LEARNING MADE EASY

Tenable Special Edition

Cyber Exposure

for dummies®

A Wiley Brand

Securing modern digital assets

Evolving from VM to cyber exposure platforms

Prioritizing cyber exposure

Brought to you by

tenable™

Stacy Moran

Steve Piper

About Tenable

Tenable is the Cyber Exposure company. More than 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus, Tenable built its platform from the ground up to deeply understand assets, networks, and vulnerabilities, extending this knowledge and expertise into Tenable.io to deliver the world's first platform to provide live visibility into any asset on any computing platform.

Tenable customers include more than 50 percent of the Fortune 500, large government agencies, and midsize organizations across the private and public sectors.

Visit us at **www.tenable.com** to learn more.

Cyber Exposure

Tenable Special Edition

by Stacy Moran and Steve Piper

for dummies®
A Wiley Brand

Cyber Exposure For Dummies®, Tenable Special Edition

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

ISBN 978-1-119-50815-1 (pbk); ISBN 978-1-119-50830-4 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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:

Development Editor: Elizabeth Kuball

Copy Editor: Elizabeth Kuball

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Amy Fandrei

Production Editor: Magesh Elangovan

Special Help: Michael Applebaum, Felix Do, Winston Chiang, Nate Dyer, Kevin Flynn, Ted Gary, Tom Parsons, David Schreiber, Kathy Simpson, Maya Smith, Dave Stuart

Table of Contents

Introduction

Today's networks are constantly evolving — and so are their attack surfaces. Information technology (IT) security professionals must now contend with digital assets that many of their predecessors never contemplated, such as cloud platforms, application containers, web applications, Internet of Things (IoT) devices, and network-connected operational technologies such as industrial control systems.

For security professionals who work in healthcare or critical infrastructure industries, the stakes are even higher. They must secure essential (in some cases, life-saving) Internet-enabled devices without affecting performance or availability.

Vulnerability management (VM) solutions have steadfastly served organizations by uncovering vulnerabilities and security misconfigurations within traditional computing assets, such as servers, PCs, and network infrastructure. But VM platforms relying on periodic scanning of traditional systems have run their course; they're no longer sufficient against attacks targeting the modern attack surface.

This is where cyber exposure comes in. Cyber exposure is a paradigm shift in the way we think about securing the attack surface and protecting against diverse threats.

About This Book

This book defines cyber exposure, including the cyber exposure gap created by legacy security offerings, and prescribes an innovative solution: the cyber exposure platform, which is designed to protect all computing assets and provide a new level of insight.

In this book, you explore the features and benefits of a cyber exposure platform, discovering how to evolve your existing security program to address new risks. You also see how to understand your cyber exposure in business terms and communicate it to top management.

If you're responsible for guarding your organization's fast-changing assets across traditional IT, cloud, and IoT environments, this book is one that you can't afford to miss.

Foolish Assumptions

In preparing this book, we've assumed a few things about you, the reader:

- You work in IT security for a private-sector or public-sector organization.
- You have professional knowledge of enterprise computing, computer networks, and IT security.
- You have a baseline understanding of what traditional VM offerings provide.

Icons Used in This Book

This book uses the following icons to indicate special content:


TIP

The Tip icon points out practical advice that can help you craft a better strategy, whether you're planning a purchase or setting up your software.


REMEMBER

You won't want to forget the information in paragraphs marked with the Remember icon.


WARNING

Look out! When you see the Warning icon, it's time to pay attention. You won't want to miss this cautionary information.


TECHNICAL STUFF

Maybe you really like to grasp all the nuts and bolts — even the most techie parts. If so, tidbits marked with the Technical Stuff icon are right up your alley.

Beyond the Book

To find out more about cyber exposure and how to move from legacy VM to a cyber exposure platform, visit `www.tenable.com/cyber-exposure`.

IN THIS CHAPTER

- Grasping the scope of today's attack surface
- Understanding technology trends that increase cyber risk
- Seeing why traditional vulnerability management solutions fall short

Chapter 1
Navigating the Modern Attack Surface

The term *attack surface* sounds ominous. What is an attack surface?

You can think of it as the points of exposure that can be attacked and lead to cyber breaches. In addition to targeting endpoints (which resulted in breaches at Home Depot, Anthem, and elsewhere), savvy adversaries now attack the full set of systems, devices, and applications — collectively referred to as *assets* — that comprise the increasingly complex, dynamic attack surface.

This ever-changing collection of assets (see Figure 1-1), encompassing everything from information technology (IT) infrastructure to cloud services and operational technology (OT), offers plenty of opportunities for attackers to infiltrate vulnerable networks and steal or destroy sensitive data, or even disrupt critical infrastructure.

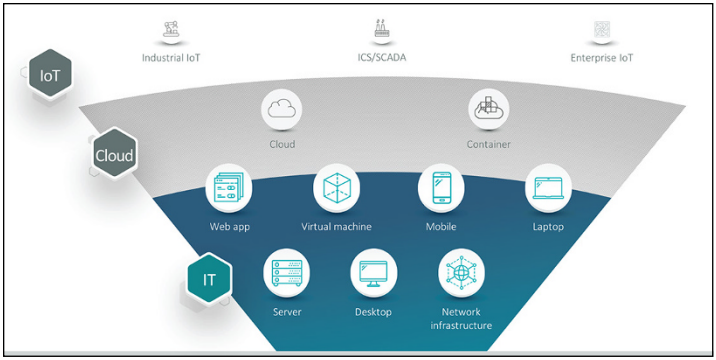

FIGURE 1-1: Modern attack surface.

TIP

For more on the specific components that comprise the modern attack surface, see Chapter 2.

How are you supposed to keep tabs on all this stuff? It's not easy. You've got to up your game. We're here to help.

In this chapter, we provide a snapshot of the technology trends, computing environments, modern assets, and emerging cyber threats that change your attack surface every day.

Trends Affecting Your Attack Surface

Not too long ago, life was less difficult for security practitioners, who typically managed traditional IT assets that lived within the four walls of a data center or at least a physical office. Today, they must protect dynamic assets such as cloud instances and Internet of Things (IoT) devices, which are often introduced without IT's knowledge.

In this section, you begin your cyber exposure journey by reviewing recent trends that affect your organization's security.

Digital transformation

Here's the good news about digital transformation: Organizations in every industry sector are embracing it to drive bold business strategies for growth and efficiency. Agile cloud-based technologies and methodologies are disrupting norms, unleashing innovation, and enabling global collaboration.

Approaches such as DevOps (development and operations; see Chapter 4) enable companies to continuously create and release new versions of software, accelerating innovation. Now here's the flip side:

- Digital transformation changes an organization's attack surface in major and often unpredictable ways, posing significant challenges for security teams tasked with protecting dynamic assets across multiple computing environments.
- As the elastic (always-changing) attack surface morphs minute by minute, it becomes increasingly difficult for IT security to maintain visibility into and understand the organization's cyber exposure and proactively manage risk across all assets.

Sophisticated threats

Not only are attackers increasingly savvy, but they also have access to the wealth of sophisticated hacking tools that are readily available on the black market. A complex threat landscape with highly motivated adversaries translates into punishing cyber attacks every week.

According to the 2017 *Tenable Global Cybersecurity Assurance Report Card* (`www.tenable.com/lp/2017-global-cybersecurity-assurance-report-card`), the overwhelming threat environment remains the number-one challenge for security professionals. Attackers have more opportunity than ever to exploit gaps in security coverage, leaving organizations of all sizes in all industry sectors vulnerable to compromise and breach.

Public cloud services

Deploying workloads in the cloud results in agility and scalability — huge enablers of digital transformation — but for most teams, securing assets in the cloud isn't easy. Most solutions built to protect traditional IT systems have blind spots around cloud-based assets, which occupy a significant piece of the modern attack surface. The primary challenges associated with cloud security involve visibility, regulatory compliance, and security policy enforcement across multiple cloud and on-premises environments.

TIP

We talk more about cloud security in Chapter 5.

DevOps and containers

The unification of development and operations processes in DevOps is changing the way that software is built and deployed at the same time as the traditional waterfall model is being replaced by agile approaches. DevOps synchronizes the activities of development, quality assurance, and operations teams, compressing cycle times from weeks to hours.

Listen closely, and you may hear your software development team chanting its mantra: "Faster, faster." They live for speed, releasing new code in hours. The application containers increasingly used to deploy new software sometimes appear and disappear so quickly that there's no time even to scan them for vulnerabilities. But because of their large numbers, these containers can lead to serious exposure.

TECHNICAL STUFF

As Spotify users play music, containers spin up and do their thing (such as retrieve track and artist data) — and then face imminent death when a task is completed. Life is short. There's no time for scanning or patching.

To avoid getting left behind, security teams must match the velocity of DevOps with new approaches that can identify and mitigate vulnerabilities in containers before deployment, without slowing development. If they're successful, they can prevent security flaws in containers from reaching production.

TIP

Find out more about DevOps in Chapter 4.

Workforce mobility

Today, employees work from everywhere, using multiple devices to access a variety of applications, so supporting workforce mobility and ensuring system availability are critical. Mobile warriors (that is, most of us) must be able to remotely access corporate data and services anytime and anywhere.

Seamless access, however, introduces significant security risks. Many organizations allow the use of mobile devices without proper security controls to protect sensitive data. These devices often run outdated operating systems and contain vulnerabilities

that can lead to malware infections, exposure of confidential data, and compromise of sensitive credentials.

As organizations continue to employ a mobile workforce, they must ensure secure remote access and information exchange without allowing compromise of critical systems or proprietary data.

Web applications

Almost every new application is a web application, and web apps are prone to a wide range of vulnerabilities. Web application attacks are responsible for many of the data breaches during the past several years. The explosive growth and sprawl of web applications make them difficult to secure. Most web apps are updated at least monthly, and it's hard to keep up when your security team is outnumbered by developers 100 to 1.

Internet of Things

Connected devices such as kiosks, HVAC systems, and cameras are increasingly common in business and industrial environments. Unfortunately, IoT devices offer hackers an even bigger playground and one that is not always appreciated by organizations.

