isn't possible to secure what isn't known — things like shadow infrastructure and rogue development, both of which abound in the cloud. Enterprise cloud footprints present unique challenges, including the following:

- The failure of existing tools to discover cloud assets across authorized and unauthorized providers in a current, reliable, and comprehensive manner
- The ease and speed with which unknown and unauthorized cloud assets can be spun up and remain active and undiscovered
- The deficiency of existing tools to reliably discover owned assets versus other assets in multi-tenant or ephemeral environments

Managing and securing assets in ephemeral IP space requires a view of assets that is current and accurate. Incumbent tools fail because they track cloud IP addresses to an organization simply because that IP address was seen hosting a company asset at one time — information that quickly gets stale and isn't useful or actionable for securing rogue cloud assets. Thus, traditional security tools designed for static networks don't work in the cloud, and relying on this ineffective approach can cause IT and security practitioners to scan, penetration-test, and waste time investigating assets that aren't even theirs — all while missing critical unknown cloud assets that create risk.

Organizations can't use these tools to build a holistic view of their cloud assets. Without a better strategy, organizations are left with an incomplete view of their Internet assets and no way to monitor critical business applications hosted in the cloud.

To fully solve the problem, organizations must take a discovery-first, "whole-Internet" approach to cloud security. When cloud assets are discovered and any misconfigurations are exposed, organizations may leverage a myriad of cloud security tools on the market to manage asset permissions and other configuration items — but cloud asset discovery must be a continuous process to maintain a clear and accurate picture of the organizational cloud footprint (see Table 4-1).

TABLE 4-1 The "Whole-Internet" Approach

	What It Does	Why It's Important
Complete global Internet coverage	Records details of all publicly routable assets, services, and their configuration details across the entire global Internet.	If this inventory isn't comprehensive, the discovery process will miss assets that should be attributed.
Comprehensive service classification intelligence	Maintains an accurate rule set that uses combinations of ports, protocols, and response details to classify specific service types. It must index every IP address across multiple ports and protocols and then apply these rules to the responses to parse and record every routable service.	Inaccurate or incomplete service classification intelligence will lead to undiscovered or misclassified cloud services.
Frequent indexing of the global Internet	Maintains a current snapshot of publicly routable assets.	Infrequent indexing will lead to stale or undiscovered cloud assets.
Detailed organizational fingerprints compilation	Maintains an accurate set of an organization's fingerprints on which to search the global Internet data set for attributable cloud assets.	Inaccurate or incomplete lists will lead to undiscovered or misattributed cloud assets.

TIP

A comprehensive ASM platform enables you to enforce asset management policies for all your assets from a single dashboard. Key capabilities to look for include the following:

- Identify all risky services running on your organization's network for remediation and attack surface area reduction.
- Update vulnerability scan target data on a daily basis to include up-to-date, accurate on-premises and cloud IP addresses hosting your organization's services.
- Alert on the appearance or reappearance of exposed services to kick off remediation workflows.

Automating Attack Surface Management

Although organizations' attack surfaces have grown exponentially in recent years, their security teams have not. Organizations need to find efficient ways to reduce their risks and gain visibility into their growing and increasingly complex attack surface.

One persistent challenge for many organizations tasked with remediating attack surface risks is that determining ownership and business context of unknown assets is a highly manual and time-consuming task that may span different teams, including IT, SecOps, and DevOps, among others.

Automating ASM empowers the modern security operations center (SOC) by:

- Reducing time spent by analysts on routing investigation tasks
- Simplifying analysis and next-step recommendations to reduce analyst expertise requirements to scale your SOC
- Preserving context discovered through ad hoc investigations in order to garner new insights and make future investigations more efficient
- Providing insights into what remediation paths have been used by your team in the past to simplify decision-making for remediation

Reducing M&A and Third-Party Cyber Risk

Global M&A activity reached all-time highs totaling $1.3 trillion during the first quarter of 2021, spiking by 94 percent compared to the first quarter of 2020 according to *Fortune.* M&A activity adds a new attack surface and risk vector that becomes the responsibility of the acquiring company.

