Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Published 1 December 2022 - ID G00779535 - 18 min read

By Analyst(s): Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts

Initiatives: Security Operations; Digital Products and Services; Meet Daily Cybersecurity Needs

Threat exposure management is a nascent initiative combining attackers' and defenders' views to minimize enterprises' exposure to present and future threats. Gartner predicts that threat exposure management will enable security and risk management leaders to build evidence-based security.

Overview

Key Findings

- The responsibility for remediation extends beyond security teams and sometimes beyond the organization's control as more critical data is accessed or owned by partners.
- Fully remote workers often lack the same security controls as workers who are within corporate networks, yet many security teams consider their remote access security problem solved.
- Enterprise threat exposure goes beyond software vulnerabilities that can often be (virtually) patched automatically.
- Ever-growing adoption of cloud services and evolving work habits expand the attack surface faster than threat detection and response controls mature.

Recommendations

Security and risk management leaders responsible for managing today's and tomorrow's enterprise exposure to threats should:

- Embrace a security posture validation approach to augment their prioritization workflow and enhance cybersecurity readiness.

- Broaden security visibility to include systems and subscriptions that are business-critical, but perhaps not owned by IT or managed by the business.
- Integrate continuous threat exposure management principles progressively, notably the inclusion of nonpatchable exposure, in the scope.
- Invest in a long-term strategy to migrate from an access management mindset to a continuous adaptive trust (CAT) approach.

Strategic Planning Assumptions

Through 2026, nonpatchable attack surfaces will grow from less than 10% to more than half of the enterprise's total exposure, reducing the impact of automated remediation practices.

Through 2025, security leaders who implement cross-team mobilization as part of their exposure management program will gain 50% more security optimization than those only prioritizing automated remediation.

By 2027, the likelihood of breaches will increase threefold for organizations who fail to continuously manage remote access architecture and processes.

Through 2026, more than 60% of threat detection, investigation and response (TDIR) capabilities will leverage exposure management data to validate and prioritize detected threats, up from less than 5% today.

Analysis

What You Need to Know

Predictions are statements of Gartner's positions and actionable advice about the future. This research highlights Gartner Predicts relevant for security and risk management leaders in charge of managing their organization's exposure to threats. Exposure management is a challenge for all organizations, even high-maturity and large enterprises, because the attack surface keeps changing and expanding.

Lower-maturity and smaller organizations struggle with the almost infinite scope of security operation activities:

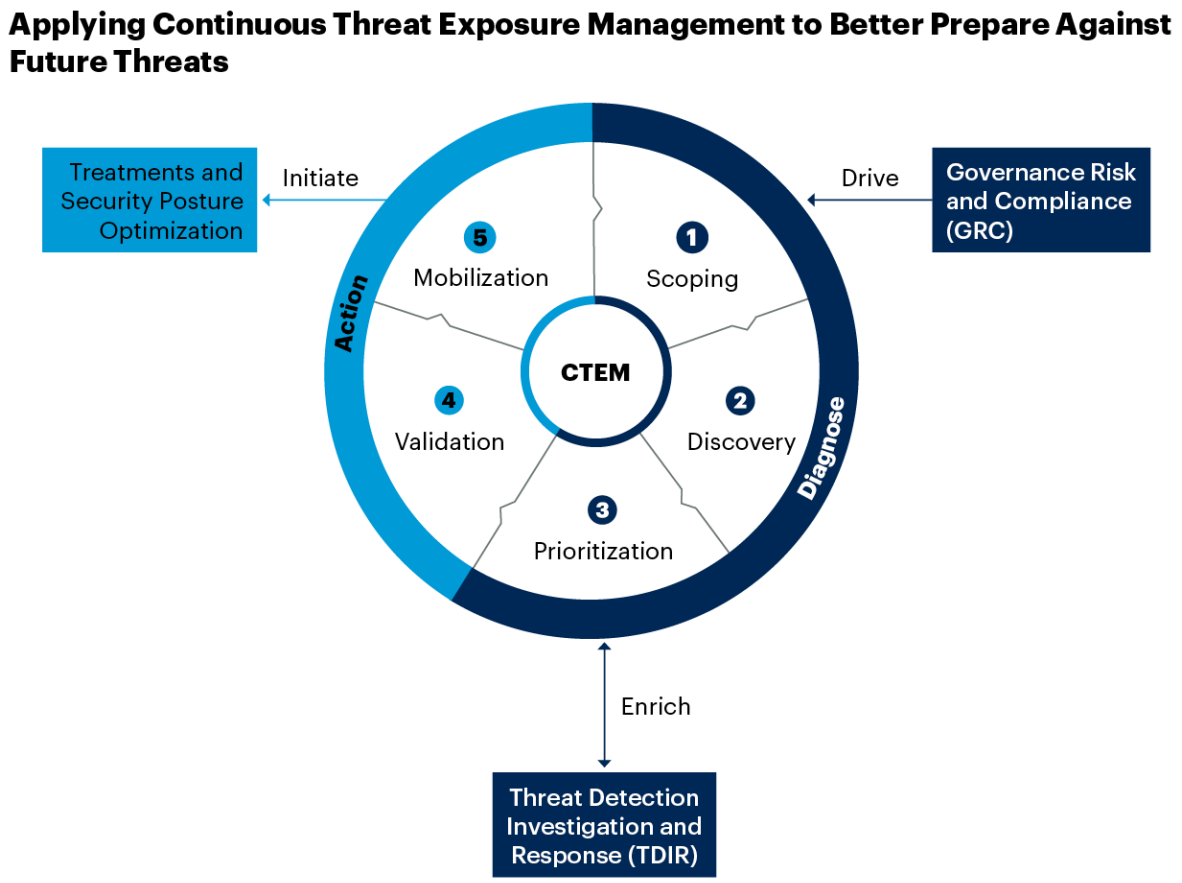
- Build and maintain business awareness on threats
- Manage in-house skills and third-party service providers
- Get funding beyond the narrow scope of preventative controls
- Select and prioritize technology and process investment to minimize exposure

