An IDC Spotlight, sponsored by CheckPoint
January 2026

# Beyond Discovery: Achieving Risk Reduction Through Exposure Remediation Based on Targeted and Tactical Threat Intelligence

Michelle Abraham
Senior Research Director, IDC

IDC

**SPOTLIGHT**

*Sponsored by: Check Point Software*

**Modern exposure management connects threat intelligence and remediation workflows to address the most exploitable risks, shifting toward continuous, outcome-driven security that emphasizes remediation and validation over static vulnerability reporting.**

# Beyond Discovery: Achieving Risk Reduction Through Exposure Remediation Based on Targeted and Tactical Threat Intelligence

*January 2026*

**Written by:** Michelle Abraham, Senior Research Director

## I. Introduction

Exposure management is rapidly evolving from a siloed, discovery-focused discipline into a unified approach that integrates vulnerability management, configuration management, and real-time threat intelligence.

Historically, organizations concentrated on scanning their IT assets for vulnerabilities; findings were prioritized for remediation based on vulnerability severity, asset context, and vulnerability exploitation. However, the complexity of modern IT landscapes and the speed at which attackers operate have exposed the limitations of traditional methods, driving the need for more dynamic and context-aware solutions.

A key advancement in exposure management is the incorporation of threat intelligence into exposure-based decision-making. Prioritization now extends beyond static severity scores to focus remediation efforts on exposures most likely to be targeted. This intelligence-driven approach ensures that resources are allocated efficiently and that the most pressing risks are addressed before they can be exploited.

The remediation process itself is increasingly recognized as the critical outcome that reduces risk. Vulnerability management teams typically identify exposures but lack direct control over remediation, while those responsible for fixing issues may not have the necessary context to prioritize or understand the urgency of their actions. This disconnect can delay remediation and leave organizations exposed to fast-moving threats, as attackers actively scan for exploitable weaknesses.