Operational technology

OT systems that provide the backbone of critical infrastructure, healthcare, manufacturing, and other production environments must be protected to ensure uptime, reliability, safety, and compliance. Securing data is not the primary focus. Because these systems are often too fragile to run active vulnerability scans on, only passive, nonintrusive assessment works in these environments. Most industrial infrastructure wasn't designed with network-based attacks in mind, but as such threats become more prevalent, companies must proactively address cyber risk across both IT and OT.

Organizations with industrial systems typically use different security tools and approaches for IT and OT. Those two worlds are beginning to converge, however, creating both challenges and opportunities (see Chapter 6).

TIP

See Chapter 3 for more about scanning technologies.

Why Traditional Vulnerability Management Falls Short

Traditional vulnerability management (VM) tools were designed for traditional workplaces, processes, and technologies. Experienced professionals probably remember when employees worked in the office every day on desktop computers that connected primarily to corporate data center servers. These assets now represent a tiny sliver of the dynamic environment that organizations must protect. If your security tools and processes haven't evolved as fast as the technology and business processes surrounding them, now's the time to rethink your approach to security.

Reliance on legacy tools

Legacy approaches and tools designed to protect traditional IT assets such as servers and network infrastructure aren't robust enough to defend the modern attack surface and digital landscape. (Speaking of landscapes, using outdated tools is like having only a weed whacker at your disposal to manicure and maintain your entire yard.)

TIP

We discuss legacy VM in Chapter 3.

Lack of continuous visibility

Given the complex digital environment and the expanding attack surface, it's easy to understand why companies struggle to maintain visibility into their broadening array of assets. As part of daily workflows, employees continually bring new devices and applications onto the organization's network, often without IT's taking notice. New applications are built, new cloud instances are deployed, and new IoT devices are connected. These blind spots can expose critical systems and sensitive data to compromise and breach.

Modern assets such as containers (see Chapter 4) that support rapid deployment of software also contribute to a lack of visibility.

Visibility challenges include the following:

- Discovering and monitoring assets that aren't on the network for long — or at all, in the case of cloud instances

- Seeing and protecting end-user devices off the network
- Finding vulnerabilities in application code that the organization builds itself
- Identifying weaknesses in IoT devices that could lead to compromise
- Assessing critical infrastructure systems without disrupting operations

Insufficient prioritization of issues

Prioritizing vulnerabilities, misconfigurations, and other security issues for remediation may be the most pressing challenge in maturing your security foundation. Getting this task right is akin to securing the doors and windows on the first floor of your house before locking the windows upstairs. They all matter, but some matter much more than others.

When IT operations gets a 300-page vulnerability report from the security team, it's hard-pressed to figure out what to do with all the issues requiring remediation. Security must guide the rest of the organization on which weaknesses pose the highest risk and which systems demand immediate attention.

TIP

For a deep dive into prioritization, see Chapter 7.

Failure to communicate cyber risk in business terms

Raw security data must be translated into information that's actionable for IT and security practitioners, as well as for executive stakeholders who seek to understand and manage cyber exposure at a higher level. Traditional vulnerability management fails to provide true business context and guidance on what action to take from a risk-based view. A new approach should provide business metrics and visualizations that executives can understand.

IMPROVING SECURITY BY 99.9 PERCENT

Security professionals find themselves chasing the "threat of the week," often to no avail. Racing ahead without context and prioritization results in reactive firefighting and pursuit of the wrong issues. Performing the security basics well demands insight and focus.

Fortunately, vulnerability remediation doesn't always have to be performed overnight, although the highest-risk issues should be addressed quickly. According to Verizon's 2015 *Data Breach Investigations Report* (`www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf`), a comprehensive assessment of global data breach statistics, "99.9 percent of the exploited vulnerabilities were compromised more than a year after the CVE [Common Vulnerabilities and Exposures] was published." In other words, if organizations would patch their vulnerabilities in less than a year, they could improve their chances of preventing an exploit-initiated data breach by as much as 99.9 percent.

IN THIS CHAPTER

- Defining cyber exposure
- Eliminating the cyber exposure gap
- Examining a cyber exposure platform

Chapter 2
Understanding Cyber Exposure

When you think about the combination of accelerating digital transformation and the proliferation of mobile, cloud, container, and Internet of Things (IoT) assets across the modern attack surface (see Chapter 1), you see why organizations of every size in every industry must rethink their approaches to cybersecurity.

Visibility is the first critical element. The farther you move from the data center, the harder it is to see and track your assets. The deck is stacked against defenders, who must protect every piece of the attack surface, even when colleagues outside IT are deploying systems beyond their control.

Seeing isn't everything, however. In fact, getting more visibility increases another challenge: making sense of all that data. It's hard to know what you should focus on, which issues matter most, and whether you're improving effectiveness over time. Sometimes, less (data) would truly be more — if it's more relevant and actionable.

Figuring out which security weaknesses to remediate first is hard enough for traditional IT. With the expansion of the attack surface and greater demands for executive reporting, the challenge

has evolved into something far more complex than traditional vulnerability management (VM), calling for a new discipline that we call *cyber exposure.*

In this chapter, we define cyber exposure in detail and highlight some of the key elements of a modern cyber exposure platform. We delve deeper into the capabilities and benefits of such a platform in Chapter 3.

What Is Cyber Exposure?

Cyber exposure is an emerging discipline for managing and measuring your modern attack surface to accurately understand and reduce your cyber risk. It provides a framework that enables you to understand and act on cyber risk at all levels of the organization. The three core inputs of a cyber exposure model are asset and business context, vulnerabilities, and threat context.

The cyber exposure gap

The *cyber exposure gap* is the blind spot that lies between the visibility provided by your current security tools and the complete set of vulnerabilities and misconfigurations across your entire attack surface (see Figure 2-1). If your current solutions can't see and assess new cloud instances, if you have no way to detect flaws in containers, or if you have no idea which operational technology (OT) systems are exposed, your cyber exposure gap is expanding. The larger the gap, the greater the odds of a business-impacting breach or operational disruption.

The cyber exposure gap changes daily as virtual machines are spun up and down, end-user devices are provisioned to employees, and IoT devices are deployed in remote offices. Hackers are aware of this gap and your limited visibility. They're always looking for the path of least resistance. Threats such as WannaCry, which racked up billions of dollars in damage, make it imperative to find and fix your critical vulnerabilities.

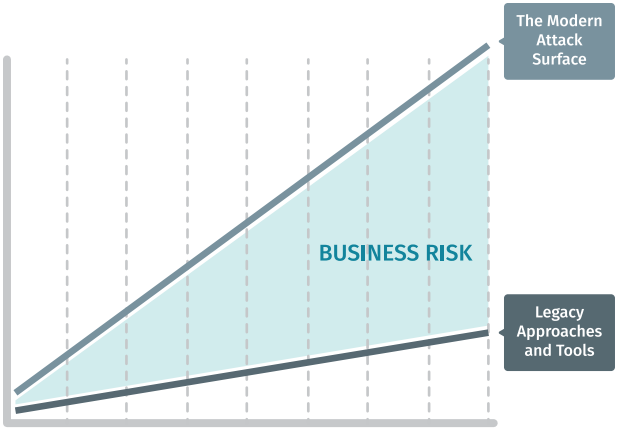

FIGURE 2-1: The cyber exposure gap.

The WannaCry and Petya/NotPetya attacks forced medical centers to shut down, halting the delivery of life-saving care to patients in need. They also affected operations around the world for Honda, Renault, Deutsche Bahn, and many other businesses. NotPetya, an aggressive worm using multiple exploits, delivered destructionware (encrypting the target's data without possibility of recovery), generating more than $200 million in damage for several victims.

The cyber exposure life cycle

The five stages of the cyber exposure life cycle (see Figure 2-2) are designed to continuously identify assets; detect vulnerabilities and security issues across all asset types; prioritize issues based on risk; apply the appropriate remediation technique in conjunction with other technologies; and provide reporting, visualization, benchmarking, and modeling to help security professionals and executives make better decisions.

Cyber exposure builds on traditional VM, achieving end-to-end visibility of traditional and modern assets ("see more") and the analytics-driven insight to know how to act ("do more"). The practice of cyber exposure is more continuous, collaborative, and focused than ever before, connecting information security, IT, and DevOps throughout the life cycle.

Leading cyber exposure platform providers adopt an open, flexible approach that integrates tools and technologies from ecosystem partners to help organizations maximize their existing technology investments, slash manual work, and ultimately reduce cyber risk.

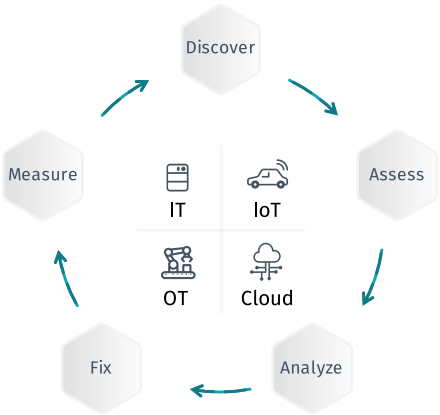

FIGURE 2-2: The cyber exposure life cycle.

Complementary ticketing/workflow, patch management, network access control, and mobile device management tools can be easily integrated to support the Fix (remediation) phase of the life cycle. This integration ensures that critical exposures are addressed properly and promptly, with complete visibility from detection to ticket assignment to remediation and validation.

The relationship between vulnerability management and cyber exposure

VM focuses on periodically scanning traditional IT assets for vulnerabilities and misconfigurations, and then providing reports to security and IT. Today, however, every aspect of traditional VM is outdated, for the following reasons:

- Periodic assessment leaves security teams in the dark about what's happening between scans.
- Scanning alone won't find every asset and can't be used on sensitive assets such as OT systems.

- Traditional IT assets are far from the only source of exposure, with breaches such as Equifax underscoring the importance of protecting web applications and other resources.
- Reports are often little more than large sets of raw information that are difficult to act on.
- Security and IT aren't the only stakeholders. DevOps has become a critical participant. Also, management increasingly wants to understand the organization's exposure in business terms and manage it proactively.

Cyber exposure builds on VM but is broader and more strategic. A cyber exposure platform delivers comprehensive and actionable information for today's dynamic attack surface.

A modern cyber exposure platform complements traditional vulnerability scanning with data sensors that provide continuous visibility into any asset, including cloud, applications, IoT, and OT. Essentially, this type of platform brings traditional VM into the modern era.