As organizations learn more, SOC activities solidify around three areas, segmented in part by their time horizon. Governance, risk and compliance (GRC) programs might span multiple years, while threat detection, investigation and response often require very timely responses. Difficulties arise for higher-maturity and large organizations when those time horizons cross paths:

- Incident response requiring weeks-long forensic investigation
- A critical new zero-day resetting all previously evaluated remediation priorities
- Business priority shifts expanding the attack surface to the point of resetting a previously agreed strategic roadmap

Threat exposure management lives between the real-time constraints of TDIR and the multiyear GRC strategy. It expands beyond patches and automated blocking to better prepare against unpredictable threats and strategically reduce the enterprise's attack surface (see Implement a Continuous Threat Exposure Management (CTEM) Program and Figure 1).

Figure 1. Applying Continuous Threat Exposure Management to Better Prepare Against Future Threats



Some of the drivers behind this year's threat exposure predictions are:

- Hundreds of client inquiries about the unbearable challenges of building a safe and secure environment for work practices that keep changing.
- The sheer number of security incidents organizations face is already more than their capability to address every last one. Organizations report conflicting priorities resulting from multiple lists for each major threat vector.
- Analysis of the threat landscape continues to indicate quick pivots from attackers that are trying to find the path of least resistance into the organization as security teams build defenses to combat current threats.

- Hastily implemented remote work technologies, including new access management workflows, often resulted in compromises between security and user experiences. What was supposed to be temporary exceptions turned into permanent, undocumented policy exceptions.
- Threats to organizations now more frequently manifest themselves as impacts to brand or availability of critical services. Dependence on third parties that support these business functions requires a broader visibility than the traditional enterprise IT estate.
- The move to use third-party systems/service for key business functions is creating a range of visibility issues for organizations that they cannot address with traditional technologies or processes.
- Effective communication of the risk to the organization to enable cross-team remediation actions is the main challenge in moving from threat to exposure management.

Strategic Planning Assumptions

Strategic Planning Assumption: Through 2026, nonpatchable attack surfaces will grow from less than 10% to more than half of the enterprise's total exposure, reducing the impact of automated remediation practices.

Analysis by: Mitchell Schneider and Jeremy D'Hoinne

Key Findings:

- The number of unpatched vulnerabilities continues to grow, and decades of improvements to vulnerability management (VM) could not stop attackers from leveraging them.
- The enterprise attack surface expands as workers move outside of corporate-owned offices and applications from corporate-owned data centers.
- With the adoption of cloud services, security teams now have to monitor a large number of settings and configurations that, if done incorrectly, may expose sensitive data and services.
- Knowing the security posture of partners and if your data is publicly accessible — not only in your environment, but in your partners — are critical.

Market Implications:

Organizations need to look beyond vulnerability patching to manage a wider set of their security exposures, including significant increase in their attack surface due to new hybrid work, accelerating use of cloud infrastructure and applications, more tightly interconnected supply chains, expansion of public-facing digital assets, and expanding Internet of Things (IoT) exposures. A shift toward an increased digital presence has changed perceptions about the security of cloud SaaS applications, infrastructure as a service (IaaS) and platform as a service (PaaS), and has also increased the diversity of the systems that organizations depend on for revenue.