## AT A GLANCE

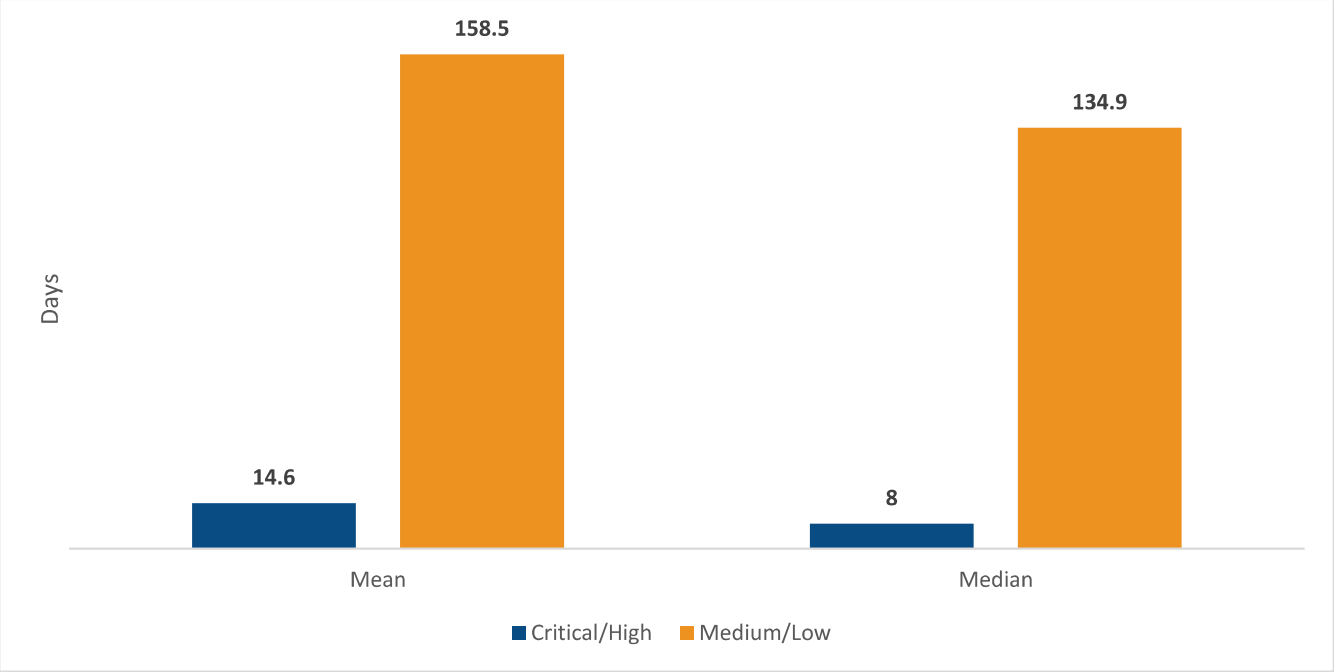
### KEY TAKEAWAYS

- Exposure management is shifting from "finding" exposures to proven risk reduction outcomes. Mitigation options such as compensating controls/virtual patching and control hardening provide solutions to long patching timelines.
- Threat intelligence improves prioritization by adding exploit context and targeting patterns beyond severity scoring.

IDC research shows that even critical and high vulnerabilities take, on average, eight days to patch. With attackers continuously scanning, looking for weaknesses, patching needs to accelerate — from days to hours.

FIGURE 1: ***Mean Time to Patch Leaves Plenty of Time for Attackers***

***Q On average, what is your organization's mean time to patch/mitigate/remediate vulnerabilities discovered by your vulnerability management platform?***




Source: IDC's *Exposure Management Survey*, March 2025 (n = 1,020)

While exposure management solutions provide remediation guidance, organizations have often relied on external ticketing systems or automation tools to execute fixes. This separation between discovery and remediation can create gaps in accountability and visibility, especially when multiple teams are involved. Establishing a feedback loop between these teams is essential to confirm that exposures are resolved and to continuously improve response processes. Exposure management is also bridging the gap between vulnerability management and configuration management, providing a more holistic view of risk. These risks are not just Common Vulnerabilities and Exposures (CVEs) but also gaps in security defenses where tools are not delivering the protection of which they are capable.

Ultimately, the evolution of exposure management is characterized by greater integration, intelligence, and operational alignment. By combining comprehensive discovery, contextual prioritization, and effective remediation workflows, organizations can move beyond simply cataloging risks to actively reducing their attack surface and improving their overall security posture.

## II. Definitions

The attack surface in vulnerability/exposure management is the sum of all points in an organization's IT environment, such as assets, interfaces, and services that are exposed and could be exploited by attackers.

Exposure management is the continuous process of identifying, assessing, and prioritizing security risks across an organization's digital assets, focusing on those that are accessible and potentially exploitable by threat actors. It enables organizations to proactively reduce risk by remediating vulnerabilities and misconfigurations before they can be leveraged in an attack.

Digital risk protection is the practice of proactively monitoring and responding to threats across the internet and dark web to include data breaches, brand impersonation, phishing, and credential leaks. The solution safeguards an organization's digital assets, reputation, and sensitive information with an external view.

## III. Benefits

There are multiple benefits to the addition of distinct types of threat intelligence into exposure management solutions:

- Strategic intelligence for analysis of attacker profiles, their methods, exploited exposures, and targeted organizations, enabling proactive defense planning.
- Targeted intelligence — such as leaked credentials, exposed data, dark web chatter, and brand impersonation — for identification and remediation specific threats before they impact the organization.
- Tactical intelligence, including real-time indicators of compromise (IoCs), for blocking malicious domains and responding to active attack campaigns targeting the organization or its industry vertical.

Threat intelligence also enables detection of ongoing threat actor campaigns, such as phishing or credential harvesting, that specifically target the organization, supporting timely mitigation. It helps prioritize exposures more accurately by providing context about which exploits and targets are actively being used.

Digital risk protection and dark web monitoring extend visibility beyond the organization's perimeter, addressing external threats and data leaks. It can provide alerts on reputational exposures and leaked credentials, reducing the risk of brand damage and unauthorized access. These external signals are also used as context in the prioritization of exposures.

Built-in remediation streamlines the management of large volumes of findings, allowing security teams to prioritize actionable risks and avoid being overwhelmed by noise; thus allowing them to focus resources on the most critical risks to the organization. Security teams can reduce the amount of time needed to mitigate exposures with the use of safe, agentless compensating controls and control hardening when immediate patching is not possible.

