Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management

Published 16 October 2023 - ID G00796532 - 10 min read

By Analyst(s): Jeremy D'Hoinne, Pete Shoard

Initiatives: Security Operations; Meet Daily Cybersecurity Needs

Enterprises fail to reduce their patchable and unpatchable exposures to threats, yet keep implementing siloed and narrow remediation processes. IT leaders must implement continuous and repeatable exposure management processes, optimizing short-term response and longer-term security posture.

Additional Perspectives

- Invest Implications: Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management
  (18 October 2023)
- Summary Translation: Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management
  (26 November 2023)

Overview

Opportunities

- Organizations often can't patch every exposure. Though they must evolve their remediation workflow, they continue struggling to determine what deserves high priority, despite many well-curated and sorted issues. Taking the attacker's view to validate the true impact of an exposure, and the real efficacy of existing defenses, has become a critical requirement.
- Conventional "risk reduction" approaches focus on infrastructure and software vulnerabilities. However, the unpatchable attack surfaces (i.e., those found in nontraditional IT environments, such as the cloud and SaaS applications) expand quickly. Optimized exposure reduction requires a consistent approach to managing the exposures across traditional application and infrastructure silos.
- Continuous threat exposure management (CTEM) is an umbrella program for forward-looking and sustainable approaches to exposure reduction. Implementing CTEM enables closer alignment to business needs and risk impact. CTEM involves business leadership in identifying key assets and processes to defend against cyberattacks/business disruption.

Recommendations

IT leaders with a focus on resilient and modern architecture must:

- Identify and address multiple types of threat exposures by expanding from software-centric assessment tools to attack surface and attack success likeliness scenarios.
- Experiment with exposure management cycles. Start with project scopes aligned with emerging threat vectors, or where business projects are potentially harmed with most impact.
- Expand from fully automated technical remediations to more comprehensive security optimization initiatives to initiate improved cross-team mobilization.

Strategic Planning Assumption

By 2026, organizations prioritizing their security investments, based on a continuous threat exposure management program, will realize a two-third reduction in breaches.

What You Need to Know

This research is part of Gartner's Top Strategic Technology Trends for 2024.

Download the Executive Guide to Continuous Threat Exposure Management.

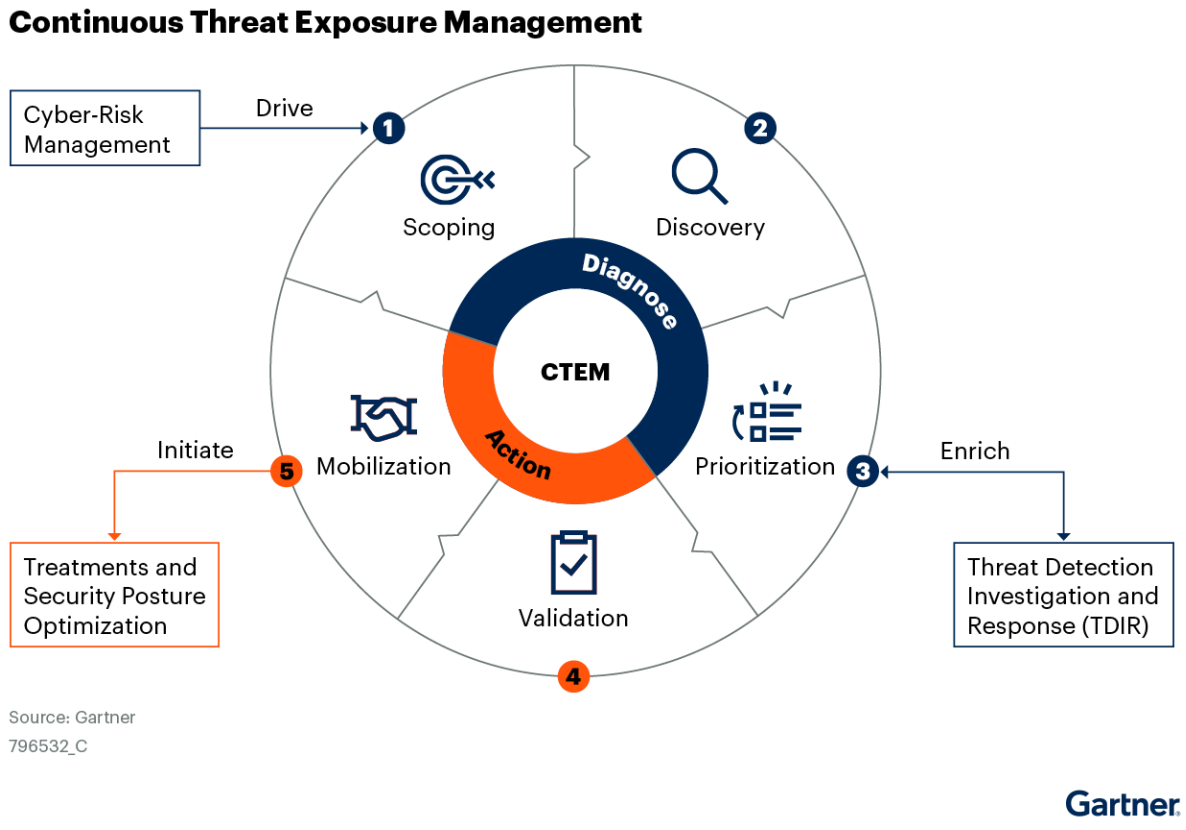
Enterprise attack surfaces continue expanding far beyond what most effective patch management programs can cover. A forward-looking defense strategy requires modernization of the assessment tool portfolio. These tools must not only inventory patchable and unpatchable exposures, but also prioritize findings based on what an attacker could really do. To achieve that, they must validate the reality of the exposure based on the ability to penetrate existing security defenses.