Cyber exposure transforms cybersecurity from identification of bugs and misconfigurations on networks and endpoints to live discovery of every asset type in any environment. It shows where assets are secure or exposed, and to what extent, and it prioritizes remediation based on the asset's business, vulnerability, and threat context.


TIP

It's impossible to deliver an effective cyber exposure platform without a solid foundation in VM. VM providers that have deep expertise in assets, networks, and vulnerabilities, and the raw vulnerability data itself, are best equipped to analyze and contextualize vulnerabilities. Without that foundation, providers are too far removed from the underlying technical issues to provide effective analysis, prioritization, and benchmarking.

Closing the Cyber Exposure Gap

The failure of legacy tools and point solutions designed for traditional IT environments means that most organizations can't see modern assets with existing tools, creating a massive gap in their ability to understand and accurately represent their cyber exposure. Organizations need a new way to gain the visibility and understanding required to close this gap across the entire attack surface.

The three fundamental requirements for closing the cyber exposure gap are

- Seeing all assets and exposures across your environment
- Understanding where to focus (operational and executive levels)
- Measuring effectiveness over time and versus industry peers

We discuss these requirements in detail in the following sections.

Seeing all assets and exposures across your environment

Many of today's breaches result from limited visibility because IT can't manage and protect what it can't see. As simple as it sounds, visibility remains a significant challenge for security teams in every industry. Legacy security tools and approaches can't detect and analyze the full set of assets across computing environments, including the following:

- Servers and network infrastructure
- Laptops
- Mobile devices
- Virtual machines
- Cloud instances
- Web applications
- Containers
- OT systems such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems
- IoT devices

Understanding where to focus

You can't fix everything, so it's essential to focus on what matters most and to address critical exposures as quickly as possible. Risk-based insight unites all the information available about an asset, its associated vulnerabilities and misconfigurations, and relevant threat context to clearly present and visualize the relative

level of exposure. This kind of exposure scoring helps security professionals prioritize remediation and provide clear guidance to their colleagues in IT operations, DevOps, and other functions on where to focus.

TIP

Read more about scoring and prioritizing cyber exposure in Chapter 7.

Measuring effectiveness over time and versus industry peers

Security leaders want to understand the organization's progress in addressing issues over time. They also seek insight on how different groups within the organization (by technology ownership, type of asset, or geography) are performing relative to one another in remediating security issues. Transparent reporting on effectiveness of groups can spur improvement of laggards through increased management attention.

To put that information in context, security leaders also want to benchmark their effectiveness against peer organizations. Understanding if an organization is in the top quartile or bottom quartile for speed of remediation can provide valuable context and urgency. It can also help with realistic goal setting.

This data and related visualizations are invaluable for enabling security managers and executives to report on their progress in business terms to senior management. Business-level reporting demonstrates the value of security investments to senior leadership and positions the chief information security officer (CISO) as a true business executive.

Key Capabilities of a Cyber Exposure Platform

In this section, we touch on the high-level capabilities that should be part of any cyber exposure platform.

TIP

See Chapter 9 for details on life-cycle services designed to ensure successful deployment of a cyber exposure platform.

You should consider a cyber exposure platform that covers both traditional and modern assets and provides clear guidance extracted from the avalanche of raw data.

A modern cyber exposure platform has the following key capabilities:

- **Unified view of exposure:** Nobody has time to evaluate, integrate, and manage multiple point solutions. You need a unified view that shows all assets and their associated vulnerabilities and misconfigurations.
- **Continuous discovery and assessment of all assets:** A cyber exposure platform should provide live discovery of all assets in all computing environments, accurately detect vulnerabilities, and then prioritize remediation based on risk (see Chapter 7) to help reduce your true cyber exposure.
- **Scalability and flexibility:** A cyber exposure platform should support the ebb and flow of activity to address rapidly evolving business requirements. Whether hosted in the cloud or on your premises, the solution should deliver visibility across all computing environments and scale to millions of assets to support large enterprises.

  
  TIP

  See Chapter 3 for more information about deployment flexibility.
- **Translation of technical data into business terms:** Asset, vulnerability, and threat data must be combined into something that stakeholders across the organization can consume and act on. For senior business executives, raw security data must be translated into meaningful metrics and contextualized to communicate the actual cyber risk for the business (see Chapter 7). Only then does the technology evolve from a security tool into a strategic solution.
- **Regulatory compliance support:** A cyber exposure platform helps simplify the reporting required to demonstrate compliance with industry regulations and organizational policies.

IN THIS CHAPTER

- Reviewing traditional vulnerability management tools and technologies
- Delving into the core capabilities of cyber exposure platforms
- Recognizing the benefits of cyber exposure platforms

Chapter 3
Evolving from Vulnerability Management to a Cyber Exposure Platform

As we discuss in Chapter 2, the cyber exposure discipline is an evolution of vulnerability management (VM) — the next phase, if you will, in VM's illustrious career of protecting the digital assets of public- and private-sector organizations. We love VM; we just need more. And so do you.

VM is being dramatically reshaped by four factors:

- A growing range of digital assets, extending beyond traditional IT to include mobile devices, Internet of Things (IoT) devices, cloud platforms, application containers, web applications, and operational technology (OT) systems.

  Industry pundits estimate that more than 9 billion IoT devices will be residing on enterprise wireless networks by 2019 — more than the entire smartphone and tablet markets combined.

REMEMBER

- Agile approaches and DevOps, which are accelerating software delivery and allowing application deployments to fly under the radar of IT security.
- The prevalent reuse of open-source software components, which are not always evaluated frequently for security flaws.
- The need to identify and address vulnerabilities in OT assets as cyber attacks against production systems increase in frequency and severity.

The modern attack surface is a complex mix of connected devices and computing platforms that's constantly expanding and contracting, much like a living organism. In this chapter, we begin by explaining why traditional VM tools alone can't tame this beast. Then we cover the core capabilities of a modern cyber exposure platform designed to build on VM and to deliver the full visibility and insight required to protect dynamic assets in the evolving threat environment.

Components and Challenges of Legacy Vulnerability Management

Traditional VM systems offer these features:

- Active, periodic vulnerability scanning and asset visibility
- Discovery and assessment of traditional IT assets
- Configuration auditing
- Customizable dashboards and reports
- Role-based access control
- Regulatory and policy compliance reporting
- Integration with complementary technologies (ticketing/workflow, patch management, credential management, network access control, and so on)

More advanced VM systems offer these features:

- Agent-based vulnerability assessment
- Continuous, passive (nonintrusive) network monitoring
- Public cloud pre-approved scanning

Legacy VM has a few drawbacks:

- **Reliance on active scanning technologies:** Active scanning tools are essential, but they capture only a single point in time, and they often miss devices that live off the corporate network such as remote employees' laptops and short-lived assets such as containers. The one-size-fits-all, scan-the-network approach designed for the world of static systems living on premises doesn't work for the modern amorphous attack surface. The dynamic nature of today's assets prevents security teams from getting an accurate view of their environment via traditional scanning methods alone.

  
  WARNING

  Active scanning tools should not be used on sensitive critical infrastructure, industrial systems, and medical devices that aren't designed to be scanned and could face disruption or outage if they're scanned.
- **Focus on traditional assets:** Legacy VM focuses on traditional IT assets such as network infrastructure, servers, and desktop PCs. These tools aren't designed to discover and assess modern assets such as cloud instances, containers, web applications, and IoT devices.
- **Lack of insight and prioritization:** Legacy VM provides great detail (perhaps too much!) on assets and their vulnerabilities. Unfortunately, it doesn't always provide tailored, actionable information with adequate context to allow IT to prioritize remediation efforts. Nor does it possess the analytics that IT security needs to easily evaluate and manage overall cyber risk.

THE 300-PAGE-REPORT SYNDROME

A classic characteristic of traditional VM that we're sure you'll agree must go is the monstrous vulnerability report being thrown over the wall from security to IT Ops. The next steps involve practitioners sorting through endless pages of vulnerabilities that attackers will never exploit, going on wild goose chases trying to find assets that don't exist or are duplicates, and cursing their colleagues at every turn. Are you tired yet? We are!

Capabilities of Cyber Exposure Platforms

In contrast with traditional VM systems, cyber exposure platforms are designed to continuously discover and assess traditional IT, cloud, IoT, and OT assets across an entire organization — and then further help you evaluate and prioritize issues, take appropriate corrective action, and measure and report on exposure in both technical and business terms. The following sections describe the core capabilities of these platforms.

Complete vulnerability assessment

The Discover and Assess phases of the cyber exposure life cycle (see Chapter 2) involve collecting data via a variety of scanning and monitoring techniques. In general, traditional vulnerability scans should be quick and easy to define. Setup should be intuitive and require a minimum of steps. Scan results should be displayed in flexible, customizable dashboards and reports for different audiences, and also be easily exportable via an open application programming interface (API).

The five main vulnerability assessment technologies are

- Network vulnerability scanner
- Web application scanner
- Agents
- Passive network monitoring
- Image registry

We discuss these technologies in detail in the following sections.

REMEMBER

There's no one-size-fits-all approach to asset discovery and vulnerability detection. Deploy all five types of data sensors to ensure comprehensive asset coverage across computing platforms. Make sure that your cyber exposure platform natively offers all sensors and doesn't charge you for each sensor deployed. An à la carte approach may work in a restaurant, but leads to unnecessarily high cost in this case.

Network vulnerability scanner

Active scanners have been around for a couple of decades and are quite mature. Serving the domain of traditional IT, active vulnerability scanners identify vulnerabilities, misconfigurations, and other security health issues in network infrastructure, servers, and PCs (including operating systems and applications).

Web application scanner

Web application scanners are similar to network vulnerability scanners, but instead of looking for specific known vulnerabilities in operating systems, applications, and related components, they focus only on web applications and look for certain *types* of vulnerabilities such as input validation errors that can lead to cross-site scripting attacks. Although web app scanners — also known as dynamic application security testing (DAST) solutions — can be used to assess commercial applications, they're particularly essential for testing an organization's custom-built applications because no outside party will ever identify those vulnerabilities for the organization.

Agents

Agents are installed directly on end-user devices or servers and are especially valuable for assessing assets that are not always on the network. Locally installed agent software should include all the capabilities required to discover vulnerabilities, audit configurations, and in some cases even detect malware running on the asset.