Overall, exposure management ensures that security tools and processes are functioning as intended, identifying and closing gaps in defenses to maintain a consistent protection level. Solutions establish measurable improvements in risk posture, providing leadership with confidence that security investments and actions are effectively reducing exposure. Security teams demonstrate accountability with validation that mitigations were applied successfully and tracking of re-exposures caused by posture drift.

## IV. Trends

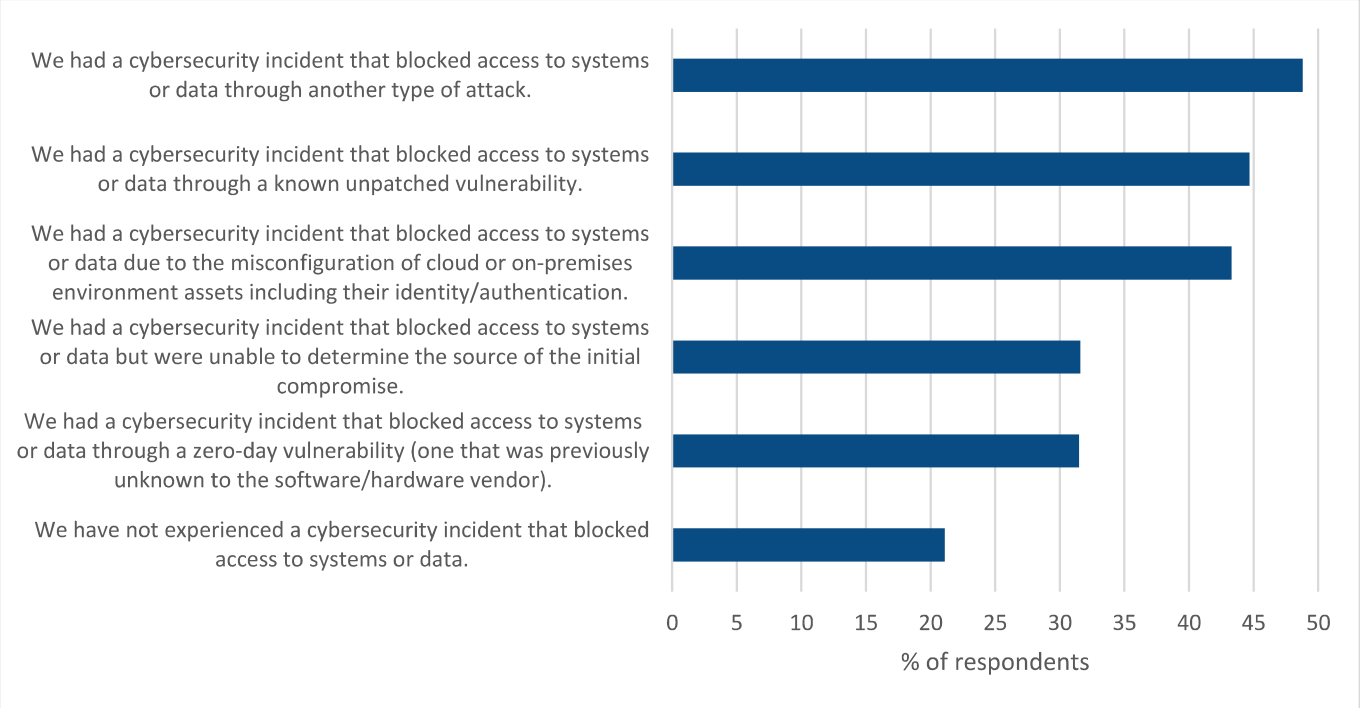
The number of published CVEs continues to rise sharply, up by 22% through the first three quarters of 2025 over the same period in 2024, overwhelming traditional scan-and-patch cycles and requiring more advanced prioritization and automation.

Organizations face a proliferation of entry points, including cloud, software as a service (SaaS), Internet of Things (IoT)/OT, and third-party integrations, making siloed risk evaluation insufficient and driving demand for holistic exposure management. Organizations still struggle to discover and manage unknown or unmanaged assets, leaving blind spots in their security posture. With an average of 49 security tools in each organization, there are many sources of vulnerability, misconfiguration, and other exposure findings.

