reflectiz

CISO'S EXPERT GUIDE TO CTEM

Executive Summary

In today's hectic cybersecurity landscape, organizations with online presence need effective strategies to manage and mitigate security risks. This report compares three key approaches to security risk management: Vulnerability Management (VM), Attack Surface Management (ASM), and Continuous Threat Exposure Management (CTEM).

Traditional Vulnerability Management focuses on identifying and patching known vulnerabilities within internal infrastructure but suffers from limitations such as point-in-time assessments and lack of business context. Attack Surface Management provides broader visibility into external-facing assets but may miss internal risks and lacks continuous validation capabilities.

CTEM emerges as the most comprehensive approach, combining the strengths of both VM and ASM while addressing their limitations.

It provides continuous monitoring of both internal and external assets, validates threats through testing and simulation, and prioritizes remediation based on business impact. While CTEM implementation can be resource-intensive and complex, it offers significant advantages in risk reduction, improved efficiency, and enhanced visibility across the entire attack surface.

Gartner predicts that by 2026, organizations prioritizing security investments based on CTEM programs will be significantly less likely to experience breaches. This also marks a shift from merely fixing vulnerabilities to exposure management.

For CISOs looking to strengthen their security posture, CTEM represents a mature and effective strategy for managing today's complex threat landscape, though it should be implemented strategically with careful consideration of organizational resources and capabilities.

Organizations implementing CTEM vs. Traditional VM/ASM see:

40%

reduction in mean time to detect (MTTD) security incidents.

35%

faster remediation cycles, leading to **fewer breach windows.**

25%

decrease in false positives, improving analyst efficiency.

2x

increase in attack surface coverage, including external and internal risks.

CTEM is projected to grow at a CAGR of 10.1% from 2024 to 2029.

Source 1 | Source 2 | Source 3

Vulnerability Management (VM)

Definition:
VM has been a cornerstone of cybersecurity for decades. It focuses on identifying and mitigating known vulnerabilities within an organization's internal IT infrastructure.

Key Features:

Vulnerability Scanning
Regularly scans systems and applications for known weaknesses using vulnerability scanners and databases like CVE.

Prioritization
Risk scoring based on severity and exploitability of vulnerabilities.

Remediation Tracking
Workflow for patching and mitigating identified vulnerabilities.

Challenges:

Limited Scope
Primarily focuses on known vulnerabilities within the internal network perimeter.

Point-in-Time Assessments
Traditional VM scans leave gaps between assessments where new vulnerabilities may emerge.

Lack of Business Context
Tools may not prioritize based on actual business impact.

Vulnerability Management (VM) Vendor Comparison

Vendor	Key Strengths	Use Cases
ManageEngine	Comprehensive VM with integrated **patch management, compliance tracking**, and automated remediation.	**Enterprises & IT Teams –** Best for organizations needing a **unified VM and patching solution** to reduce manual efforts and meet compliance (e.g., SOC 2, ISO 27001).
secpod	Lightweight, **agent-based scanning** with AI-driven risk prioritization and continuous monitoring.	**Mid-sized businesses & MSSPs –** Ideal for those looking for a **low-overhead, automated vulnerability assessment** without complex infrastructure.
FLASHPOINT	Intelligence-driven VM with **deep insights into emerging threats** and threat actor tracking.	**Financial & Government Sectors –** Perfect for **threat intelligence-driven risk assessment,** ensuring proactive mitigation of high-risk vulnerabilities.
invicti	Automated **web application security scanning** with **built-in DAST and IAST** capabilities.	**DevSecOps & Software Development –** Best for companies needing **continuous web security testing and secure SDLC integration.**
deepfence	**Container and Kubernetes-native** VM solution with real-time runtime protection.	**Cloud & Microservices Environments –** Essential for securing **cloud-native applications, containers, and serverless workloads** from runtime threats.

Attack Surface Management (ASM)

Definition:
ASM takes a broader perspective by focusing on the organization's attack surface, which includes all assets that are exposed to the internet and potentially exploitable by attackers.

Key Features:

External Asset Discovery
Discovers internet-facing assets, including websites, applications, APIs, and cloud resources.

Security Posture Monitoring
Assesses the security configuration of these assets and identifies potential weaknesses.

Risk Prioritization
Focuses on vulnerabilities that are most likely to be exploited by attackers.

Threat Intelligence Integration
Identifies emerging threats and vulnerabilities.

Challenges:

Limited Internal Visibility
ASM provides excellent external visibility but may lack insight into internal vulnerabilities.

Lack of Continuous Validation
Risks may not be validated, leading to potential false positives.

