CHECK POINT

EXPOSURE MANAGEMENT

UNDER PRESSURE

The 2026 Exposure Gap Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Attackers are moving faster across a larger and more complex exposure surface. In 2026, vulnerabilities more than doubled as a share of critical exposures, rising from 18.7% to 42.6%, while phishing website exposure grew from 1.0% to 10.5%. As automation and AI-assisted tools accelerate testing across systems, credentials, phishing infrastructure, and known weaknesses, traditional patch cycles and manual triage are struggling to keep pace. This is the exposure gap: the distance between visibility, prioritization, and safe remediation.

That gap is why exposure management cannot stop at visibility. As vulnerability-related risk grows, teams need a way to separate urgent, exploitable issues from the broader alert population.

Across the analyzed vulnerability alert population, only 7.8% warranted Critical or High attention after exploitability validation. More than 90% did not require the same immediate remediation focus. This is the value of Exposure Management: reducing a large alert population into a smaller, validated set of exploitable issues that security teams can prioritize with confidence.

Check Point Exposure Management helps close this gap by connecting discovery, evidence-based prioritization, exploitability validation, control assessment, and safe remediation in one workflow. The report shows faster remediation is achievable: Utilities led one-hour remediation at 30.0%, followed by Financial Services at 23.1%, Government at 14.3%, and Healthcare at 7.7%. Across the four industries, organizations acted on 85.9% of recommended fixes on average.

Exposure management is becoming a measure of operational readiness. Mature programs will be defined by how quickly they identify urgent exposures, validate risk, assess control coverage, apply fixes safely, and reduce exposure before attacker opportunity becomes business impact.

KEY METRICS

30% of Utilities organizations resolved critical exposures within one hour, the highest of any industry

42.6% Critical exposures identified as Vulnerabilities

76% of all critical exposures camefrom just two categories: vulnerabilities and internal information disclosure

7.8% Vulnerability alerts validated as Critical or High after exploitability testing

EXPOSURE SHIFT

18.7% to 42.6%

% of Critical Vulnerability Exposures more than doubled from 2025 to 2026

1.0% to 10.5%

Phishing Websites grew as a proportion of critical exposures from 2025 to 2026

56.8% to 33.3%

Internal Information Disclosure Critical Risk % declined but remained a leading exposure

INDUSTRY HIGHLIGHTS

78.2%
of critical exposures in Utilities were vulnerabilities

63.6%
of critical exposures in Healthcare were internal information disclosures

91.7%
of Financial Services organizations acted on recommended fixes

12.6 hours
fastest median time to remediation, achieved by Utilities organizations

10,155
average monthly remediations per Financial Services organization

WHY IS THERE AN EXPOSURE GAP?

Healthcare, Financial Services, Government, and Utilities showed distinct exposure patterns that help explain why remediation priorities differ by sector. Healthcare was led by Internal Information Disclosure, Financial Services showed a broader mix of exposure types, and Government and Utilities were primarily shaped by vulnerability related risk.

Closing this gap depends on three capabilities.

First, organizations need broad discovery across vulnerabilities, exposed information assets, phishing sites, impersonation campaigns, leaked credentials, and other external exposures. Gaps in discovery allow risk to remain invisible until it becomes operational.

Second, teams need accurate prioritization. Discovery creates volume, but not every alert deserves the same response. Security teams need to identify which exposures are exploitable, active, business relevant, and urgent.

Third, organizations need safe remediation. Exposure reduction requires more than creating a ticket. Teams need workflows that can validate changes, use existing controls, and reduce risk without disrupting production systems.

This report analyzes how organizations are performing across these stages. The findings show where critical exposure is concentrated, which alerts warrant immediate action, and how mature programs are reducing exposure through faster, safer remediation.

EXPOSURE

The Exposure Landscape

The 2026 exposure landscape was defined by concentration. Vulnerabilities became the largest source of critical exposure, while Internal Information Disclosure remained a major contributor across customer environments. Together, these two categories accounted for approximately 76% of all critical exposures, showing that risk was concentrated around exploitable weaknesses and exposed information assets.

The Critical Exposure Landscape

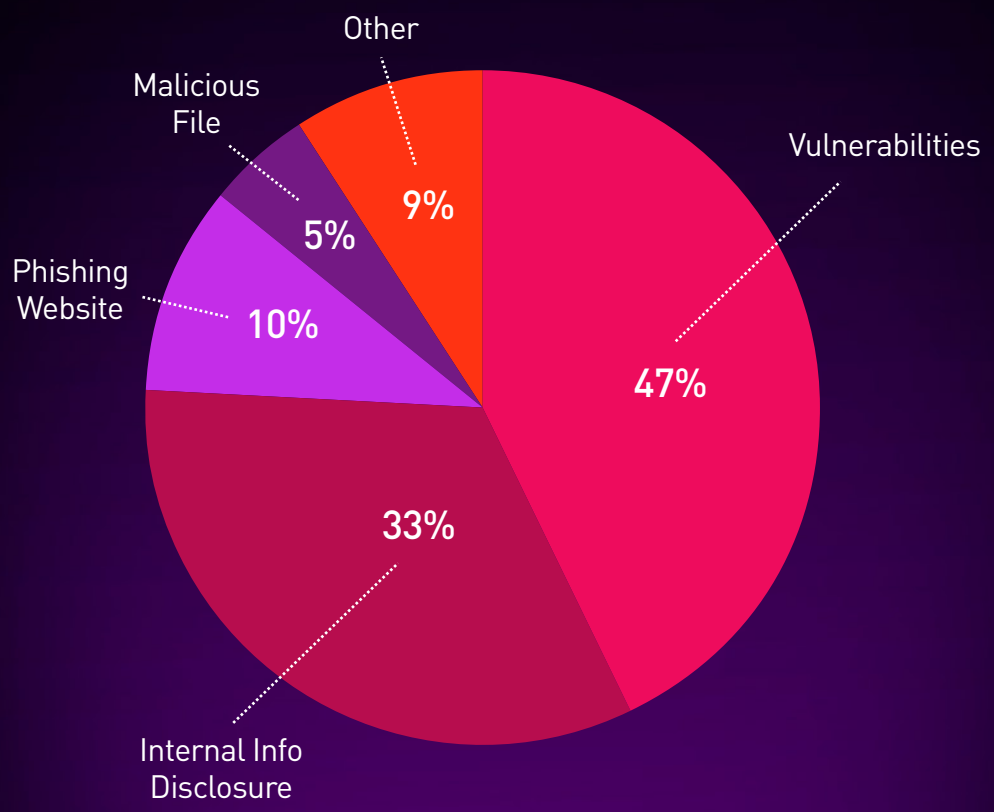


Figure 1: Distribution of critical exposure types across customer environments in 2026.

Exposure Composition

Vulnerabilities represented the largest category of critical exposure in 2026 at 42.6%, followed by Internal Information Disclosure at 33.3%. Phishing Websites were the third largest category at 10.5%, while Malicious Files and Compromised Access Tokens accounted for 4.6% and 1.8%, respectively.

The remaining exposure categories collectively accounted for less than 10% of critical exposures. This distribution shows that while risk came from several exposure types, the critical exposure landscape was primarily shaped by vulnerability management and information exposure.

See Appendix A for all exposure type definitions.

Exposure Change Over Time

Critical exposure composition shifted significantly between 2025 and 2026. In this report, critical exposure refers to alerts classified as Critical by Check Point Exposure Management. The percentages reflect each exposure type's share of all Critical exposure alerts, not total alert volume.

Vulnerabilities increased from 18.7% to 42.6% of all Critical exposures, becoming the leading exposure category. Phishing Website exposure also rose sharply, increasing from 1.0% to 10.5%. At the same time, Internal Information Disclosure declined from 56.8% to 33.3%, while Malicious File exposure fell from 18.3% to 4.6%.

Overall, the data shows a clear shift from disclosure and malware dominated exposure toward vulnerability and phishing related risk. Internal Information Disclosure remained the second largest category in 2026, showing that exposed information assets continue to be a major part of the critical exposure landscape.

