tenable | eBook

How to Chart a Path to Exposure Management Maturity

14 Powerful People, Process and Technology Changes to Drive Measurable Cybersecurity and Risk Management Results

Table of contents

Your quick-start guide to exposure management

Exposure management is a strategic approach to proactive security designed to continuously identify, prioritize and close an organization's most urgent cyber exposures — those toxic combinations of preventable risks (e.g., vulnerabilities, misconfigurations and excessive permissions) that provide threat actors with a path to an organization's most critical assets.

Exposure management encompasses vulnerability management, web application security, cloud security, identity security, external attack surface management and other proactive security functions. Consequently, many organizations have at least some of the functional components of exposure management in place. The challenge they face, however, is that each of these functions operates at different levels of maturity and typically uses different tools and processes to identify, score and facilitate remediation of risks. At the same time, their tools lack the business and technical context needed to understand attack paths and distinguish true exposures with potential for significant business impact amid a constant onslaught of alerts.

The end result: Organizations lack an accurate and unified view of their cyber exposure, impeding CISOs' ability to report on and mobilize their security teams to remediate the most urgent risks.

To realize the full value of exposure management (see page 2: 6 Reasons CISOs Make Exposure Management a Cornerstone of Their Security Strategy), organizations can implement a few strategic people, process and technology changes aimed at unifying security visibility, insight and action across the attack surface to better contextualize, prioritize, quantify and remediate those highest risk exposures.

Tenable pioneered the concept of exposure management in 2017 to help security leaders move beyond noisy, siloed security to a unified, business-aligned program focused on identifying and remediating true exposures. On the pages that follow, we present our proprietary exposure management maturity model, developed based on our years of experience helping our vast customer base implement robust vulnerability and exposure management programs that drive measurable risk management outcomes.

Indeed, one food company we worked with reduced its cyber exposure by $45 million in 2024 alone.

Each stage of our maturity model captures common characteristics we've observed among our customers. We've designed it to help security leaders identify their organization's current state of exposure management maturity and steps they can take to advance it. While the model appears to prescribe a linear journey, moving from one stage to the next, maturing an exposure management program doesn't have to proceed from point A to point B, and so on. It's possible to bypass certain stages, and on the following pages, we show you exactly how. Continue reading to learn more.

The role of vulnerability management in exposure management

Organizations with a mature vulnerability management function have a significant head start when it comes to implementing exposure management because they're already working with established frameworks, remediation processes and strong business alignment. In addition, vulnerability management teams are increasingly responsible for securing more and more of the attack surface, including unseen or under-managed externally facing assets, cloud workloads, OT and IoT devices, and cyber-physical systems. This facilitates gaining the end-to-end attack surface visibility required for exposure management.

6 reasons CISOs make exposure management a cornerstone of their cybersecurity strategy

1. Exposure management helps to increase the productivity and efficiency of the cybersecurity function, while reducing overall costs and exposures.

2. It gives security and business leaders a unified view of their organization's true cyber exposure.

3. It improves proactive security and remediation teams' efficiency and effectiveness by prioritizing exposures and facilitating a single, unified process for remediating them.

4. It helps to shrink an organization's exploitable attack surface, which reduces the burden on reactive security teams (e.g., incident responders, SOC analysts, threat hunters).

5. Exposure management provides security leaders with a mechanism for unifying siloed proactive security functions and the data their disparate tools produce.

6. It provides a scalable, sustainable path for raising the maturity levels of proactive security teams.

Stage 1

Ad-Hoc

You know you're at this stage if your organization:

- Relies largely on manual audits to identify assets in its environment.
- Is more reactive than proactive, with limited or no tools in place to detect risk for each security domain.
- Has not adopted any frameworks or benchmarks.
- Lacks defined remediation workflows.
- Relies on fragmented, inconsistent and manual tracking of metrics.

To move from ad-hoc to defined, the most important step you can take is:

Implement standard processes for managing and fixing the risks and issues identified within each security domain (e.g., vulnerability management, cloud security, identity security, OT security, attack surface management, etc.).

Want to do more? Some additional ways to move from ad-hoc to defined:

Adopt a framework, such as the NIST Cybersecurity Framework 2.0, for managing cyber risk.

Look to expand your organization's attack surface visibility. Consider focusing on a specific segment of the attack surface that's important to the business, such as industrial control systems.

Level of effort to move from ad-hoc to defined: **Low**

Want to leapfrog Defined and and jump from Ad-Hoc to Standardized?