Vulnerability Management (VM) Vendor Comparison

Vendor	Key Strengths	Use Cases
BITSIGHT	Security ratings platform that provides **continuous monitoring of third-party risks and benchmarking against industry peers.**	**Vendor Risk Management & Compliance** – Ideal for organizations needing **third-party risk assessment and security scoring** for partners, suppliers, and vendors.
HALO SECURITY	Comprehensive **external attack surface discovery** with built-in vulnerability scanning and security assessments.	**SMBs & Enterprises –** Best for **identifying exposed digital assets** and mitigating risks from unknown or misconfigured external-facing infrastructure.
CYCOGNITO	AI-driven **asset discovery and risk prioritization**, identifying shadow IT and cloud misconfigurations.	**Global Enterprises & Cloud-Heavy Businesses** – Designed for organizations needing **automated external attack surface mapping and continuous threat monitoring.**
RiskProfiler	Focuses on **shadow IT risk visibility**, helping businesses uncover hidden and orphaned assets.	**Banks & Regulated Industries** – Ideal for companies needing to **minimize unmonitored internet-facing assets** to prevent compliance violations and breaches.
weborion by cloudsine	Specializes in **web security posture management**, including website defacement protection and SSL monitoring.	**E-commerce & Media Companies –** Best for businesses needing **continuous monitoring of web applications** to prevent defacement, hijacking, and certificate mismanagement.

Continuous Threat Exposure Management (CTEM)

Definition:
CTEM is a more holistic and proactive approach that builds upon the strengths of both VM and ASM. It emphasizes continuous monitoring, validation, and prioritization of threats across the entire attack surface.

Key Features:

Continuous Monitoring
Monitors the attack surface for new assets, vulnerabilities, and threats.

Risk Validation
Validates identified risks through techniques like penetration testing and attack simulation.

Business Impact Prioritization
Prioritizes threats based on potential business impact and context.

Remediation Orchestration
Automates and orchestrates remediation efforts across the organization.

Challenges:

Enhanced visibility
Provides a holistic view of an organization's threat exposure.

Preemptive measures
Enables proactive identification and validation of risks before exploitation.

Here's the **Continuous Threat Exposure Management (CTEM) Vendor Comparison Table** with key strengths and real-world use cases.

Continuous Threat Exposure Management (CTEM) Vendor Comparison

Vendor	Key Strengths	Use Cases
reflectiz	**Client-side attack detection** focusing on third-party web supply chain risks like **Magecart and formjacking.**	**E-commerce & SaaS – Perfect** for businesses relying on **third-party scripts** and **ensuring web security without impacting performance.**
Cymulate	Advanced **Breach & Attack Simulation (BAS)** platform with continuous security validation across networks, endpoints, and cloud.	**Enterprises & MSSPs –** Ideal for organizations needing **automated attack simulations** to test and improve cyber resilience in real-time.
XM Cyber	**Continuous risk validation** and **attack path analysis**, helping organizations detect lateral movement threats.	**Finance & Healthcare** – Best for **identifying hidden attack paths** and securing sensitive data from advanced persistent threats (APTs).
tenable	Comprehensive **exposure management solution,** integrating **vulnerability scanning, attack surface management, and risk-based prioritization.**	**Large Enterprises & Cloud-First Companies** – Essential for businesses seeking **unified exposure management** across hybrid environments.

PENTERA	**Automated penetration testing** platform that validates security controls and provides real-world exploit scenarios.	**Security Teams & SOCs** – Best for organizations needing **continuous, automated ethical hacking** to test and improve defenses.

Security Management Approaches Comparison

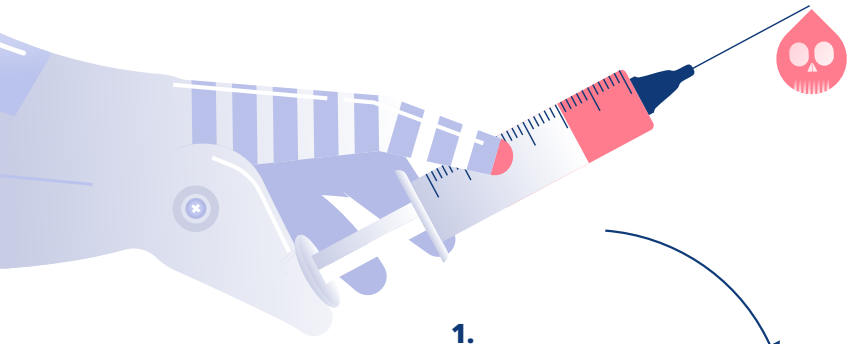
	VM	ASM	CTEM
Capability level	Limited	Moderate	Comprehensive
Scope	**Internal IT infrastructure** Focus on internal perimeter	**External-facing assets** websites, APIs, cloud resources	**Entire attack surface** internal and external assets
Focus	**Known vulnerabilities** CVE database driven	**Potential vulnerabilities** External exposure focused	**Validated threats and business impact** Continuous validation with business context
Approach	**Reactive** Point-in-time assessment	**Proactive** Regular external monitoring	**Continuous and proactive** 24/7 monitoring and validation
Validation	**Limited** Basic vulenerability	**Primarily theoretical** External observation based	**Continuous validation through testing** Including penetration testing and simulation
Prioritization	**Based on vulnerability severity** CVSS scores focused	**Based on exposure and explitability** External risk focused	**Based on potential business impact** Risk-based with business context
Remediation	**Manual tracking and patching** Traditional patching workflow	**Guidance and recommendations** Suggested mitigations	**Orchestrated and automated remedition** Automated workflow with validation