Supply chain attacks are not new, but they have garnered renewed media attention in the wake of various high-profile attacks over the past few years. As such, companies must ensure their critical supply chain partners, both upstream and downstream, don't introduce unacceptable risk to the organization. At the same time, organizations must understand their own role in the supply chain and ensure that they don't introduce unacceptable risk to their partners. Third-party assessment capabilities should be an integral part of a comprehensive ASM solution to help ensure visibility and control of your extended attack surface.

Key capabilities include the following:

- **Vulnerability management:** Identify unknown assets and Internet-facing misconfigurations to include them in vulnerability assessments and responses.
- **Cloud security:** Identify and eliminate cloud sprawl and centrally enforce cloud policies.
- **Penetration testing:** Identify unknown assets to include in penetration testing efforts to increase efficiency and improve security posture.
- **Compliance services:** Identify exposed assets that aren't compliant with industry standards and regulatory requirements.
- **Incident response:** In the event of major vulnerabilities or zero days, confirm if customers have been impacted.
- **M&As:** Discover an acquisition's Internet assets and exposures to inform M&A strategy and process.
- **Net new ASM service:** Build a net new service to help customers manage and mitigate the risk of their entire attack surface.

CASE STUDY: FORTUNE 500 BANK

Challenges

- Outside-in cyber due diligence needed for multiple acquisitions
- No visibility into different cloud providers, certificates, and domains

Cortex Xpanse Outcome

- Discovered, evaluated, and mitigated risk for the assets of three acquisitions
- Managed 21,481 assets
- Surfaced 25 high-priority issues and marked them for remediation

TIP

A comprehensive ASM platform enables key capabilities, such as the following:

- Conduct cybersecurity due diligence on ongoing and historical acquisitions.
- Audit the inventory of M&As and monitor the rate of IT integration.
- Verify asset deprecation and successful network integration during an M&A event (for example, identifying M&A assets utilizing other cloud environments, like Amazon Web Services [AWS] or Microsoft Azure, and migrating those assets onto your organization's AWS account or Azure tenant).

IN THIS CHAPTER

- Automatically discovering assets and remediating risks
- Enabling centralized, policy-driven management of your attack surface
- Reducing mean time to detect and mean time to respond

Chapter 5
Automating Attack Surface Management with Cortex Xpanse

In this chapter, you discover how Palo Alto Networks Cortex Xpanse help you automate attack surface management (ASM) to help improve your organization's security posture.

Don't Just Find Risks, Fix Them

Cortex Xpanse helps organizations discover and classify their risky Internet exposures, identify and prioritize risks, and quickly remediate them. Xpanse delivers important ASM capabilities and features, including the following:

- **Comprehensive attack surface discovery:** See and monitor all assets exposed to the Internet:
  - Discovery and inventory of all assets including external (IPv4, IPv6, web), cloud, devices, and applications

- Current, complete, and accurate views with machine learning–based asset attribution
- Discovery confidence scores and explanations

- **Immediate zero-day visibility:** Quickly know and react to discovered threats and vulnerabilities:
  - Assets and issues discovered within hours of publication
  - Fast vulnerability scans — minutes to run across an entire attack surface
  - Up-to-date dashboard views of vulnerability and weaponization efforts, worldwide exposure statistics, and issues on your attack surface
- **Risk prioritization:** Proactively manage risk to focus on highest-impact areas:
  - Customizable policy definitions adapt to business needs and priorities, including new policies built by Xpanse researchers (policy factory) and self-service policy management
  - Recommended policies to drive best practices
  - Artificial intelligence (AI)–driven issue prioritization to focus analyst time and improve return on investment (ROI)
- **Automated in-built remediation:** Reduce risk with actionable context and automation:
  - Context on assets and risks including people (asset and service owners), processes (where assets are used, consequences of compromise), and external and internal data stitching to ensure actionability
  - Automated response including deploying missing agents, scanning unmanaged assets, onboarding missing cloud accounts, and automated remediation of exposures