Then don't implement more siloed tools. Take a programmatic, platform-based approach. This can streamline procurement, enable better negotiation of discounts and improve integration across tool sets.

Think you know where you fall on the maturity curve? Take our quick assessment to find out. You may be more advanced than you think.

Stage 2

Defined

You know you're at this stage if your organization:

- Has staff with defined roles aligned to individual security domains, even if the maturity of each domain varies (e.g., some teams have more advanced expertise and processes).
- Has better asset and attack surface visibility, but large gaps in coverage may remain due to intermittent use of automated discovery tools across some security domains.
- Uses tool-specific or industry-standard risk scoring and has begun factoring threat intelligence into that scoring to help prioritize individual findings.
- Has some remediation tools in place and has taken initial steps to define basic remediation processes.
- Has taken initial steps to define a base set of metrics and reporting for each domain, but lacks business alignment and consistency across domains.

To move from defined to standardized, the most important step you can take is:

Expand the responsibility of your vulnerability management team and extend their scope of visibility into related domains, such as web application scanning and external attack surface management, that can add more context. In this manner, your vulnerability management team can begin looking at toxic risk combinations and unifying some reporting.

Level of effort to move from defined to standardized: **Medium**

Want to do more? Some additional ways to move from defined to standardized:

- Automate more of your risk prioritization and remediation workflows.
- Begin enriching prioritization at the domain level with business context.
- Get the right people and processes in place across security domains.

Want to leapfrog Standardized and and jump from Defined to Advanced?

Then don't implement more siloed tools. Take a programmatic, platform-based approach. This can streamline procurement, enable better negotiation of discounts and improve integration across tool sets.

Think you know where you fall on the maturity curve? Take our quick assessment to find out. You may be more advanced than you think.

Stage 3

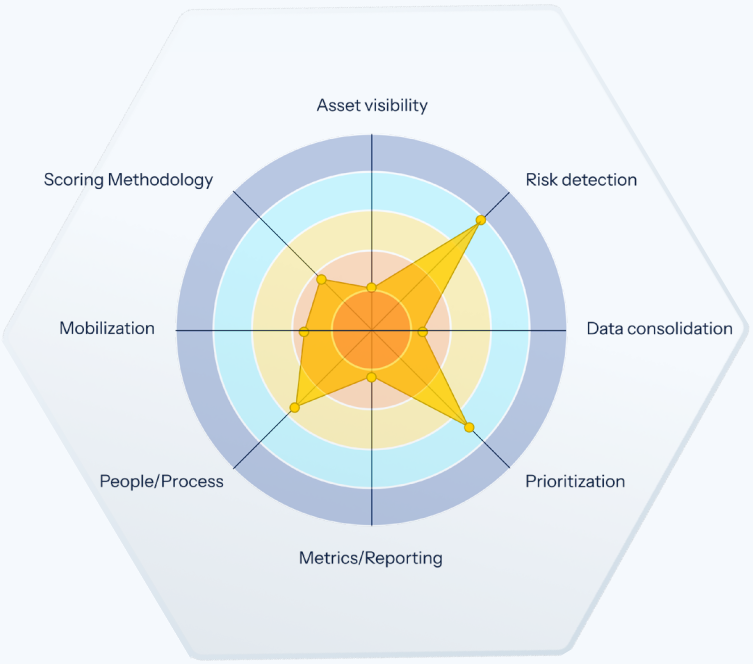
Standardized

Where most organizations begin the journey to exposure management

You know you're at this stage if your organization:

- Has automated visibility into a broad cross-section of asset types across its attack surface, with risk detection focused primarily on vulnerabilities (CVEs).
- Layers threat intelligence and asset criticality on top of tool-specific or industry-standard risk scoring to understand the probability of an exploit and the business value of an asset.
- Aggregates some asset and risk data into a single data store, whether a database, reporting tool or unified data lake.
- Has mature prioritization processes across individual security domains, along with well-documented remediation processes integrated into tools.
- Has baseline metrics and reporting defined for each security domain, with the ability to tailor them for business units.

Level of effort to move from standardized to advanced: **HIGH**



To move from standardized to advanced, the most important step you can take is:

Get all of your asset and risk data into a single, unified data store or data lake.

Want to do more? Some additional ways to move from standardized to advanced:

- Apply workflow orchestration and automation to drive greater productivity.
- Normalize and incorporate business context into risk scoring across security domains.
- Begin looking at toxic risk combinations to improve prioritization and remediation.

