⌘ COMMAND IS

UNIFIED EXPOSURE MANAGEMENT:

Uncovering unknown assets and vulnerabilities

WHITEPAPER

RAPID7

Executive summary

In today's threat landscape, traditional vulnerability management is falling short. Security teams face a rapidly expanding and increasingly complex attack surface, rising regulatory pressure, and adversaries who think in terms of attack paths—not isolated Common Vulnerabilities and Exposures (CVEs). The challenge isn't just identifying assets and vulnerabilities anymore; it's knowing which exposures truly matter, and being able to act on them with precision, context, and confidence.



This whitepaper introduces a unified, risk-first approach to exposure management—one that helps organizations get more value out of their existing scanners, endpoint detection, and identity security tools by automatically mapping findings to action. Security teams with unified exposure management continuously discover assets and identities, validate risks with real-world context, and drive scalable, targeted remediation.

The shift away from siloed solutions like Cloud Attack Surface Management (CASM), External Attack Surface Management (EASM), Cloud Native Application Protection Platform (CNAPP), or Application Security (AppSec) point solutions is not just an operational refinement—it's a strategic evolution. Unified exposure management empowers CISOs and IT leaders to reduce tool fragmentation, improve cross-team collaboration, and gain a clear, actionable view of their true attack surface. The outcome is a security program that's not only more efficient, but fundamentally more resilient.

CAPABILITY	TRADITIONAL VM	UNIFIED EXPOSURE MANAGEMENT
Asset Discovery	Partial (agent-based only)	Full (internal + external)
Contextual Prioritization	CVSS focused	Threat-aware + business impact
Remediation Workflow	Manual, siloed	Automated, integrated
Risk Validation	Static	Continuous
Identity Awareness	Absent	Integrated

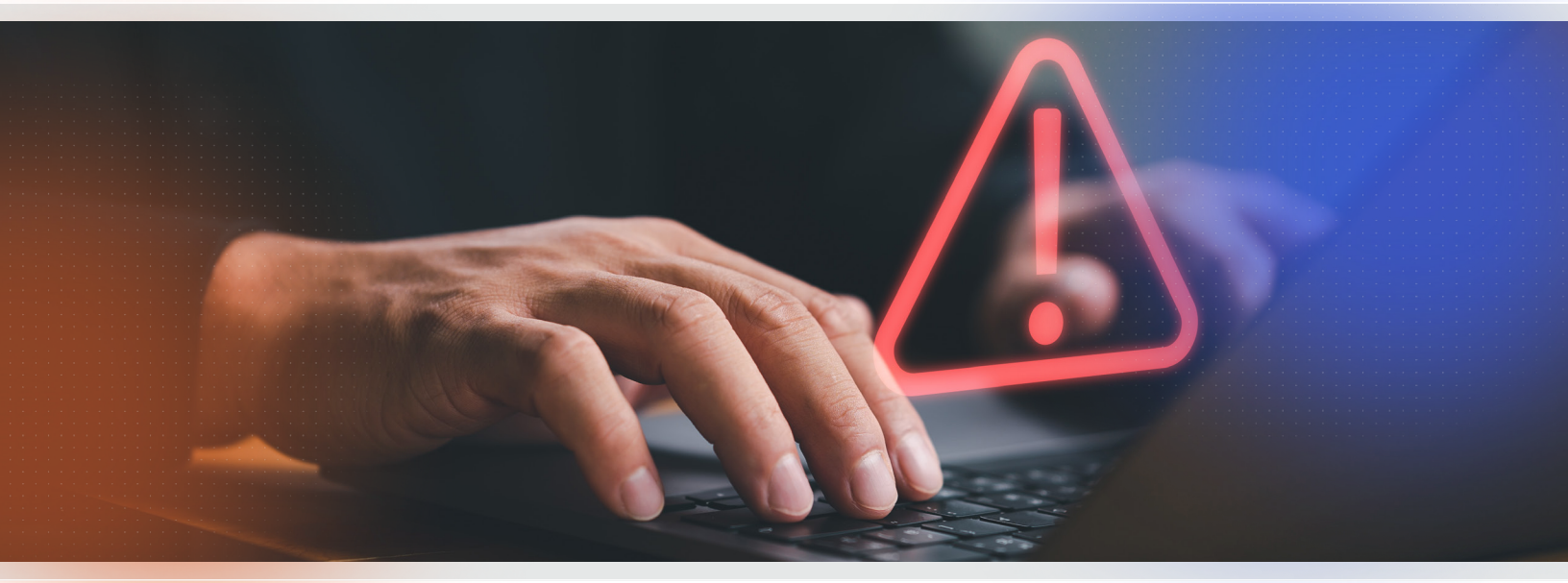
Attackers don’t care what your assets are, they care what’s exposed

