CHECK POINT

EXPOSURE MANAGEMENT

State of Exposure Management From Intelligence to Preemptive Action

Why Exposure Management's Moment Is Now

January 2026

Table of Contents

Executive Summary

Organizations already see more threats, vulnerabilities, and misconfigurations than ever before. What has changed is how quickly attackers operationalize them and how slowly most organizations can safely respond.

Attackers now move from discovery to exploitation in hours, while security teams still require days or weeks to coordinate analysis, prioritization, validation, and remediation across siloed tools and teams. At the same time, operational risk has increased: remediation actions themselves can disrupt business, causing teams to hesitate or delay.

The data makes the gap clear when a Continuous Threat Exposure Management (CTEM) model is implemented:

701M+
new threat intelligence items identified in a single year, 5,700+ new threat intelligence sources

13,333
exposures identified per organization annually

Only **50%**
of exposures remediated each year

3.5
Day average MTTR

6B
attacks blocked in one year

The market is adopting Exposure Management and evolving from finding and prioritizing risk to safely reducing it. This requires combining threat intelligence, contextual exposure analysis, and validated remediation into a single, continuous operational flow so that exposure dwell time is reduced without disrupting the business.

This is why Exposure Management has emerged now.

Not to surface more dashboards, but to turn intelligence into prioritized, validated, and safe action, reducing exposure before attackers exploit it.

The Exposure Explosion

The exposure problem is no longer about scale, it's about control. Security teams are operating in an environment that no longer behaves like the one their programs were designed for.

Attack surfaces expand continuously. Infrastructure changes hourly. Threat Actors reuse, adapt, and weaponize exposures at machine speed. It's not just more threats, it's a disconnect between how fast risk appears and how fast organizations can eliminate it.

701M+

new threat intelligence items in 2025 across 5,700+ new threat intelligence sources

3.7B

websites & files inspected daily

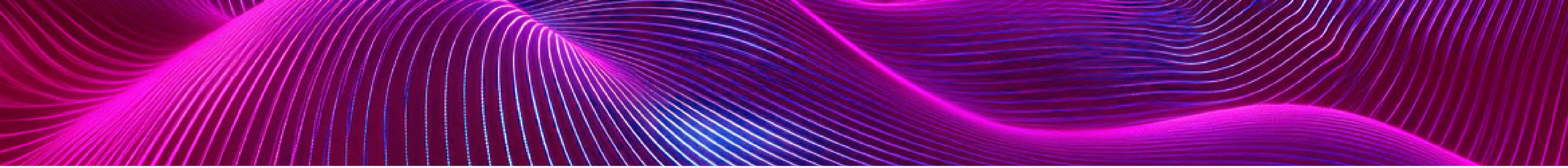
Across global environments, hundreds of millions of new threat intelligence signals emerge every year. Billions of digital assets are inspected daily. Millions of malicious indicators surface every 24 hours. This volume is not random. It is the new baseline.

The implication for security leadership is clear:
Human-scale processes cannot keep up with machine-scale exposure.

This is the context in which Exposure Management emerges, as a necessary evolution in how organizations reduce risk.

1.7M

malicious indicators detected every day



Visibility Won. Control Didn't

Scan more. Detect more. Score everything. That strategy succeeded… and then it didn't.

Modern organizations identify thousands of exposures per year, yet a significant portion never translate into meaningful risk reduction. Lists grow. Dashboards multiply. Severity scores fluctuate. Meanwhile, the same classes of breaches repeat.

The problem is no longer a lack of insight. It is an inability to convert findings into decisive, confident action.

1,112

monthly exposures found per organization

133K

false positives detected

36.8M

New malware logs detected in 2025

Legacy vulnerability management, risk-based prioritization, and siloed attack surface monitoring approaches all share a common of optimizing for discovery, not outcomes. As a result:

- Teams chase issues that never become exploitable
- Real risk hides among false positives and stale findings
- Exposure accumulates faster than it is retired

In 2025 seeing more did not make organizations safer. Acting too slowly made them vulnerable.

The Action Gap

Even when organizations know what is at risk, taking action comes to a halt.

