



EXPOSURE MANAGEMENT

THE GREAT EXPOSURE RESET

HOW CYBER SECURITY TEAMS TAKE BACK CONTROL

JANUARY 2026



Table of Contents

Executive Summary	3
Chapter 1	
Why Exposure Management Exists Now	4
Chapter 2	
The CTEM Framework	7
Chapter 3	
What Good Exposure Management Looks Like	9
Chapter 4	
The Mobilization Gap	17
Chapter 5	
How Check Point Maps to CTEM	18
Chapter 6	
Exposure Management in Action	21
Chapter 7	
Building Your Exposure Reset Roadmap	27
Postface	
Taking back control	31
Contact Us	32

Executive Summary

Exposure Management is often described as better prioritization or broader visibility. This document takes a different position. It defines exposure management as an intelligence-led, remediation-first operating model where external adversary activity, internal reachability, and security control enforcement are continuously combined into one decision system. Instead of starting with asset inventories or CVE lists, this approach starts with how attackers operate: which campaigns are active, which techniques are being weaponized, and where those threats intersect with your actual environment. By correlating live threat intelligence with internal telemetry and enforcement coverage, the model in this ebook filters thousands of findings down to the exposures that are both exploitable and preventable, and couples each one with a safe, validated path to closure.

This document provides a practical blueprint for implementing effective Exposure Management using the Continuous Threat Exposure Management (CTEM) model. It breaks down what good exposure management looks like in practice, how to prioritize based on real adversary behavior and business impact, and how to safely mobilize remediation across security and IT teams without disrupting the business. The outcome is an actionable operating model you can apply immediately that aligns intelligence, prioritization, and remediation into a repeatable process that measurably reduces exposure dwell time and cyber risk starting as soon as tomorrow.



The future belongs to teams that can see, understand, validate, and fix - continuously.

It's time to take back control.

Welcome to the Exposure Reset.

Chapter 1

Why Exposure Management Exists Now

The Transition from Visibility to Action

There is a growing realization across the security industry that something is fundamentally broken. Organizations have never had more tools, more telemetry, yet they continue to struggle with the same root problem that exposures linger far too long, and attackers take advantage long before defenders can respond.

For years, cyber security strategy revolved around visibility. The mindset was simple, if we can find every vulnerability, misconfiguration, and threat indicator, we can stay ahead. This made sense in a world where environments changed slowly and attackers needed time to build their campaigns. That world no longer exists.

Today, everything moves faster. Cloud assets appear and disappear within hours. Developers push new code dozens of times a day. Identities accumulate permissions faster than teams can track. SaaS grows without centralized oversight. Infrastructure evolves. And adversaries, often using AI, discover and weaponize exposures in hours, not weeks. Threat intelligence plays a growing role here, revealing not only which vulnerabilities exist, but which ones attackers are actively exploiting.

This operating reality explains why vulnerability management alone has not delivered the outcomes organizations expected. Scanners bring to light issues, but they cannot tell which are reachable by an attacker. Threat feeds show what adversaries use, but they do not reveal which assets are exposed. IT operations enforce changes, but often without the context of how a fix impacts risk or performance. Each group works with part of the picture, but no single team owns the full exposure story.

Components of Exposure Management



Source: Gartner

Note: "Scope," "discover," "prioritize" and "mobilize" are the phases of Gartner's continuous threat exposure management (CTEM) approach. 809126_C

Disconnected Tools and Noise Overload

Gartner's recent research reflects this. The inaugural [Magic Quadrant for Exposure Assessment Platforms](#) describes a market moving beyond legacy scanning toward true exposure understanding. Continuous Threat Exposure Management extends that thinking by providing a repeatable, programmatic approach to discovering, prioritizing, validating, and treating exposures across internal and external surfaces.

This change is happening because traditional workflows cannot keep up. Organizations often maintain dozens of security tools, each producing alerts and findings. The average enterprise has more than 45 cyber security products, generating thousands of signals every day. Without a unifying model, the result is noise, duplication, and slow action. Intelligence becomes fragmented across products and teams, making it nearly impossible to understand attacker intent in context of what is actually exposed.



Team Fragmentation and Operational Misalignment

Security leaders face a second challenge of fragmentation across teams. **The SOC investigates threats.** The vulnerability team manages scans. The infrastructure team manages controls. Cloud teams manage configuration. Third-party risk teams manage external surfaces. Each group operates with its own KPIs, tooling, and prioritization logic. Coordination is often manual, slow, and inconsistent. When everything is urgent, nothing is.

This is the environment attackers exploit. They do not need a zero-day. They rely on misconfigurations, weak credentials, exposed assets, unprotected web applications, reachable vulnerabilities, and gaps between controls. Modern breaches typically start with something simple like a forgotten port, an unpatched internet-facing service, a weak credential reused in the wrong place, or a configuration mismatch that went unnoticed.

Focusing on the Wrong Threats

Exposure dwell time has become the metric that is at the top of the list for risk management teams. The longer an exposure remains open, the higher the probability it will be used. Gartner predicts that by 2027, organizations with mature exposure programs will reduce remediation timelines by roughly 30 percent. More importantly, by 2030 they expect organizations to cut critical exposure dwell time by up to 60 percent through structured mobilization and alignment between security, IT, and business stakeholders.

This is the core reason exposure management exists. It is not another tool category, not a rebranding of vulnerability management, and not an attempt to replace existing solutions. It is a recognition that cyber security needs to flip the page on proactivity and go from producing alerts to producing outcomes. From identifying weaknesses to removing them. From visibility to control.

Across industries, organizations are discovering the same truth that the teams that succeed are the ones that continuously reduce exposures, and do so proactively before attackers reach them. This requires more than visibility. It requires context, validation, workflows, and the ability to mobilize action across every security layer.

Exposure management is the model that brings these pieces together. It creates a shared language across teams. It helps organizations understand what is exploitable, what is reachable, and what will have business impact if compromised. Most importantly, it helps them act with confidence.