Because every organization has too much to fix, security posture won't improve without changes. These changes must start with the way that organizations scope their assessments and collaborate on remediation.

Continuous threat exposure management (CTEM) guides the evolution of enterprises' process for dealing with risk reduction cycles, and aims to facilitate remediations. Figure 1 shows the five steps of a CTEM cycle:

- Scoping
- Discovery
- Prioritization
- Validation
- Mobilization

Figure 1: Continuous Threat Exposure Management



CTEM impacts existing technology markets with the convergence of cybersecurity validation and exposure assessment platforms. CTEM also fosters innovation by transforming cybersecurity remediation workflows to support cross-team and cross-time-horizon planning.

During Gartner interactions with larger and well-funded organizations, security leaders report the need for better cross-pollination of skills and best practices. They acknowledge the need to go beyond the immediate time horizons. Many individual initiatives and technologies that compose a CTEM cycle are already implemented in silos with suboptimal integration and analysis of their outputs. Mobilization, the last step in a CTEM cycle, shifts the focus to teamwork because risk management programs neglect long-term optimization.

Focusing on mobilization helps facilitate effective communication and workflow channels between various teams. Security operations — in charge of exposure intelligence, and the infrastructure and operations team, often charged with security control maintenance — can then align their priorities and resource investments. Shared data resources and well-integrated remediation processes help CTEM promote a business-led approach to risk reduction.

Profile: Continuous Threat Exposure Management

Description

CTEM is a systemic approach to continuously refine cybersecurity optimization priorities. Its objective is to design actionable security exposure remediation and improvement plans that business executives can understand, and that architecture teams can act on. A CTEM cycle includes five stages: scoping, discovery, prioritization, validation and mobilization. Organizations building a CTEM program use tools to inventory and categorize assets and vulnerabilities, and simulate or test attack scenarios and other forms of posture assessment processes and technologies.

CTEM programs expand traditional cybersecurity assessment. They use cybersecurity technology to:

- Align the scopes of exposure assessment cycles with specific business projects and critical threat vectors.
- Address threat exposures, regardless of whether they're patchable. They address traditional vulnerabilities, but also more modern, unpatchable threat exposures that are relevant to these business risks and priorities (e.g., exposures in SaaS applications).
- Validate the enterprise's exposure and remediation priorities by including the attacker's perspective, and testing the effectiveness of security controls and incident response processes.
- Shift expected outcomes from tactical and technical responses to cybersecurity optimizations supported by improved cross-team mobilization.