Good practice is to patch systems. Better practice is to patch systems regularly. Best practice is to utilize risk-based vulnerability management (RBVM) as the framework into which patching fits as an enabling process.

This is because patching is an important contributor to fixing vulnerabilities; however, it also needs to be supplemented with configuration management and software upgrades to fully remediate vulnerabilities.

Additional enabling practices are configuration and asset management, which multiply the value of the risk-based prioritization where the asset base and the service criticality enabled by those systems is able to be used as a part of the prioritization process. Similarly, a vulnerability steering committee/group that brings together all stakeholders in the vulnerability management process for the initial review and prioritization of vulnerabilities is critical.

Organizations must consider the business impact, mitigations or other controls that are available, as well as the success of the components of the VM process, such as:

- Effective vulnerability management is the “why” to the “how” of patch management. Improving visibility of both the in-scope systems and the vulnerabilities that are present on those systems is foundational to determining how to deal with the vulnerabilities effectively.
- Organizations that view patch management as an integral component to a vulnerability management program drive more effective patch delivery activities. Critical to this is the integration of vulnerability assessment into both the assessment of the current environment and the results of the postpatching activity to ensure that patching efforts are effective in driving down vulnerability counts and also efficient in the delivery of patching.
- Patching is only one of the three means by which vulnerabilities are remediated, which are patching, configuration change and software update. This is where the effective testing activities prior to production implementation can provide improvements to the vulnerability profile of the organization. Embedding this testing into the patching policy ensures that accountable team members are performing the testing that is needed prior to the implementation into production of the patches.

Recommendations:

- Continue to strengthen your risk-based vulnerability management program by identifying places where there is telemetry, but no vulnerability coverage, and/or find gaps/misconfigurations in your security controls.
- Expand to a broader exposure management to include nonpatchable attack surfaces and assess the need for solutions, such as digital risk protection services (DRPS), external attack surface management (EASM) and/or security rating services (SRS) for coverage of other exposure points, such as supply chain and shadow IT in the cloud.
- Embrace a security posture validation approach to augment your prioritization workflow and enhance cybersecurity readiness. This helps prioritize remediation/mitigation activity from the biggest named attacks, what exposures organizations have and how (and whether) that can be leveraged by threat actors to execute and move laterally throughout the IT environment.

Related Research:

The Top 5 Elements of Effective Vulnerability Management

Tracking the Right Vulnerability Management Metrics

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Strategic Planning Assumption: Through 2025, security leaders who implement cross-team mobilization as part of their exposure management program will gain 50% more security optimization than those only prioritizing automated remediation.

Analysis by: Jeremy D'Hoinne and Chris Saunderson

Key Findings:

- As the attack surface expands and fragments across multiple ecosystems, exposures with roots in architecture design and configuration will grow as a significant percentage of enterprise exposure.

- Managing enterprise threat exposure extends beyond vulnerabilities that can be (virtually) patched automatically.
- Organizations tend to prioritize tactical and automated responses, trying to avoid cross-team approvals that seem impossible to achieve.
- The abundance of security tool dashboards results in diagnostic fatigue and leads to long lists of unactioned recommendations.
- High-maturity enterprises are starting to leverage cross-functional teams to rebalance their efforts on strategic security posture optimization and replace more tactical ad hoc remediation programs.

Market Implications:

A large and growing number of cybersecurity dashboards have long exceeded the ability for even the largest security team to take action. Be immersed in it over a long period of time, add a brutal disruption of work practices, and organizations of all sizes struggle to keep the pace of attackers.

> **Enterprise security leaders suffer from the industrywide "diagnostic fatigue" that slowly anesthetizes their ability to take on necessary security optimization programs. The most practical, yet very tactical, approach of enabling automated controls and patches when applicable, has quickly become the only response for many.**

Despite strong improvements in the vulnerability assessment and prioritization practices, the (virtual) patching approach shows its limits in terms of scope, but also invites a 'apply and repeat' approach that hurts long-term strategic improvements.

As attackers shift tactics again and target flaws and gaps in emerging work practices, Gartner predicts that a growing proportion of security findings will require more than a technical fix. Security and risk management leaders need to evolve their methodology to reduce their exposure to threats because more of these decisions will require cross-team collaboration. In the absence of improved procedures, security teams will see a growing number of unresolved issues.