While phishing and social engineering are top attack vectors for cyberattacks, unpatched vulnerabilities and misconfigurations have resulted in cybersecurity incidents for more than 40% of respondents in the last 12 months. Organizations need to improve their mean time to patch and, if patching is not an option, use compensating controls to mitigate the exposure until a permanent solution is found.

FIGURE 2. ***Unpatched Vulnerabilities and Misconfigurations Are Leading Causes of Cyber Incidents***

***Q Which of the following applies to your organization regarding cybersecurity incidents that blocked access to systems or data in the last 12 months due to vulnerabilities?***




Source: IDC's *Exposure Management Survey*, March 2025 (n = 1,020)

The elements that determined reasonable cybersecurity a few years ago are no longer sufficient. New regulations (e.g., NIS2, DORA) and cyber-insurance requirements are raising the bar for continuous, demonstrable risk reduction. Threat actors are leveraging AI to accelerate exploit development and vulnerability discovery, while security vendors are integrating AI and generative AI(GenAI) for asset classification, ownership inference, and automated remediation workflows. The pace of change is accelerating on both fronts, requiring organizations to look for solutions that are at the forefront of exposure management and all that it entails.

## V. Vendor Profile

Check Point is extending its exposure management approach by aligning exposure signals, threat intelligence, and remediation with preventive controls across hybrid environments. Rather than focusing only on discovery and prioritization, the approach emphasizes operationalizing exposure decisions to accelerate time-to-mitigation for high-risk conditions and improve evidence of risk reduction over time. Exposure management has been added as a fourth pillar to Check Point's portfolio, alongside network security and connectivity protection, workspace security (which covers security for the browser, mobile device, and endpoint), and AI security. The pillars include both internally developed capabilities and recent acquisitions.

The exposure management solution is augmented with Check Point's threat intelligence to provide richer context about external threat activity and its relevance to internal vulnerabilities. The intent is to help security teams understand not only where exposures exist, but also who is exploiting them, how they are being exploited, and what evidence supports these conclusions. This context is designed to support more informed prioritization and response decisions based on real-world threat activity rather than theoretical risk.

Cross-layer integration and action execution are core elements of the platform. It is designed to ingest exposure signals from heterogeneous tools and environments and translate prioritized exposure decisions into mitigation actions through existing enforcement points across network, cloud, and workspace or endpoint security layers. This supports a control-aware workflow in which prioritization accounts for both risk context and existing defensive coverage, helping teams determine when patching is required versus when compensating controls or alternative mitigations are more appropriate.

The solution leverages real-time telemetry from millions of deployed Check Point firewalls globally. This telemetry is correlated and analyzed within Check Point's threat intelligence framework to assess the prevalence, sophistication, and activity level of threats targeting specific vulnerabilities or attack techniques. Vulnerability and exposure data is sourced from third-party scanning tools, enabling organizations to integrate existing vulnerability management investments without deploying additional agents on endpoints.

By enriching vulnerability data with threat intelligence, the platform enables prioritization based on observed exploitation. Organizations gain visibility into active attackers, the techniques they are using, and associated IoCs, which can be utilized directly within security controls to support prevention and response. Customers receive a private IoC feed tailored to their environment, enriched by anonymized intelligence from the broader customer base.

The solution is designed to take existing security posture into account, including deployed network and endpoint protections. By understanding which controls are already in place, the platform helps organizations focus remediation efforts on remaining gaps and avoid redundant actions. This context supports more effective hardening of controls and prioritization based on both exposure severity and current defensive coverage.

Beyond vulnerability and configuration-related exposures, Check Point incorporates digital risk protection capabilities into the platform. This expands coverage to additional risk domains such as external-facing digital assets and potential brand or infrastructure abuse. Attack surface management functionality is included, with support for IPv6 scanning to improve visibility across modern network environments.