Nonintrusive and easy to install, agents are ideal for monitoring the security health of laptops and mobile devices and enabling accurate vulnerability reporting, even with devices constantly changing IP addresses.

Passive network monitoring

Passive monitoring sensors provide live asset discovery and monitoring to eliminate the blind spots created by periodic active

scanning. They also enable safe vulnerability detection for critical infrastructure such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that would be disrupted by traditional active scanning, aren't appropriate for agent deployment, and often can't be shut down for months or years at a time.

WARNING

Passive network monitoring is essential. If you don't scan sensitive systems because active scanning is your only option, you're widening your cyber exposure gap and leaving production assets at risk. You also can't know about everything in your environment if you rely only on point-in-time scans and agent monitoring. Doing so leaves critical blind spots.

Image registry

This approach integrates security into the software development life cycle by providing a registry (repository) that can house and scan images for assets such as containers and public cloud instances. The ability to test assets such as Docker containers and cloud images for security issues at the build stage, just like any other software quality check, is essential because it enables those issues to be addressed before deployment. It also provides confidence for increasing the use of open-source software components.

TIP

See Chapter 4 for more about securing containers during the build phase.

TECHNICAL STUFF

Security tests can be integrated into continuous integration/continuous deployment (CI/CD) systems via application programming interfaces to check for vulnerabilities and malware as part of quality assurance.

Comprehensive asset coverage

You need to know exactly what devices and resources are on your network at any time. Unified visibility and vulnerability assessment capabilities across traditional IT, cloud, IoT, and OT systems, no matter where they reside, empower you to manage cyber exposure across the entire attack surface.

REMEMBER

Broad asset coverage is a core cyber exposure capability that's required to discover all potential vulnerabilities. *Broad* means exhaustive coverage encompassing vulnerabilities across operating systems, applications, and other components — all Linux and UNIX variations, as well as Windows and Mac platforms, for example.

Asset tracking and elastic licensing

Historically, VM tools tracked vulnerabilities on assets by IP address, which worked well when IT assets were fixed. This approach is flawed now, because mobile assets such as laptops typically use multiple IP addresses over time. Instead, an advanced asset identification algorithm is required to track both static and dynamic assets for purposes of vulnerability reporting and remediation. Cyber exposure platforms offer this capability, which uses multiple attributes to track changes in assets, regardless of where they roam or how long they last, providing a more accurate, complete view of assets and vulnerabilities for effective remediation.

Why is this approach important? Suppose you're a security analyst, and you share vulnerability reports with IT Operations for remediation, but you don't know which vulnerabilities are duplicates. IT then looks for those assets based on IP address and finds that many of them don't exist anymore because they were duplicates. This process is a big waste of time. IT Ops is unhappy, and the security team loses credibility and goodwill.

The ability to track unique assets is also important for licensing because without it, you're paying for each IP address. IP-based licensing is the legacy VM approach and a poor fit for today's dynamic environments. Cyber exposure platforms offer asset-based licensing that accurately reflects the true environment, consuming one license unit per asset, even if the asset has multiple IP addresses.

Elastic licensing is another innovation that makes cyber exposure platforms a good fit for current environments. Assets with short life spans, such as containers and cloud instances, spin up to perform a function and may spin down as soon as minutes or hours later. An IP-based licensing model can't accommodate this reality; instead, it charges for each IP that it sees.

An elastic model automatically recovers licenses for short-lifespan assets and even permits scanning when license counts are temporarily exceeded. This enables one-time bursts without penalizing you through the typical hard license enforcement.

Advanced risk-based scoring and prioritization

The decision about what to fix and when to fix it has to be based on more than raw vulnerability results. A cyber exposure platform integrates and correlates asset, vulnerability, and threat data to provide an accurate, comprehensive view of the environment. Data science–driven analytics further allow you to precisely measure and analyze exposure, providing the insight you require to focus on what matters most.

Moving from a vulnerability-focused approach to an exposure-focused mind-set requires more continuous data, more complete context, and the algorithms to make sense of it all. There's little value in trying to prioritize remediation based solely on any one factor such as vulnerability severity. Risk-centric prioritization must reflect numerous factors, including an asset's function and business value and the likelihood of attack (the threat context). These factors differ from one organization and industry to another.

TIP

For more on scoring and prioritization, see Chapter 7.

Visualization of assets and exposure

The approaches used by many security solutions for presenting information are ineffective, making it difficult for users to see what matters most or grasp subtle trends and patterns. It's time to replace raw reports and poorly designed dashboards with an updated approach to visualization that reflects current best practices in user-centric design. A cyber exposure platform should provide modern visualizations that make it easy to understand and intuitively explore large sets of data, at any level of detail, and quickly identify "hot spots" and other elements of interest.

Deployment flexibility

Deployment flexibility is invaluable in a cyber exposure platform, which should serve customers effectively, either in its more common cloud-based form or as an on-premises software solution for organizations that require it.

WARNING

Solutions that only come as traditional on-premises software may not be able to serve all your asset discovery, vulnerability detection, and exposure scoring and benchmarking needs. At the same time, solutions that are cloud-based (Software as a Service [SaaS]) may not meet the needs of certain customers. If you're

seeking the ultimate in long-term flexibility, choose a platform that offers both options. And with any solution, understand which capabilities are delivered as traditional software and which are cloud-based.

Reaping the Benefits of Cyber Exposure Platforms

The benefits of a full-featured cyber exposure platform are both numerous and compelling. Here are just a few of the main benefits:

- **Eliminating blind spots:** A robust platform gives you comprehensive visibility across all assets, including traditional IT, laptops and mobile devices, cloud instances, containers, web applications, and OT systems. You can see everything across all computing environments via one platform.
- **Prioritizing what matters most:** Complete asset and vulnerability information is foundational; adding business and threat context facilitates effective prioritization. A cyber exposure platform analyzes all of these inputs and provides a clear view of your risk-based exposure. This allows you to optimize remediation efforts by illuminating what matters most.
- **Supporting closed-loop remediation:** A cyber exposure platform integrates seamlessly with other security and IT operations technologies and enables you to collaborate with colleagues to execute the appropriate remediation action for each issue. With the ability to validate reported remediations, the platform can track remediation progress and help ensure issues are resolved.
- **Understanding and communicating cyber exposure:** The cyber exposure discipline enables business-focused conversations about cyber risk. A cyber exposure platform helps you translate vulnerability data into metrics that are meaningful even to stakeholders who lack security expertise.

TIP

For more on effective stakeholder communications via cyber exposure, see Chapter 7.

IN THIS CHAPTER

- Securing DevOps
- Securing applications during development
- Working with containers
- Keeping assets secure during production

Chapter 4
Securing Applications at the Speed of DevOps

Adoption of public cloud environments and the mainstreaming of DevOps continue to accelerate digital innovation. At the same time, these advancements are creating major disruptions in security, given their significant contribution to the cyber exposure gap. Business requirements for secure, rapid, and efficient delivery of applications are driving fundamental changes in the ways that organizations approach cybersecurity.

As you shift your perspective to today's expanded attack surface, it makes sense to think about incorporating security into the software development life cycle (SDLC).

In this chapter, we talk about reducing costs, eliminating blind spots, and enabling rapid development and deployment by integrating security into the DevOps process.

Adding Security to DevOps

DevOps accelerates development through a collaborative philosophy that knocks down the walls between development and

operations. DevOps is about speed and streamlining software delivery processes. Unfortunately, security is often an afterthought.

WARNING

Developers avoid anything and anyone who looks capable of road-blocking innovation or clogging the software build pipeline. Don't make DevOps call the plumber, and don't ask developers to become security experts.

Industry estimates suggest that by 2021, DevSecOps practices will be embedded in 80 percent of rapid-development teams, up from 15 percent in 2017.

Shifting security left

Information security leaders must adopt a new mind-set, build new relationships internally, and find innovative ways to implement security while enabling fast-moving DevOps environments. One way is to integrate vulnerability and malware detection into software build workflows in the development stage rather than waiting until those assets are deployed in production (see Figure 4-1). Finding and fixing vulnerabilities before they're exploitable reduces your cyber exposure gap and prevents what could become a blind spot if those assets spin up and down frequently.

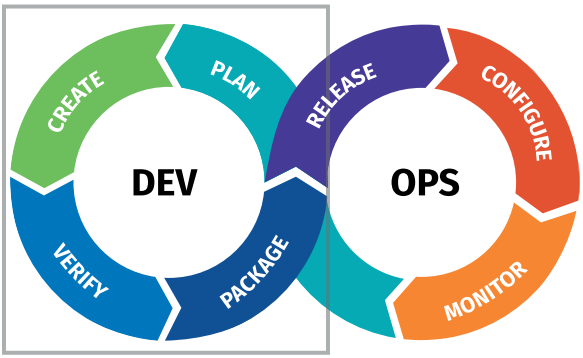

FIGURE 4-1: Shifting security left in the DevOps process.

Wiring security into the build phase of the DevOps pipeline alongside other quality validation tests enables you to easily detect issues during development and ideally prevent deployment of vulnerable applications.

TECHNICAL STUFF

The continuous integration/continuous deployment (CI/CD) pipeline spans the entire SDLC. Developers use CI, focused on development, to collaboratively validate and continuously test new code. CD, focused on operations, enables automatic release of code changes into production without human intervention.

REMEMBER

When we talk about security during the build phase, we're referring to automated tests of images, not conventional scans of running assets, which don't work in this context and have negative connotations (such as being slow and manual) for DevOps. Security testing has to be automatic and lightning fast — less than a minute — so that it doesn't inhibit DevOps.

Addressing issues early reduces costs

Incorporating security into the DevOps process helps prevent issues before production — which is important because it costs a lot more money to fix broken things after deployment. The only way to ensure security throughout the life cycle is to identify and address vulnerabilities and misconfigurations during the build phase.

After deployment, it's more difficult to identify application owners and more time-consuming to change code. Incorporating security earlier in the SDLC, as new applications and services are being created, is a fundamental change for security teams, but a good one.

Engaging security early in the DevOps process is not only smart but also a lot cheaper. The cost of addressing a problem during the maintenance phase, for example, is estimated to be 100 times the cost of addressing that same issue during the design phase (see Figure 4-2).