A continuous threat exposure management (CTEM) program is a multiyear initiative that helps organizations moving beyond only tactical and technical remediation to reduce their long-term exposure (see Implement a Continuous Threat Exposure Management (CTEM) Program). It acknowledges and outlines the challenges of traditional approaches with a few key characteristics:

- CTEM puts all kinds of exposure in scope, not only software-based vulnerabilities, and includes practices to validate the findings as a means to facilitate difficult remediation decisions.
- CTEM keeps treatment and security posture optimization as a separate program because it is the only way to address the cross-team elements of successful remediation.
- CTEM defines outcomes and success metrics as “mobilization” because, often, there is more than one fix to an issue, or there might be no fix available at all and other compensatory measures could be needed.

It is easy, but dangerous, to downplay the importance of the mobilization phase and revert back to known tactics, but there will be long-term consequences for organizations. As a component of an infrastructure (e.g., a VPN gateway) gets a disruptive issue (e.g., remotely exploitable vulnerability), the common wisdom says to improve patching SLAs or better automate the deployment of in-line security controls. Real, long-term improvements require many teams to be involved as a sustainable approach to a well-run CTEM program should include — but not be limited to — security, I&O, application architecture and business teams.

Recommendations:

- Integrate CTEM principles progressively, notably the inclusion of nonpatchable exposure, in the scope.

- Start with quick wins that frequently lie in improving the prioritization of findings through validation techniques.
- Emphasize the cross-team requirements of a successful CTEM program and initiate a strategic improvement plan to better balance strategic mobilization and tactical response.

Related Research:

Implement a Continuous Threat Exposure Management (CTEM) Program

Strategic Planning Assumption: By 2027, the likelihood of breaches will increase threefold for organizations that fail to continuously manage remote access architecture and processes.

Analysis by: John Watts

Key Findings:

- Organizations focused on business enablement for the sudden shift to remote work often compromised security for productivity, leading to a rise in security incidents due to compromised remote workers.
- An organization's remote workforce attack surface includes exposure to unsecure networks, increased use of legacy remote access methods, reliance on weak authentication mechanisms, and an increasing number of remote access entry points.
- Fully remote workers often lack the same security controls as workers who are within corporate networks.
- Implementing new security controls for the remote workforce requires increased budgets as new technology often costs more, requires additional staff or training for existing staff, and rarely fully replaces existing controls.

Market Implications:

To support the rise in remote work, organizations expanded access for remote workers based on their old practices of “remote work by exception” rather than strategically planning for remote-first work arrangements. This has led to an increase in the exploitation of remote workers who may be more distracted at home and less connected to business processes. For example, workers may not know the expectations for handling sensitive data in a home environment that lacks physical security controls. Some organizations that prioritize productivity over security allow less secure remote access methods using single password or weak second factors of authentication to connect workers into their networks. As a result, there is evidence of an increase in successful exploitation of organizations from remote work arrangements. [1]

Organizations that view remote work as a “solved problem” face an increasing threat. Attackers are often opportunistic and primarily financially motivated. Even sophisticated attackers prefer to find a quick and easy path to monetize their malicious activity over a more complicated malware campaign. There is evidence that organizations have seen a rise in extortion attempts from business email compromise (BEC), ransomware and phishing attacks targeted at remote workers [3] and will continue to do so if left unchecked.

However, improved remote work security typically comes with increased costs. Organizations may be able to retire some legacy security controls, but the cost savings in security tools may not justify the increased cost to secure the hybrid remote workforce. In a 2022 Gartner Cost Reduction Quick Poll, [2] 35% of CFOs said they expect to see a decrease in real estate and facilities budgets in the next 12 months. This is by far the largest corporate function expected to maintain or reduce budgets. For many CISOs, this is an opportunity to argue for redirecting decreased real estate and facilities budgets into increased investments in security for remote workers in 2023.

Recommendations:

- Plan for budget increases to address security gaps in securing the hybrid remote workforce.
- Establish a flexible work policy that clearly defines organizational expectations and requirements for security of network and data access.
- Provide equipment for remote workers that can be hardened, patched, protected and managed remotely using cloud services without the need to connect endpoints to corporate networks.
- Immediately eliminate all single factor authentication and implement stronger second factors of authentication for remote access where possible.

- Invest in a long-term strategy to migrate to continuous adaptive trust to provide more granular and appropriate levels of authentication for workers rather than a one-size-fits-all authentication scheme.
- Inventory all external exposure points using an attack surface management process to find exposed services such as remote desktop protocol (RDP), secure shell protocol (SSH) and VPN. Close inbound ports where possible, and implement processes to patch any required external-facing services as quickly as possible.
- Implement security service edge (SSE) services as part of a secure access service edge (SASE) framework to secure the hybrid remote workforce access to web, cloud services and private applications, eliminating legacy VPN where possible.