Today’s adversaries are not targeting specific technologies. They’re targeting weaknesses - any entry point that allows them to escalate privileges, move laterally, and disrupt operations. Whether it’s a misconfigured cloud bucket, a forgotten SaaS integration, or an unpatched internal system, attackers see opportunity in exposure.

This shift in attacker behavior has coincided with seismic changes in IT environments:

- **Cloud-native adoption and hybrid architectures now dominate enterprise infrastructure.**
- **SaaS applications, IoT devices, and ephemeral workloads constantly appear and disappear.**
- **Third-party integrations and supply chain dependencies expand the potential blast radius.**

As environments grow more dynamic, so do the threats. Ransomware groups operate like enterprises. Zero-day vulnerabilities are exploited faster than ever. And human-centric risks like credential compromise and insider threats continue to evade static controls.



Visibility is essential to targeted remediation

You can’t secure what you can’t see - but the inverse is also true: You can’t prioritize what you don’t understand.

Organizations with fragmented visibility struggle to connect the dots between vulnerabilities, identities, and business impact. Without full situational awareness across their attack surface, they remain in a cycle of reactive triage.

Unified exposure management provides the foundation for true visibility—one that spans cloud and on-prem infrastructure, identity and access, internal and external threats. With this unified view, security teams can shift from reacting to alerts to anticipating threats and proactively addressing risks before they escalate.

The limits of traditional vulnerability management

Why traditional VM alone falls short

For many years, vulnerability management meant scheduled scans, a list of CVEs, and assigning tickets for remediation. That approach is no longer enough.

Legacy VM tools can detect known vulnerabilities but struggle to keep up with modern environments. They often lack real-time context and rarely support collaboration across teams. More importantly, they fall short in several critical ways:

1. **Coverage gaps:** Assets, such as unmanaged cloud resources or shadow IT, are not covered by agents or scanning engines.
2. **Overload:** CVSS scores do not reflect active risk, causing teams to waste time responding to low-impact vulnerabilities.
3. **Tool sprawl:** CASM, CNAPP, EASM, and AppSec tools each serve a purpose, but without integration, they create friction.
4. **Lack of prioritization:** Treating all vulnerabilities equally leads to wasted effort and unresolved threats.

> “Enterprises fail at reducing their exposure to threats through self-assessment of risks because of unrealistic, siloed and tool-centric approaches. Security and risk management leaders must initiate and mature a continuous threat exposure management program to stay ahead of threats.”
>
> **Gartner®, 2023[1]**

Some security stacks attempt to close visibility gaps by layering aggregation tools on top of disconnected systems. Others depend on narrowly scoped tools that only monitor specific domains—like endpoint-only agents or standalone scanners—leaving uncovered critical areas like cloud workloads, identity management, and external assets.

Aggregators can only report on what has already been scanned, and single-domain tools miss the broader context needed to understand how risk flows across the environment. The result is a fragmented, incomplete view of exposure. And when visibility is partial, prioritization becomes flawed and response efforts are often misdirected.

---

[1]Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D’Hoinne, Pete Shoard, Mitchell Schneider, 11 October 2023 (For Gartner subscribers only)

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.

Introducing a risk-first security approach

Prioritization over protection

The modern security mindset focuses less on chasing vulnerabilities and more on remediating legitimate risk. While many organizations have started the transition toward modern exposure management, confidence in the effectiveness of these initiatives remains limited. At the 2025 Take Command Summit, only 30% of respondents reported being "very confident" in their ability to respond to risks surfaced through these programs. To rebuild trust in their security programs, security teams need continuous answers to the following questions:

- **Discover:** Which exposures are most likely to be exploited?
- **Prioritize:** What is the potential business impact of each vulnerability?
- **Mobilize:** How should we remediate the risk?