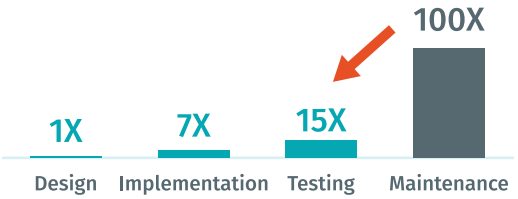

FIGURE 4-2: Fixing defects early in the SDLC reduces costs.

REMEMBER

The integration of security into DevOps needs to be automated, seamless, and transparent to support the high-velocity philosophy of DevOps. Automation translates into precise alignment with proven specifications, less human error, and minimal possibility of delay before production. Information security must enable developers' productivity and adapt to DevOps tools and processes. In a DevOps world, security practitioners can't expect developers to adjust to their ways of operating.

Safeguarding Vulnerable Applications in DevOps

Maintaining application security is hard. Nearly all applications have at least one vulnerability, and most have several. More important, the average time it takes to remediate critical vulnerabilities is four months.

WARNING

Most organizations focus on protecting mission-critical applications such as transactional systems and e-commerce sites, but these apps represent less than 10 percent of the attack surface. Other applications make up the other 90 percent of the portfolio, yet relatively few resources are dedicated to securing them because they're viewed as being lower-priority.

Modern software is composed mostly of publicly available open-source components and a little custom code. You can scan your source code to determine which open-source elements are in your applications and fix vulnerabilities early in the development cycle, before applications are assembled.

Scanning web applications

Many data breaches start through exploits of web applications, which makes them a top priority for information technology (IT) security teams. Web applications are updated frequently, challenging security teams to keep up with the DevOps pace. When you realize that organizations typically have one application security employee for every hundred developers, you understand why securing web applications is a monumental challenge.

A modern cyber exposure platform includes web application scanning as part of a comprehensive approach to identifying and managing cyber risk across assets in all computing environments.

You can secure your web applications without disruption via fast, automated, high-accuracy scans. In fact, nearly all web application scanning can be automated. Manual security tests are reserved for only the most complex, high-value applications such as banking websites.

Detailed scan results should include vulnerabilities categorized by type and severity, plus specific guidance on remediation. At a minimum, scan both internal and external web applications for the top ten vulnerabilities designated by the Open Web Application Security Project (`www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf`).

TIP

Expertise in application security testing is a scarce commodity, so the more you can automate the process, the greater your effectiveness and team productivity will be.

Avoiding the "perfect security" trap

Perfect security and zero cyber risk aren't possible with web applications (or any asset type). Don't waste valuable time chasing down every last vulnerability. Instead, focus on the vulnerabilities that create the most actual cyber exposure (risk) for your organization. Use new security tools and approaches that minimize friction for developers and that don't inhibit DevOps innovation, speed, and agility.

Continuous vulnerability assessment in the software development process should prioritize remediation based on risk-centric quantification of exposure. As with other types of assets, this prioritization must reflect asset, vulnerability, and threat context.

Understanding Containers

Sometimes described as the next generation of virtualization, *containers* are portable, lightweight, self-contained software packages that house everything required to run an application: dependencies, libraries, binaries, and configuration files. Because containers can be deployed and run the same way in different environments, they give developers confidence to write an application once, package it, and deploy it anywhere without failure.

REMEMBER

Container images are built by developers, stored in a registry, and used to generate running containers in production.

The container market is the fastest-growing cloud-enabled technology, expected to grow 40 percent annually from 2016 to 2020 to reach $2.7 billion, according to 451 Research. To date, Docker Hub has more than 900 million applications, and more than 29 billion Docker containers have been downloaded.

Containers are popular for good reason. All the elements that comprise an efficient, dynamic application are distilled into one immutable object — a container — that's designed to serve a single purpose and then be discarded or replaced.

Seeing the good and bad in containers

Containers allow developers to build and launch new services and applications quickly and easily. More web applications run in containers as part of the cloud-native environment.

The downside of containers is that they represent a blind spot for most security teams. Short life spans, lack of IP addressability, and sheer volume and variety make securing containers a formidable challenge, and traditional vulnerability management (VM) processes and solutions don't work for containerized applications.

WARNING

Many developers rely on code in the Docker Hub registry and other potentially vulnerable open-source software to assemble (versus code from scratch) container images as part of a software supply chain. Yet a shared image in Docker Hub contains more than 40 vulnerabilities, on average.

Securing containers in the build phase

An effective approach integrates security into the container build process to do all of the following:

- Identify, assess, and remediate vulnerabilities.
- Detect malware in code.
- Enforce policies before container deployment.

Automatic testing of container images helps ensure protection against a wide range of threats.

Preproduction visibility into container images during development helps secure the code being produced by DevOps processes and reduce cyber exposure. Knowing what's inside every container before it's pushed to production is critical. A comprehensive cyber exposure platform with complete asset coverage eliminates container blind spots without slowing application development.

Protecting Assets in Production

Secure service delivery starts during development, but long-running containers might evolve over time, creating the need for runtime container security as well. Automated scanning capabilities are required to assess containers in production, providing full coverage from development through operation.


TIP

Dynamic application security testing solutions help secure running applications in the deployment phase of the SDLC (versus static images during development).

Securing containers in production is quite different from traditional VM. Legacy VM tools can't even see containers, let alone address vulnerabilities. And in many cases, patch management doesn't apply. If you find a vulnerability in a production container, you might fix the issue directly in the container image and then deploy a new secure container in place of the old one.

Containers are designed to be *immutable* — unchanged throughout operation. If their immutability holds true, there is some assurance that deployed containers are as secure as when they were first tested during development. However, you should monitor running containers rather than assume immutability, and receive alerts if containers change during operation.

Scan running containers to gain visibility into image changes, vulnerabilities, and other information. Runtime assessment helps you understand the full cyber exposure of containers and extends your security controls from development through production.

IN THIS CHAPTER

- Exploring the challenges of the cloud
- Using cyber exposure principles for cloud assets

Chapter 5
Boosting Cloud Visibility and Security

A significant majority of organizations now run services in public cloud environments, with many using the cloud for web, analytics, and content management workloads. At the same time, most security teams still have limited visibility into what their business units deploy and consume beyond the four walls of the data center.

Cloud security concerns remain barriers to adoption. These concerns are primarily related to data security, privacy, and regulatory compliance. Organizations must continually analyze and understand the scope of their cloud services, including what security weaknesses exist and what data is being accessed, and maintain continuous assessment practices to prevent a breach or regulatory violation.

In this chapter, we explore cybersecurity challenges in the cloud environment and discuss effective ways to discover and assess cloud-based assets.

Recognizing the Challenges of the Cloud Environment

Public cloud solutions, including Infrastructure as a Service (IaaS), have become extremely popular, with Amazon Web Services (AWS), Microsoft, and Google being among the leading providers. All cloud environments have unique challenges that information technology (IT) security must address. We discuss some of these challenges — visibility, policy and regulatory compliance, and shared responsibility — in the following sections.

Visibility

Visibility into cloud infrastructure is the number-one headache for security teams. IaaS cloud instances often come and go quickly, so it's easy for periodic active scans to miss them. Also, because instances can be deployed by anyone, IT is no longer in charge. Further, configuration management databases (CMDBs) that track details about digital assets and their relationships are a poor fit for the volume and pace of change of dynamic cloud environments.

Policy and regulatory compliance

As organizations migrate to the cloud, compliance becomes more difficult in terms of adhering to specific regulations and corporate policies. Because employees are able to deploy cloud instances without IT approval (or even awareness), much greater opportunity exists for noncompliant cloud assets to be deployed and run for extended periods before being discovered by IT security.

Shared responsibility

Securing cloud assets is a shared responsibility of the customer and the cloud provider. In a shared-responsibility model, the cloud provider is responsible for the physical security of the cloud environment and the cybersecurity of the shared digital infrastructure, and the customer is responsible for the security and compliance of its workloads and data in the cloud, which includes identifying and remediating vulnerabilities.

Applying Cyber Exposure Discipline to the Cloud

If your organization is using public cloud services, your security team must be able to answer these questions:

- How quickly can we discover workloads running in the cloud, and how effectively can we assess their security health?
- What vulnerabilities and configuration issues are present in our cloud assets, and how should we prioritize remediation relative to all other issues across the organization?
- Are our cloud instances in compliance with corporate polices and external regulations?

As in other areas of information security, a lack of staff resources, expertise in cloud security, and well-designed and integrated technology solutions impede responsible cloud adoption. The solution involves additional staff training, automation, and especially new approaches that make it easier to secure cloud assets without adding point solutions.

Automating asset discovery

Traditional security tools aren't designed for the cloud. Dynamic cloud assets behave very differently from legacy IT assets, contributing to the growing cyber exposure gap. New capabilities and approaches — including functionality specific to individual cloud platforms — are required to protect digital resources in this fast-changing computing environment. You need accurate visibility and insight to effectively manage security and compliance in evolving cloud environments.

Automation enables you to identify production assets and assess vulnerabilities and misconfigurations at cloud speed. This complements the identification of weaknesses at the image stage, providing a complete approach.

Asset discovery and tracking can be performed automatically via cloud platform application programming interfaces (APIs), enabling timely vulnerability and configuration assessment, and reducing manual work. This provides security professionals with live, continuous visibility into an otherwise opaque environment.

Gaining unified visibility

The goal is to achieve centralized visibility across assets and computing environments, which is finally possible through a comprehensive cyber exposure platform.

Here are some things that a cyber exposure platform should perform to secure public cloud assets:

- Automatically identify new assets in cloud environments via API-driven connectors and assess those assets for vulnerabilities, compliance issues, and malware.
- Assess the configurations of cloud instances, using active scanners or agents.
- Integrate security into the development process (see Chapter 4) to gain early visibility into security flaws, prevent them from reaching production, and enable developers to remediate those flaws just as they'd address other quality issues.

SECURING AMAZON WEB SERVICES

AWS CloudTrail is a service that records activity in AWS accounts, including details on new and retired AWS instances. You can use this information to automatically and continuously track asset changes in AWS and pull the information into your cyber exposure platform. This way, you ensure that cloud workloads are seen, assessed, and consistently reported alongside other types of assets, solving the key challenge of achieving accurate visibility into cyber risk in cloud environments.

Additionally, you want to harden configurations based on industry best-practice guidance, such as the Center for Internet Security's Amazon Web Services Foundations benchmark (`https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf`).