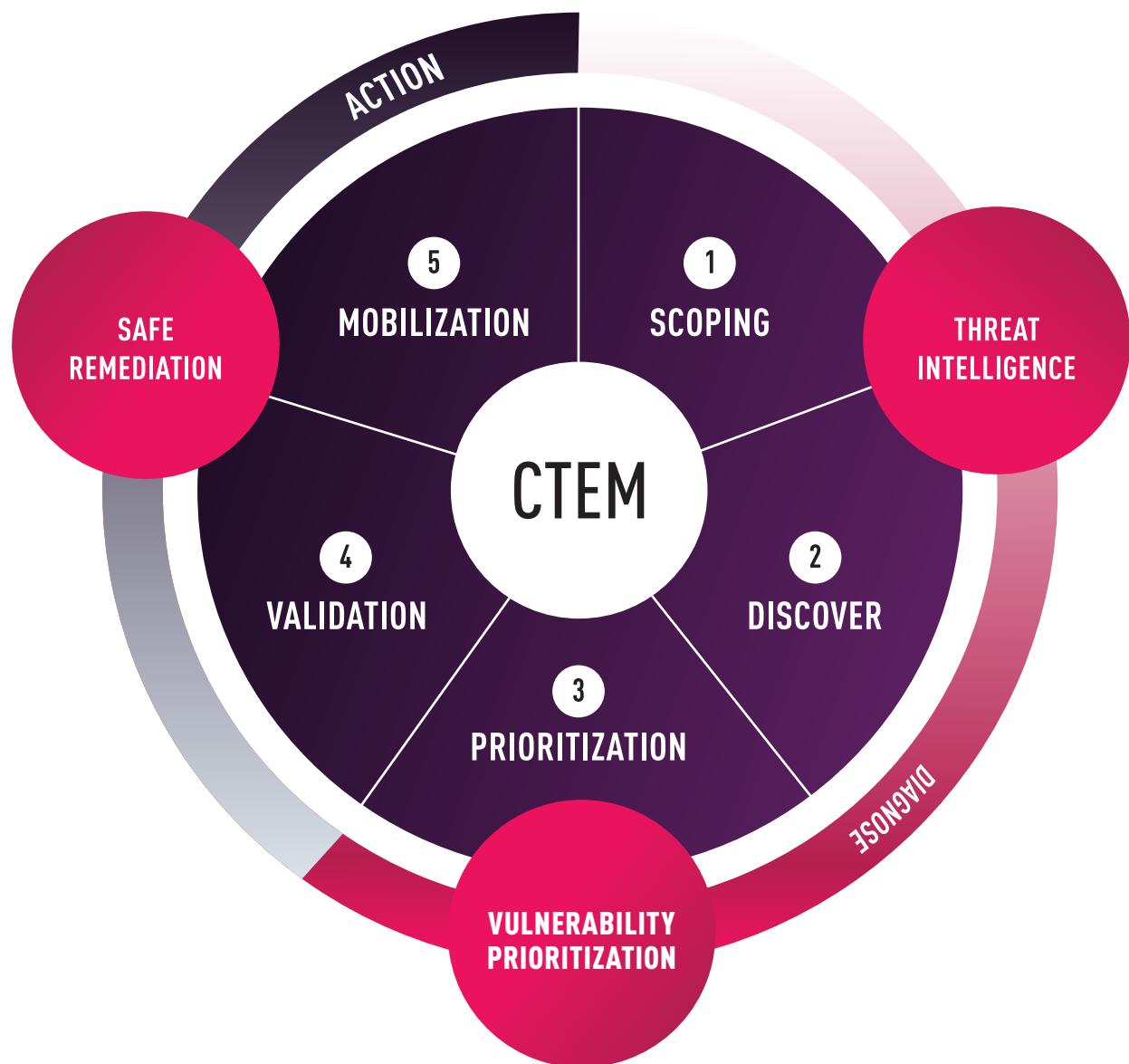
Chapter 2

The CTEM Framework

As security programs evolve, many organizations discover that the increasing volume of exposures and understanding which exposures need immediate attention, why they need it, and what to do about them, is the real challenge. This requires a structure that goes beyond lists and dashboards. It requires a discipline that turns the constant noise of findings into a predictable, repeatable, outcome-driven process.

Gartner's CTEM framework has become the reference model for modern exposure programs because it captures the full lifecycle of exposure reduction. It provides a way for organizations to move from fragmented activities to a coordinated approach that unifies security, IT, cloud, and risk teams around the same objective. Most importantly, CTEM helps organizations go from reactive defense to preemptive action. It takes the idea of continuous assessment and combines it with the need for validation and timely remediation. Rather than asking "how many vulnerabilities do we have," CTEM forces teams to ask "what exposures can truly lead to compromise, and how do we close them with confidence."

The framework consists of five phases. Each phase introduces a different perspective on the exposure landscape, and when executed together, they create an operational rhythm that reduces risk consistently over time.



1. Scoping

Scoping defines the boundaries of what needs protection. It establishes the assets, environments, identities, configurations, external surfaces, and business services that must be included in the exposure program. Shadow SaaS, unmanaged identities, internet-facing services, and security control misconfigurations often surface here for the first time. Scoping gives teams a realistic understanding of the attack surface before they begin trying to reduce exposures.

2. Discovery

Discovery identifies exposures across the scoped environment. It combines internal scanning, configuration assessments, risk analysis, posture evaluation, and external attack surface monitoring. The goal is not to find everything. It is to find everything that is critical within the defined scope.

3. Prioritization

Prioritization is the heart of exposure management. It answers the question which exposures create real risk right now. When organizations implement this phase correctly, the number of exposures that actually require action drops dramatically. The program becomes leaner, more focused, and more aligned with business objectives.

4. Validation

Validation ensures that remediation actions are safe before they are deployed. This is one of the most overlooked steps in cyber security programs, even though it protects business continuity. It tests whether an IPS rule or WAF policy will generate false positives, whether a configuration change will break a business application, or whether a patch can be safely applied or should instead be compensated for with another control.

5. Mobilization

Mobilization is where the program becomes operational. It connects the prioritized, validated exposures to the teams responsible for action. It ensures that fixes flow to the right owners with the right urgency and the right context. Mobilization is the most difficult phase because it requires coordination across functions that traditionally operate independently. It addresses the biggest blind spot in modern security programs: the gap between knowing what to fix and actually fixing it.

CTEM is much more than a framework. It is a way to bring structure and predictability to what has historically been a chaotic process. Each phase builds on the one before it, and together, they help security teams move from isolated findings to meaningful, measurable risk reduction.