This risk-first approach emphasizes a threat-aware understanding of vulnerabilities by focusing on real-world exploitability and business impact, rather than simply reacting to scanner results.

Think like an attacker

Threat actors don't see vulnerabilities in isolation. They look for paths—ways to chain weaknesses together to gain access, escalate privileges, and execute their attacks. By revealing these points of weakness, exposure management helps security teams uncover high-risk combinations, such as:

- Weak identity controls on mission-critical systems
- Unrestricted or unnecessary access to sensitive data
- Unmonitored external-facing applications

Rapid7 Exposure Command delivers comprehensive vulnerability findings, and enriches them with threat-aware risk scores that combine threat intelligence, system telemetry, and business impact to reveal which exposures are most likely to compromise critical parts of your enterprise. This all-in-one approach empowers organizations to make informed, confident security decisions—before an attacker does.

> "Security operations managers should go beyond vulnerability management and build a continuous threat exposure management program to more effectively scope and remediate exposures."
>
> **Gartner®, 2024[2]**

[2]Gartner, *How to Grow Vulnerability Management Into Exposure Management,* Mitchell Schneider, Jeremy D'Hoinne, Jonathan Nunez, Craig Lawson, 8 November 2024

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.

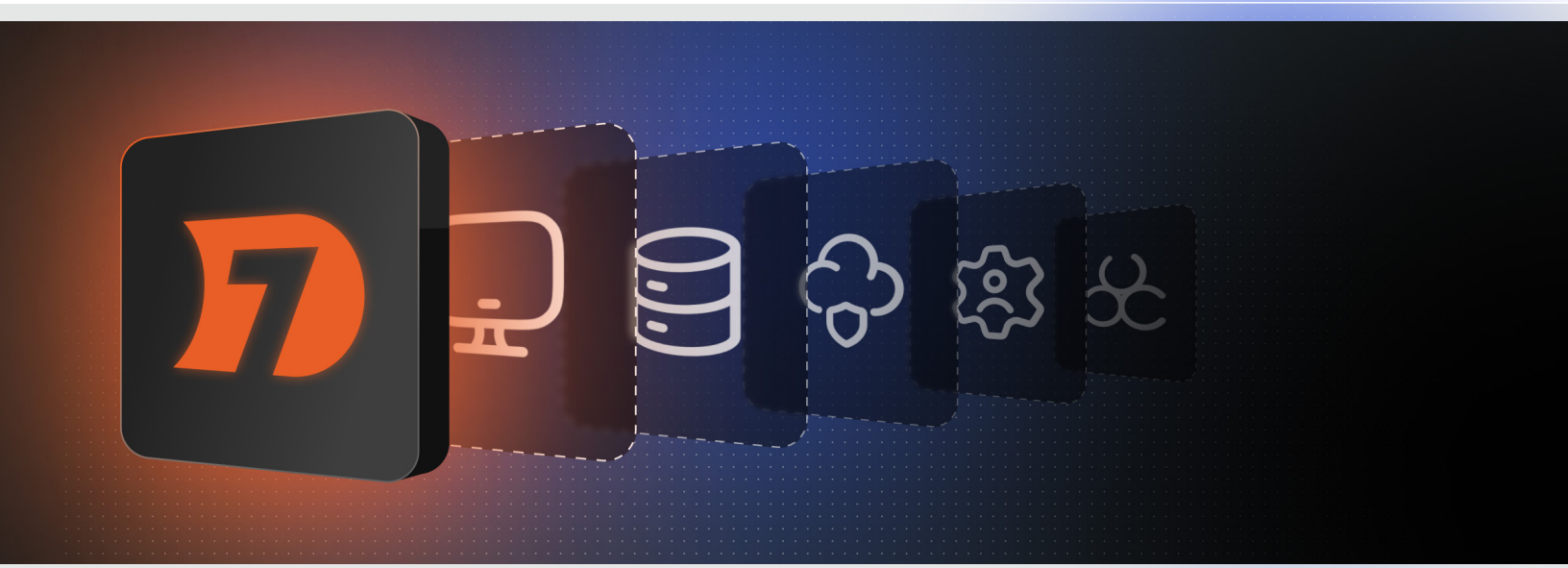
Building resilience through unified exposure management

Security resilience today is measured by how quickly an organization can identify risk, understand its impact, and act with precision. Unified exposure management unlocks this by combining visibility, context, and remediation into a single, streamlined workflow. It's no longer about reacting to alerts; it's about building a proactive, sustainable process for managing exposure at scale.