The risk around this is becoming better recognized, as several compromises of AWS instances occurred in 2017 due to misconfigurations. In fact, a recent study found that 73 percent of companies using AWS have at least one critical AWS security misconfiguration, such as remote Secure Shell (SSH) open to the entire Internet.

IN THIS CHAPTER

- Getting a unified view of information technology and operational technology assets
- Protecting critical industrial control systems and supervisory control and data acquisition infrastructure
- Safeguarding plant operations

Chapter 6
Unifying Information Technology and Operational Technology Security

Organizations with industrial systems have historically managed security with different approaches for information technology (IT) and operational technology (OT). IT and OT are converging, however, creating both challenges and opportunities related to visibility and remediation of vulnerabilities. The increasing connectedness of IT and OT is forcing two very different worlds to examine opportunities for collaboration and improvement.

There's always a balancing act between flexibility and security — a tradeoff between increased operational efficiency and greater control. Energy (oil and gas), utilities, and manufacturing companies that rely on OT systems to automate and control plant processes must understand cyber exposure in the context of an evolving attack surface and threat landscape.

The increased prevalence of interconnected IT and OT systems has made production networks vulnerable to cyber attacks that threaten major disruptions of critical infrastructure. Defenses aren't keeping pace with network connectivity in this sector, and the failure to accurately understand security weaknesses is contributing to a growing cyber exposure gap (see Chapter 2).

In this chapter, we explore some of the challenges associated with asset discovery and vulnerability management (VM) in industrial environments.

Protecting Operational Technology Systems

For many organizations with production assets, a major security challenge is simply knowing what systems are in place across various operating environments. Plant managers and engineers aren't always aware of all the assets on their networks.

Protecting OT begins with building and maintaining a comprehensive inventory of networked assets. Only then can you proceed to the next step: acquiring visibility into the security status of these assets.

REMEMBER

Threats can affect both OT and Internet of Things (IoT) systems in organizations outside the industrial sector. Nearly every organization maintains heating, ventilation, and air conditioning (HVAC) systems, for example. If these enterprise IoT systems are part of a networked environment, they're part of the modern attack surface.

Achieving a Unified View

IT and OT represent two distinct, unique environments. IT security (which is chiefly concerned with the confidentiality, integrity, and availability of data) has a much different focus from OT security (which prioritizes safety, uptime, efficiency, and productivity).

Approaches used to discover assets and detect vulnerabilities in traditional IT environments don't necessarily work in OT environments. Conventional active scans, for example, can adversely affect OT systems and even knock them offline because those systems simply weren't designed to withstand such probing. As a result, traditional active scans can't be performed on sensitive industrial systems. If an electrical distribution network is disrupted, it can have major consequences for millions of people. Asset criticality and sensitivity put industrial systems in a separate category when it comes to security measures.

It's no wonder that security practitioners in industrial environments don't want active scanners anywhere near their plants. These ubiquitous IT security tools are deemed too risky. Instead, these critical infrastructure networks require nonintrusive *passive monitoring* — deep packet inspection of network traffic to fingerprint assets and identify vulnerabilities without disrupting operations.

TIP

See Chapter 3 for a review of the scanning technologies best suited for various environments.

Frequently, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems directly or indirectly interact with IT networks. In other words, OT systems are now part of the broader networked environment. Additionally, on nearly every OT network, you'll find lots of supporting IT devices, such as Windows servers and workstations. And in attacks against OT devices (such as programmable logic controllers), initial penetration often occurs through the IT network.

You can't limit your security concerns and initiatives either to IT or OT and ignore the other side of your enterprise. But seeing everything isn't easy because IT typically has little visibility into OT networks.

WARNING

Bad actors need only one exploitable hole for entry. If they're attacking OT systems, they don't care whether they enter via the IT or OT side. The more gaps, the better. They follow the path of least resistance to achieve their objectives.

As we discuss in Chapter 3, a cyber exposure solution that features complementary active and passive data collection sensors ensures full visibility across IT and OT assets.

INTEGRATING INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY PERSPECTIVES

Interconnected IT and OT systems force organizations to address increased cyber exposure in their production environments. Cross-functional teams of information security and plant/operations engineers should collaborate to understand their cyber exposure and proactively protect operational performance.

Security goals differ between IT and OT:

- IT focuses on data confidentiality, data integrity, and data access and availability. If a hack occurs, systems and business operations are shut down to protect critical data.
- The OT risk model focuses less on data and more on safety, uptime, efficiency, and productivity. If an attack occurs, management is concerned about avoiding operational interruption.

Securing Industrial Control Systems and Supervisory Control and Data Acquisition Systems

ICS and SCADA networks are designed for continuous, reliable operation. They're meant to be walled off from the IT network and isolated from threats, so robust security generally hasn't been built into these systems. Traffic may not be encrypted, and login passwords may not be required. But as organizations embrace increased connectivity of assets, industrial systems become more accessible — and, thus, create increased risk.

Passive monitoring of OT assets is required to discover and address vulnerabilities before they're exploited (and potentially disrupt essential public services, such as electricity). A cyber exposure platform must provide passive analysis of network traffic for continuous discovery of OT assets and vulnerability identification on critical ICS and SCADA systems.

WEIGHING RISK AS CONTEXT CHANGES

In industrial environments, security focuses on developing a complete understanding of risks, evaluating remediation options, and determining what level of risk to accept in different areas of production. Here are two examples that illustrate the industrial security perspective:

- An HMI computer in your OT environment has several critical vulnerabilities. However, firewall rules prevent it from communicating with the Internet. Therefore, patching the vulnerabilities is not an issue unless Internet access is added.
- Some of your older OT assets can be accessed with default credentials. Now these systems can be remotely accessed by service technicians, causing you to replace the default credentials with unique, strong credentials for each user who can access the assets.

Likewise, vulnerability remediation practices aren't as straightforward in industrial environments. Patches may not be available from the vendor, or the vendor may be required to apply the patch on-site, creating delays. Also, you may have to take a system offline temporarily to apply a patch — rarely an option for critical infrastructure, which may shut down briefly for patching only once or twice a year.

REMEMBER

There's such a thing as a noncritical SCADA network, by the way. A big retailer may deploy these systems in its distribution center, but because they aren't critical infrastructure, they can be taken out of service temporarily for active scanning.

Extending Security to Plant Operations with Capabilities Designed for OT

Relying on a modern cyber exposure platform to visualize and understand the state of OT assets at all times gives plant managers and compliance professionals the information they need to manage and reduce cyber risk. As a result, they can achieve the delicate balance between flexibility and security that we mention at the beginning of the chapter.

Here's a scenario that demonstrates the benefits of such an approach: Suppose that you're a plant engineer assigned to complete an asset inventory. How much time would it take you to walk around a 40,000-square-foot plant to check the status of every machine that's active on the network versus the time it would it take to pull up the same data on a laptop?

Significant risk reduction, as well as cost and efficiency benefits, are associated with managing IT and OT security with a single solution — as long as it effectively serves the needs of OT and doesn't force use of solutions that are ill-suited for the production environment. It's critical to remember that the increased connectivity of production systems contributes to an expanding attack surface, and the resulting risk requires serious attention.

IN THIS CHAPTER

- Measuring and reporting cyber exposure
- Calculating your organization's exposure score
- Understanding how to reduce cyber exposure

Chapter 7
Measuring and Prioritizing Cyber Exposure

Security teams must understand where cyber exposure is most concentrated across the business and how to best reduce it. Visibility is important, but without context-driven analysis and prioritization that tells information technology (IT) what to focus on, it's useless. Organizations need an objective way to quantify cyber risk and help stakeholders make smarter decisions. Cyber exposure helps prioritize remediation at the operational level and guide broader decision making at the strategic level.

In this chapter, we explore how advanced approaches enable you to measure, benchmark, and communicate cyber exposure.

Measuring Cyber Exposure

The discipline of cyber exposure empowers organizations to transform static, fragmented views into live, unified visibility. Raw technical data is translated into meaningful business metrics, which management can track alongside other key risk metrics.

Ingesting and correlating data

A cyber exposure platform integrates and analyzes asset, vulnerability, and threat data to provide the clear insight that security and IT operations teams need for remediation.

To gain a true understanding of your cyber exposure, you need to synthesize information from multiple vendors. A comprehensive cyber exposure platform imports asset, vulnerability, and threat data from other vendors as needed and integrates that with its own data to provide a continuous, comprehensive view of the modern attack surface.

WARNING

When evaluating cyber exposure solutions, choose a vendor that natively provides both vulnerability assessment and advanced analytics. Otherwise, you'll be forced to purchase, integrate, and manage multiple solutions from different providers. You'll also miss out on capabilities that can be delivered only by a solution that integrates vulnerability assessment and exposure analysis.

TECHNICAL STUFF

In addition to importing data from third parties into the platform, cyber exposure findings can be exported to partner solutions that perform downstream activities such as IT service management (ticketing/workflow); remediation (patch management and network access control); asset management (such as a configuration management database [CMDB]); threat analysis (such as security information and event management [SIEM]); and governance, risk management, and compliance (GRC).

Employing data analytics

To truly minimize cyber risk, you need to make smart business decisions, which means leveraging all available data. Advanced algorithms can analyze numerous inputs to provide a meaningful measure of cyber exposure (risk) for your organization.

In the Analyze phase of the cyber exposure life cycle (see Chapter 2), analytics adds business and threat context to vulnerability data. As a result, security personnel can identify exposure hot spots and prioritize actions based on a true view of risk, not one-dimensional vulnerability data. In the subsequent Fix stage, the security team selects the right remediation technique for

each issue, leverages integrations with complementary solutions, and collaborates with other departments to achieve closed-loop resolution.

Intelligent analysis of asset, vulnerability, and threat data translates raw information into prioritized issues and provides a meaningful view of exposure across the organization. To get there, your cyber exposure solution should normalize and analyze all the vulnerability data that it collects natively and imports from other solutions so that you can confidently answer the following three questions:

- Where are we exposed?
- Where should we prioritize based on risk?
- How are we reducing our exposure over time?