Why Trending

Security vulnerabilities are often one of the main reasons for cybersecurity incidents. Organizations could avoid many of these vulnerabilities with better exposure management. However, decades of using vulnerability assessment tools have shown that even large, well-funded organizations can't patch every discovered vulnerability. Enterprise exposure to threat includes unpatchable issues, such as IT supply chain dependencies, operational technology environment vulnerabilities, or misconfigurations of assets and security controls.

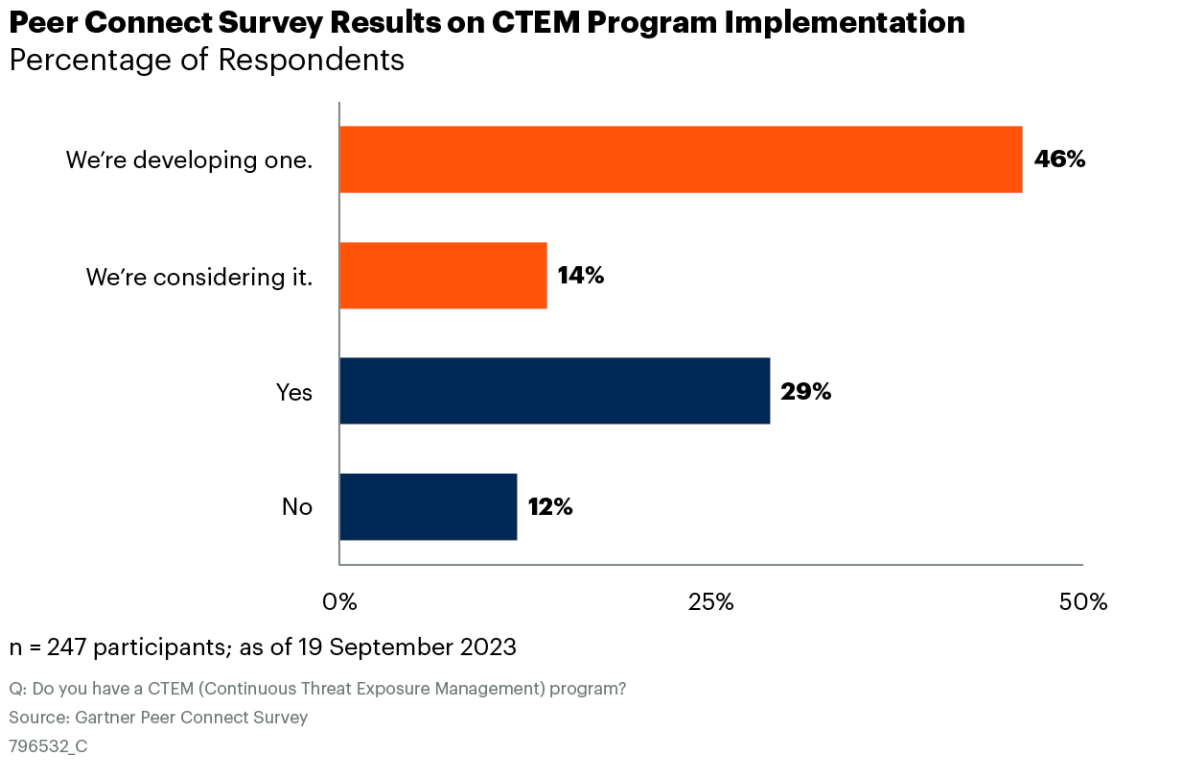
CTEM drives technology disruptions in a variety of assessment markets. A growing number of startups offer tools to support one or more steps of the CTEM framework. For example, they offer:

- Attack surface management products and services. These supported the first initiatives to shift from extensive inventory to risk-driven assessments.
- Security posture management as embedded features of cloud infrastructure and applications, or delivered as separate audit tools.
- Cybersecurity validation capabilities, such as breach and attack simulations, which enable larger-scale approaches to take the attackers' view. They enable more automated, frequent and consistent approaches to extend previously niche initiatives using penetration testing and red-teaming initiatives. One-third of vendors of breach and attack simulation and automated pentest technologies have added attack surface management features. They're starting to position their products as exposure management platforms.

New tools continue to emerge in the exposure assessment and cybersecurity validation categories. They support more consistent, accurate and faster remediation workflow, or specialized audit of security product configurations.