Survey data from the 2025 Take Command Summit reveals the top challenges security teams face in exposure management: 53% struggle with identifying unknown assets, while 40% find prioritizing vulnerabilities difficult. These gaps directly impact remediation speed and risk reduction

Complete, real-time visibility

Traditional tools often specialize in a single domain—whether endpoint, cloud, or identity—but they rarely communicate or share insights across systems. The resulting gaps in coverage, incomplete asset inventories, and overlooked risks have created an inflection point for security teams: continue investing in point security solutions or standardize on an exposure management platform that delivers a holistic view of their environment.



Exposure Command provides an integrated lens across the full technology stack. It combines critical insights, such as endpoint activity and identity access logs, with external signals like domain and port scans. This dual view gives teams a high-fidelity understanding of their attack surface, including:

- Known and unknown assets across cloud, on-prem, and SaaS
- External-facing infrastructure like APIs, IPs, and domains
- User accounts and authentication protocols
- Infrastructure misconfigurations and policy gaps

Even with identity and access management tools in place, many organizations still lack visibility into how user accounts actually map to systems and assets across their environment. According to Verizon's 2025 Data Breach Investigations Report, 46% of systems compromised by infostealers that included corporate credentials were non-managed devices, highlighting how frequently identity-related exposures fall outside of IT's control. Without unified visibility, security teams can't assess which users have access to critical endpoints—or how that access might be exploited. Unified exposure management brings these signals together to reveal overprivileged accounts, misconfigured identities, and high-risk access paths that legacy tools often miss.

With this advanced level of continuous visibility, organizations eliminate the dark corners of their IT estate and stay ahead of both accidental oversights and deliberate threats.

46% of systems compromised by infostealers that included corporate credentials were non-managed devices

VERIZON, 2025 DATA BREACH INVESTIGATIONS REPORT

Context that drives action

Discovering a vulnerability is only the beginning. The real challenge lies in understanding what the risk means to the business—and what to do about it. Legacy systems tend to rank threats using severity scores alone, but that ignores exploitability, business impact, or likelihood of attack.

Exposure Command applies a risk-first approach by layering multiple dimensions of context onto every finding. For example, a known vulnerability might appear in two systems, but only one has administrative access to a payment processing server. That's the one that should be fixed first. Security teams can focus on exposures that truly matter by incorporating factors, such as:

- **Active exploitation in the wild**
- **Reachability and lateral movement paths**
- **Identity and authentication exposure**
- **Business criticality of the asset**

Instead of chasing down hundreds of CVEs, modern security teams prioritize the few that have real breach potential—and allocate time and resources accordingly.

> "Many security operations managers focus too much on discovering issues without evaluating their impact on the business."
>
> **Gartner, 2024[3]**

[3]Gartner, *How to Grow Vulnerability Management Into Exposure Management*, Mitchell Schneider, Jeremy D'Hoinne, Jonathan Nunez, Craig Lawson, 8 November 2024

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.

KEY TAKEAWAY

Not all vulnerabilities are equal.

Prioritizing risk without attacker context leads to wasted time and unresolved threats. Unified exposure management helps focus teams on what matters most.

Seamless, scalable remediation

Once prioritized, the final challenge is efficiently remediating risk. Many organizations rely on manual handoffs between security, IT, and DevOps teams, often using email threads or disconnected ticketing queues. This time-consuming, often chaotic process, is an opportunity for attackers, and a growing risk for the business.

Exposure Command addresses this with a centralized remediation hub designed for scale. Teams can assign, track, and close exposures with the same platform they use to detect them. With over 290 out-of-the-box integrations, remediation can happen directly within the tools teams already use, including ServiceNow, Jira, Microsoft Teams, or Slack. Key capabilities include:

- Automated task creation with built-in SLAs and deadlines
- Role-based assignment and escalation workflows
- Grouping of exposures by root cause to enable “act once, fix many”
- Audit trails for tracking completion and accountability

Rather than patching in isolation, teams now operate with shared awareness, predictable timelines, and clearly defined responsibilities.