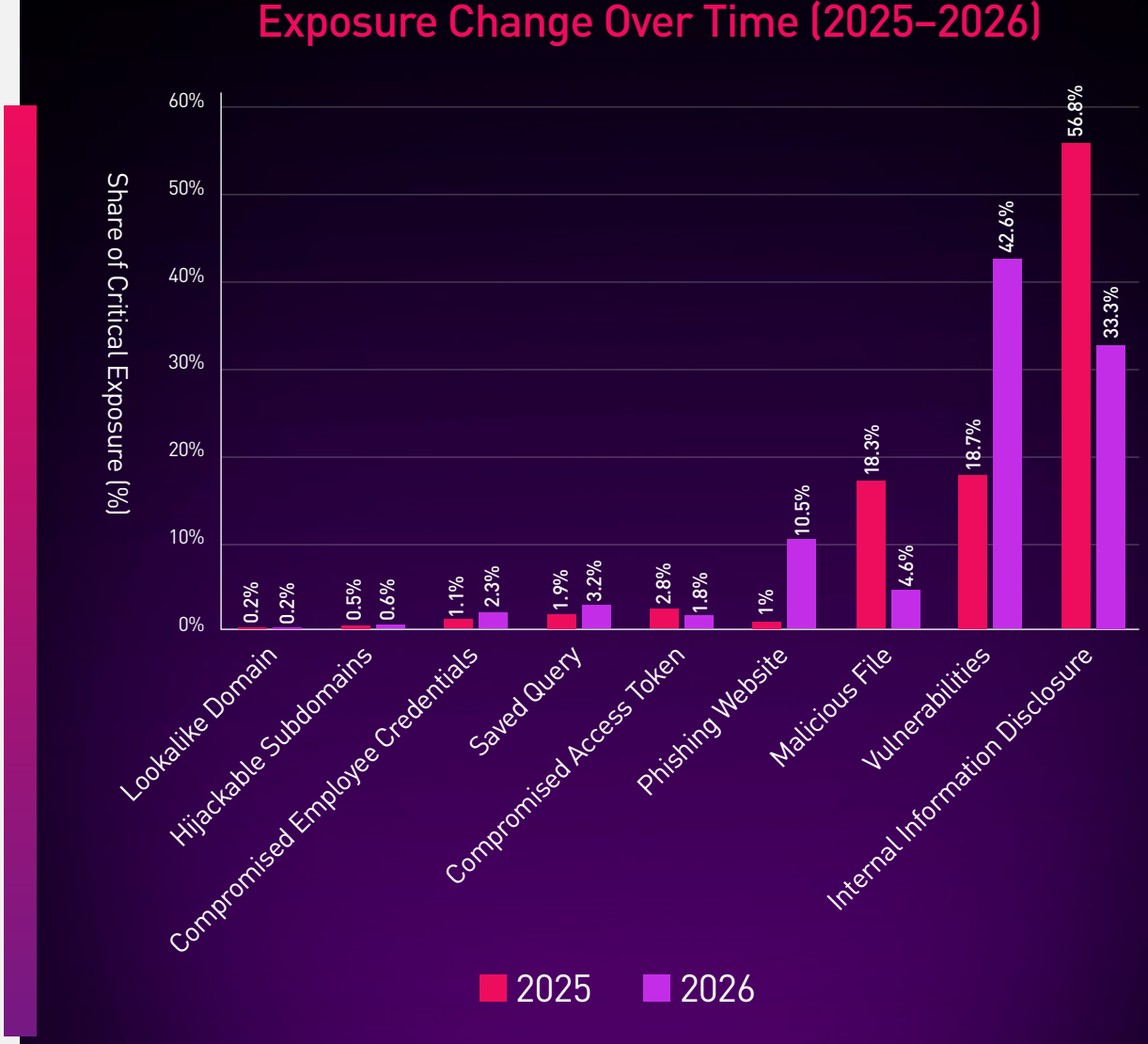


Figure 2: Comparison of the share of critical exposures by exposure type in 2025 and 2026 .

Exposure by Industry

Exposure profiles varied sharply by industry. Utilities, Government, and Manufacturing were primarily shaped by Vulnerabilities, while Healthcare, Telecom, Technology and IT, and Financial Services were led by Internal Information Disclosure. These differences show why exposure management priorities should vary by sector.

Industry Exposure Composition

Utilities recorded the highest concentration of vulnerability exposure, with Vulnerabilities accounting for 78.2% of critical exposures. Government and Manufacturing also showed vulnerability led profiles, with Vulnerabilities representing 56.4% and 52.9% of critical exposures, respectively. These results show that exploitable weaknesses remain the primary exposure driver across several operational, industrial, and public sector environments.

Internal Information Disclosure was the leading category in Healthcare, Telecom, Technology and IT, and Financial Services. Healthcare recorded the highest concentration at 63.6%, followed by Telecom at 58.9%, Technology and IT at 53.1%, and Financial Services at 42.7%. These patterns show that exposed information assets, configuration gaps, and data governance challenges remain central concerns across service oriented and information intensive sectors.

Financial Services stood out for its more balanced exposure profile. Internal Information Disclosure was the largest category, but Malicious Files accounted for 27.8% of critical exposures, while Compromised Employee Credentials and Vulnerabilities each represented approximately 9%. This indicates that Financial Services organizations face risk across disclosure, malware, identity related exposure, phishing, and exploitable weaknesses.

Exposure Composition by Industry

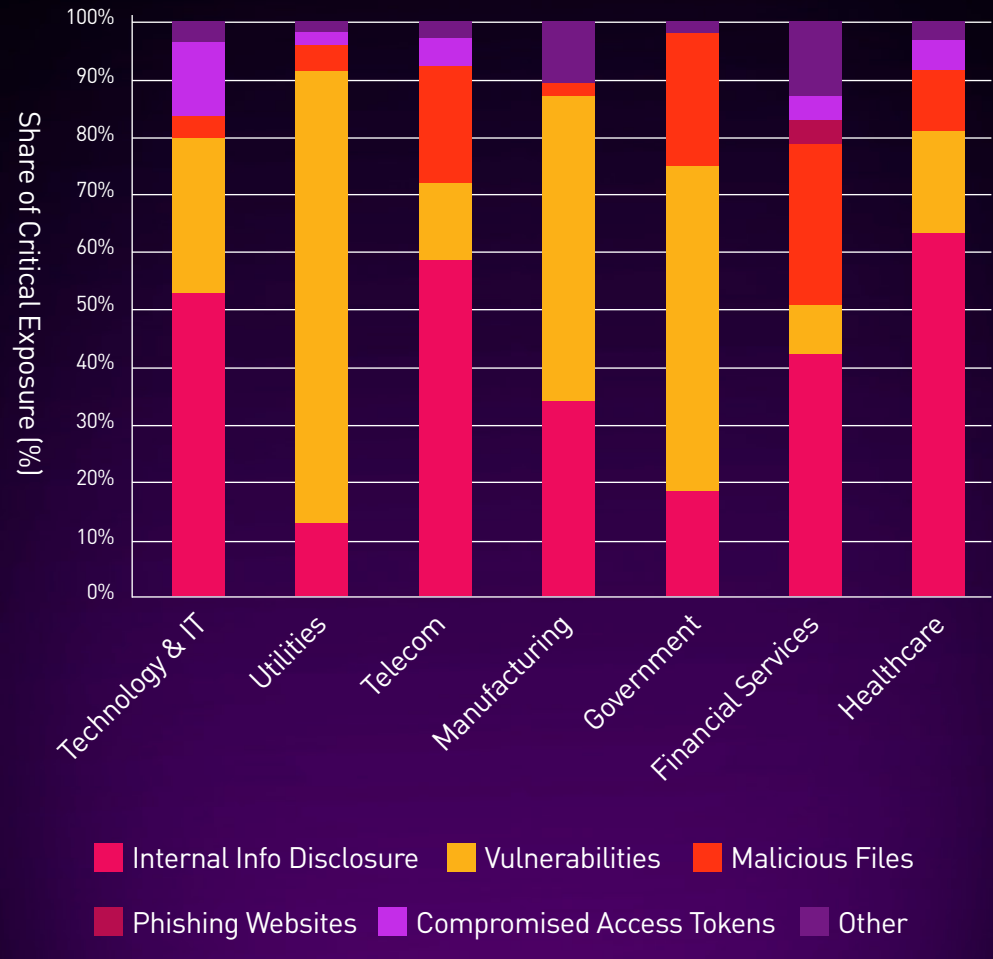


Figure 3: Distribution of critical exposure types across industries in 2026.

