FORESCOUT

Building Operational Resilience with Continuous Threat Exposure Management (CTEM)

FORESCOUT

Table of Contents

Building Operational Resilience with Continuous Threat Exposure Management (CTEM)

Executive Summary

Faced with surging connected asset growth and an increasingly complex threat landscape, cybersecurity teams often find it difficult to make sense of fragmented data across disconnected security platforms.

Let's put asset growth in perspective: The number of global Internet of Things (IoT) devices is forecast to grow from **19.8 billion** in 2025 to more than **40.6 billion** by 2034, according to data from Statista.

At the same time, attackers aren't slowing down. Consider these numbers from Forescout Research – Vedere Labs—with data sourced from 19 billion endpoints in our customer data lake:

- 900M cybersecurity attacks in 2024
- 33% increase in threat actors YoY
- 114% increase in attacks YoY
- 668% increase in critical Infrastructure incidents from 2022 to 2024
- 20 ransomware attacks per day in 2025
- 46% increase in zero-day attacks in 2025

To stay ahead, organizations require a streamlined approach to continuously track and understand every device and their potential exposures and vulnerabilities — whether it's managed or unmanaged, virtual or physical, including OT/ICS systems, IoT endpoints, and specialized assets like medical equipment.

Without this level of intelligence, they risk elevated operational burdens, degraded performance, unexpected outages, and threats that can lead to serious security incidents.

Leading industry analyst firm Gartner developed the concept of Continuous Threat Exposure Management (CTEM) which represents a paradigm shift in how enterprises approach risk, moving beyond traditional point-in-time assessments to continuous visibility, prioritization, and remediation of exposures and potential threats.

What Is CTEM?

Gartner defines CTEM as an iterative and integrated approach to prioritizing risk mitigation and continuously refining security posture. CTEM is not a single product, but rather a continuous program aimed at reducing the likelihood and impact of breaches.

Every organization faces more security challenges than it can address, so meaningful improvements in security posture require a shift in approach. That shift begins with how organizations define the scope of their assessments and how they collaborate on remediation efforts.

CTEM supports these efforts by guiding enterprises through more effective risk reduction cycles and enabling faster, more coordinated remediation.

Why Does CTEM Matter?

With threats evolving faster than traditional security assessments can keep up, CTEM enables organizations to proactively manage cyber risk by continuously identifying, assessing, and mitigating threats and vulnerabilities across their digital footprint, giving enterprises the visibility, control, and agility they need to stay ahead of modern cyber threats before they cause damage.

It's a Strategic Shift, Not Just a Tool: Gartner emphasizes that CTEM is a program - a convergence of risk, threat, and actionability - that enables organizations to move from reactive security postures to proactive exposure management, helping teams focus on what truly matters

Business-Aligned Risk Reduction: CTEM helps security teams prioritize threats based on business impact, not just technical severity. This ensures that remediation efforts are aligned with what's most critical to the organization

Operational Efficiency: By continuously identifying and prioritizing only the most critical exposures, CTEM reduces alert fatigue and helps focus resources where they're needed most

Validation of Security Controls: CTEM enables organizations to test and validate whether their existing defenses are effective against real-world attack scenarios

Proven ROI and Breach Reduction: According to recent industry data, organizations that adopt CTEM practices can reduce breach risk by up to 69% and achieve ROI of 150–300% through better threat detection and faster remediation

The Five Steps of CTEM

The primary goal of a CTEM program is to create actionable remediation and improvement plans that are clear to business leaders and executable by architecture teams. Organizations implementing CTEM use tools to inventory and classify assets and vulnerabilities, simulate attack scenarios, and conduct posture assessments using various technologies.

A typical CTEM cycle includes five key stages: **scoping**, **discovery**, **prioritization**, **validation**, and **mobilization**:

1 Scoping: Define which assets, networks, and applications fall under your CTEM program. Traditional vulnerability management often excludes IoT, OT, and shadow IT assets-yet these remain high-value targets for attackers.

Quick tip: Collaborate early with stakeholders from security, IT, and business units to define what's in scope based on real risk, not just asset count.

2 Discovery: Identify exposures beyond CVEs: misconfigurations, policy violations, and risky behaviors.

Quick tip: Through continuous monitoring of the network, you can determine every asset's configuration, patch level, and security posture in real-time.

3 Prioritization: Determine which vulnerabilities matter most to your organization's risk profile.

Quick tip: Correlate asset data with threat intelligence to rank exposures based on exploitability, criticality, and business context.