Remediation still depends on manual coordination across siloed teams. Infrastructure owners hesitate to change production systems without confidence. Security teams lack proof that fixes will not disrupt the business. Ownership becomes liability. Accountability fades.

MTTR averages

3.5 days while attackers move in hours

More than 80%

of enterprises experience operational disruption

The result is exposure dwell time which is the period when known weaknesses remain open, reachable, and exploitable.

While attackers adapt in hours, remediation often stretches into days or weeks. And despite enormous effort, only a fraction of exposures are actually closed each year.

This gap is not caused by a lack of tools or talent. It is caused by the absence of a safe, validated path from exposure to action.

Until remediation becomes as routine as detection, risk will continue to outpace response.

50%

of exposures remediated annually

Intelligence Without Action Is Noise

Collecting high-fidelity threat intelligence is not easy—it is increasingly complex and adversarial.

Collecting high-fidelity threat intelligence today requires operating inside environments deliberately designed to evade detection. Threat actors actively control access to forums and marketplaces, rotate identities, shift geographies, and obfuscate activity across closed platforms. Intelligence collection now depends on advanced image and text recognition, language and behavioral analysis, and continuous adaptation to adversary countermeasures.
Yet even when intelligence is successfully collected, most organizations struggle to operationalize it. Intelligence remains disconnected from internal exposure context and security controls, turning valuable insight into static reports rather than timely, preventative action.

Putting it into context and operationalizing is also not easy. Millions of indicators, sources, and signals flood security teams every month. But intelligence only creates value when it changes priorities and accelerates action.

High-fidelity intelligence does something fundamentally different:

- It distinguishes active exploitation from theoretical risk
- It connects threat actor behavior to an organization's actual exposure
- It reduces noise by proving what is at risk now

When intelligence is validated, contextual, and tied directly to exposure, it becomes a decision engine, not a reporting function. In this framework, intelligence does not inform dashboards. It drives remediation, takedowns, brand protection and preemptive enforcement.

59M
intelligence items collected per month

20K+
takedowns executed annually

93%
true-positive alerts

98–99%
takedown success rates (Impersonations/ Social/Phishing)

From Exposure to Preemptive Action

Exposure Management reaches its turning point when organizations stop asking what should we fix and start asking how do we mitigate this safely, right now, with the security tools I have in place.

From reactive remediation to preemptive action:

- Validate fixes before enforcement
- Prefer compensating controls when patching is risky
- Automate response where confidence exists
- Enforce consistently across the environment

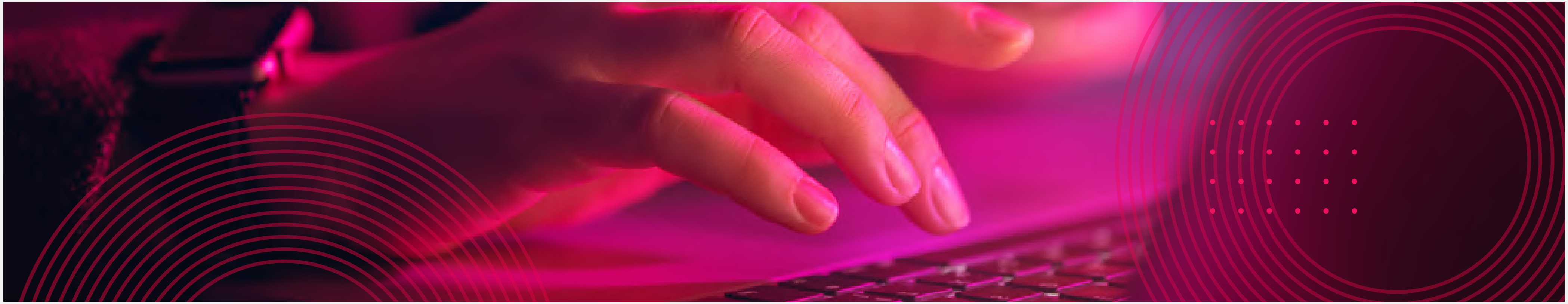
Safe remediation changes the equation. It removes fear from action. It accelerates decision making. It allows organizations to reduce exposure before attackers exploit it, not after damage is done.