Exposure Composition in Healthcare

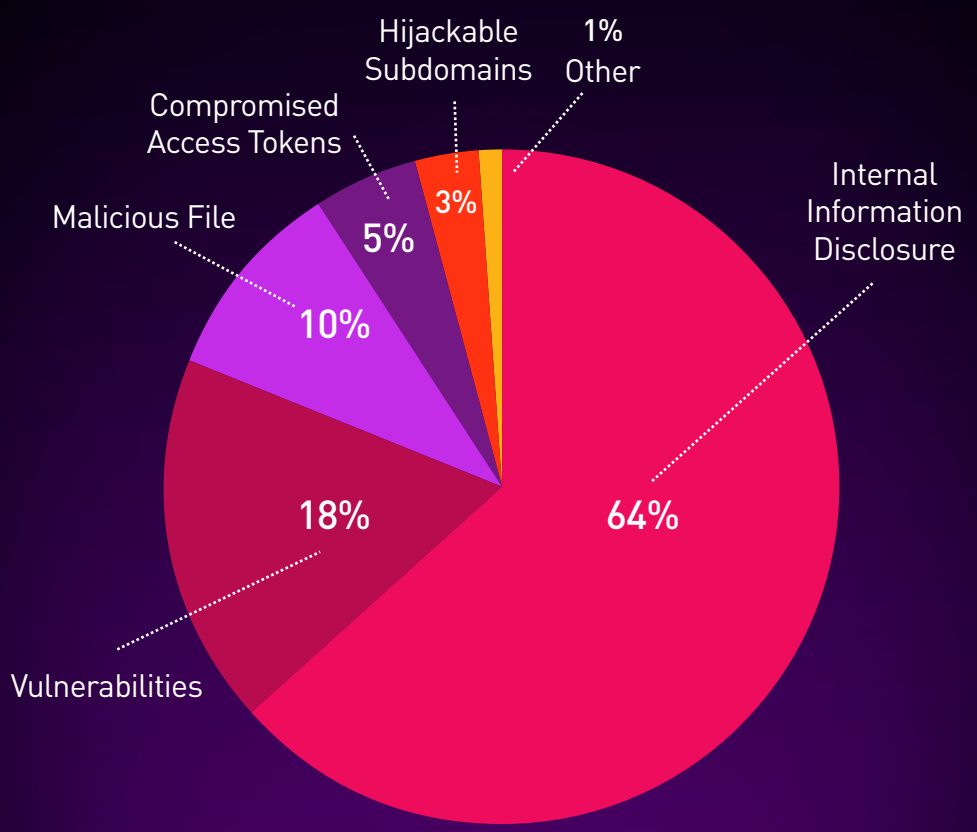


Figure 4: Distribution of critical exposure types within Healthcare organizations in 2026.

Industry Spotlights

Security teams have always faced a gap between when risk appears and when it is fixed. In 2026, that gap has become harder to manage because attackers can test more exposures, across more organizations, at greater speed.

Automation and AI assisted attack tools have changed both the scale and pace of exposure discovery. Threat actors can rapidly test exposed systems, credentials, phishing infrastructure, and known weaknesses until they find a usable entry point. Once that entry point exists, follow on activity such as lateral movement and data access can also accelerate. The result is a shorter window for defenders to identify, prioritize, and reduce exposure before it turns into impact.

Healthcare

Healthcare had one of the most concentrated exposure profiles among the industries analyzed. Internal Information Disclosure accounted for 63.6% of critical exposures, followed by Vulnerabilities at 17.6% and Malicious Files at 10.5%. Together, these three categories represented more than 90% of critical exposures in Healthcare environments.

This profile suggests that Healthcare exposure management should prioritize exposed information assets alongside vulnerability remediation. Healthcare environments often include legacy medical devices, internet connected clinical systems, sensitive patient data, and numerous third-party providers. These factors can increase the likelihood of disclosure related exposure and make remediation more complex.

Financial Services

Financial Services had one of the most balanced exposure profiles among the industries analyzed. Internal Information Disclosure was the largest category at 42.7%, followed by Malicious Files at 27.8%. Compromised Employee Credentials and Vulnerabilities each accounted for approximately 9%, while Compromised Access Tokens and Phishing Websites added further exposure.

This distribution shows that Financial Services organizations face risk across multiple attack paths, including exposed information assets, malicious content, identity related exposure, phishing, and exploitable weaknesses. The sector's reliance on customer facing applications, digital banking platforms, and identity based workflows helps explain why exposure management must cover both technical vulnerabilities and non-vulnerability risks.

Exposure Composition in Financial Services

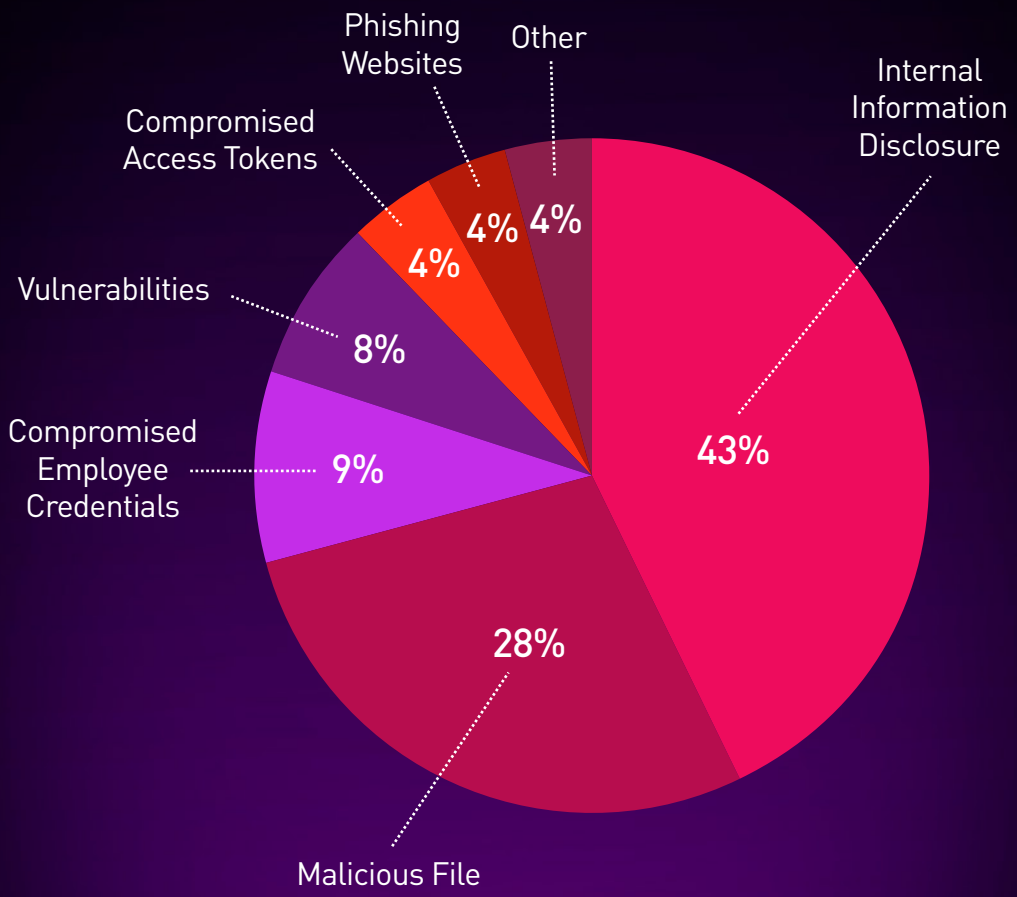


Figure 5: Distribution of critical exposure types within Financial Services organizations in 2026.