Deploy Policies to Centrally Manage Your Attack Surface

Cortex Xpanse mitigates risk through a native policy engine to highlight policy violations across all your known and unknown assets in real time. In addition, Xpanse creates alerts for out-of-policy

assets using dozens of natively built integrations — including ServiceNow, Splunk, and Palo Alto Networks Cortex XSOAR — to create a workflow to quickly remediate the exposure to reduce mean time to detect (MTTD).


TIP

Additionally, you can develop custom policies using known indicators of compromise (IoCs) to centrally identify and remediate assets exposed to the latest common vulnerabilities and exposures (CVEs). Key Xpanse policy management capabilities and features include the following:

- Configure customized alerting on all public-facing asset issues and kick off remediation according to your organization's service-level agreements (SLAs).
- Integrate with existing security orchestration, automation, and response (SOAR) platforms and remediation playbooks to ensure consistent resolution of issues in a timely manner.
- Create an accurate, consolidated, and referenceable list of issue owners in a single tool to enrich issue investigation.
- Verify successful remediation of exposed services using Xpanse disappearance logic.

Integrate with SOAR to Reduce MTTD and MTTR

Cortex XSOAR unifies case management, automation, real-time collaboration, and threat intelligence management to transform every stage of the incident life cycle, enabling significantly faster MTTD and mean time to respond (MTTR) with less manual review.

The Xpanse content pack for Cortex XSOAR provides full coverage of the Expander product capabilities from Xpanse to enable your security operations center (SOC) to automate remediation of your company's attack surface (see Figure 5-1). The integrations included in the pack enable fetching and mirroring of Xpanse issues into Cortex XSOAR incidents, as well as ingestion of indicators (Internet Protocol [IP] addresses, domains, and certificates) referring to the corporate network perimeter as discovered by Xpanse.

CORTEX XSOAR MARKETPLACE CONTENT PACK OVERVIEW

The Cortex XSOAR Marketplace is a digital storefront for discovering turnkey security orchestration content packs centrally within Cortex XSOAR.

Content packs are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security orchestration use cases.

The Xpanse content pack automates ASM to identify unknown Internet assets and quickly remediate misconfigurations with playbooks that hunt for internal activity related to detected services, provide incident enrichment from the Internet and public cloud assets, and much more.

The pack is easily deployed with a single click from the in-product Cortex XSOAR Marketplace, giving you all the content needed to automate ASM with Cortex XSOAR.

To discover new SOAR content, visit `https://paloaltonetworks.com/cortex/xsoar/marketplace`.

FIGURE 5-1: Cortex XSOAR and Xpanse integration.

Leveraging both technologies, your security team can respond to asset vulnerabilities and incidents with automated orchestration playbooks. You can trigger scans to enrich incidents and automatically generate tickets for on-premises and cloud assets. Your team can use this powerful integration to:

- Assign incident severity.
- Automate vulnerability management.

- Orchestrate certificate management.
- Diagnose end points.
- Threat-hunt for compromised assets.

Through a powerful set of playbooks, analysts can correlate the discovered information with data provided from internal security systems (for example, Cortex Data Lake, Cortex XDR, Prisma Cloud, Panorama network security management, Active Directory, and security information and event management [SIEM]) to help pinpoint the right owners of assets and automate remediation.

INCIDENT USE CASE

Challenge

Your attack surface is constantly shifting and expanding with the addition of new cloud instances, infrastructure, web gateways, contracted service providers, assets from mergers and acquisitions (M&As), and much more. You need a way to quickly inventory and discover exposures across this shifting landscape. You also need to remediate vulnerabilities from exposures in real time and prevent threats, including breaches and data loss.