More mature offerings and feedback from industry peers enable a growing number of organizations to implement exposure management programs. However, implementing at scale and skills management remains a challenge. A survey conducted by Gartner Peer Connect [1] found that 71% of organizations could benefit from a CTEM approach, with 60% of respondents already pursuing a CTEM program or considering doing so (see Figure 2).

Figure 2: Peer Connect Survey Results on CTEM Program Implementation



Implications

As organizations initiate their roadmaps for exposure management, they revise how they conduct assessments and prioritize tooling investment. The notion of cybersecurity validation is gaining momentum in more security teams. Much increased automation and more pragmatic outcomes are enabling stakeholders from various teams to make more effective decisions on remediation options.

Organizations realize that, despite the multitude of cloud security tools, it remains difficult to manage the exposure of cloud assets consistently and efficiently. They might try to lift and shift their existing practices, but can't achieve the same success. When selecting posture and exposure management technologies, they face the difficult choice between:

- Cloud-native vendors claiming only they can understand cloud security
- Established vulnerability management providers
- Cybersecurity validation vendors, and even threat detection vendors, arguing that their main approach also works for cloud assets

Organizations can start by:

- Adding a validation step to existing assessments
- Adding new attack surfaces to the scope of their existing intelligence programs
- Using attack surface management to align more closely the priorities of remediation to business initiatives

Several organizations that Gartner has interviewed have begun implementing CTEM programs, focusing on one step first:

- The University of Westminster in the U.K. expanded the scope of its vulnerability management program to include assets that weren't managed by its IT team, and started effectively measuring the exposure of these assets. [2]
- Several midsize institutions in Europe added automated cybersecurity validation assessments to their mandatory quarterly penetration testing assessments. They did so in anticipation of Tiber-EU framework [3] requirements to reduce gaps found in security posture within days instead of months.
- A U.S. financial institution expanded its vulnerability management by adding attack surface management technology. It started by improving discovery and prioritization of assets' exposure. This has enabled the firm to partner security operations with other organizational departments to better mobilize on remediations.
- A U.K. financial organization initially used its nascent cloud security deployment (Amazon Web Services (AWS) and Microsoft Azure) to "beat compliance" with a cybersecurity validation pilot.

Conducting an exposure management program doesn't mean that every assessment is part of a defined CTEM scope. Security and risk management teams progressively add notions of the CTEM framework to their existing practices. Cybersecurity validation, through attack simulation, is a technical capability that can improve confidence in discovered issues. It's the next stage that an organization should tackle to enable the CTEM initiative's validation stage.

Similarly, it's not necessary to narrow every discussion of remediation to a single CTEM cycle. A survey conducted by Gartner Peer Connect found that 26% of organizations have yet to start a CTEM program, but many have existing vulnerability intelligence programs helping to prioritize remediations more broadly. [1]

Actions

- Shift from generic inventory and discovery to exposure assessment scopes aligned with specific business projects or identified threat vectors, crossing multiple defense technology market boundaries. Establish relationships outside of the security team and plan mobilization.
- Adopt exposure management to manage a wider set of security weaknesses. Measure improvements against identified threat vectors or targeting critical business projects.
- Establish repeatable cycles for exposure scopes that are easier to define. Start with one attack surface or a new application initiative. Begin cybersecurity validation pilots to achieve quick operational wins.

