MANDIANT
NOW PART OF Google Cloud

PROACTIVE EXPOSURE MANAGEMENT
WHITE PAPER

# Proactively respond to exposures before your adversaries do

## The Security Leaders’ Guide to Exposure Management

# Shifting the security operations paradigm left

The enterprise world is rapidly moving from digital transformation into a new phase of digital expansion that puts unprecedented strain on enterprise risk and security teams. Organizations are accelerating the expansion of digital ecosystems as they look to develop new revenue streams and create competitive differentiators around speed, agility, collaboration, and innovation. Multi-cloud strategies, SaaS, IaaS and the growing digital supply chain of third-party partners, and the ongoing challenges around securing the remote workforce all converge to present an enterprise attack surface of incredible breadth and complexity.

Adversary numbers are also growing—feeding on the proliferation of enterprise exposures. The World Economic Forum estimates cybercrime will cost the world $10.5 trillion by 2025—enough to rank as the world's third-largest economy.[1] The big business of cybercrime breeds more organized, well-funded, sophisticated, and patient threat actors, including a marked increase in nation-state actors seeking to further geo-political goals through targeted financially motivated attacks.

Organizations were notified of breaches by external entities in **63%** of incidents investigated by Mandiant[2]

**69%** of security teams admit feeling overwhelmed[3]

## From reactive operations to cyber resiliency

Facing the increasing reality that preventing attacks is all but impossible, the security world has seen a shift in the past several years—from the concept of security operations toward a new paradigm of cyber defense resiliency that focuses on ensuring an organization is prepared to respond to an intrusion without allowing it to damage or disrupt the business. Today, industry leaders and analysts are coalescing around a more proactive model for achieving cyber resiliency, defined by Gartner® in 2022 as Continuous Threat Exposure Management, or CTEM. According to Gartner®, the Continuous Threat Exposure Management (CTEM) programme is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets."[4]

[1] https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/#:~:text=Cybercrime%20is%20big%20business.,%2410.5%20trillion%20annually%20by%202025
[2] M-Trends 2023, https://www.mandiant.com/resources/blog/m-trends-2023
[3] Global Perspectives on Threat Intelligence, https://mandiant.widen.net/s/lnltwn85jj/global-perspectives-on-threat-intelligence-2-08-23
[4] Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program. Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, July 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

# Solving the flaws of vulnerability management

Exposure management was born out of the growing frustration with vulnerability management—a response to traditional patch management's shortcomings and the need for a more proactive approach to cyber resiliency. Though fundamentally sound, vulnerability management proves challenging to execute.

Google is reporting MORE ZERO-DAY VULNERABILITIES than ever[5]

Two-thirds of CVEs are now rated HIGH SEVERITY OR GREATER[6]

84% of security leaders worry they're missing threats and incidents because of ALERT AND VULNERABILITY FATIGUE[7]

- **Vulnerability fatigue:** Patching vulnerabilities has always been a never-ending task, but the volume keeps growing in the current environment, and prioritization is difficult. IT and security teams are overwhelmed with never-ending alert point solutions aimed at monitoring the different areas of their rapidly expanding digital ecosystems. These siloed alert feeds make it difficult to objectively prioritize what matters most and allocate resources effectively.
- **Non-patchable vulnerabilities:** While technological vulnerabilities are becoming more common, the human element remains the most significant threat vector—evidenced by the fact that phishing was the third-most-common initial infection vector in M-Trends 2023.[8] Updating a widely adopted technology (hardware application, agent-based software, etc.) is a complex, hands-on process that can take months—and requires careful planning and testing to ensure that the fix does not introduce new problems.
- **Need for faster remediation and mobilization:** Tech-driven or not, vulnerabilities increasingly present issues that security alone can't handle. Remediating or patching becomes precarious when there is potential for business disruption. And they require the mobilization of teams in large, cross-functional, multi-layer organizations. Other issues sit entirely outside the enterprise's control, within the so-called digital supply chain—the complex ecosystem of third-party vendors that connect to or access an organization's systems or data as part of their operational technology (OT) and IT stacks.

[5] https://www.zdnet.com/article/google-were-spotting-more-zero-day-bugs-than-ever-but-hackers-still-have-it-too-easy/
[6] NIST, National Vulnerability Database Dashboard, https://nvd.nist.gov/general/nvd-dashboard
[7] Global Perspectives on Threat Intelligence, https://mandiant.widen.net/s/lnltwn85jj/global-perspectives-on-threat-intelligence-2-08-23 8.
[8] M-Trends 2023, https://www.mandiant.com/resources/blog/m-trends-2023

# Cyber resiliency through response readiness

With the volume and complexity of security issues today, the reality is no security team can address everything. But the cyber resiliency paradigm moves security teams from a reactive stance to a focus on proactive readiness that centers on four essential capabilities:

1. **Know where you're exposed**

   Identify the attack surface and where the exploitable entry points are

2. **Know who's targeting you**

   Gain visibility into adversary targeting and malicious orchestration

3. **Know if you're prepared**

   Proactively validate security control effectiveness against targeted attacks

4. **Know if you're being attacked**

   Operationalize intelligence in near real-time within security operations

# What is Exposure Management?

Exposure management is not a single tool, technology platform, or a one-time activity. Instead, exposure management should be thought of as a process for a modern, proactive approach to cybersecurity. Critically, that proactive approach centers on taking a holistic perspective of an organization's exposure profile: considering both the organization's assets and internal infrastructure, as well as the intent and activities of threat actors. In other words, this *holistic* view must combine a broader, continuous look at the expanding attack surface with real-time *threat intelligence* feeds that narrow focus through the concept of attack or breach *feasibility*.