Chapter 3

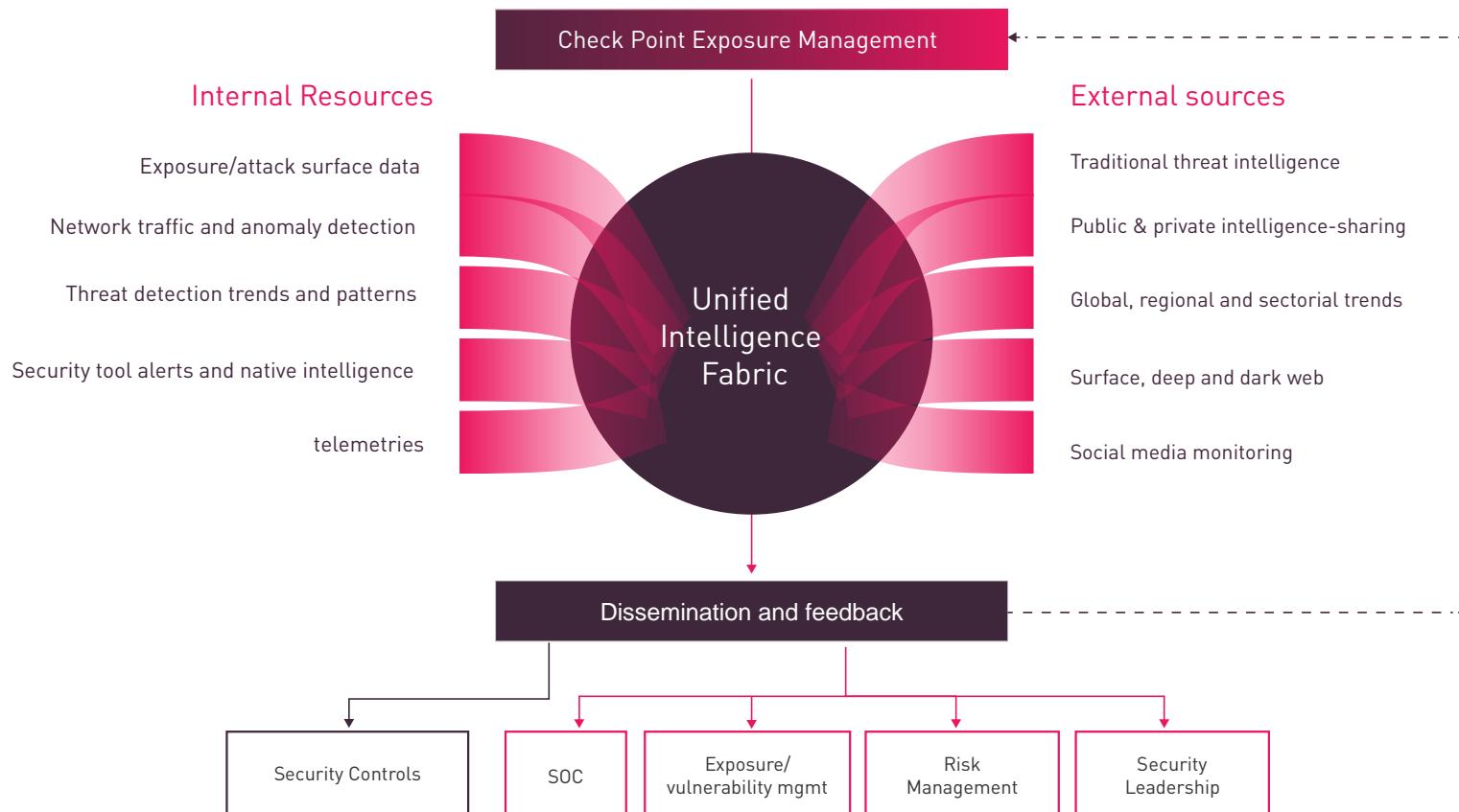
What Good Exposure Management Looks Like

Exposure management can feel overwhelming when viewed through the lens of every vulnerability, misconfiguration, identity risk, and external signal flowing through an enterprise. Yet the organizations that succeed share something in common, they all focus on outcomes, not outputs. They build programs that reduce risk measurably and repeatedly, instead of reacting to endless lists.

Good exposure management contains the following essential characteristics.

1. Intelligence-Driven Understanding of Assets and Exposures

Effective exposure management starts with intelligence, not inventory. Organizations need a holistic intelligence view that continuously correlates internal telemetry with external adversary activity to understand how their environment is being targeted in real time. This means linking assets, identities, cloud resources, configurations, and vulnerabilities with live threat campaigns, exploited techniques, and attacker infrastructure. When an exposure is identified, teams must know whether it is actively weaponized, reachable within their environment, and if it can be mitigated by existing controls. Intelligence-driven programs eliminate static risk assumptions, reduce noise, and focus remediation on exposures that attackers are most likely to exploit.



2. Context-driven prioritization

Prioritization should not revolve around severity scores or the total number of findings. In mature programs, priority is determined by four questions:

- Can an attacker reach the asset?
- Is the exposure exploitable?
- How important is the asset to the business?
- Are protections already in place?

Security Posture Alerts (3) SEE ALL >

TITLE	ALERT ID	SEVERITY	CONFIDENCE	CREATED DATE
Exploit Found On Company Asset	ARG-5198	!	90	November 20, 25
Exploitable Vulnerability found on a Company Asset	ARG-5195	!	90	June 11, 25
Exploit Found On Company Asset	ARG-5196	!	90	November 20, 25

Exploitable Vulnerability found on a Company Asset

Category: Vulnerabilities | Type: Vulnerabilities
Last content update: Jun 11, 2025 03:04:26, Severity Changed

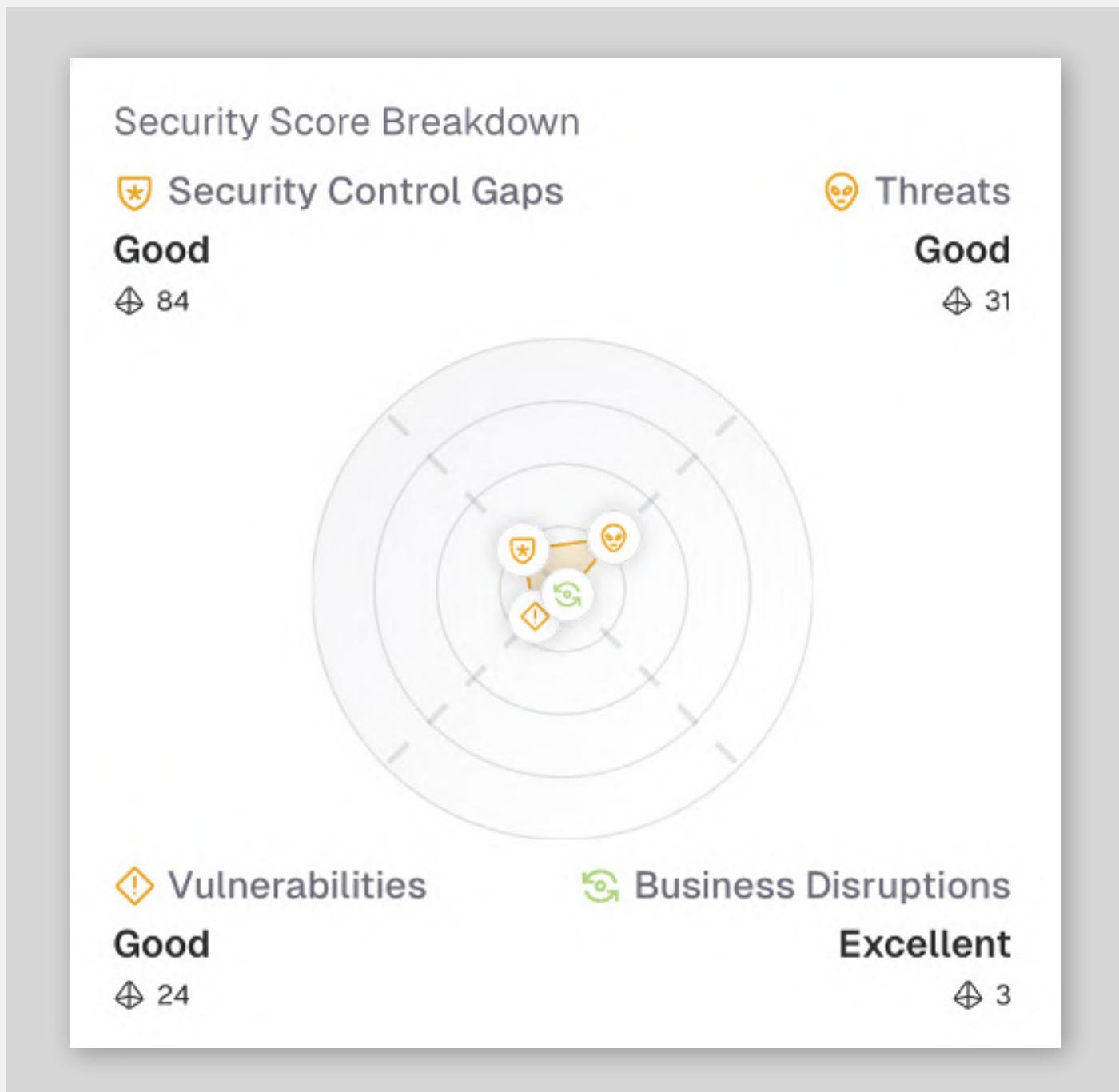
SEVERITY	CONFIDENCE	TAGS			
! Very High	90	Nikas	Basic Demo	Bmed Demo	Add Tags
CVE	ASSET	PORTS	TECHNOLOGY	VERSION	VENDOR
9.0 CVE-2024-4577	danamon.co.id	80	php	*	php
CONFIDENCE REASON		TARGETED VECTOR		SOURCE CATEGORY	
Detected by Check Point Active Vulnerability Scan		Business		Attack Surface Monitoring	
DESCRIPTION					
Argos Active Vulnerability Scan has detected and exploitable vulnerability on an exposed company asset. Evidence supporting this exploitability is detailed in the section below.					
In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.					
Security vulnerabilities are flaws in a software product that can be exploited to compromise an application or system. Active exploits aim to disrupt performance, steal data, and hijack computer resources, putting accessible systems and assets at risk.					