Exposure Composition in Government

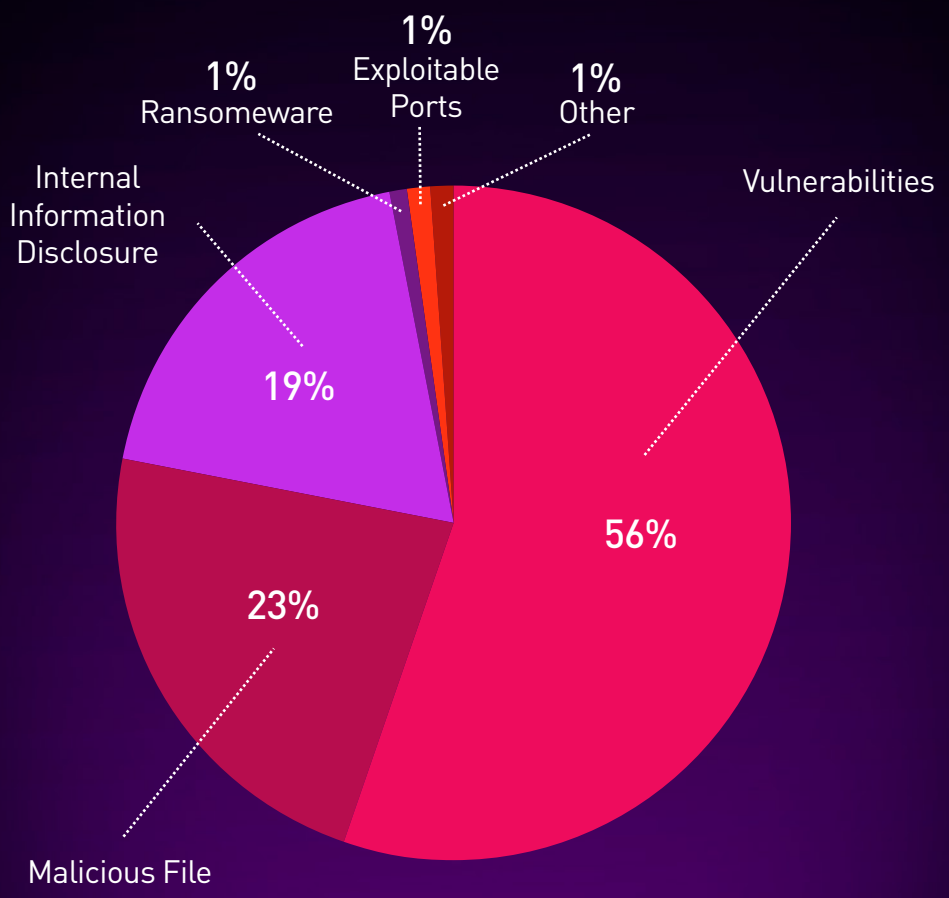


Figure 6: Distribution of critical exposure types within Government organizations in 2026.

Government

Government organizations showed one of the clearest shifts in the report. In 2025, Malicious Files were the dominant category at 39.9%. By 2026, Vulnerabilities had become the leading exposure type, accounting for 56.4% of critical exposures.

This shift indicates that vulnerability management is becoming a larger driver of exposure reduction across public sector environments. Malicious Files remained significant at 22.9%, while Internal Information Disclosure accounted for 18.7%.

Many public sector organizations manage large, decentralized environments that may include legacy technologies, externally accessible services, and critical infrastructure systems. These characteristics can increase the likelihood that exploitable weaknesses remain exposed.

Utilities

Utilities had the most concentrated exposure profile among the major industries analyzed. Vulnerabilities accounted for 78.2% of critical exposures, meaning nearly four out of every five critical exposures in Utilities environments were vulnerability related. Internal Information Disclosure was a distant second at 13.3%, while all remaining categories together accounted for less than 10%.

This concentration suggests that reducing risk in Utilities environments depends heavily on identifying and remediating exploitable weaknesses quickly. Utilities organizations often operate operational technology environments and geographically distributed infrastructure, which can increase exposure to vulnerable systems and make remediation more operationally sensitive.

The vulnerability concentration also increased over time, rising from 73.9% in 2025 to 78.2% in 2026. This reinforces that vulnerability management remains the central exposure reduction priority for Utilities organizations.

Exposure Composition in Utilities

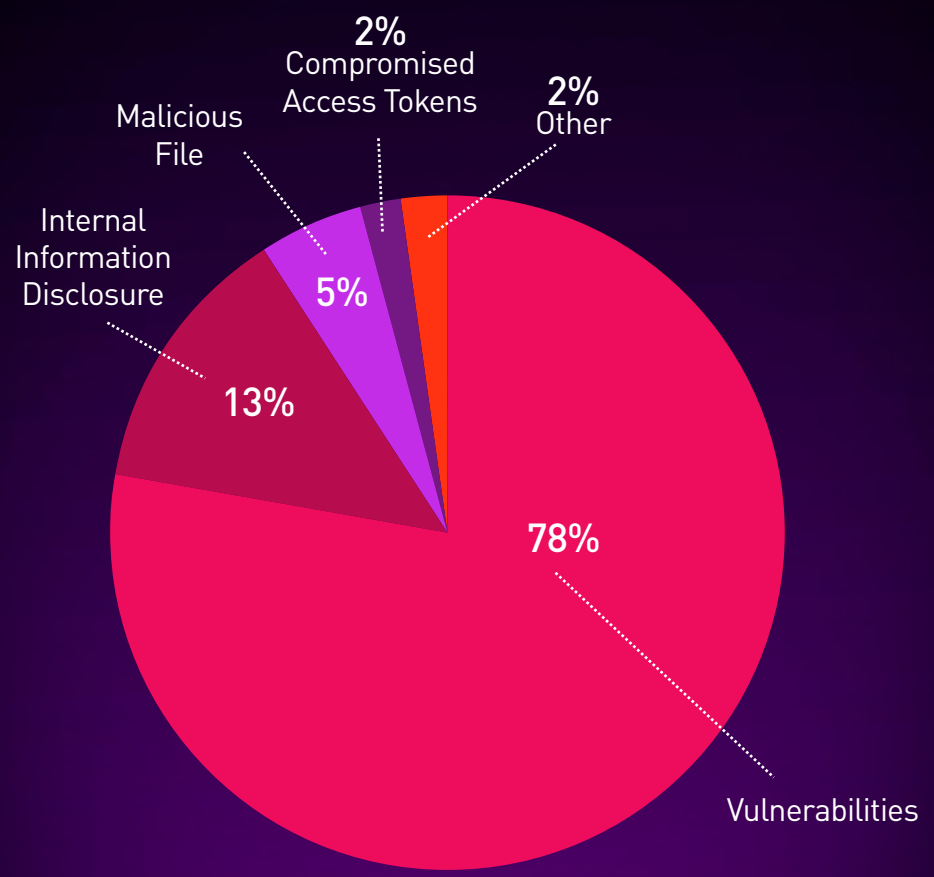


Figure 7: Distribution of critical exposure types within Utilities organizations in 2026..

PRIORITIZATION

Prioritization remains one of the central challenges in exposure management. Large organizations generate high volumes of alerts across vulnerabilities, external risk, threat intelligence, Cyber Asset Attack Surface Management, and exposure monitoring. The challenge is identifying which exposures are urgent, exploitable, relevant to the business, and ready for action.

Check Point Exposure Management addresses this through a connected prioritization workflow. It identifies critical exposure using context, as shown above, by threat activity, weakness type, exposure conditions, asset criticality, and the defensive controls already present in the environment.

Through continuous security control assessment and an open garden approach, the platform evaluates coverage across existing network, endpoint, cloud, email, identity, and operating system controls.

For vulnerability findings, exploitability validation further narrows alerts by confirming which issues are exploitable and lack sufficient security controls.

This is the key finding:

Vulnerabilities became the largest critical exposure category in 2026, but only 7.8% of vulnerability alerts warranted Critical or High attention after exploitability validation. Exposure Management helps find the small subset of vulnerability findings that require immediate focus inside a much larger alert population.

Novel findings add another layer of prioritization by identifying exploitable issues that may require action before they become publicly known.

Prioritization of Exploitable Vulnerabilities

Not every vulnerability alert requires the same level of urgent action. Across the analyzed vulnerability alert population, only 7.8% were validated as Critical or High. This finding highlights the purpose of prioritization: reducing a large alert population to the smaller set of exploitable issues that require immediate investigation and remediation.

AEV helps organizations prioritize vulnerability alerts by proving exploitability and identifying the subset of findings that require focused attention. Rather than treating every vulnerability alert as equal, teams can focus on issues with demonstrated exploitability and supporting context.