### Understanding exposures vs. vulnerabilities

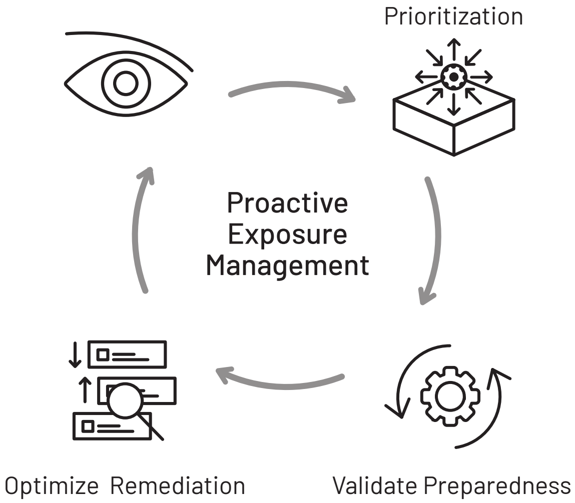
Exposures go beyond vulnerabilities to include all potential exploitable entry points that can be used by an adversary to gain initial compromise into an organization or supply chain ecosystem. Exposures include conventional vulnerabilities but also include:

- Server misconfigurations
- Security controls missing detections for specific indicators of compromise (IOCs) or commonly used threat actor tactics, techniques and procedures (TTPs)
- Vulnerable software
- Zero-days
- Stolen credentials
- Unknown

## The Four Capabilities of Proactive Exposure Management

The exposure management process can be more easily understood through four essential capabilities of proactive exposure management:

### Steps to success



**Extend Visibility**
*Continuously identify the attack surface, crown jewels, and threat landscape*

**Intelligence-led Prioritization**
*Inform business decisions and resource allocation based on trusted intelligence*

**Validate Preparedness**
*Measure and test cyber defense effectiveness with targeted attack emulations*

**Optimize Response**
*Improve resource allocation, patching cadence and response time to active breaches*

# Expand visibility

To create the foundation of proactive exposure management, security teams need to 1) properly assess all assets; 2) assign criticality; and 3) understand the business impact of a potential breach. This all depends on broad and reliable visibility across the expanding attack surface—specifically at the edges of the enterprise ecosystem. Security teams need tools that can see into the digital expanse: into SaaS applications, IaaS and cloud-based environments, and the apps, systems and data owned and operated by third parties in the digital supply chain.

## Essential aspects of the attack surface

Security leaders can divide this attack surface visibility into three aspects—and should leverage a suite of tools and services to  gain visibility into each. The following are examples:

| Internal Attack Surface | External Attack Surface | Digital Risks |
|---|---|---|
| • Asset Management<br>• Configuration Management Database (CMBD)<br>• Cloud Security Posture Management (CSPM)<br>• Directories. | • External Attack Surface Management<br>• Cloud Security Posture Management<br>• Red Teaming<br>• Penetration Testing | • Threat Intel<br>• Digital Risk Protection Devices<br>• External Attack Surface Management<br>• Dark Web Monitoring |

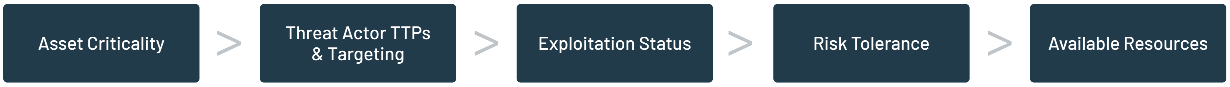
More mature security organizations may already have visibility across all three aspects of the attack surface. Yet as mentioned earlier, it's often siloed in disparate feeds coming from point solutions. This attack surface visibility needs to be centralized and integrated so it can be holistically understood and effectively prioritized.

# Intelligence-led prioritization

Today's most dangerous threat actors have moved from spray-and-pray tactics to well-organized, well-funded, and patient land-and-expand tactics. The upside is that these more advanced attack patterns often leave a trail, and a new generation of tools and technologies allows security teams to track digital activities, ranging from discussions and planning on the dark web to initial recon activities targeting an organization's ecosystem. Yet 79% of security leaders today say they make decisions on cyber attacks without insights on who's targeting their organization.[9]

## Using threat intel as an exposure filter

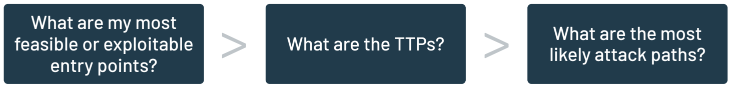
A key difference in moving from vulnerability management to proactive exposure management is harnessing the potential of real-time threat intelligence. With this intelligence-led prioritization, CISOs and security leaders can take a progressive filtering approach:



Asset Criticality > Threat Actor TTPs & Targeting > Exploitation Status > Risk Tolerance > Available Resources

# Validated preparedness

Security validation has always been part of a security posture. The concept of cyber resiliency adds nuance to validation, as testing is not a binary "Do the controls block entry?" but rather, "How will the integrated security stack respond to a given attack pattern?" The proactive exposure management framework uses threat intelligence to advance the application of security validation by focusing on three essential questions:



What are my most feasible or exploitable entry points? > What are the TTPs? > What are the most likely attack paths?