This combination gives vulnerability and SOC teams a shared language. Instead of arguing about severity, they discuss risk in terms of exposure paths, compensating controls, and active adversary activity. The list of exposures requiring action shrinks dramatically. And remediation work begins to have visible impact.



3. Business-aware risk scoring

Not all applications, users, or systems carry equal risk. A misconfiguration on a development server does not have the same implications as a reachable vulnerability on a payment processing system. Mature exposure programs incorporate business impact directly into their scoring. This allows executives and risk leaders to understand exposure not as a technical problem, but as a business problem. It also gives teams a common way to answer the question: what happens if this is compromised.



4. Continuous validation

A critical trait of well-run exposure programs is their avoidance of unvalidated changes. Teams validate patches, configuration changes, virtual patches, and control updates before enforcement. This prevents disruptions to business applications and reduces the friction often found between security and infrastructure teams. Validation builds trust. When teams know a remediation has been tested, they act faster. And when operations teams see that changes do not break systems, collaboration improves. Validation accelerates risk reduction by eliminating hesitation.

Network

Business Disruption

Classified as disruptive to business operations for the following reasons:

- High-risk application 0%
- CPU-intensive protections 100%
- Potential business disruption 0%

Controls Hardening

Control	Status	Progress (%)	Actions	Overall Status	Reason (%)
Network Hardening	Disabled	42%	Safe To Enable	Protected	53%
Endpoint Hardening	Detected	39%	Safe To Remediate	Protected	61%
OS Hardening	Detected	28%	Safe To Remediate	Protected	73%





5. Safe-by-design remediation

Good exposure management does not rely solely on patching. It uses a mix of options like compensating controls, virtual patching, access restrictions, takedowns, configuration corrections, and identity adjustments. Teams choose a path based on risk, timing, and business context. For example, if a patch carries operational risk, activating an IPS protection or tightening segmentation may neutralize the exposure safely while the patch is tested.

The key is that remediation becomes proactive, not reactive. Exposures are addressed quickly, consistently, and without unnecessary business impact.

The screenshot shows a remediation task for a host named 'r81-gw-1' under 'Protection Hardening'. It indicates that 8 hosts are vulnerable to CVE-2021-34527. The task is labeled 'Remediate' and includes tags for 'Critical', 'CISA', 'CERT/CC', 'Armis', and 'Engineering'. A note from CISA and CERT/CC states: 'This activity is reported by CISA and CERT/CC'. The 'Highlights' section shows three categories: 'Root Cause' (with an icon of a document and a checkmark), 'Remediation' (with an icon of a shield and a minus sign), and 'Posture Gain' (with an icon of a shield and a plus sign). Below these, specific actions are listed: 'Protection is in 'Detect' mode' (with an icon of a document and a checkmark), 'Change action to 'Prevent'' (with an icon of a shield and a minus sign), and '0.07%' (with an icon of a shield and a plus sign). A note at the bottom states: 'No false positive detections were recorded for this protection "Remote Code Execution" in the past seven days. Enabling this protection holds no business impact, and will improve your security posture against CVE-2021-34527 that was spotted in real life attacks and that 5abcdcd_d17 is vulnerable to'.



6. Cross-team collaboration

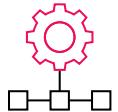
One of the biggest differentiators of mature exposure programs is their ability to move exposures to closure across multiple teams. This requires workflow alignment between security, IT, DevOps, cloud, and risk.

Freshservice ITSM Freshworks IT Service Management (ITSM) Through Threat Exposure Management (TEM), Freshservice to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	IT Service Management ServiceNow IT Service Management (ITSM) By extending Threat Exposure Management (TEM) into ServiceNow to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Jira ITSM Atlassian IT Service Management (ITSM) Powered by Threat Exposure Management (TEM), Jira to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Microsoft Teams Microsoft Collaboration Threat Exposure Management (TEM) extends Microsoft Teams to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect
ServiceDesk Plus Manage Engine IT Service Management (ITSM) By extending Threat Exposure Management (TEM) into ManageEngine ServiceDesk Plus to improve visibility, reduce exposures, and optimize security... Capabilities + Connect	Slack Slack Collaboration Threat Exposure Management (TEM) enhances Slack to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Torq Torq Security Orchestration, Automation and Response... Threat Exposure Management (TEM) augments Torq to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	
Freshservice ITSM Freshworks IT Service Management (ITSM) Through Threat Exposure Management (TEM), Freshservice to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	IT Service Management ServiceNow IT Service Management (ITSM) By extending Threat Exposure Management (TEM) into ServiceNow to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Jira ITSM Atlassian IT Service Management (ITSM) Powered by Threat Exposure Management (TEM), Jira to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Microsoft Teams Microsoft Collaboration Threat Exposure Management (TEM) extends Microsoft Teams to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect
ServiceDesk Plus Manage Engine IT Service Management (ITSM) By extending Threat Exposure Management (TEM) into ManageEngine ServiceDesk Plus to improve visibility, reduce exposures, and optimize security... Capabilities + Connect	Slack Slack Collaboration Threat Exposure Management (TEM) enhances Slack to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	Torq Torq Security Orchestration, Automation and Response... Threat Exposure Management (TEM) augments Torq to improve visibility, reduce exposures, and optimize security operations. Capabilities + Connect	

In effective programs:



Security identifies and prioritizes the exposure



Infrastructure assesses the remediation path



SOC validates that controls enforce the right protections



Cloud and DevOps own configuration and identity fixes



Risk teams monitor exposure dwell time and program maturity

This practice turns exposure management into a living process rather than a series of independent tasks. It reduces bottlenecks and speeds up remediation cycles.