Think you know where you fall on the maturity curve? Take our quick assessment to find out. You may be more advanced than you think.

Stage 4

Advanced

You know you're at this stage if your organization:

- Has a robust, unified view of most assets across its attack surface. However, some visibility gaps may remain due to a reliance on point-in-time automated discovery.
- Has robust capabilities for detecting vulnerabilities and misconfigurations across the attack surface but typically lacks visibility into exposures from excessive human and machine permissions.
- Normalizes risk scoring across domains and factors in threat intelligence and asset criticality.
- Automatically aggregates, deduplicates and correlates security data into a unified data lake.
- Has a unified approach to prioritization across domains that includes tagging with business context to understand potential business impact.
- Dedicates and assigns staff to cross domain roles and uses existing, mature processes to mobilize remediation.
- Has consistent metrics and reporting aligned to the business across domains.

To move from advanced to optimized, the most important step you can take is:

Evolve your security program from risk-centric to exposure centric. You may continue to manage individual risks as you undertake this shift, but you'll add more context to understand exposure.

Want to do more? Some additional ways to move from advanced to optimized:

- Incorporate technical context into risk scoring and prioritization.
- Dedicate resources to attack path analysis to connect all the dots between domains, risk and revenue streams, to optimize prioritization and further accelerate remediation.

Level of effort to move from advanced to optimized:

HIGH

If you opt to build the underlying infrastructure yourself

MEDIUM

If you implement a new cyber asset attack surface management (CAASM) tool to aggregate data (drawback: CAASM tools don't perform attack path analysis, a requirement of exposure management)

LOWER

If you implement an exposure management platform

Think you know where you fall on the maturity curve? Take our quick assessment to find out. You may be more advanced than you think.

Stage 5

Optimized

Highest level of exposure management maturity

You know you're at this stage if your organization:

- Has a robust, unified view of its end-to-end attack surface with continuous discovery of assets.
- Proactively detects all preventable forms of risk that attackers can exploit: vulnerabilities, misconfigurations and excessive permissions.
- Has advanced, exposure-centric scoring that can determine total asset exposure, as well as exposure scores for different business units.
- Takes action based on a prioritized view of the attack paths and exposures threat actors can exploit to breach critical assets and cause disruption.
- Has a dedicated, mature, cross-domain team in place that is continuously optimizing processes and remediation workflows to drive maximum productivity and risk reduction.
- Consistently measures and reports on true exposures rather than just individual risks.

Think you know where you fall on the maturity curve? Take our quick assessment to find out. You may be more advanced than you think.

Accelerate Your Path to Exposure Management Maturity

While the Tenable Exposure Management Maturity Model outlines five distinct stages, the journey to exposure management maturity doesn't have to be incremental. It's possible to leapfrog stages and jump from ad-hoc to standardized (bypassing defined) or from defined to advanced (bypassing standardized).

In fact, there may be drawbacks to taking a traditional approach to maturing your proactive security program, where you evolve in silos, aggregate data and add more context over time. Applying this traditional approach, you may never achieve exposure management maturity because visibility and context will remain in disconnected tools and you'll be left with disparate processes — particularly if you rely on implementing individual point solutions for each security domain to improve asset and risk visibility.

The key to accelerating maturity, then, is not to get hung up on point solutions, which only exacerbate the complexity, inefficiency and exposures created by security silos. Instead, stay focused on the end goal of exposure management and leverage existing security investments in people, processes and technology to gain that unified, contextualized and prioritized view of exposure across security domains. Ultimately, this hinges on having three things:

- End-to-end attack surface visibility.
- A unified data lake where security data is automatically aggregated, deduplicated, correlated and enriched with threat intelligence and business and technical context in real time.
- Consistent risk scoring across domains to facilitate prioritization and remediation.

To bypass certain stages and accelerate maturity, look for an exposure management platform that can:

- Collect data natively and aggregate, normalize and enrich your existing security data with technical and business context.
- Provide unified visibility, scoring, prioritization and reporting across domains.
- Automate and streamline remediation workflows.
- And seek partners with deep experience helping organizations implement exposure management programs, who can help you navigate the strategic people and process considerations associated with exposure management as deftly as they can help you implement a solution.

Ready to take the next step?

1. Assess Your Exposure Management Maturity
2. Stand Up an Exposure Management Program

About Tenable

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact

050625