## Holistic, continuous security validation

Security validation cannot be a one-time or period exercise. Rather, security teams should be continuously running through testing scenarios, objectively measuring performance, and re-tuning to drive continual improvement. Beyond testing security controls, validation should provide a holistic view that quantifies the effectiveness of the entire SecOps program in defending against targeted attacks. This includes testing each discrete security team response workflow. Critically, security teams need to test communication processes to ensure high-priority exposures are properly escalated through the right.

[9] Global Perspectives on Threat Intelligence, https://mandiant.widen.net/s/lnltwn85jj/global-perspectives-on-threat-intelligence-2-08-23

# Optimized remediation

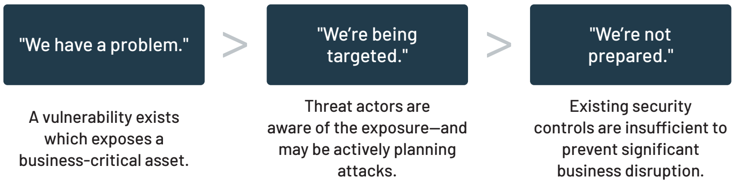
Automated tools play a critical role in modern security strategies, but the rapidly growing volume and proportion of non-patchable exposures cannot be solved with automated remediation tools. Organizations need to balance automation with cross-team collaboration and communication to resolve these more complex exposures.

To foster shared understanding and responsibility for cross-functional exposures, and to get the buy-in needed to execute remediation strategies, security teams need to implement more strategic, cross-functional risk reduction tactics, such as:

- Integrating threat intelligence into a SIEM or detection and response function
- Establishing lines of communication with key stakeholders and asset owners
- Reallocating resources to cover gaps or focus on the critical exposures
- Communicating the current status or posture of the security program and the go-forward plan with executives

## Getting buy-in for cross-functional remediation

In addition, the exposure management process acts as a filter to narrow an organization's focus on its most business-critical and feasible, exploitable, or attackable exposures. This naturally empowers security teams to make a compelling business case to key stakeholders:



"We have a problem."

A vulnerability exists which exposes a business-critical asset.

"We're being targeted."

Threat actors are aware of the exposure—and may be actively planning attacks.

"We're not prepared."

Existing security controls are insufficient to prevent significant business disruption.

# Building cyber resiliency: Prioritize and address your most business-critical exposures—before your adversaries do.

The move from cyber defense to cyber resiliency is far from a surrender to the inevitability of attacks. Rather, it's about getting smart, pragmatically recognizing finite resources, and focusing attention where it matters most. The modern CISO needs to build a security posture that protects critical assets and supports business continuity from increasingly sophisticated attacks, while also empowering the speed, agility, collaboration, and innovation of the business by enabling the promise of digital transformation.

Achieving that complicated goal fundamentally demands a shift toward the new model of proactive exposure management, powered by a radically simple notion: Know who's targeting you; know what they're targeting; and know how they're planning to attack. Leveraging this real-time threat intelligence, security teams can triangulate their most attackable, exploitable business-critical assets—and refine that focus through continuous validation to identify where they're prepared, and where they're not. This comprehensive framework arms security leaders with the intelligent, evidence-based prioritization to effectively mobilize cross-functional remediation where it matters most to stay ahead of adversaries.

## Mandiant Proactive Exposure Management

As a leader in cyber defense and a trusted advisor to high-assurance organizations building and maturing their cyber security programs, Mandiant has developed a purpose-built solution to address the exposure management model: Mandiant Proactive Exposure Management can help enterprises reliably and continuously reduce the most critical and attackable exposures—before adversaries act on them.

### A Complete Solution to Drive **Essential Business-Enablement Outcomes**

| Know where you're exposed | Know who's targeting you | Know if you're prepared | Know if you've been breached | Be threat ready before, during, and after a breach |
|---|---|---|---|---|
| Mandiant Attack Surface Management and Technical Assurance Services | Mandiant Threat Intelligence, Intelligence Services and VirusTotal | Mandiant Security Validation and Technical Assurance Services | Mandiant Breach Analytics for Chronicle and Chronicle Security Operations | Cyber Defense Assessments, Strategic Readiness Services, Technical Assurance Services, Transformational Security Services, and Incident Response |

Be proactive, talk to a Mandiant expert.
https://www.mandiant.com/solutions/proactive-exposure-management

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud