tenable one
Exposure Management Platform

WHITE PAPER

3 REAL-WORLD CHALLENGES FACING CYBERSECURITY ORGANIZATIONS

How an Exposure Management Platform Can Help

Contents

Introduction

The complexity of the modern attack surface — an ever-changing, expanding and interconnected assortment of systems and users — is the key driver behind the emergence of exposure management programs. Security teams are challenged to keep up with the constant influx of data from the array of point solutions they're using to manage vulnerabilities, web applications, identity systems and cloud assets. And, they're challenged with effectively analyzing all that data to make informed, proactive decision-making about which exposures represent the greatest risk to the organization.

The benefit of implementing an exposure management program? To enable security professionals to better allocate time and resources so they can focus on taking the actions that legitimately reduce their risk.

Adopting an exposure management program involves people and process changes. It requires security teams to place as much importance on proactive efforts as they currently do on reactive incident response efforts. It requires security professionals to consider how siloed organizational structures — and the myriad security tools used in support of those silos — are hindering their ability to see what an attacker sees. And it requires a way for security professionals to analyze the data coming from disparate tools to empower them to draw meaningful insights they can apply to their risk reduction goals.

The bottom line? When a threat actor evaluates a company's attack surface, they're not thinking in terms of organizational silos. They're probing for the right combination of vulnerabilities, misconfigurations and identity privileges that will give them the greatest level of access the fastest.

Source: Anatomy Of An External Attack Surface, Microsoft, April 2022

3 real-world challenges facing cybersecurity organizations

We see three distinct real-world challenges facing cybersecurity professionals that can be addressed with an exposure management program:

Security programs today are reactive when they should be proactive.

The attack surface isn't siloed, but most security programs are.

There's more data available than ever before, yet it's difficult for security professionals to correlate and apply the data in meaningful ways.

Security programs today are reactive when they should be proactive

In most large organizations, security functions are highly specialized. Teams handling crucial proactive and preventive measures — such as vulnerability management, cloud security and identity security — are likely operating in their respective vacuums, each using their own bespoke tools and each cranking out piles of data and disparate reports every day.

Meanwhile, teams working on the reactive side — including threat hunters, security operations center (SOC) analysts and incident responders — may have a valuable outside-in view, but they're not necessarily focused on the daily steps that need to be taken to keep the organization secure.

While crisis events garner more than their fair share of attention from business executives and the media, most cybersecurity professionals understand that the real work of reducing risk is a proactive effort that needs to take place daily and consistently over weeks, months and years. Modern, proactive cybersecurity requires the ability to: continuously assess the attack surface; understand the interconnectedness of users, assets and systems; and take steps to address vulnerabilities, fix misconfigurations and harden user identities and access privileges long before they're on the radar of an attacker.

The attack surface isn't siloed. So why are most cybersecurity programs set up that way?

There are many valid reasons from an organizational structure standpoint for security programs to be siloed. But a security program built upon a hodgepodge of technologies, all of which serve a bespoke function, makes it virtually impossible for security teams to effectively reduce risk. To do so, cybersecurity teams need a unified, predictive and proactive way of managing exposure across the entire attack surface.

There's more data available than ever before. So why can't security leaders quantify risk?

There is too much information being churned out daily by myriad security tools with no contextual way to analyze it. Security teams are left with few options for achieving a unified view of their attack surface other than by dumping the data into spreadsheets, validating the old joke that Excel is the most widely used security tool in the world. Managing exposure across today's massive, complex and ever-changing attack surfaces requires the kind of constant decision-making, collaboration and prioritization that simply cannot be achieved using spreadsheets. Concise, meaningful and impactful output is what's needed in order for security teams to perform to the best of their abilities. Organizations need the ability to continuously assess their vulnerabilities, misconfigurations and user privileges all in context with one another across the entirety of the attack surface.

An exposure management program, underpinned by a technology platform, can help address these real-world problems. Successfully implemented, an exposure management platform allows organizations to:

- **Gain comprehensive visibility across the modern attack surface**
- **Anticipate threats and prioritize efforts to prevent attacks**
- **Communicate cyber risk to make better decisions**

An exposure management platform extends beyond traditional vulnerability management, which concentrates on the discovery and remediation of publicly disclosed Common Vulnerabilities and Exposures (CVEs). To be a functional part of an exposure management program, the platform needs to include data about configuration issues, vulnerabilities and attack paths across a spectrum of assets and technologies — including identity solutions (i.e. Active Directory); cloud configurations and deployments; and web applications.

> *By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach.*
>
> — Implement a Continuous Threat Exposure Management (CTEM) Programme, Gartner, July 2022.

Gartner

Read the Gartner report:

Implement A Continuous Threat Exposure Management (CTEM) Program

The building blocks of an exposure management program

An exposure management program combines technologies associated with exposure management (such as vulnerability management, web application security, cloud security, identity security, attack path analysis and attack surface management) with the organizational operations and processes required to understand the exposures and take the actions needed to reduce them through remediation and incident response workflows.