4 Validation: Test and validate the impact of potential threats and confirm the effectiveness of current controls.

Quick tip: Evaluate the effectiveness of your organization's security controls to ensure that they are correctly implemented, operating as intended, and producing the desired outcome.

5 Mobilization: Tune security posture continuously with fully automated Zero Trust security policies and dynamic compliance enforcement with closed-loop feedback from integrated systems and tools.

Quick tip: With policy-based automation, you can quarantine vulnerable devices, apply security patches, or send tickets to ITSM tools like ServiceNow to close the gap between detection and action.

Forescout eyeSentry Helps Enterprises Operationalize an Effective CTEM Program

Forescout eyeSentry is designed to help enterprises continuously identify, assess, and reduce cyber risk across all connected assets - managed or unmanaged, IT, OT/ICS, IoT, and IoMT. Unlike traditional vulnerability management tools that focus narrowly on known CVEs, Forescout eyeSentry provides real-time visibility into the full attack surface, factoring in asset criticality, active exploits, misconfigurations, and business impact to prioritize remediation efforts effectively.

The solution integrates key capabilities such as **persistent asset intelligence**, **automated threat detection and response**, and **risk scoring** into a unified, cloud-native platform that is easy to deploy and configure. It supports proactive risk reduction by enabling security teams to swiftly discover and close exposure gaps, streamline incident response, and reduce mean-time-to-resolution (MTTR). Features like passive discovery for IoT and medical devices, and support for compliance frameworks further enhance their value in complex, regulated environments.

Mapping Forescout eyeSentry Capabilities to the CTEM Framework

CTEM STEP	GARTNER DESCRIPTION	FORESCOUT EYESENTRY CAPABILITIES
Discovery	Identify visible and hidden assets, vulnerabilities, misconfigurations, and risks.	Forescout eyeSentry provides agentless, real-time discovery of all connected assets across IT, OT, IoT, and cloud environments. It integrates with third-party tools to enrich asset context and risk posture.
Prioritization	Assess urgency, business impact, and exploitability to rank exposures.	Forescout eyeSentry leverages contextual risk scoring based on asset criticality, threat intelligence, and environmental factors. It integrates with vulnerability management tools to refine prioritization.
Validation	Confirm exploitability and assess the effectiveness of current defenses.	Forescout eyeSentry performs security controls assessment, including CIS SCAP scoring, dashboards, and reporting to evaluate posture against security compliance frameworks.
Mobilization	Operationalize findings through collaboration and workflow integration.	Forescout eyeSentry enables ownership assignment, integrates with ITSM platforms (e.g., ServiceNow), and tracks remediation progress with centralized dashboards and reporting, including metrics and KPIs to measure MTTR, exposure reduction, and compliance alignment.

Key Forescout eyeSentry Differentiators

Agentless Visibility

Real-time discovery and classification across managed and unmanaged devices, enriched with behavioral and contextual data

AI-Driven Threat Detection

Uses machine learning to detect anomalies, lateral movement, and policy violations

Automated Remediation

Integrates with EDR, SIEM, and ITSM tools to orchestrate response actions and close the loop on remediation

Cross-Domain Coverage

Supports IT, OT, IoT, and cloud environments with a single platform

Conclusion

Cybersecurity teams struggle to contextualize information from multiple siloed security tools. Organizations need a simplified way to maintain real-time and persistent asset intelligence for every device – managed or unmanaged, physical or virtual, including operational technology and industrial control systems (OT/ICS), Internet of Things (IoT) devices and specialty subsets like medical devices. Without this capability, organizations face high operational overhead, performance issues, downtime, and risk of security breaches due to weakness in their security posture, caused by lack of asset intelligence.

By aligning with the Gartner-defined CTEM lifecycle - scoping, discovery, prioritization, validation, and mobilization – Forescout eyeSentry empowers organizations to move from reactive to proactive security operations. It helps cybersecurity teams contextualize threats, reduce operational overhead, and make data-driven decisions that strengthen enterprise resilience.

Why Choose Forescout

The Forescout 4D Platform™ provides complete asset intelligence and control across IT, OT, IoT, and IoMT environments. For more than 20 years, Fortune 100 organizations, government agencies, and large enterprises have trusted Forescout as their foundation to manage cyber risk, ensure compliance, and mitigate threats with seamless context sharing and orchestration across more than 180 fully featured security and IT product integrations. With Forescout, every cybersecurity investment is more effective.

Learn more at **forescout.com**.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591