See Appendix B for a validation walkthrough of a critical CVE middleware auth bypass.

AEV Prioritization of Vulnerability Alerts

AEV Prioritization Signal	Share of Vulnerability Alerts
Critical and High AEV findings	7.8%
High AEV findings	6.8%
Critical AEV findings	1.0%

Figure 8: Distribution of critical exposure types within Utilities organizations in 2026.

Across the analyzed vulnerability alert population, Critical and High AEV findings represented 7.8% of vulnerability alerts. High findings accounted for 6.8%, while Critical findings accounted for 1.0%. This shows how AEV can help security teams narrow vulnerability alert volume to a smaller set of findings that warrant closer investigation and remediation.

Exploitability Signals

After AEV identifies vulnerability findings that require attention, exploitability signals help teams prioritize further. Known Exploited Vulnerabilities indicate issues already associated with known exploitation activity, while Novel findings identify exploitable conditions that require attention even though they are not previously known CVEs or KEVs.

KEV & Novel Findings Identified Through AEV

Exploitability Signal	Share of AEV Findings
Known Exploited Vulnerability (KEV)	3.6%
Novel Finding	0.8%

Figure 9: Share of vulnerability alerts validated by AEV as Critical, High, and Critical or High.

Novel findings are important because they identify exploitable conditions that traditional vulnerability prioritization may miss. While KEVs point to issues already associated with known exploitation activity, Novel findings show where AEV can surface critical risk before it is publicly known or broadly exploited. Together, KEV and Novel findings help organizations prioritize further within AEV findings by separating known exploited risk from newly validated exploitable conditions that also require attention.

Prioritization of Other High Severity Exposures

Not all high severity exposures are vulnerabilities. Information disclosure, phishing websites, malicious files, compromised credentials, and access token exposure can also create material risk, even when they are not software vulnerabilities. These exposure types may enable data exposure, credential theft, brand abuse, initial access, or follow on attacker activity.

See Appendix C for a validation walkthrough of a live phishing attack.

Severity Distribution of Non-Vulnerability Alerts

Severity	% of Total (excl. vulnerabilities)
Medium	46.9%
High	34.4%
Low	13.0%
Very High	3.9%

Figure 10: Severity Distribution of Non-Vulnerability Alerts

Across the analyzed non vulnerability alert population, 38.3% were Critical or High severity. This shows that prioritization must extend beyond software vulnerabilities. Security teams also need to identify which non vulnerability exposures are severe enough to require timely investigation and remediation.

The practical implication is clear: exposure management cannot rely on vulnerability severity alone. Mature prioritization combines exploitability validation, exposure context, threat intelligence, control coverage, and business impact to identify which issues require action first.

REMEDIATION & RESPONSE

Identifying and prioritizing critical exposures are only the first steps in reducing organizational risk. Agentic attack tools have compressed the time between initial access and impact. In 2026, MTTR benchmarks that were acceptable in previous years are no longer sufficient. Organizations that measure remediation in weeks may remain exposed longer than the attack window allows.

Mean Time to Exploit vs Mean Time to Remediate

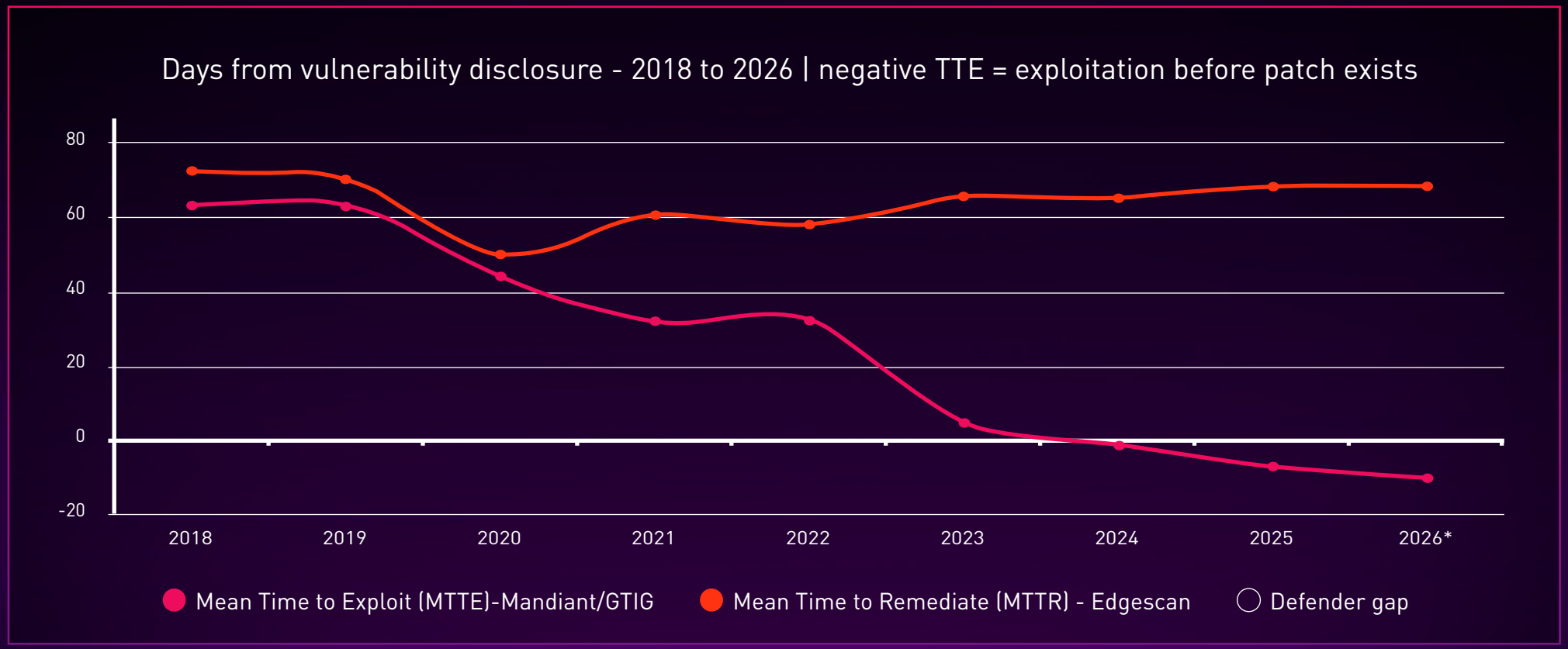


Figure 11: Mean Time to Exploit vs Mean Time to Remediate

The chart shows why remediation speed has become central to exposure management. As attacker exploitation timelines compress, organizations have less time to validate, assign, and remediate critical exposures before risk turns into impact. Remediation benchmarks that were acceptable in previous years no longer match the pace of modern attack activity.

Remediation Speed & Activity

Safe remediation is the stage where prioritized exposure findings are converted into controlled action. Check Point Exposure Management uses an open garden approach, API integrations, and agentless methods to work across the controls and tools already present in the environment. Fixes can be validated before changes are pushed, ensuring the safety of the remediation. Teams reduce exposure through direct remediation, virtual patching, IPS activation, IoC enforcement, takedowns, or other appropriate actions without disrupting business operations.

A negative TTE means attackers are now exploiting vulnerabilities before a patch even exists, so the fix arrives after the breach, not before it.

Remediation has held flat at 60-plus days for years while exploitation has crossed into negative territory. The two lines no longer just diverge, they cross the zero line in opposite directions which is why the defender gap is no longer a window of risk but a breach already underway.