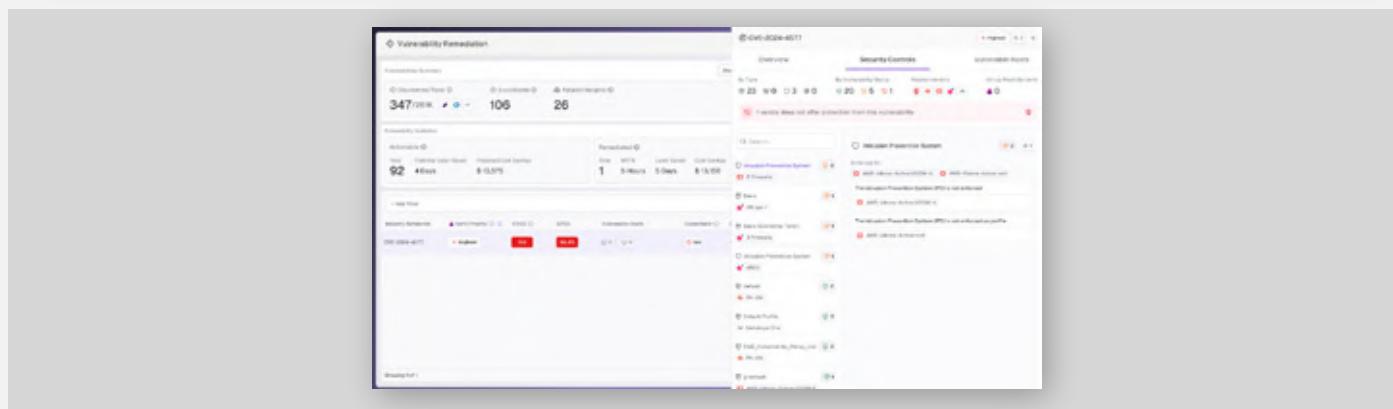


7. Metrics that measure real progress

Good exposure programs measure outcomes. They focus on metrics that reflect actual risk reduction, not activity volume. Key metrics include:

- Exposure dwell time
- Threat trends over time
- Mean time to safe remediation
- Exposure reduction percentage
- Validation success rate
- Ratio of exposures addressed through compensating controls
- Business impact reduction
- Security Posture Improvement vs Decline

These metrics help leaders communicate progress to the board and regulators. They also make it possible to track whether the exposure program is improving over time or whether underlying processes need correction.



This model becomes the backbone for aligning teams that previously worked in isolation. Now, they reduce noise, improve focus, accelerate remediation, and decrease the likelihood of successful compromise.

Chapter 4

The Mobilization Gap

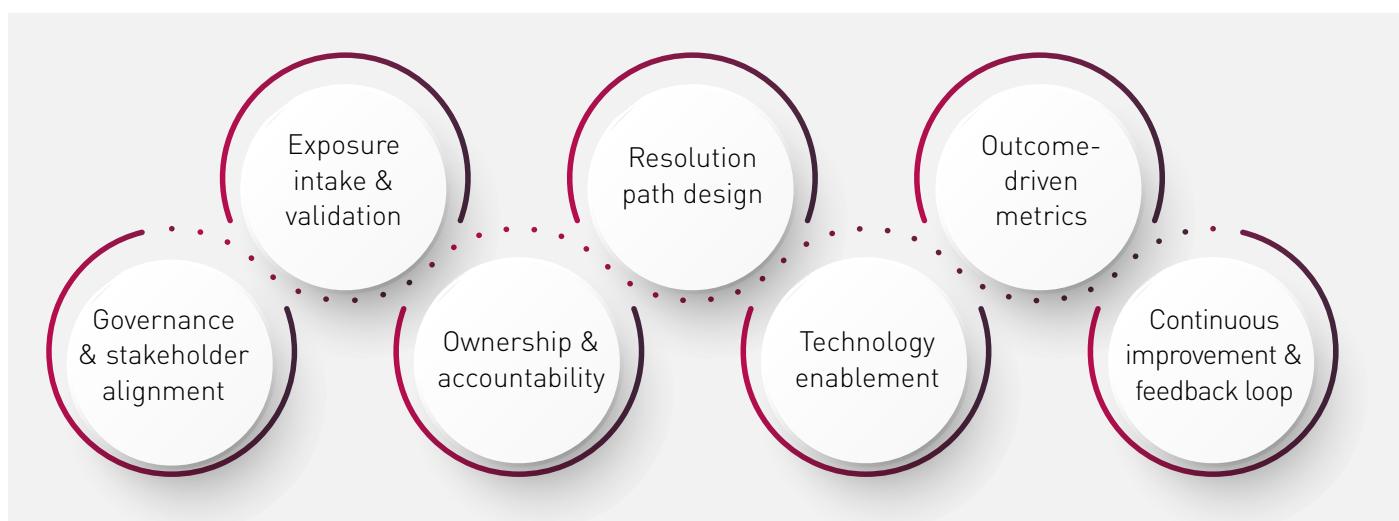
The gap between knowing what is wrong and taking the right action quickly is where modern breaches happen. This is the mobilization gap, and it is arguably the most overlooked weakness in cyber security today.

Security teams often assume that prioritization is the hardest part of exposure reduction, but prioritization is only meaningful if it leads to action. In practice, the largest delays happen after an exposure has already been identified, scored, and communicated. The challenge is not visibility or execution, it's both.

Understanding the mobilization gap begins with recognizing what stands in the way of action.

Fragmented ownership	Misaligned priorities across teams	Manual and inconsistent workflows	Lack of validation before remediation	No unified system of accountability
Each team addresses its own alerts, but no one owns the outcome. This leads to delays, confusion, or, worse, inaction.	Mobilization requires all teams to view exposures through a single, shared context. Without that, even the best prioritization model cannot translate into coordinated action.	Teams spend more time reconciling data than reducing risk. Meanwhile, exposures remain open, sometimes for weeks or months. Attackers do not wait for change management cycles to complete.	When remediation actions are unvalidated, teams slow down. They seek approvals, run manual tests, or defer action entirely. These delays add to exposure dwell time and increase the likelihood of compromise.	Infrastructure teams manage changes but do not always understand the risk context. Leadership sees reports but lacks insight into how exposures progress from discovery to closure.

Mobilization is not the end of the exposure management journey. It is the moment where security efforts turn into outcomes. It connects people, processes, and technology in a way that allows organizations to reduce risk continuously, not periodically.





Chapter 5

How Check Point Maps to CTEM

Exposure management is not a product. It is a discipline. A program. A way for security, IT, cloud, and risk teams to work from a shared understanding of what is important and how to fix it safely. But programs do not operate in the abstract. They require data, context, validation, and workflows that connect strategy to reality.

The Check Point approach aligns directly with the CTEM framework by combining three pillars into a unified capability:



Unified Threat Intelligence – Know What's Targeted

Attackers don't start from your CVEs - they start from your attack surface. Check Point combines the industry's richest threat intelligence with live external-risk visibility - brand abuse, leaked credentials, dark-web chatter, phishing kits - all mapped to your environment.