Calculating Exposure Scores

Large organizations own thousands or even millions of assets, each of which may be prone to countless vulnerabilities. Security teams are inundated with vulnerability results but often don't know where to focus their efforts. In the end, security professionals may prioritize their remediation efforts based on imperfect out-of-the-box indicators from a VM solution or custom scoring managed manually outside the VM solution.

Exposure analysis translates raw security data into actionable information and visualization that delivers insight at both the operational and strategic levels. It helps the security, IT, and DevOps teams focus scarce resources on the most important vulnerabilities and weaknesses while giving management the visibility and understanding needed to improve the organization's overall security posture over time.

Vulnerabilities don't generate equal risk. One key factor in prioritization is exploitability, which reflects the kind of access needed to exploit the vulnerability, the existence of exploit code that can leverage the vulnerability, and other factors. Another critical

factor is the potential effect of a successful attack. The impact of an attack on a low-value asset would be quite different from that of an attack on an asset that contains mission-critical data or provides an essential service.

Quantitative exposure scoring helps you confidently prioritize your remediation activities. A modern cyber exposure platform calculates scores based on factors such as the following:

- Vulnerability severity and exploitability.
- Threat context such as prevalence of a vulnerability (or similar vulnerabilities) being exploited in the wild.
- Asset and business context. (For example, a test server containing no sensitive data that resides on a segregated part of the network may be less critical than an external-facing server supporting an e-commerce website. Prioritize mission-critical systems, valuable data, and assets governed by compliance regulations.)

Individual asset scores can be rolled up by geographic location, organizational entity, or asset type, for example, to calculate overall exposure scores. You can use such scores to track hot spots and trends in cyber exposure.

REMEMBER

A small number of vulnerabilities account for the vast majority of actual exploits. In fact, only about 13 percent of all vulnerabilities are exploited, according to industry estimates.

As part of your shift from an approach that focuses on vulnerabilities to one that focuses on exposure (risk), it's important to understand which vulnerabilities currently being exploited by hackers pose the greatest risk to your most critical assets — in other words, which exposures are most important to your organization.

Advanced exposure scoring weighs these vulnerabilities and contextual information, providing clear guidance about what to focus on while giving you the flexibility to tune the scoring as you like.

BENCHMARKING EFFECTIVENESS AGAINST PEERS

Comparing your organization's cyber exposure with that of your peers provides a broader perspective that helps you understand your effectiveness, demonstrate progress to senior management, and decide where to focus future cybersecurity investments.

Benchmarking is about more than raw numbers — how many vulnerabilities you have compared with other organizations, for example, or how significant those vulnerabilities are. It's also about process maturity — for example, how long it takes your organization to remediate critical vulnerabilities versus the industry average, and how your peers are responding to new vulnerabilities.

Comparing your security posture with that of peers provides insights you can't get any other way and identifies improvement opportunities that help you objectively mature your security program.

Communicating Cyber Exposure

Most of your stakeholders — from the finance department to senior management and the board of directors — lack the cybersecurity expertise (and interest) required to make sense of technical security data. They're business professionals who need to make decisions based on understandable business metrics.

Security teams must translate technical data into digestible information that summarizes the cyber risks affecting the organization. Doing so facilitates meaningful discussion, rigorous problem solving, and risk-informed decision making on tactical and strategic questions. It also positions the IT security leader as a business leader rather than a technologist, giving him or her greater credibility and a seat at the table when more-significant decisions are made.

REMEMBER

Good communication is even more critical in light of the cybersecurity talent shortage, which is estimated to reach 6 million openings worldwide by 2020. Because not enough people are available to analyze all the data, security solutions must be more intuitive and intelligent, with powerful analytics and decision-support capabilities.

Visualizing cyber exposure

Shifting your focus from VM to cyber exposure promises much greater insight, but to realize that potential, you need powerful visualization capabilities to see all assets and explore the global exposure. A modern user experience can present massive sets of disparate data in intuitive ways that invite exploration. Hot spots can be highlighted for immediate action. Assets can be categorized by location, business function, and type, offering lots of possibilities for asking and answering questions.

New tools and technologies for visualizing cyber exposure allow you to see your environment in a new way. Cyber exposure platforms can deliver the latest advances in user experience design and data visualization. Think videogames and virtual reality rather than spreadsheets. Old-school reports are being augmented by easy-to-navigate visual views of exposure, informed by different lenses that allow you to truly understand your cyber risk.

Modern visualization delivers simple ways of viewing and interacting with vulnerability and configuration data.

Reporting cyber exposure

Vulnerability management products can produce reams of data, leading to poor prioritization, little understanding of risk, and friction between IT security and operations teams.

A cyber exposure platform, however, can correlate and distill this data into meaningful results displayed in user-friendly dashboards and modern visualizations, providing relevant views of your assets and exposure.

Customizable dashboards reflecting business context provide different views for different groups of stakeholders (see the nearby sidebar "What stakeholders want to know about cyber exposure").

With these capabilities, security teams can provide tailored, actionable information to all parties, including the following:

- Chief information security officer, senior executives, and board members
- Risk management and compliance professionals

- Information security managers/directors and analysts
- Line-of-business managers
- IT operations professionals
- DevOps teams
- Operational technology (OT) plant managers, engineers, and compliance professionals

WHAT STAKEHOLDERS WANT TO KNOW ABOUT CYBER EXPOSURE

Stakeholders across the organization, many of whom lack cybersecurity expertise, have different interests and needs when it comes to cyber exposure. Therefore, technical data must be translated into relevant business terms for these stakeholders:

- **Chief information security officers** don't care about the minutiae in vulnerability reports or technical data. They want to understand the big picture, benchmark their organization against peers, and quantify which parts of the organization are generating the most cyber risk. They want to demonstrate progress in reducing exposure over time and versus peers, which helps them foster risk-based discussions and decision making, justify security investments, and position themselves as business leaders.
- **Senior executives and board members** want visibility into the degree and sources of cyber exposure, as well as relevant information to support risk/benefit discussions. They want to understand how the organization stacks up against its peers and competitors.
- **Information security managers and directors** want to reduce cyber risk across the attack surface. They want to see exposure broken down by geographical location, business unit, and other dimensions and to drill down into hot spots. They also need support for cross-functional workflows that drive closed-loop remediation. Comparing performance of organizational units can also help colleagues up their game to the level of high-performing departments.

(continued)

(continued)

- **Line-of-business managers** need to know the cyber risk considerations of various IT and business decisions — information previously not presented in useful form.
- **OT managers and engineers** want to identify and understand vulnerabilities in production systems that could lead to compromise and downtime. They also need to maintain regulatory compliance.
- **Information security analysts and IT operations professionals** are interested in exposure scores and prioritization of vulnerabilities and misconfigurations. They need to know what to focus on to secure the overall attack surface.

A cyber exposure platform should support all these stakeholders and use cases. Security teams must communicate cyber risk in business terms and provide insight that all stakeholders can use to make better business decisions.

IN THIS CHAPTER

- Using cyber exposure solutions with existing security infrastructure
- Integrating third-party solutions with a cyber exposure platform

Chapter 8
Integrating Cyber Exposure with Existing Infrastructure

In today's complex, dynamic threat environment, you need to combine the best cyber defense solutions to stay a step ahead of malicious actors. All the components of your arsenal must fit together seamlessly to thwart sophisticated cyber attacks and leverage the limited time and resources of your team.

A comprehensive cyber exposure platform is the foundation of a modern defense strategy. You must be able to see all types of assets and vulnerabilities across multiple computing environments to rapidly identify and remediate the most critical weaknesses.

In this chapter, we identify complementary technologies that can be integrated with your cyber exposure platform.

First, however, we need to discuss the building blocks that make these integrations possible: *application programming interfaces* (APIs) and *software development kits* (SDKs). An API is essentially a means through which disparate applications can exchange information (such as vulnerabilities detected) and/or issue commands (such as triggering a vulnerability scan). An SDK typically builds on an API and makes it even easier to build full-fledged integrations.


TIP

Leverage native APIs and SDKs to seamlessly integrate the applications that address your business requirements. Enrich your infrastructure by building custom capabilities to support your workflows.

Public Cloud Platforms

Running services in the cloud enables organizations to increase agility, accelerate time to market, and reduce costs, but cloud computing presents unique cybersecurity and regulatory compliance challenges.

Leading cyber exposure solution providers offer purpose-built software designed for scanning public cloud infrastructure — preferably from the inside. The software scans hosts in the cloud and then exports scan data to a management console for centralized analysis and reporting.

Sample vendors include Amazon Web Services (AWS), Microsoft, and Google.

Configuration Management Databases

A configuration management database (CMDB) acts as a data repository that documents IT installations. It holds relevant information about the IT assets that comprise your infrastructure, as well as descriptions of the relationships among these assets. The CMDB is meant to track all configuration items within the environment and any changes made to them.


TIP

A CMDB gives you rich visibility to manage and understand your traditional information technology (IT) assets, providing essential input to cyber exposure solutions.

Sample vendors include ServiceNow, BMC, and Micro Focus.

Network Access Control

Network access control (NAC) technology detects and quarantines endpoint devices that don't comply with company

security policies, including mandated patches, current antivirus signatures, and the use of personal firewalls. Many NAC solutions trigger scans via cyber exposure solutions to document compliance with company security standards.

Sample vendors include ForeScout, Aruba Networks, and Cisco.

Mobile Device Management

Cyber exposure solutions can be integrated with mobile device management solutions to monitor mobile devices and detect vulnerabilities, misconfigurations, and compliance issues in mobile operating systems and applications. This approach allows you to

- Identify iOS, Android, and Windows mobile devices accessing the company network.
- Detect known mobile vulnerabilities, including out-of-date operating system versions.
- See detailed device information.
- Discover unauthorized and jailbroken iOS devices.

Sample vendors include Apple, Citrix, Good, Microsoft, MobileIron, and VMware.

Privileged Access Management

Privileged access management (PAM) solutions enable IT to carefully control and monitor access to computing assets by authorized (privileged) IT personnel. This type of solution helps organizations reduce the risk of unauthorized system access by external threat actors and malicious insiders such as disgruntled employees and dishonest contractors.

Modern PAM solutions do the following:

- Provide single sign-on and support for multifactor authentication.
- Manage passwords and other credentials for administrative, service, and application accounts.

- Monitor, record, and audit commands and actions of privileged users.
- Granularly delegate and control access permissions for privileged users.