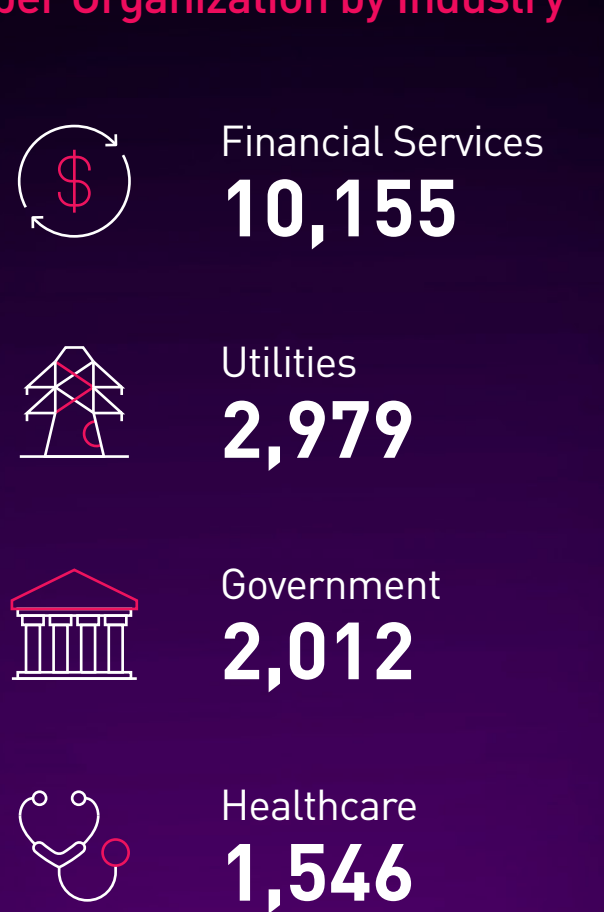


Figure 12: Remediation volume across monitored industries.

Median MTTR for Critical Alert Closure by Industry

Healthcare
158.8 hr.

Financial Services
48.5 hr.

Government
25.4 hr.

Utilities
12.6 hr.

Figure 13: Remediation median time to remediation (MTTR) across monitored industries.

Financial Services recorded the highest average monthly remediation volume per organization at 10,155, followed by Utilities at 2,979, Government at 2,012, and Healthcare at 1,546. When viewed alongside MTTR, the data shows that remediation performance cannot be measured by volume alone.

Utilities had the fastest median MTTR at 12.6 hours despite the second-highest remediation volume. Government followed at 25.4 hours, while Financial Services managed the highest workload with a 48.5-hour MTTR. Healthcare had the longest MTTR at 158.8 hours, reflecting constraints such as legacy technology, uptime requirements, change control, and third-party dependencies.

Overall, stronger exposure management programs are those that can remediate at scale while reducing the time critical exposures remain open.

Organizations Resolving Critical Exposures Within One Hour

A significant proportion of Check Point Exposure Management customers are remediating critical exposures within one hour (Between 7.7%-30% depending on industry), showing what mature exposure management programs can achieve when validation, ownership, and response workflows are operationalized.

Organizations Resolving Critical Exposures Within One Hour

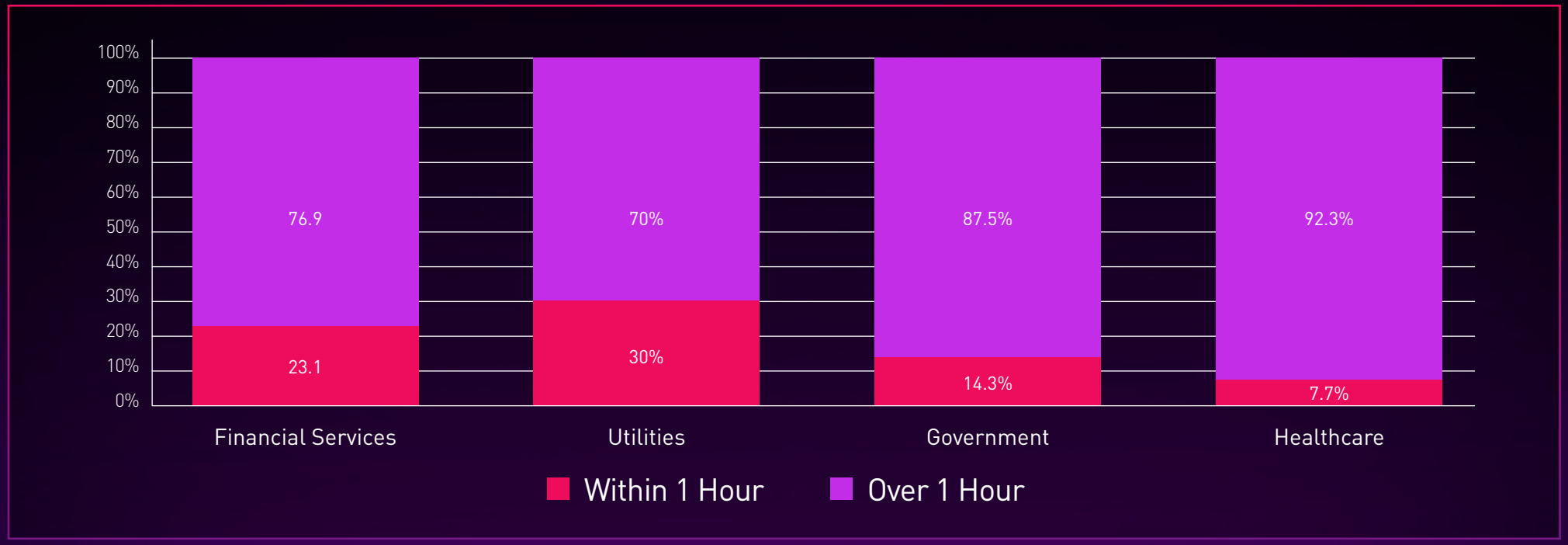


Figure 14: Percentage of organizations achieving critical exposure remediation within one hour.

A meaningful share of Check Point Exposure Management customers resolved critical exposures within one hour, showing what mature exposure management programs can achieve when validation, ownership, and response workflows are operationalized.

Utilities recorded the highest share of organizations resolving critical exposures within one hour at 30.0%, followed by Financial Services at 23.1%, Government at 14.3%, and Healthcare at 7.7%. Utilities and Financial Services are especially notable because they also handled the two highest remediation volumes. This shows that rapid remediation is not only a function of lower workload. Mature programs can move quickly even when remediation volume is high.

Remediation Effectiveness

Recommended fixes show whether exposure findings are converted into measurable risk reduction. Across the industries analyzed, implementation rates were high, although performance varied by workload, maturity, and operating environment.

Across the four monitored industries, organizations acted on an average of 85.9% of recommended fixes. Financial Services recorded the highest implementation rate at 91.7%, followed by Healthcare at 85.5%, Utilities at 84.0%, and Government at 82.5%.

Financial Services stood out because it combined the largest remediation workload with the highest implementation rate. Healthcare also achieved a strong implementation rate despite recording the longest median MTTR, suggesting that Healthcare organizations are acting on recommended fixes even when remediation takes longer due to operational complexity.

Stronger programs combine high implementation rates, remediation at scale, and the maturity needed to close critical exposures quickly and safely.

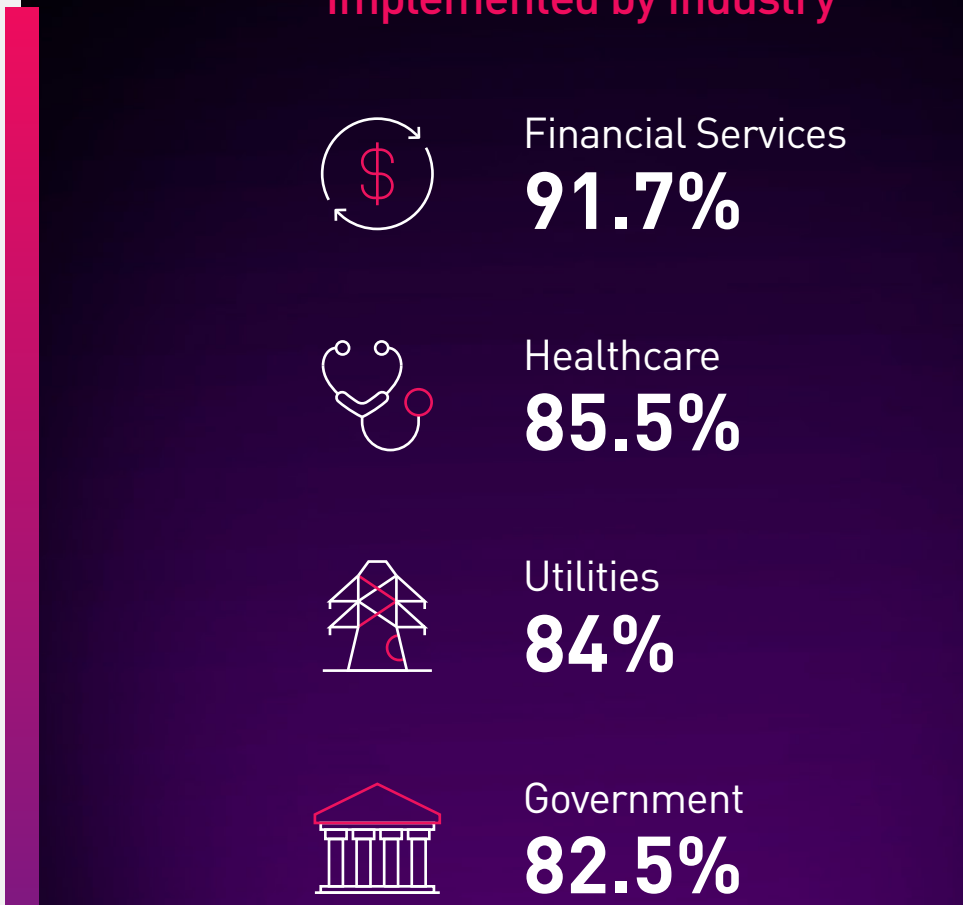


Figure 15: Percentage of recommended remediation actions implemented by organizations within each industry.