This is where exposure stops being a vague risk metric and becomes an operational discipline with measurable impact.

60 remediation actions performed every time users access the platform

504 safe remediations per month

6B attacks blocked in one year

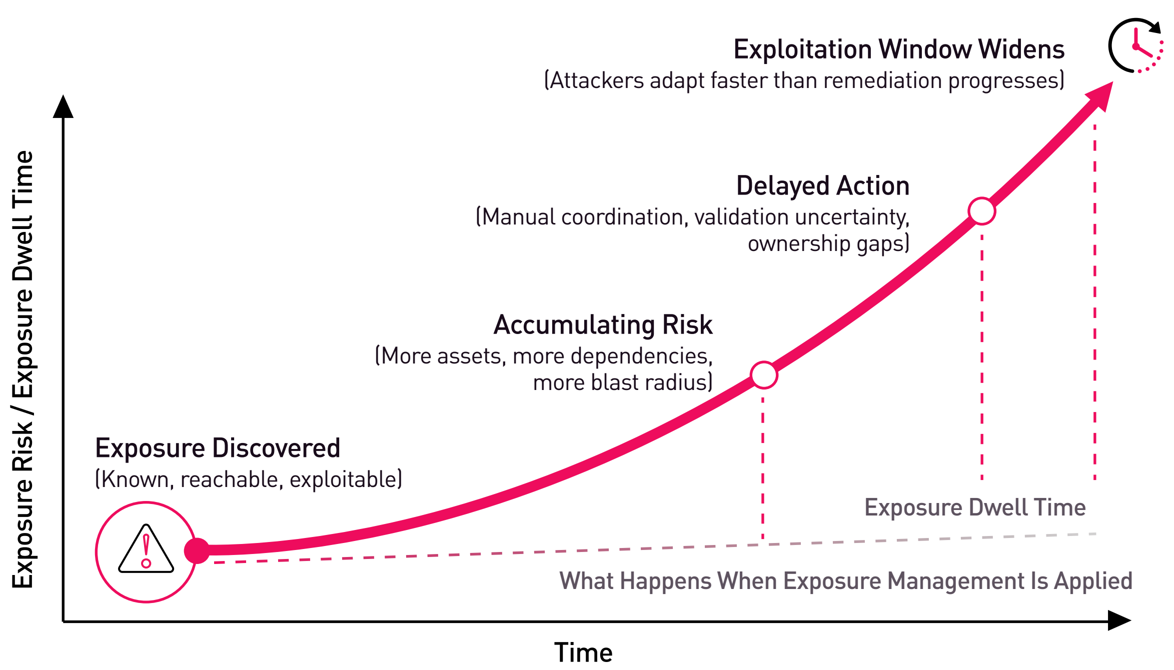


Why Security Teams Hesitate to Fix What They Find

Patching, configuration changes, and security control hardening can introduce outages, performance degradation, or business disruption. Validating the safety of a fix often requires more coordination and testing than identifying the exposure itself.

- Teams hesitate to act without confidence the change is safe
- Fixes are delayed, batched, or deferred
- Exposure dwell time increases even when risk is well understood

To reduce exposure at the speed of attack, remediation must be validated, contextual, and reversible. Fixes must account for existing controls, business impact, and operational risk before enforcement, not after.



Exploitation Window Widens
(Attackers adapt faster than remediation progresses)
Delayed Action
(Manual coordination, validation uncertainty, ownership gaps)
Accumulating Risk
(More assets, more dependencies, more blast radius)
Exposure Discovered
(Known, reachable, exploitable)
Exposure Dwell Time
What Happens When Exposure Management Is Applied
Exposure Risk / Exposure Dwell Time
Time

When No Action Is Taken, Risk Only Moves in One Direction

The Business Impact of Getting This Right

When exposure is managed continuously and preemptively, the benefits extend well beyond security operations.

Organizations reduce disruption.
Teams reclaim time lost to manual efforts.
Costs associated with incidents, downtime, and external response shrink measurably.

Most importantly, leadership gains confidence, confidence that known risks are being reduced, not merely tracked.