Building an effective exposure management program requires security teams to complete the following five steps and answer the related questions:

1

Assess the security technologies you have right now. Are they working together to give you comprehensive insights into your exposure? Or are they siloed?

2

Understand your visibility into your attack surface, from endpoints to the cloud. What can you see? What do you need to see?

3

Prioritize your efforts. What do you need to do first? How can you prioritize your remediation efforts in a predictive manner? Are you incorporating threat intelligence to understand the threat landscape? Are you able to analyze all of the various attack paths to reach your most critical assets?

4

Measure your remediation processes. How well are you doing at fixing the things you find right now? What do you need to do to improve those processes? Can you compare your efforts to others in your industry? Can you compare different aspects of your organization to see where improvements are most needed?

5

Communicatie and take action. Can you answer the question "how secure are we?" How well can you communicate that status to both executive business management and your security organization? How are you using data to guide resource decisions across the security organization? Who owns the processes? Who takes responsibility?

Key benefits of an exposure management platform

A comprehensive exposure management program requires a platform that can help meet the needs of a variety of stakeholders. Here's how three key cybersecurity constituencies can each use an exposure management platform to aid their efforts:

- **Security practitioners.** This group needs full visibility into the attack surface along with a unified view of all assets. An exposure management platform can help security practitioners prioritize their efforts in remediating vulnerabilities in software, configurations and entitlements. Such comprehensive visibility and prioritization capabilities give these users the ability to understand their attack surface, eliminate blind spots and build a baseline for effective risk management, all while improving decision making.
- **Security managers.** This group needs to focus available resources on their most pressing security needs through insight and context about threats, assets and privileges. An exposure management platform helps security managers eliminate windows of risk while reducing the resources needed to remediate and respond. It gives these users the ability to anticipate the consequences of an attack by providing a contextual view of how assets and users are interrelated across the attack surface. Further, it provides security managers with clear and easily communicated key performance indicators (KPIs), yielding insights into the organization's progress over time as well as benchmark comparisons within the organization.
- **CISOs, BISOs and other security executives**. This group requires accurate risk assessments to improve investment decisions, make decisions about insurability, meet regulatory and compliance requirements and drive organizational improvement. An exposure management platform provides actionable metrics to help security leaders measure, compare and communicate cyber risk not only to operating teams within IT and security, but also up and out to non-technical executives and operating teams throughout the enterprise. A unified view of cyber risk with clear KPIs allows executives to measure progress over time and benchmark comparisons against industry peers and within the organization. The goal? Helping security leaders answer the question "how secure are we?"

3 things to look for in an exposure management platform

To be an effective part of any exposure management program, a platform needs to offer three key features:

1. **Comprehensive visibility.** A unified view of all assets and associated software vulnerabilities, configuration vulnerabilities and entitlement vulnerabilities, whether on-premises or in the cloud, is essential to understand where an organization is exposed to risk. An exposure management platform needs to continuously monitor the internet to rapidly discover and identify all external-facing assets to eliminate areas of known and unknown security risk. This helps to reduce the time and effort required for security teams to understand the complete attack surface, eliminate blind spots and build a baseline for effective risk management.

2. **Prediction and prioritization.** An exposure management platform needs to help users anticipate the consequences of a cyberattack by drawing upon the large data sets available from various point tools and providing context about the relationships amongst assets, exposures, privileges and threats across an attack path. Cyber risk prioritization is required to help cybersecurity teams continuously identify and focus on the attack pathways that present the greatest risk of being exploited. By providing accurate and predictive remediation insights, these features enable security teams to proactively reduce risk with the least amount of effort to help prevent attacks.

3. **Effective metrics to communicate cyber risk.** Security executives and business leaders require a centralized and business-aligned view of cyber risk with clear KPIs to show progress over time as well as benchmarking capabilities to compare against external peers. An exposure management platform needs to provide actionable insights into an organization's overall cyber risk — including the value of the proactive efforts happening daily. It also requires the ability for users to be able to drill down for specifics about each department or operational unit. It needs to deliver accurate, business-aligned cyber risk assessments to improve overall communication and collaboration among different constituencies. Actionable metrics enable security teams to show the value of their proactive security efforts as well as save time, improve investment decisions, support cyber insurance initiatives and drive improvement over time — all while tangibly reducing risk to the organization.

Introducing the Tenable One Exposure Management Platform

The Tenable One Exposure Management Platform unifies a variety of data sources into a single exposure view to help organizations gain visibility, prioritize efforts and communicate cyber risks. Building on proven Tenable products, it's designed to take advantage of the integrations that already exist between Tenable and its partners, such as ServiceNow. It is designed to form the foundation of an exposure management program, alongside the other tools (such as endpoint detection and response (EDR) and firewalls) and business processes required.