Defensive Effectiveness

Defensive controls help reduce risk while exposures are investigated and remediated. IoC enforcement, IPS and WAF rules, and takedown services each play a different role in exposure reduction: blocking known malicious activity, preventing attacks from reaching exposed systems, and removing malicious infrastructure at the source.

Average Attacks Blocked via IoC Feeds

Across a subset of organizations analyzed in this report, IOC feed enforcement blocked an average of 4.52 million attacks per organization. This shows the scale of protection that can come from distributing known malicious indicators across connected enforcement controls.

Average Attacks Blocked via IPS & WAF Rules

Across the same subset of organizations, IPS and WAF rules blocked an average of 2,032 attacks per organization. This should be read as a subset average, showing how rule-based controls can provide an additional prevention layer while remediation is underway.

Takedown Services

Takedown services reduce exposure by removing malicious infrastructure at the source. Common takedown targets include phishing websites, executive and brand impersonation campaigns, rogue applications, leaked sensitive data, and other malicious content that can increase organizational risk.

In 2026, Check Point's takedown team reported an overall success rate exceeding 99%, with an average takedown MTTR of 12 hours and 78% of requests completed within 12 hours.

Unlike controls that block malicious activity after it is observed, takedowns help reduce exposure by removing malicious assets entirely. This can limit the effectiveness of phishing campaigns, reduce brand abuse, prevent distribution of malicious applications, and shorten the lifespan of attacker infrastructure.

Together, remediation, IoC enforcement, IPS and WAF protections, and takedown services help reduce exposure while teams work through underlying fixes. They do not replace remediation, but they reduce the likelihood that known threats and active attack attempts can progress further before exposure reduction is complete.

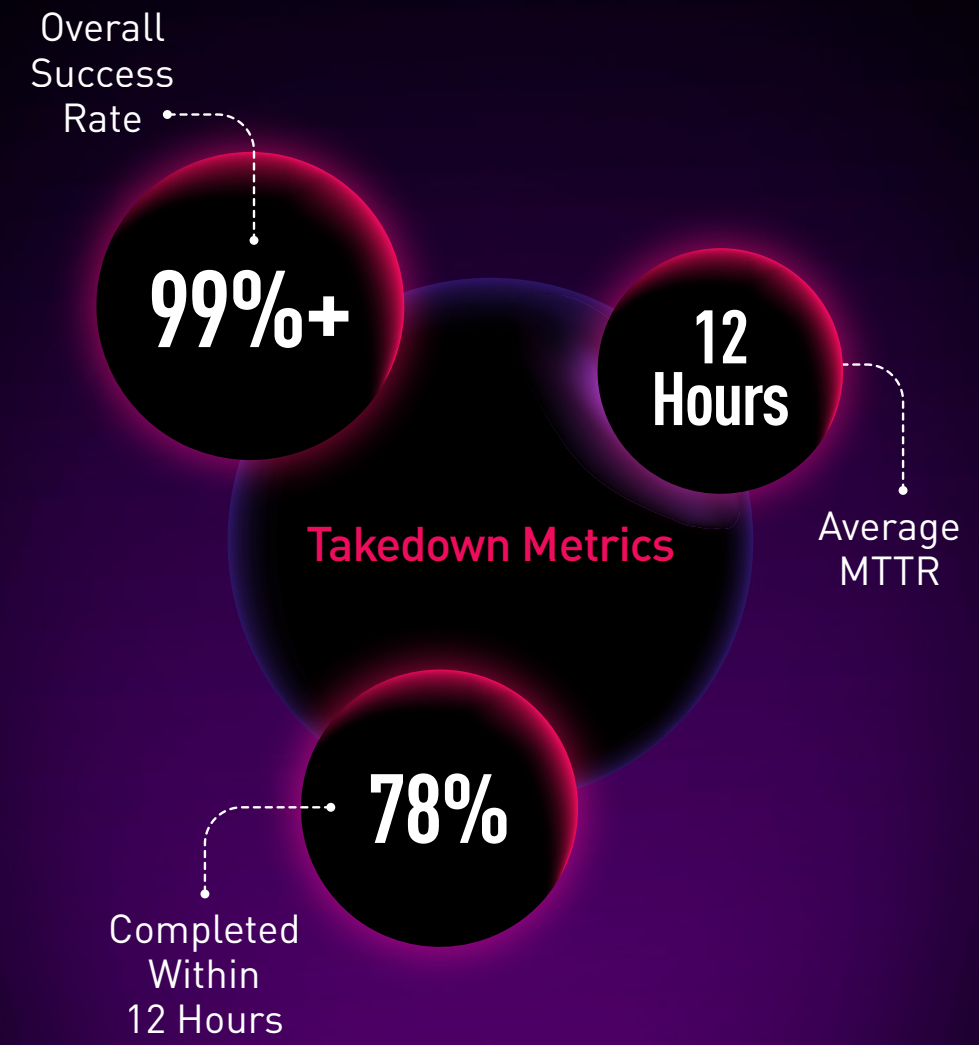


Figure 16: Takedown Metrics.

CONCLUSION: EXPOSURE & REMEDIATION PROFILE

Industry Exposure & Remediation Profile

Severity	Dominant Exposure Type	Share of Critical Exposures	Median MTTR (Hours)	Fixes Implemented	Organizations Resolving <1 Hour
Financial Services	Internal Information Disclosure	42.7%	48.5	91.7%	23.1%
Healthcare	Internal Information Disclosure	63.6%	158.8	85.5%	7.7%
Government	Vulnerabilities	56.4%	25.4	82.5%	14.3%
Utilities	Vulnerabilities	78.2%	12.6	84.0%	30.0%

Figure 17: Comparison of dominant exposure types and remediation performance across key industries.

Exposure and remediation performance varied sharply by industry, showing that organizational risk is shaped by both exposure type and response capability. Financial Services showed the strongest implementation profile, combining the highest fix implementation rate at 91.7% with the largest remediation workload and a median MTTR of 48.5 hours. Utilities recorded the fastest median MTTR at 12.6 hours and the highest share of organizations resolving critical exposures within one hour at 30.0%.

Healthcare presented a different risk profile. Internal Information Disclosure accounted for 63.6% of critical exposures, the highest disclosure concentration among the industries analyzed. Healthcare also recorded the slowest median MTTR at 158.8 hours and the lowest share of organizations resolving critical exposures within one hour at 7.7%, even though its fix implementation rate remained strong at 85.5%. This suggests that Healthcare organizations are acting on recommended fixes, but remediation may be slowed by operational complexity, legacy systems, clinical uptime needs, and change control requirements.

Government and Utilities were both vulnerability driven. Vulnerabilities accounted for 56.4% of critical exposures in Government and 78.2% in Utilities. Government showed relatively fast remediation, with a median MTTR of 25.4 hours and an 82.5% fix implementation rate. Utilities stood out for speed, while Financial Services stood out for scale, implementation, and response performance.

Overall, exposure concentration alone does not determine organizational risk. Strong exposure management outcomes depend on accurate prioritization, timely remediation, high fix implementation rates, and the ability to reduce exposure before it contributes to a larger security incident.