Remediation options extend beyond traditional patching. Actions can include takedown of malicious or abused domains, modification of network infrastructure settings (such as enabling intrusion prevention system protections) or adjustment of security posture for specific assets. Configuration changes are validated prior to execution to reduce operational risk. Check Point reports performing thousands of domain takedowns each month, many linked to attacker infrastructure identified through its intelligence analysis.

The platform also supports virtual patching by applying compensating controls that mitigate risk while permanent fixes are prepared. This approach is intended to provide flexibility for systems that cannot be immediately patched due to operational constraints, thus reducing exposure without introducing instability into critical systems.

Integration is a principal component of the solution. Check Point supports connectivity with a broad range of internal and third-party security tools, including firewalls, web application firewalls, SASE platforms, breach and attack simulation tools, attack surface management solutions, and endpoint detection and response products. These integrations enable automated or semi-automated actions such as isolating hosts, blocking traffic or removing malicious infrastructure. For patching workflows, integrations are available with tools such as BigFix, Intune, and NinjaOne, with the system identifying which exposures are suitable for virtual patching versus other remediation methods.

Granular controls are provided for defining adaptive network blocking policies. Each customer has access to a private exposure map that shows which assets and connections are protected or unprotected. Post-remediation validation is included to confirm that identified gaps have been closed. According to Check Point, the ability to act directly from the exposure management platform has significantly reduced mean time to respond. An AI-driven interface supports querying findings, understanding risk drivers, and receiving remediation guidance. The solution can be deployed on premises or as a SaaS offering, with managed services available for organizations requiring additional operational support.

### *Challenges*

- As Check Point expands capabilities through acquisitions and performs the necessary platform integration, the result must present a unified workflow and consistent model across use cases.
- Exposure management buyers may not immediately associate Check Point with this category, requiring clear messaging around use cases, outcomes, and differentiation.
- The market remains competitive. Solutions that demonstrate measurable risk reduction outcomes, especially through safe, coordinated remediation, are more likely to shine compared to solutions focused primarily on asset discovery and exposure prioritization.

## *VI. Conclusion*

Exposure management is no longer about identifying weaknesses in isolation, but about continuously reducing risk in an environment defined by scale, speed, and constant change. The convergence of vulnerability management, configuration

management, threat intelligence, and remediation reflects a broader shift toward operationally aligned security, where prioritization is driven by real-world attacker behavior and remediation is treated as the primary measure of success. As the volume of CVEs grows, traditional scan-and-patch models are proving insufficient. Modern exposure management addresses these challenges by providing contextualized prioritization and enabling faster mitigation through integrated workflows and compensating controls when immediate patching is not feasible.

Organizations need solutions that demonstrate continuous, measurable risk reduction, validate that controls are functioning as intended, and maintain visibility beyond their own perimeter to include digital risk and brand exposure. By unifying intelligence, automation, and accountability, these solutions help organizations move from reactive vulnerability management to a proactive, risk-based posture that can keep pace with evolving threats and regulatory demands.

# About the Analyst

***Michelle Abraham,*** *Senior Research Director*

Michelle Abraham is a senior research director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM), Exposure Management and Related Artificial Intelligence Technologies practice. Ms. Abraham's core research coverage includes SIEM platforms, exposure management platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device vulnerability management alongside AI-related security topics.

## MESSAGE FROM THE SPONSOR

As exposure management evolves toward intelligence-driven prioritization and measurable risk reduction, organizations are increasingly focused on closing the gap between identifying exposures and safely mitigating them. Effective exposure management requires not only comprehensive visibility across internal and external attack surfaces, but also the ability to operationalize threat intelligence, validate remediation actions, and reduce exposure dwell time without disrupting business operations.

Check Point Exposure Management is designed to support this model by integrating exposure signals, threat intelligence, and safe remediation across hybrid environments. By correlating real-world attacker activity with vulnerability, configuration, and control context, organizations can prioritize exposures based on exploitability and business impact and apply validated mitigation actions where patching is not immediately feasible.

Visit the website to learn more about Check Point Exposure Management:

https://www.checkpoint.com/exposure-management/

Curious about the benefits of Exposure Management? Download Check Point's report on the state of Exposure Management to help you assess your readiness:

https://checkpoint.cyberint.com/state-of-exposure-management

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com