> “By 2027, 75% of organizations will restructure security operations to support exposure management as a primary function.””
>
> **Gartner, 2024[4]**

Strategic benefits of a unified approach

Adopting unified exposure management is not just a tactical improvement—it delivers long-term strategic value across the business. By aligning security with business risk, optimizing team performance, and improving regulatory posture, organizations move beyond reactive firefighting and toward sustained resilience.

[4]Gartner, Top Trends in Cybersecurity for 2025, Richard Addiscott et al., 12 December 2024

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.

Efficiency, ROI, and team empowerment

Traditional exposure management is resource intensive. It demands time-consuming correlation, prioritization guesswork, and repeated back-and-forth across teams. This manual burden increases operational costs and reduces the impact of skilled security staff. By unifying visibility, risk context, and response into one workflow, Exposure Command:

- Reduces investigation time and analyst fatigue
- Enables faster time-to-remediation with higher precision
- Maximizes existing investments in security tools through integration
- Helps reduce duplicate work between security, IT, and cloud teams

In practical terms, this means security leaders can do more with the resources they have, reduce burnout, and create space for more strategic initiatives like threat modeling, automation, and red teaming.

KEY TAKEAWAY

Security doesn't scale through headcount alone.

Organizations that unify visibility, context, and remediation free up teams to focus on strategic work—not just ticket triage

Compliance and audit readiness

With new and evolving regulatory requirements such as the SEC's cybersecurity disclosure rules and expanded global data protection laws, organizations must now demonstrate control over risk exposure and remediation practices. Unified exposure management supports compliance efforts by:

- Providing a continuously updated inventory of assets and exposures
- Documenting risk scores, remediation efforts, and resolution timelines
- Supporting real-time dashboards for board-level and audit reporting
- Offering evidence trails that align to frameworks like NIST, ISO 27001, and SOC 2



These capabilities not only reduce audit overhead but also position security teams as strategic enablers of trust, transparency, and due diligence.

Cross-functional alignment

One of the most underappreciated benefits of a unified approach is how it fosters collaboration. Traditional security processes often operate in silos, with limited visibility across IT operations, DevOps, and compliance teams. This fragmentation can lead to delays, duplicated work, and unresolved gaps.

With a shared platform, everyone involved in managing risk—security analysts, system administrators, application owners, and even business stakeholders—works from the same data set. Exposure Command acts as the single source of truth that drives alignment by integrating seamlessly into existing workflows and facilitating communication across the entire risk lifecycle.

The result is a more agile, coordinated response to threats, along with greater transparency and accountability across teams.

> “Organizations typically have 25 to 49 different security tools that often operate in isolation.”
>
> **Gartner, 2024[5]**

[5]Gartner, Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson, 8 April 2021 (For Gartner subscribers only)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.

RAPID7 CUSTOMER STORY

AMERICOR POWERS A UNIFIED APPROACH TO RISK REDUCTION



Challenge

Americor, an A+ rated debt relief company, was navigating rapid growth, acquisitions, and new market expansion. At the time, its security operations were rudimentary, relying on an MSSP and a fragmented toolset to manage vulnerabilities, cloud security, and external threats. “Over time,” recalled fractional CISO Daniel Akiva, “it became clear we weren’t getting the depth of coverage or the necessary level of collaboration with DevOps and IT.” Manual reconciliation across tools slowed down remediation and introduced blind spots across their hybrid, multi-cloud environment. Leadership wanted greater visibility and integration—while also reducing security spend by 15%.

Solution

Akiva brought security in-house and overhauled the company's toolset and structure. Americor standardized on Rapid7 for its breadth, depth, and ability to centralize telemetry across infrastructure, cloud, and SaaS environments. "We wanted more than just tools," he said. "We wanted a partner that could move at our speed and do most of the manual work for us, that way our time can be better spent driving true outcomes and reflecting to leadership what our attack surface is comprised of, identify and confirm with them what is accepted risk, and how we are reducing exposures that fall outside of our organization's established risk appetite." With Exposure Command and 24/7 MDR monitoring, the team prioritized threats based on real-world risk, not just triggered alerts.