The data in this report makes one thing clear: exposure management has become a front-line operational capability. The organizations in this report resolving critical exposures within one hour provide a benchmark for exposure management maturity. Organizations with mature discovery, prioritization, validation, and remediation workflows can close critical exposures faster and more safely.

APPENDIX A. EXPOSURE TYPE DEFINITIONS

Reference definitions for the exposure categories analyzed in this report.

Critical Exposure Type	Definition
Vulnerabilities	Software, system, or configuration weaknesses that could be exploited by an attacker to gain access, escalate privileges, disrupt services, or compromise data.
Malicious File	A file identified as harmful or suspicious, including malware, trojans, droppers, payloads, or other files that may support attacker activity.
Phishing Website	Software, system, or configuration weaknesses that could be exploited by an attacker to gain access, escalate privileges, disrupt services, or compromise data.
Internal Information Disclosure	Exposure of internal data or assets, such as leaked credentials, exposed source code, sensitive files, misconfigured public resources, or other information not intended for public access.
Phishing Website	A website designed to impersonate a trusted brand, service, or login page in order to steal credentials, payment details, or other sensitive information.
Internal Information Disclosure	Exposure of internal data or assets, such as leaked credentials, exposed source code, sensitive files, misconfigured public resources, or other information not intended for public access.
Compromised Access Tokens	Authentication tokens, session tokens, API tokens, or similar credentials that have been exposed, stolen, or made available for unauthorized use.
Hijackable Subdomains	Subdomains that point to inactive, unclaimed, or misconfigured services and may be taken over by an attacker.
Compromised Employee Credentials	Employee usernames, passwords, or account credentials exposed through breaches, infostealers, phishing, or other credential theft activity.
Exploitable Ports	Open network ports or services that are externally exposed and may allow attackers to access, probe, or exploit systems.
Ransomware	Malicious software or attacker activity designed to encrypt, steal, or disrupt data and systems in order to demand payment.
Lookalike Domain	A domain that closely resembles a legitimate brand or company domain and may be used for phishing, impersonation, fraud, or brand abuse.
Saved Query	A stored search or monitoring rule used to identify recurring exposure patterns, suspicious assets, or risk signals across the environment.
Other	Additional exposure types that do not fall into the named categories above but were still classified as critical exposure findings in the dataset.

APPENDIX B. CRITICAL CVE MIDDLEWARE AUTH BYPASS VALIDATION WALKTHROUGH

A recent critical CVE the stock scanner template would miss — the agent fingerprints the middleware, injects the bypass header, and proves the authorization layer is defeated by a control-vs-bypass differential.

VULNERABLE STACK
Next.js 14.x on two banking apps

→

CVE MATCH
CVE-2025-29927
CVSS 9.1 auth bypass

→

BASELINE
Control request: 307 →/login (middleware on)

→

INJECT BYPASS
Add the x-middleware-subrequest header

→

VALIDATE
404 + no redirect - **middleware skipped**

Resources consulted autonomously

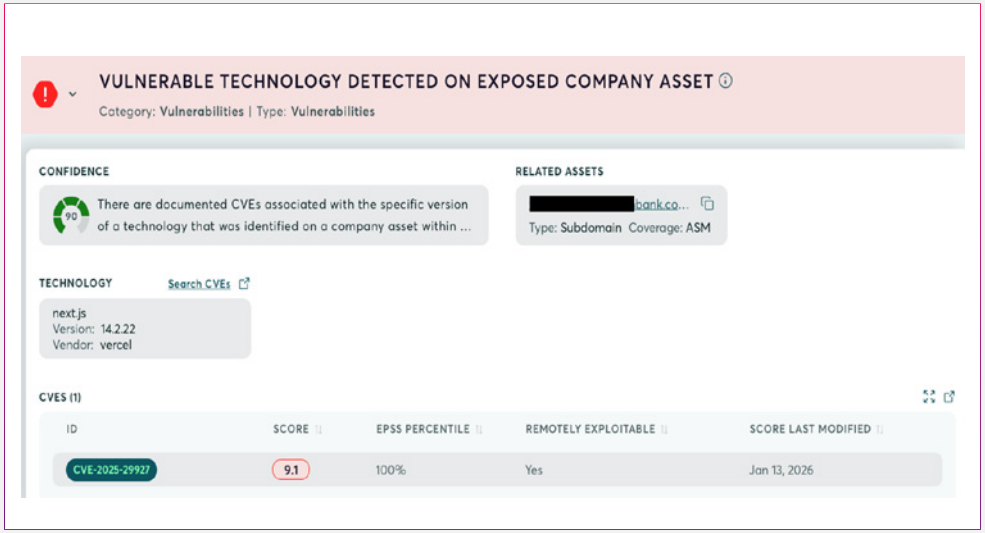
Exposed Assets
2 internet-facing banking apps

CVE Database
NVD: CVSS 9.1, EPSS 0.93

Bypass Technique
header: x-middleware-subrequest

Differential Probe
control 307 vs bypass 404

Beyond the Stock Template
stock needs 200; bypass is 404



10 min

The intelligence chain no scanner can replicate

- Flags vulnerable Next.js 14.x on banking apps
- Matches CVE-2025-29927 — CVSS 9.1 auth bypass
- Baseline: middleware enforces the /login redirect
- Injects x-middleware-subrequest → redirect vanishes
- Stock template needs a 200 — would miss this 404
- Agent builds a differential that proves the bypass

APPENDIX C. LIVE PHISHING ATTACK VALIDATION WALKTHROUGH

Beyond a login-page alert — the agent proves an active phishing kit is harvesting employee VPN credentials on a trusted subdomain, and exposes the attacker's own cloud infrastructure.

STANDARD ALERT
"Exposed login page" on a company subdomain

→

SPOT THE CLONE
FortiGate VPN clone - not the real thing

→

READ THE KIT
Kit JS posts creds to an attacker endpoint

→

CANARY PROBE
Canary username reflected - **harvester is live**

→

EXPOSE ATTACKER
Attacker AWS keys found in an exposed .env

What the agent validates at each step

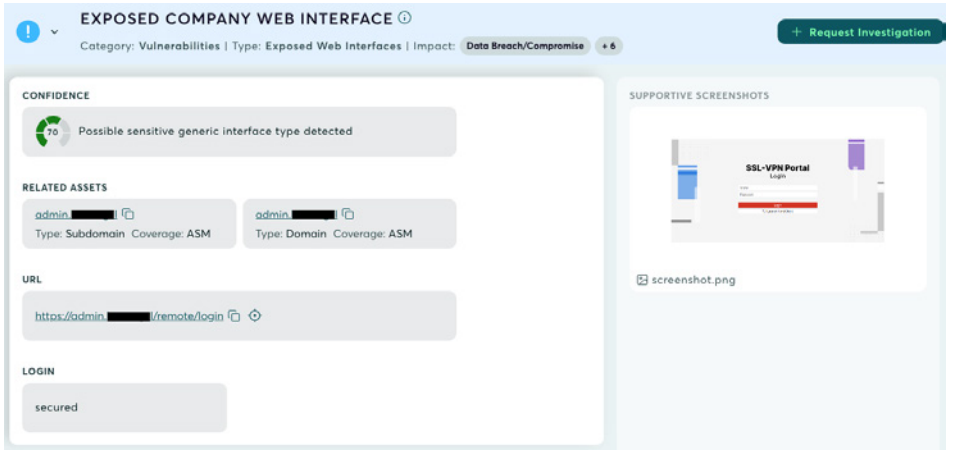
Is it a clone?
Native FortiGate path missing

Is the backend live?
Canary reflected in real time

What does it steal?
VPN creds → network access

Whose infra is it?
Attacker AWS keys exposed

Still active?
Live across the assessment



14 min

Generic scanner vs. agentic attacker

- Scanner sees HTTP 200 on a login page → stops
- Agent reads the page → recognizes a FortiGate clone
- Reads the kit JS → finds the credential-harvest endpoint
- Sends a safe canary → backend reflects it (live)
- Finds the attacker's AWS keys in an exposed .env
- Attributes them to the attacker — not the customer

→ **An active breach, surfaced from a routine alert.**

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

CHECK POINT
EXPOSURE MANAGEMENT