Outside-in insight meets inside-out telemetry from security tools across network, cloud and endpoints. You don't just see exposures; you see what's being weaponized right now.



Vulnerability Prioritization – Prioritize Your Risk

Attackers don't start from your CVEs - they start from your attack surface. Visibility alone doesn't reduce risk. Check Point correlates vulnerabilities, misconfigurations, and control gaps across your hybrid environment, ranking them by exploitability, exposure level, and existing compensating controls.

Every finding is scored dynamically and tied to live adversary behavior, so teams know not just what's critical, but what's critical to fix first. The result: a short, verified list of exposures that truly introduce risk to your business - prioritized, validated, and ready for safe remediation.



Safe Remediation - Close the Loop Without Breaking Anything

Remediation without disruption is the new security benchmark. Check Point provides risk reduction through virtual patching, IPS activations, IoC dissemination, adaptive blocklists, phishing-kit takedowns, and configuration hardening, validated for business continuity before enforcement.

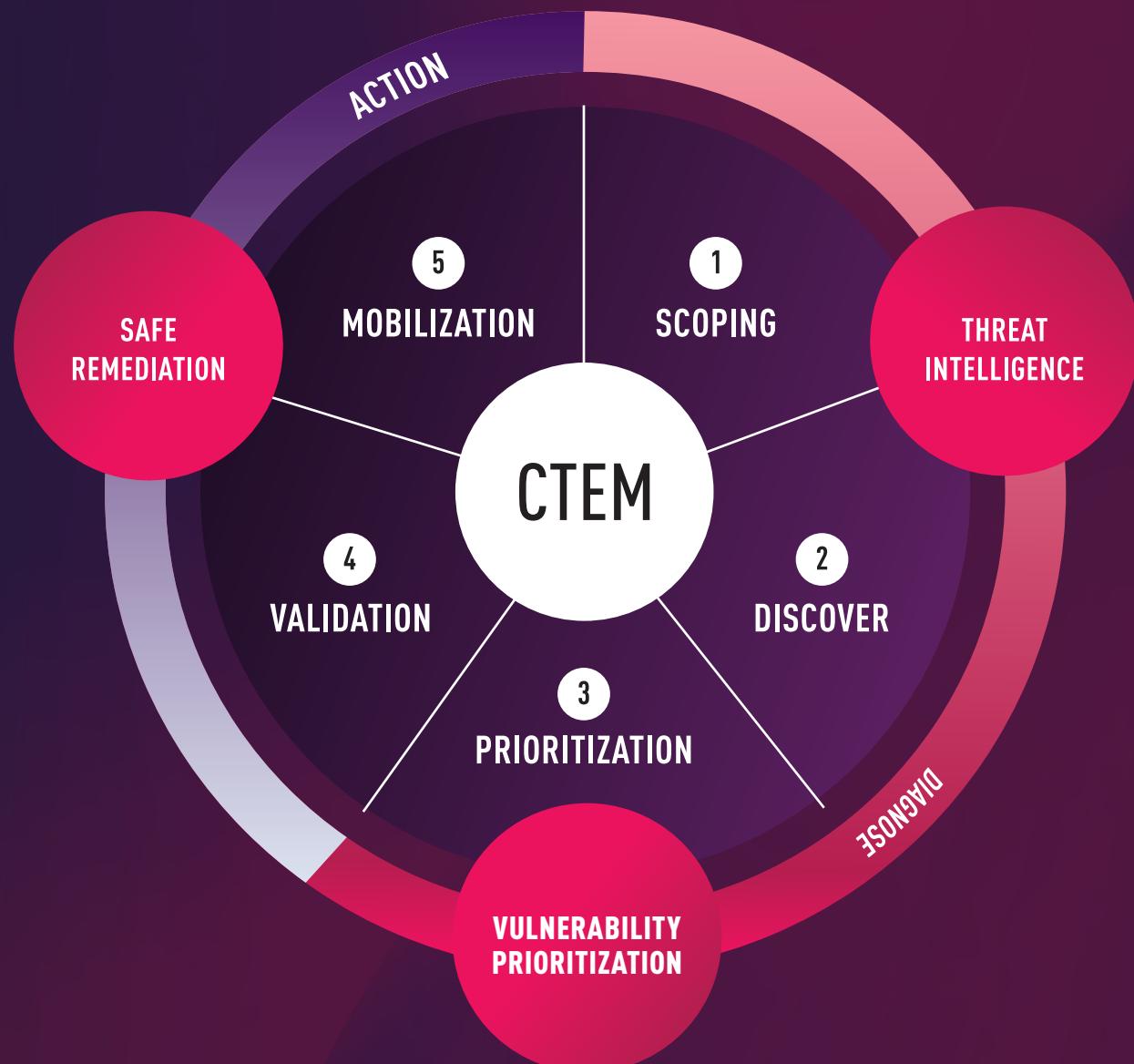
Externally, attacker infrastructure is dismantled. Internally, protections are optimized and re-enabled where coverage was missing or misconfigured. The result: continuous exposure closure - safe, verified, and measurable.

Each pillar maps to CTEM phases and enables the continuous reduction of exposure dwell time across internal and external surfaces.

A mature exposure management program completely restructures the model from reactive to preemptive. Instead of paying for incidents, unplanned downtime, and rushed remediation, organizations invest in reducing exposures before they cause harm. This is where the economics flip. When teams prioritize and validate changes before enforcement, and mobilize remediations quickly and safely, the entire cost structure improves fewer incidents, fewer hours spent on noise, fewer disruptions, and better use of existing controls.

Rather than adding more tools or hiring more analysts, exposure management helps organizations reclaim efficiency from within. SOC teams spend less time triaging low-value findings. IT spends less time responding to chaotic requests. Threat intelligence teams focus on what is actionable, not everything that moves. Compliance work shrinks because exposures do not linger. And business units feel the impact through fewer interruptions and stronger operational continuity.

The economic benefit of exposure management is simple - by lowering exposure dwell time, you reduce both the probability and the cost of bad outcomes. Organizations that make this change see a smaller reactive TCO, a more efficient preemptive TCO, and a clear ROI driven by fewer incidents, reduced downtime, and better utilization of existing technology. The financial argument becomes as strong as the security argument, which is it costs far less to prevent exposures than to react to them.



1. Scoping

Continuously define and map the expanding attack surface from external assets to internal infrastructure, cloud, network, and security controls.

2. Discovery

Identify vulnerabilities, misconfigurations, exposures, and attacks across the security stack with unified correlation.

3. Prioritization

Rank risk based on exploitability, business context, and exposure severity, not CVSS alone, to eliminate noise and false urgency. This allows organizations to focus on exposures that are both actionable and relevant.

4. Validation

Confirm real-world exploitability, verify control efficacy, and eliminate false positives to ensure remediation targets real risk. Validation enables faster action because teams can make decisions with confidence.

5. Mobilization

Safely enforce remediation across firewalls, cloud, endpoints, network, and security controls - agentless, API-driven, fully validated, and non-disruptive.

Exposure management programs fail when they rely on disjointed tools, manual workflows, and siloed functions. Programs succeed when intelligence, assessment, validation, and remediation are connected.