Exposure Management reframes security from a cost center into a resilience function:

- Fewer emergency changes
- Faster containment of external threats
- Predictable, auditable risk reduction

This is the language boards understand and increasingly expect.

$270K

average annual cost savings

1,200

business days of labor saved per year

21-22-hour

average takedown MTTR (Impersonations/Social/Phishing)

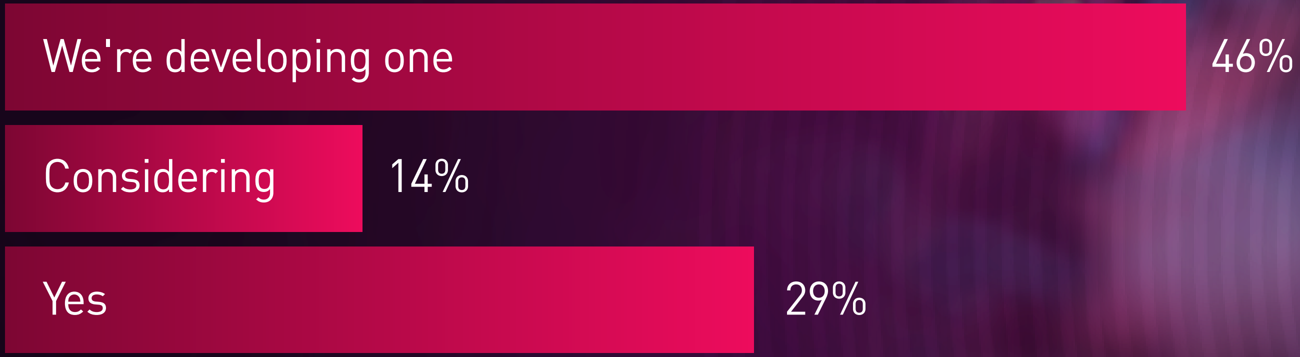
You Are Not Alone

This is the top-of-mind topic for most organizations

Gartner Peer Connect Survey:

89% have or plan a CTEM Implementation

% of Respondents



> Organizations that prioritize based on a continuous exposure management program will be **3x less likely to suffer a breach**

> Organizations use an average of 45 cybersecurity tools, yet many struggle to correlate findings into **actionable intelligence**

Analyst Perspective

Industry analysts are converging on the same conclusion:

Modern exposure programs must connect intelligence, prioritization, validation, and remediation into a continuous cycle focused on outcomes. Assessment only approaches stall without remediation. Siloed ownership delays action. Static SLAs ignore real risk.

The market is now rewarding platforms and programs that:

- Reduce exposure dwell time
- Mobilize fixes across teams
- Validate remediation before disruption occurs

IDC

"Many organizations still make critical decisions based on incomplete or under-refined threat data"

-The Evolution of Threat Intelligence Is Unified Cyber Risk Intelligence (15 September 2025, ID G00825638).

FORRESTER®

"Despite visibility gains, remediation remains the persistent challenge."

-Forrester, Unified Vulnerability Management Landscape. 2025.

Gartner®

"By 2028, organizations that have implemented continuous threat exposure management with special focus on mobilization, across business units, will see at least a 50% reduction in successful cyberattacks."

Gartner, Emerging Tech: Exposure Management Must Shift From Detection to Remediation. 2025.

The Path Forward

Exposure Management is not about seeing more. It is about turning intelligence into action, safely, continuously, and before attackers do. Organizations that succeed will:

- Know which exposures are being weaponized
- Act with confidence
- Reduce risk faster than adversaries can exploit it

The moment is now. The gap is clear. The path forward is actionable. Start building your Exposure Management roadmap.

First 30 Days	Days 30-60	Days 60-90	Download The Ebook
Establish clarity and alignment	**Prioritize and validate**	**Operationalize remediation**	
A clear understanding of what needs protection, how it will be measured, and who is responsible.	A working exposure prioritization model and the beginnings of safe, predictable remediation workflows.	A functioning exposure management program where exposures consistently move from discovery to closure with transparency and accountability.	

Contact Us

ISRAEL
Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA
Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE
Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES
Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND
Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN
Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management