Related Research:

Shift Focus From MFA to Continuous Adaptive Trust

Remote Access Options for Enterprise Endpoints

The Corporate Functions Set for Spending Cuts or Increases in 2022 and 2023

Innovation Insight for Attack Surface Management

The Future of Work Requires Executive Leaders to Embrace Radical Flexibility

How IT Can Enable the Remote Workforce Life Cycle

Strategic Planning Assumption: Through 2026, more than 60% of threat detection, investigation and and response capabilities will leverage exposure management data to validate and prioritize detected threats, up from less than 5% today.

Analysis by: Pete Shoard

Key Findings:

- For most organizations, the adoption of cloud infrastructure is increasing and diversifying their attack surface. These expansions are rarely being paralleled with coverage by detection and response initiatives, leaving the organization unaware of a variety of threat vectors.

- Organizations relying more massively on SaaS providers for flexibility give security teams the impression that they have fewer options to mitigate or control discovered threats through response actions. SaaS underlying platforms are not owned or hosted by internal IT teams and options for reaction are limited by the SaaS provider.
- Exploiting legitimate credentials, misconfigurations and the exploitation of software vulnerabilities remain top causes for security incidents. Organizations still suffer huge volumes of irrelevant or poorly prioritized security alerts, leading them to miss important, but poorly prioritized, security issues.
- Validation of perceived threat paths, vulnerabilities and security control effectiveness can greatly increase confidence in security team outputs and provide directional guidance for prioritizing legitimate threat responses.

Market Implications:

An approach to modern security operations requires that there are people with specialist skills, and processes to govern those skills and enable effective recording and reporting as well as technologies to enable those skills to be utilized to derive outcomes. TDIR capabilities enable this, providing a unified platform or ecosystem of platforms where security operations functions can be carried out uniformly. TDIR capabilities enable modern SOC staff to design, configure and manage security detection use cases. Staff also can carry out detailed investigation of discovered issues and mitigative response to those threats and perceived threats that are discovered directly in the platform. To a broad degree, SOC technologies promise to offer these capabilities for the market, although some organizations implement simpler versions of them leveraging endpoint detection and response (EDR) or network detection and response (NDR) technologies, for example.

Currently, the core use cases and compatibility of these products is centered around the business ownership of the platforms and infrastructure that is distinct to the organization. More recently, the adoption of cloud-based applications and SaaS running in environments not owned and managed by organizations has left a substantial gap in security visibility.

A combination of broader visibility, new detection techniques and new skill sets is required to engage with modern infrastructures. It is likely that many traditional detection solutions, heavily dependent on their current processed dataset and telemetry, will fail to adapt to these new requirements. This will lead to a period of unawareness for organizations, followed by rapid adoption of a subset of these products that are flexible enough to reorient toward these new datasets or those that invest in new technologies to integrate with their existing platforms. Identity threat detection and response (ITDR) will also be centrally aligned to the needs of the modern SOC organization. Identity is one of the main inflection points that will cross all modern infrastructure. ITDR represents a fundamental methodology shift in use-case development approaches for detection.

To combat the drastic change of methodology and focus for threat detection and response, organizations and technology providers will shift their focus onto measuring and understanding the accessibility of vulnerabilities. They will also seek to understand new vectors for exposure, in areas such as social media platforms, open-source development code repositories and communications platforms. These exposures will be vast and will require validation through automated testing of existing security controls, policies and monitoring visibility.

Recommendations:

- Broaden security visibility to include systems and subscriptions that are business critical, but perhaps not owned or managed by the business.
- Utilize knowledge of security posture weaknesses and threat exposure to help prioritize and validate the importance of discovered security threats.
- Spend time regularly reviewing business-critical functions and those areas seen as high risk by business leaders for new potential threat vectors and gaps in visibility or response capability.
- Implement a continuous program of threat exposure management. In line with detection and response, risk understanding, and the ability to mitigate and reduce impact through preventative controls should be key parts of the security strategy.

Related Research:

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

This report is too new to have on-target or missed predictions.

Evidence

[1] Psychology of Human Error 2022 Research Report, Tessian.

[2] **2022 Gartner Cost Reduction Quick Poll,** n = 211-226. This study was conducted to understand the areas of the business organizations are targeting for cost reductions over the next 12 months. The research was conducted online during July 2022 among 234 respondents across multiple industries. Respondents were CFOs or other finance leaders (including heads of FP&A, controllers and finance transformation leaders).

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

[3] Enduring From Home: COVID-19's Impact on Business Security, Malwarebytes.

Recommended by the Authors

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

Implement a Continuous Threat Exposure Management (CTEM) Program

The Top 5 Elements of Effective Vulnerability Management

Innovation Insight for Attack Surface Management