The value of mapping CTEM to a concrete platform is not in the platform itself. It is in showing how the principles become operational reality. Exposure data becomes understandable, threat activity becomes actionable, validated remediations become safe and predictable, ownership becomes clear, and risk becomes measurable.





Chapter 6

Exposure Management in Action

Let's take a look at how we turn intelligence into action and safely mitigate exposures before patching

The screenshot shows the Check Point Attack Surface Monitoring (ASM) interface. The top navigation bar includes 'Attack Surface Monitoring > Assets'. The main dashboard features several key metrics and charts:

- Posture Score:** 305 (Very High, 69)
- Categories Contributing to Posture Score:** Vulnerabilities (42%), Cloud Storage (33%), Hijackable Subdomains (23%), and Exposed Interfaces (6.9%).
- Risk Reduction by Asset Severity:** Very High (69), High (3), Medium (231), and Low (2).
- Scoping Management:** Tasks include 'Validate Primary Assets (27)', 'Decide on ASM Monitoring for Assets (3)', and 'Decide on TI Monitoring for Domains (29)'.

The main table displays 23,056 assets, filtered to show 'Monitored (ASM)' and 'Monitored (ASM + TI)'. The table columns include:

ASSET	ASSET SEVERITY	ACTIVE ALERTS	EXPOSURE ITEMS	DISCOVERY INFO	PARENT ASSETS
plymouthrock.prucenter.co	1	4 alerts	0 items	99 DNS, 1 Certificate	prucenter.co
54.68.225.162	1	3 alerts	1 items	99 CERTIFICATE, 1 DNS	prucenter.co
35.79.149.250	1	3 alerts	1 items	99 CERTIFICATE, 1 DNS	pru-trust.co.jp
64.187.239.229	1	3 alerts	2 items	99 DNS, 1 Certificate	rocksolidtreas...

A high severity risk has been discovered and identified as an internet-facing server running a vulnerable version of a known protocol. Check Point intelligence confirms that this CVE is actively exploited in the attackers' campaigns.

The screenshot shows the Check Point Exposure Management interface. At the top, it displays the domain 'danamon.co.id' with a status of 'Monitored (ASM)'. Below this, there are sections for 'Posture Alerts' (1), 'Discovery Origin' (danamon.co.id), 'Descendants' (0), 'Direct Children' (0), and 'Last AV Scan' (NA). On the left, a sidebar lists 'Risk', 'Discovery Details', 'Exposure Items (0)', 'Technologies (0)', 'Certificates (0)', and 'Status History'. The main content area is titled 'SECURITY POSTURE ALERTS (1)' and shows a single alert: 'Exploitable Vulnerability found on a Company Asset' with Alert ID ARG-5195, Severity 1 (red), Confidence 90 (green), and Created Date June 11, 2025.

When investigating the vulnerability, the exposure management solution enriches it with intel from the deep and dark web, in this example, there are over 50 mentions of this CVE, and proof that it is exploited by a threat actor group "Ms up edge".

This screenshot provides a detailed view of the 'Exploitable Vulnerability found on a Company Asset' alert. The alert is categorized as a 'Vulnerability' with a 'Very High' severity and a confidence of 90. It is associated with the domain 'danamon.co.id' and the CVE 'CVE-2014-1637'. The alert was detected by 'Active Exposure Validation' and is categorized under 'Business' with 'Attack Surface Monitoring'. The alert status is 'Open' (June 11, 2025) and has been 'Acknowledged'. The 'RECOMMENDATIONS' section notes that a fix for the vulnerability has been made available in PHP versions 8.3.8, 8.2.20, and 8.1.29. The 'DISCUSSION BOARD' section shows a message from 'Cyberint Support Analyst' stating 'No comments have been added yet'.



By using active exposure validation, organizations can confirm that it is not just vulnerable but exploitable. Reviewing the evidence, an arbitrary code was ran on a server and a response was received, which confirms it is exploitable.

The second layer of exposure management is continuously assessing and prioritizing exposures. Check Point correlates the Attack Surface Monitoring finding with internal telemetry, logs, our threat intelligence, vulnerability scanners, and validates that the asset is reachable from the internet, no compensating IPS or WAF control is active, and the asset is indeed business critical. All the related security controls and their vulnerability status can be seen, where there is a virtual patch or what's actually been enforced.



⌚ Vulnerability Remediation

Hide Analytics

Vulnerabilities Summary

Discoveries / Total: 347 / 261K | Exploitability: 106 | Related Insights: 26

Discoveries | Virtually Patched

Vulnerabilities by Status

Virtual Patch Available: 171 | Virtually Patched: 140 | Virtual Patch Unavailable: 31

Vulnerabilities Discovered: 171

CVSS 8.7: 140 | Exploitability: 55

140 | 48 | 55

Vulnerability Statistics

Actionable: 92 | Potential Labor Saved: 4 Days | Projected Cost Savings: \$13,575

Remediated: 1 | MITRE: 5 Hours | Labor Saved: 5 Days | Cost Savings: \$13,156

Last Week

+ Add Filter

CVE-2024-4577

Industry Reference: Veris Priority: CVSS: EPSS: Vulnerable Hosts: Exploitability: Cybersecurity Agency: Vulnerability Status: Open Insights: MITRE Techniques: Vulnerability Source:

CVE-2024-4577 | Highest | 5.8 | 94.4% | 1 | Yes | CISA | 1 | 8 | 20 | 2 | T1106 | +6 | N/A

Showing 1 of 1

Vulnerability Remediation

Vulnerabilities Summary

Discovered/Total: 347/261K | Exploitable: 106 | Related Insights: 26

Vulnerability Statistics

Actionable	Remediated
Total: 92 Potential Labor Saved: 4 Days Projected Cost Savings: \$13,575	Total: 1 MTTR: 5 Hours Labor Saved: 5 Days Cost Savings: \$13,156

[Add Filter](#)

Industry Reference

CVE-2024-4577	Verilis Priority: Highest	CVSS: 9.8	EPES: 94.4%	Vulnerable Hosts: 0	Exploitable: Yes

Showing 1 of 1

CVE-2024-4577

Overview **Security Controls** **Vulnerable Hosts**

By Type **By Vulnerability Status** **Related Vendors** **Virtual Patch By Vendor**

1 vendor does not offer protection from this vulnerability

Search...

Profile	Control	Enforced On
	Intrusion Prevention System	2 Firewalls
	Basic	1 r81-gw-1
	Basic (Cloned by Tamil)	5 Firewalls
	Intrusion Prevention System	1 r8100
	default	2 PA-VM
	Default Profile	3 Netskope One
	DMZ_Vulnerability_Policy_198	2 PA-VM
	q-default	1 PA-VM

From here organizations can be taken directly to the insight of the exposed asset. With visibility into a protection that is not activated, they can move it to detect mode directly on the firewall.

• r81-gw-1 | Protection Activation

You are not protected for CVE-2024-4577

Protection Activation 05/05/2025 11:11

Configuration Misconfiguration 11/18/2024 02:00

Intrusion Prevention System Threat protection...