About Gartner's Top Strategic Technology Trends for 2024

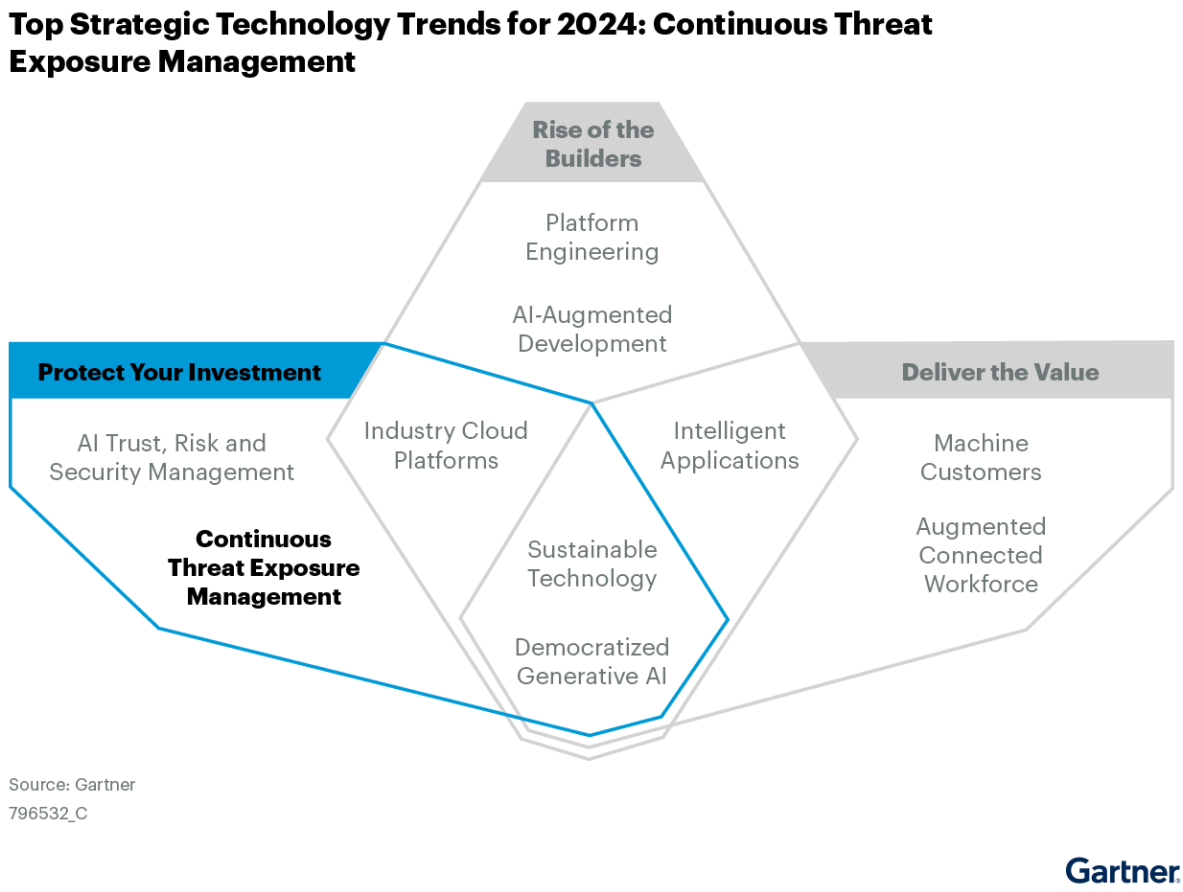
This trend is one of our Top Strategic Technology Trends for 2024. These are the trends we consider most relevant and impactful. Our trends fall into three main themes:

- **Protect your investment.** Preserve your investments and secure the benefits from past and future strategic technology decisions to make them durable.
- **Rise of the builders.** Unleash creative powers by using the appropriate technology for the appropriate functions.
- **Deliver the value.** Refine and accelerate value optimization, built on top of durable operational excellence.

These technology trends don't exist in isolation — they interconnect (see Figure 3) and several fall into more than one theme. The trends' potential importance for your organization differs by organizational maturity, but also by industry, business needs and previously devised strategic plans.

Work with other executives to evaluate the impacts and benefits of our trends. This will enable you to determine which single trends — or strategic combination — will have the most significant impact on your organization, and the ecosystem in which it operates. Examine the trends' potential relative to your organization's specific situation, factor them into your strategic planning for the next few years, and adjust your business models and operations appropriately.

Figure 3: Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management



Evidence

The number of Gartner client inquiries related to exposure management grew by 61% in the 12 months leading up to publication of this research compared with the preceding 12 months.

Gartner conducted one-to-one interviews with multiple end-user organizations to validate the use of, and transition to, CTEM. The objective was to identify the areas in which organizations struggled and the areas in which they succeeded.

[1] Do You Have a CTEM (Continuous Threat Exposure Management) Program?

[2] Case Study: Proactive Approach to Cybersecurity in Higher Education

[3] How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming, European Central Bank.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How To Implement a Risk-Based Vulnerability Management Methodology

Implement a Continuous Threat Exposure Management (CTEM) Program

Top Trends in Cybersecurity 2023

Innovation Insight for Attack Surface Management