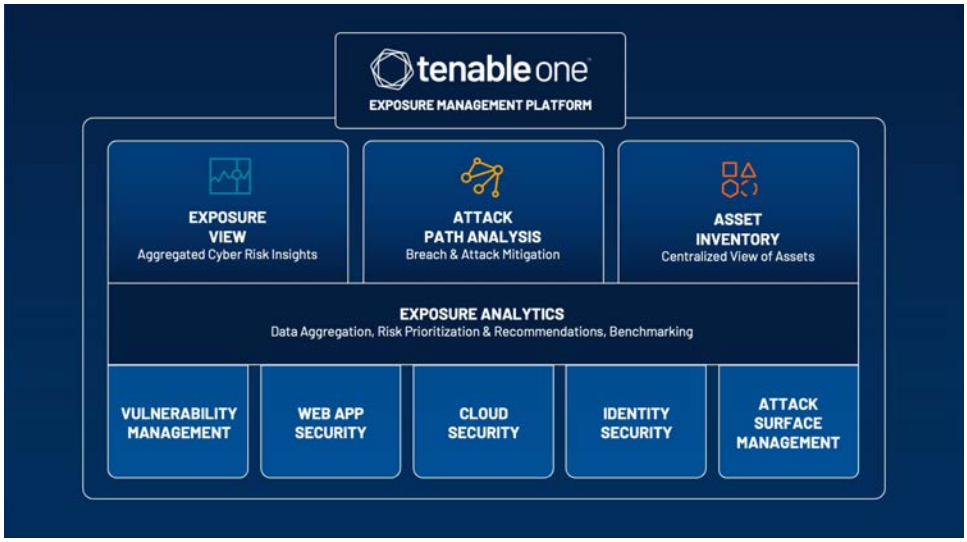
With Tenable One, organizations can translate technical data about assets, vulnerabilities and threats into clear business insights and actionable intelligence for security executives and practitioners alike. The platform combines the broadest vulnerability coverage in the industry, spanning IT assets, cloud resources, containers, web apps and identity systems. It builds on the speed and breadth of vulnerability coverage from Tenable Research. And, it adds aggregated exposure view analytics, guidance on mitigating attack pathways and a centralized asset inventory..

The Tenable One Exposure Management Platform incorporates these Tenable products:

- **Tenable.io vulnerability management:** Risk-based vulnerability management
- **Tenable.io Web Application Scanning:** Web application security.
- **Tenable Lumin:** Vulnerability and risk analytics
- **Tenable.cs:** Cloud security
- **Tenable.ad:** Active Directory security
- **Tenable.asm:** Attack surface management

Tenable One is no mere dashboard for accessing Tenable products. Rather, it is an Exposure Management Platform that takes the variety of data offered up by our tools and applies it to a host of new features that offer a comprehensive and contextualized view that helps you manage your exposure to attacks. New features and capabilities in Tenable One include the following:

Source: Tenable, August 2022



Aggregated risk-view analytics

- **Exposure View.** Provides clear, concise insight into an organization's security exposure, enabling users to answer such critical questions as "how secure are we" and "where do we stand in our preventative and mitigation efforts." "how are we doing over time and what are the key events?" It provides a unified global exposure score drawn from a variety of different data sources.
- **Custom exposure cards.** Allows users to have concise, flexible communication of specific security insights.
- **Tag performance.** Addresses what tags make up an exposure card and how much that group of assets contributes to a given exposure score.

Breach and attack path mitigation

- **External Attack Surface Management (EASM).** Offers insight into the external attack surface, enabling organizations to identify and reduce risks from the attacker's perspective.
- **Attack Path Analysis.** Provides attack path visualization and prioritization capabilities to enable security practitioners to take a proactive approach to disrupt common attack paths long before attackers seek them out. Tenable One performs this function by mapping critical risks to the MITRE ATT&CK framework to visualize all viable attack paths continuously — both on-premises and in the cloud.

Asset inventory

- **Centralized asset inventory.** Offers a centralized view of assets from a variety of data sources with the ability to create specific asset tags from a variety of sources.
- **Comprehensive assessment.** Provides insight into the exposure of all assets, including vulnerabilities, misconfigurations and other potential security threats

About Tenable

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

Conclusion

The foundational platform for an exposure management program requires the integration of a variety of different security technologies. Equally as important, it requires people and process changes to break down silos and improve communication across the various infosec functions in the organization. Traditional approaches to vulnerability management need to evolve into a comprehensive exposure management program, enabling users to translate data about assets, vulnerabilities and threats into actionable insights. Tenable One is the first such platform in the industry — drawing information from a range of technologies into a singular analytic tool.

The Tenable One Exposure Management Platform represents the natural evolution of Tenable's vision. It's a strategic and long-lasting approach to cybersecurity that is poised to transform how organizations around the world manage risk.

Exposure management gives cybersecurity leaders a way to reclaim the narrative from the reactive, headline-grabbing breaches and attacks. It enables them to clearly explain the effectiveness of proactive, preventive security programs in a language the business will understand. And it transcends the limitations of siloed security programs.

Learn more

More information about Tenable's approach to exposure management and the Tenable One Exposure Management Platform can be found here:

Read theTenable One
Blog

Visit the Tenable One
Product Page

Gartner

tenable