> Rapid7's Exposure Command helps tie together our previously fragmented attack surface and define what it truly is, what our assets are comprised of and the existing vulnerabilities/gaps in coverage to take action on it."
>
> **Daniel Akiva, Fractional CISO, Americor**

Impact

Americor quickly gained visibility into its multi-cloud environments, identified misconfigurations, surfaced unauthorized access patterns, and uncovered gaps that had previously gone undetected. "We're now getting up-to-date understanding on vulnerabilities, and have the right platform that gives us the tangible evidence and justification to drive the necessary change and evolve," Akiva said. Security is now a core partner to IT, DevOps, legal, and compliance—breaking down silos and enabling coordinated response. "We're not just reacting anymore. We're building ahead of the business. That's where security belongs." Americor reduced costs, hired three full-time security employees, and now operates with transparency, expert SOC support, and pricing predictability—all on a unified platform that scales with the business.

Actionable recommendations for security leaders

When asked about their top priorities for improving detection and response, 64% of 2025 Take Command Summit attendees pointed to exposure management—reinforcing its growing role as a foundational security capability. If you're considering a move toward unified exposure management, the following steps can help set your organization on the right path:

1. MAP YOUR REAL ATTACK SURFACE

Start with a complete asset inventory, then go further. Use internal telemetry and external scans to uncover:

- Shadow IT, unmanaged cloud assets, and third-party integrations
- Risky user accounts with weak or missing MFA
- External-facing services or APIs that may be overlooked

Build a dynamic, continuously updated map of what's exposed —both inside and outside your perimeter.

2. RETHINK HOW YOU PRIORITIZE TASKS

Move beyond CVSS-based prioritization. Instead, assess each exposure based on:

- Whether it's actively exploited in the wild
- The sensitivity and role of the affected system
- The presence of compensating control
- Its potential role in an attacker's path to a critical asset

This contextual approach dramatically improves efficiency and reduces remediation of low-impact issues.

3. BUILD THE CASE FOR UNIFICATION

Create internal momentum by highlighting inefficiencies in your current process. Quantify:

- Manual hours spent triaging vulnerabilities
- Inconsistent or siloed visibility across tools
- Audit and compliance challenges

Then model the projected impact of a unified platform—faster MTTR, fewer missed risks, clearer reporting.

4. ALIGN YOUR KPIS WITH RISK AND BUSINESS VALUE

Track metrics that reflect progress against real threats and organizational goals. These might include:

- Mean time to risk mitigation (MTTR)
- Percentage of critical exposures resolved within SLA
- Disruption of attacker paths or lateral movement
- Risk reduction by business unit, geography, or cloud provider

The more closely your metrics align with impact, the more compelling your security narrative becomes[6].

5. MATURE INTO CONTINUOUS THREAT EXPOSURE MANAGEMENT

Unified exposure management lays the foundation for continuous threat exposure management (CTEM). Once you have established unified visibility and prioritized response, consider:

- Regular threat simulation and adversary emulation
- Scenario-based exposure testing (e.g., ransomware, insider threats)
- Tighter integration with offensive security and incident response
- Trend reporting and exposure heat maps for executive planning

According to Gartner, by 2026, organizations that prioritize CTEM programs will be three times less likely to experience a breach than those that do not. We believe this underscores the strategic value of exposure management as a driver of measurable, long-term security outcomes.

[6]Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, 11 October 2023 (For Gartner subscribers only)

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.

Clarity, confidence, control

"Cyber resilience embraces a 'when, not if' mentality, and seeks to minimize the impact of cyber incidents on the enterprise and enhance adaptability, rather than engage in misguided notions of outright prevention."Gartner, 2024[7]

Security teams don't need more dashboards. They need more decisions—driven by real risk, not just raw data.

COMMAND IS... EXPOSING YOUR RISKS NOT YOUR ASSETS

Unified exposure management isn't a trend—it's a strategic imperative. It moves beyond visibility to help organizations actually reduce risk at scale. And with Rapid7's Exposure Command, security leaders finally have a platform built for the complexity of modern environments and the urgency of today's threats.

With Rapid7 Exposure Command, organizations gain the control they need to manage risk with purpose, precision, and measurable results.

KEY TAKEAWAY

Visibility is the beginning. Command is how you win.

With unified exposure management, CISOs gain measurable control over risk, enabling smarter decisions, faster action, and stronger collaboration.

[7]Gartner, *Top Trends in Cybersecurity for 2025*, Richard Addiscott et al., 12 December 2024

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

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**

© RAPID7 2025 V1.0