Solution

Xpanse ASM provides an in-depth look at your constantly changing attack surface and highlights all existing known and newly discovered vulnerabilities across your environment. Using the Xpanse content pack for Cortex XSOAR, your team can automate discovery, incident handling, and response for all the vulnerabilities discovered by Xpanse. The Xpanse integration provides additional context for any Cortex XSOAR incident.

Benefit

Automate the identification and remediation of web-facing exposures and vulnerabilities with Cortex XSOAR and Xpanse to scale your organization's security posture. Defend your attack surface without adding new staff or expertise to your current SOC team.

Chapter 6
Ten (or So) Key Attack Surface Management Capabilities and Features

Here are ten (or so) important capabilities and features to look for in an attack surface management (ASM) platform for your organization:

- **Comprehensive attack surface discovery:** Your ASM platform must help you discover, evaluate, and mitigate your external attack surface globally, including multicloud, private and public cloud, and on-premises environments, as well as remote worker and ephemeral assets.
- **Immediate zero-day exposure visibility:** Attackers scan the entire Internet for vulnerable assets within 15 minutes of new common vulnerabilities and exposures (CVEs) being published. Your ASM platform must provide the same, if not better, speed and accuracy to help you identify and protect vulnerable entry points across your attack surface.

- **Integrations with existing security operations center (SOC) workflows:** Organizations already contend with stretched-thin cybersecurity resources. Your ASM platform must be flexible and powerful enough to integrate with your existing SOC workflows to drive automation and orchestration.
- **Automated risk prioritization:** As the attack surface rapidly grows and constantly evolves, your ASM platform must automatically evaluate the risk of every asset to help prioritize mitigation and remediation and drive compliance.
- **Automated remediation:** Your ASM platform must integrate with your existing security orchestration, automation, and response (SOAR) platforms and remediation playbooks to ensure consistent and rapid resolution of issues in a timely manner.
- **Remote worker ASM:** Organizations have been forced to accelerate the migration to a remote workforce model despite very limited visibility into the security of their employees' remote networks. Unfortunately, organizations have no way of knowing how secure remote worker networks are and whether there are unknown exposures or critical issues open on remote employee devices that are accessible from the public Internet. Look for an ASM platform that extends coverage to your remote workers and includes the following capabilities:
  - Ensuring that insecure network configurations aren't exposing risky services on corporate devices
  - Gaining visibility into dynamically change policies to alter access controls based on employee location
  - Identifying end points connecting through known vulnerable routers and assessing the need to deploy enterprise-grade hardware to key employees
  - Measuring the organizational risk associated with key employees working from their home or temporary networks

- **Unparalleled value and return on investment (ROI):** Your ASM platform should be able to deliver exceptional value and a quantifiable ROI through:
  - Faster mean time to detect (MTTD) and mean time to respond (MTTR) with comprehensive asset discovery across the entire digital estate and the ability to discover and evaluate ephemeral assets
  - Money saved due to downtime avoided by identifying expired security certificates, reduced cybersecurity breaches, and associated financial impacts, as well as improving ROI on your existing tools
  - Hours freed by automating asset discovery and evaluation, as well as automated remediation through integrations

Automate attack surface management

Attack surface management (ASM) is not new, but how organizations view their attack surfaces should be updated. Traditionally, IT has looked at an organization's attack surface from the inside out, asking, "What assets connect to the Internet?" and "What are our mean times to detect and respond?" Instead, security teams should be looking from the outside in, asking questions like, "How many unknown assets are connected to our network?" and "What is our mean time to inventory every asset that can put us at risk?"

Inside...

- Automatically find and fix exposures
- Centrally manage your attack surface
- Increase security effectiveness
- Improve cloud vulnerability management
- Protect remote workers
- Recognize top attack surface exposures

CORTEX® XPANSE™
BY PALO ALTO NETWORKS

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the coauthor of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

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

ISBN: 978-1-394-18314-2
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.