High CISA

This activity is reported by CISA

Highlights

Root Cause	Remediation	Posture Gain
Protection in 'Inactive' mode	Change action to 'Detect'	0.59%

Enabling all security protections is an industry best practice. CVE-2024-4577 was spotted in real life attacks and "PHP CGI Argument Injection (CVE-2024-4577)" protection status is currently "Inactive" and is impacting your security posture exposing you to attacks.

The 3rd layer of exposure management is, safe, preemptive remediation, virtual patching in our case. Once an organization clicks confirm, the mitigation takes place, agentless, all directly via APIs.

Protection Name	Configured Action	Action After Remediation
PHP CGI Argument Injection (CVE-2024-4577)	Inactive	Detect

Affected Targets: 1 selected 1 items

PHP CGI Argument Injection (CVE-2024-4577) is exposing you to attacks.

Cancel Confirm

The screenshot shows a software interface for managing network security policies. On the left, a sidebar lists categories like 'Access Control', 'Threat Prevention', and 'HTTPS Inspection'. The main area displays a table of threat profiles, with one row selected for 'Microsoft Windows Media Foundation H265 Stream Parsing Remote Code Execution (CVE-2024-4577)'. The table columns include 'Industry Reference', 'Release Date', 'Update Date', 'Performance Impact', 'Severity', 'Confidence Level', and 'Strict'. To the right of the table is a 'Filters' panel with options for 'Performance Impact', 'Type', 'Severity', and 'Confidence Level'. Below the table, a 'Details' tab is selected, showing threat information: Attack ID (CPAI-2020-1004), Last Update (13-October-2020), and Industry References (CVE-2024-4577). The 'Threat Description' section states: 'A code execution vulnerability exists in Microsoft Windows Media Foundation. The vulnerability is due to improper validation of H265 media files. A remote attacker could exploit the vulnerability by enticing a victim user to open a maliciously crafted media file or open the folder containing the file.' The 'IPS Protection' section is partially visible.

Security management of the firewall now activates the relevant IPS Protection for this CVE on affected gateways (or WAFs). The change is validated for zero business disruption, ensuring false positives are eliminated. And now, we have closed the loop on the alert. With Check Point Exposure Management, organizations can resolve every exposure before attackers can weaponize it. Unify threat intelligence, vulnerabilities, and safe remediation into a prioritized and preemptive defense loop - so you don't just see risk, you eliminate it.



Chapter 7

Building Your Exposure Reset Roadmap

Exposure management is not a single project. It is a performance discipline that evolves gradually, gains strength over time, and requires alignment across teams. The most successful organizations do not treat exposure management as a tool rollout. They treat it as a program — one that blends technology, process, and roles into a continuous loop of understanding and action.

The 30-60-90 Exposure Reset Plan:

The following roadmap is designed for organizations at any maturity level. It creates momentum by focusing early on clarity and alignment, then expands into prioritization, validation, and mobilization as processes mature.

First 30 Days: Establish clarity and alignment

Focus areas	Details	Outcome
Scope the environment	Identify critical systems, cloud resources, external surfaces, identities, and controls that must be included. This becomes the core of your CTEM scoping phase.	
Create a unified exposure catalogue	Align teams on the categories that crucial: vulnerabilities, misconfigurations, identity risks, external exposures, and missing controls.	
Define ownership	Clarify which teams own which exposure types, and establish escalation paths for cross-domain issues.	A clear understanding of what needs protection, how it will be measured, and who is responsible.
Establish business context	Map key applications and services to business impact. This becomes essential during prioritization.	
Integrate internal and external visibility	Connect internal scanning and telemetry with external surface monitoring and threat intelligence. Even basic integration at this stage dramatically reduces blind spots.	

Once the scope and ownership are set, the next phase focuses on reducing noise and establishing a defensible model for where to act first.

Days 30-60: Prioritize and validate

Focus areas	Details	Outcome
Implement context-driven prioritization	Incorporate exploitability, reachability, business impact, and control coverage. This ensures teams focus on what truly reduces risk.	
Align cross-team workflows	SOC, vulnerability management, cloud, infrastructure, and risk teams should review exposure lists together in a structured cadence. The goal is to build shared understanding.	A working exposure prioritization model and the beginnings of safe, predictable remediation workflows.
Establish validation practices	Before enforcing changes, test virtual patches, IPS rules, policy updates, and access adjustments for performance impact.	
Connect prioritization to action	Start routing validated remediations into existing ticketing and change management processes. This is where exposure management begins to influence day-to-day operations.	



Days 60-90: Operationalize mobilization

Focus areas	Details	Outcome
Create predefined remediation paths	Define your standard approaches like direct/virtual patching, compensating controls, configuration hardening, identity adjustments, risk acceptance or exceptions. Teams should know when to use each path.	
Establish consistent exposure SLAs	Tie timelines to risk, not severity can be for example: high-risk exposures: 48 hours, medium-risk exposures: one week, low-risk exposures: next cycle.	
Introduce a mobilization role	This does not need to be a new full-time job. A designated lead, often in vulnerability management or GRC, coordinates exposure workflows across teams and ensures closure.	A functioning exposure management program where exposures consistently move from discovery to closure with transparency and accountability.
Automate correlation and routing	Integrate exposure findings with ITSM, SOAR, and collaboration tools so that prioritized exposures automatically reach the right owners.	
Start measuring dwell time	Begin tracking how long exposures remain open from discovery to safe remediation. This metric becomes the anchor for program improvement.	

This phase focuses on transforming exposure management from an ad-hoc effort into a repeatable, end-to-end process supported by reliable workflows.

After the first 90 days, exposure management settles into an ongoing rhythm that mature organizations follow consistently. Teams meet weekly to review new exposures, align on prioritization changes, and discuss validation results. Each month, they step back to assess trends, measure exposure dwell time, track control coverage, and identify recurring problem areas. Quarterly, they convert exposure data into business aligned insights, reporting on reduction percentages, time to safe remediation, validated control improvements, reachable attack path reduction, and the retirement of external exposures. Throughout the year, they continuously rescope the environment as new cloud services, security controls, and vendors emerge, and they refine validation tests as applications and networks evolve.

The organizations that sustain this cadence of exposure management, scoping, discovering, prioritizing, validating, mobilizing, and repeating it -



Are the ones that see the fastest improvement, the sharpest reduction in risk, and the strongest confidence in their overall security posture.

Taking back control

The great challenge in cyber security is no longer visibility. It is control.



Control over misconfigurations.



Control over vulnerabilities.



Control over identities.



Control over external surfaces.



Control over how quickly exposures move from discovery to safe remediation.

Exposure management gives organizations this control.

It creates the discipline, structure, and repeatability that allow teams to stay ahead of adversaries, not chase them. It prepares the organization for a world where environments change constantly and attackers move faster than ever before.



Taking back control begins with a decision.

The decision to stop reacting and start reducing.

To stop drowning in findings and start focusing on outcomes.

To replace scattered tools and workflows with a unified exposure program.

The organizations that make this upon themselves will define the next era of cyber resilience. And the journey begins with one simple commitment: reduce what attackers can exploit, continuously and safely.

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, 2026. All Rights Reserved.