Sample vendors include BeyondTrust, CyberArk, Lieberman Software, and Thycotic.

Security Information and Event Management Systems

A security information and event management (SIEM) system is a sophisticated solution for monitoring IT and security events across an organization to detect and prioritize threats. Identified vulnerabilities and configuration issues from the cyber exposure platform can be automatically fed into a SIEM to help prioritize potential threats, based on understanding which assets are vulnerable to which types of attacks.

Sample vendors include IBM, LogRhythm, McAfee, Micro Focus, and Splunk.

Governance, Risk Management, and Compliance

An IT governance, risk management, and compliance (GRC) system is an essential element of many information security programs. Vulnerability assessment and configuration compliance data can be provided to the GRC solution and combined with additional controls data to provide a consolidated view of IT risk.

GRC can help you align IT activities with business goals, manage risk effectively, and stay on top of compliance.

Sample vendors include LockPath, RiskVision, and RSA.

Information Technology Service Management

IT service management (ITSM) is a set of policies, procedures, and frameworks for managing IT services. At the core of an ITSM software suite are a workflow management system and a CMDB for discovering and mapping configuration items and their dependencies.

Bringing these technologies together links assets and vulnerability remediation service requests, making it easier to accelerate remediation. By integrating with these solutions, the cyber exposure platform makes it easier for security and IT operations teams to remediate vulnerabilities and misconfigurations faster, gain visibility into patching progress, and ultimately reduce cyber risk.

Sample vendors include ServiceNow and BMC.

Patch Management

A cyber exposure platform can integrate with patch management solutions and allow security teams to audit the results of those solutions. Scanners scour the environment for vulnerabilities and correlate their discoveries with earlier vulnerabilities reportedly addressed by the patch management system. This process quickly identifies inconsistencies and reduces risks that might have gone unnoticed.

Sample vendors include IBM, Microsoft, Red Hat, and VMware.

IN THIS CHAPTER

- Considering must-have capabilities
- Identifying the platform requirements based on your organization's needs

Chapter 9
Ten Buying Criteria for Cyber Exposure Platforms

In this chapter, we summarize the ten criteria you'll want to consider when evaluating cyber exposure solutions. These criteria are the core capabilities you need to narrow your cyber exposure gap.

Continuous Visibility

You can't fix what you can't see. A panoramic cyber exposure platform allows you to continuously discover and assess both traditional IT (network infrastructure, servers, desktops) and dynamic modern assets (cloud instances, containers, web apps, operational technology [OT], Internet of Things [IoT] devices) across all computing environments. Continuous visibility eliminates blind spots on your modern attack surface.

Broad, Unified Coverage

Broad coverage starts with exhaustive detection of vulnerabilities and configuration issues across asset types. But it doesn't stop there.

A comprehensive cyber exposure platform also ingests and analyzes third-party asset, vulnerability, and threat data. The information collected from numerous sources is normalized and correlated to provide an expansive view of your cybersecurity posture.

A unified solution delivers clear visibility into assets, vulnerabilities and risk-based cyber exposure through an integrated set of data collection, analysis, visualization, and reporting capabilities. This eliminates the need to manually integrate or process data from multiple solutions to gain organization-wide insight.

Data Collection Flexibility

No single approach works for all assets, which means you need the full gamut of sensor technologies to cover your bases:

- **Network vulnerability scanners** identify vulnerabilities, misconfigurations, and other security health issues in your traditional IT infrastructure, servers, and PCs (including operating systems and applications).
- **Web application scanners** focus only on web applications and look for certain *types* of vulnerabilities such as input validation errors that can lead to cross-site scripting attacks. Web app scanners are particularly essential for testing an organization's custom-built applications.
- **Agents** installed directly on end-user devices or servers are especially valuable for assessing assets that aren't always on the network. Locally installed agent software includes all the capabilities required to discover vulnerabilities and audit configurations and in some cases even detect malware running on the asset.
- **Passive network monitoring** sensors provide live asset discovery and monitoring to eliminate the blind spots created

by periodic active scanning. They enable safe vulnerability detection for critical infrastructure such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that would be disrupted by traditional active scanning, aren't appropriate for agent deployment, and often can't be shut down for months or years at a time.

- The **image registry** integrates security into the software development life cycle by providing a repository that can house and scan images for assets such as containers and public cloud instances.

Seamless Integration with DevOps Tools

Information security leaders must find innovative ways to ensure security while enabling agile DevOps environments, such as integrating security into workflows early in software development.

REMEMBER

Introducing security early translates into significant business value in terms of eliminating blind spots, enabling DevOps velocity, and reducing manual effort.

SECURING WEB APPLICATIONS AND CONTAINERS

Safely identify issues across your entire portfolio of web applications via fast, automated, high-accuracy security testing. A modern cyber exposure platform includes web application scanning as part of a comprehensive approach to identifying and managing cyber risk across assets in all computing environments.

You can bring security even earlier into the software development life cycle through preproduction visibility into container images as they're created. This helps you seamlessly and securely enable DevOps processes and reduce cyber exposure. Knowing what vulnerabilities are inside every container and having the chance to remediate those issues before the images are pushed to production are critical to protecting these dynamic assets. A cyber exposure platform that integrates with the DevOps tool chain eliminates container blind spots without slowing the application development process.

Translation of Cyber Risk into Business Terms

Security teams must translate reams of raw vulnerability and security health data into language that all stakeholders can understand and act on. The following advanced capabilities of a cyber exposure platform help everybody in an organization see, understand, and act on cyber exposure:

- **Exposure scores for prioritization:** In-depth analysis is performed on asset, vulnerability, and threat data from multiple sources to calculate exposure scores for groups of assets and the overall organization. Exposure analysis translates security data into a meaningful quantification of cyber risk at the operational and strategic levels so you can optimize resources, focus on what matters most first, and improve your overall security posture.
- **Visualization for an intuitive understanding of assets and exposure:** A cyber exposure platform also presents information with a modern visual approach that facilitates rapid understanding and easy exploration. Trends and hot spots are seen immediately, and breaking issues can be highlighted. This approach helps you understand your cyber exposure in a way that reports and dashboards alone can't facilitate.
- **Benchmarking for competitive advantage:** Benchmarking your level of cyber exposure internally among different groups and externally versus industry peers (see Chapter 7), as well as tracking effectiveness over time, provides valuable information about where additional attention or investments are needed. A cyber exposure platform shows how you stack up against other organizations and highlights opportunities for improvement.
- **Clear insights for decision support:** Security teams can use a cyber exposure platform to provide actionable information and guidance to colleagues who have no cybersecurity expertise. In this way, the organization can conduct meaningful discussions about cyber risk and make better-informed decisions.

Support for IT/OT Convergence

A cyber exposure platform also helps organizations with industrial assets build an accurate inventory of all IT and OT assets, as well as achieve the centralized visibility required to assess security across the entire organization.

As IT and OT converge, with OT systems increasingly becoming interconnected with IT infrastructure, a cyber exposure platform helps organizations see and manage security weaknesses in critical infrastructure and other production assets. Identifying this exposure in OT networks requires capabilities that are purpose-built for industrial systems, such as nonintrusive passive monitoring, to provide broad asset discovery and vulnerability detection without disrupting sensitive systems.

Flexible Deployment and Elastic Licensing

A flexible cyber exposure platform can scale to meet the needs of a small business with a modest IT environment or a global enterprise with millions of assets. Private- and public-sector organizations with requirements for either on-premises software or cloud-based (Software as a Service) architectures should be able to reap the benefits of a cyber exposure platform.

Elastic asset-based licensing instead of IP address–based licensing works well for modern assets with multiple IP addresses and assets that frequently spin up and spin down.

Easy Integration with Existing IT Environments

A cyber exposure platform integrates with current IT infrastructure, allowing organizations to leverage their existing investments. An open, flexible approach relies on well-documented

application programming interfaces (APIs) and software development kits (SDKs) that enable integration with complementary tools and technologies so that critical issues can be addressed quickly and completely. A comprehensive ecosystem of partners reduces integration effort, delivers frequent innovation, and provides additional peace of mind.

Robust Services and Resources

Services offered by your cyber exposure platform vendor and partner ecosystem extend your cybersecurity capabilities, helping you leverage best practices and augment the capabilities of existing personnel. Services help you unlock the full value of your platform throughout the cyber exposure life cycle, including assessment, planning, and design; product training; platform implementation and operation; integration and automation; and ongoing support.

Knowledge and Expertise

Look for a partner that deeply understands assets, networks, and vulnerabilities, demonstrating proven industry leadership in VM and credible vision and capabilities for cyber exposure.

Your provider should have the following:

- A dedicated team of experienced cybersecurity researchers who continually enhance the platform and deliver data science–driven insights to address emerging threats and vulnerabilities
- In-depth knowledge of modern technologies and a compelling vision for the future
- Experienced security professionals who can help you master cyber exposure capabilities within your organization

If you're flying blind into the widening cyber exposure gap, that's untenable. Join the movement, and begin the journey of measuring and reducing your cyber risk across the modern attack surface.

CAN'T UNDERSTAND
YOUR CYBER EXPOSURE
WITH THE SAME
PREDICTABILITY AS
OTHER BUSINESS
EXPOSURE?

THAT'S JUST
UNTENABLE.

#cyberexposure

tenable.com

Mitigate the risks of modern digital assets

Today's corporate networks comprise modern digital assets, including mobile devices, web applications, virtual machines, cloud computing platforms, DevOps containers, and IoT devices. Legacy VM offerings were never designed to keep up with today's agile computing environments. To keep pace with a sophisticated threat landscape, IT organizations must think differently about how they prioritize and communicate cyber risks. Welcome to the age of cyber exposure and the era of cyber exposure platforms.

Inside...

- Navigating the modern attack surface
- Closing the cyber exposure gap
- Exploring cyber exposure platforms
- Securing apps at the speed of DevOps
- Boosting cloud visibility and security
- Enabling the convergence of IT and OT
- Prioritizing and communicating IT risks

Stacy Moran is a freelance writer specializing in IT security. She has developed compelling content for technology providers for decades. **Steve Piper** is a CISSP with 25 years of high-tech experience. He has authored more than a dozen books on IT security topics.

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

Also available as an e-book

ISBN: 978-1-119-50815-1
Not for resale

WILEY END USER LICENSE AGREEMENT

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