Case Study Comparison

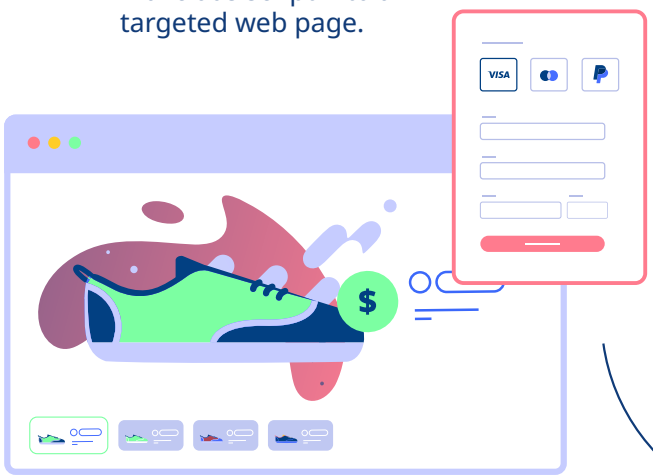
ADDRESSING FORMJACKING

Take a look at this example scenario:

A global e-commerce retailer suffered a formjacking attack that compromised its payment pages. Hackers injected malicious JavaScript into the retailer's website, intercepting customers' credit card details during checkout. The breach went undetected for weeks, causing financial loss, reputational damage, and regulatory penalties. Here's how VM, ASM, and CTEM would address the attack:



1.
Attacker injects malicious script into a targeted web page.



2.
The user loads the infected web page and makes a purchase by filling out a form.

3.
While submitting the purchase form, the data, including personal information and payment details, is sent to both the merchant and the attacker.

How the Three Frameworks Handle Formjacking Attacks

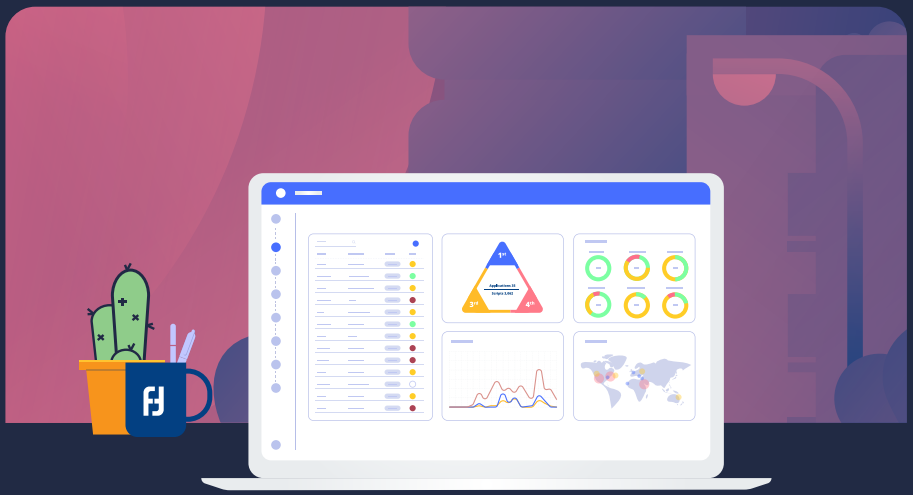
	VM	ASM	CTEM
Actions Taken	Regular scans to detect outdated CMS or plugins.	Identifies external-facing changes (e.g., modified payment page).	Simulates attacks to validate malicious JavaScript. Continuously monitors payment pages for anomalies.
Challenges/Limitations	May miss malicious script injections in client-side code.	Focuses on theoretical risks; no exploit validation.	Requires significant resources for continuous validation.
Outcome	Limited detection; reliant on periodic scans, leaving gaps in visibility.	Flags modified assets but doesn't confirm malicious activity.	Detects and prioritizes critical risks, ensuring timely mitigation of the script injection.

CTEM's continuous monitoring and attack simulation capabilities make it the most effective framework for detecting and mitigating formjacking attacks.

Conclusion

While VM and ASM remain valuable components of a security program, CTEM represents the most mature and effective strategy for managing today's complex threat landscape. Its comprehensive approach to continuous monitoring, validation, and business-aligned prioritization provides organizations with the best framework for reducing risk and improving security posture.

The key to success lies in strategic implementation, starting with critical assets and gradually expanding while maintaining focus on business objectives and resource efficiency. Organizations should view CTEM as an evolution of their security program rather than a revolution, building upon existing VM and ASM capabilities to create a more robust and effective security posture.



See for yourself how Reflectiz can help safeguard your online business

Book a demo

reflectiz