Hive Pro

WHITEPAPER

Enabling Proactive Security with Continuous Threat Exposure Management (CTEM) for Managed Service Providers

Executive Summary

Facing resource limitations and complex IT infrastructures, companies rely on MSPs for cyber risk management. Continuous Threat Exposure Management (CTEM) addresses these challenges by integrating and evolving on traditional vulnerability management and threat hunting practices. CTEM's five-step process reduces the mean time to detect (MTTD) and respond (MTTR) to threats, optimizes resources, and enhances visibility into assets. The goal is to preempt threats and manage risks accordingly. This approach has been proven to boost operational efficiency, provide strategic security insights, and continuously foster client trust, positioning MSPs as leaders in providing cybersecurity services.

Table Of Contents

Introduction	04
What is Continuous Threat Exposure Management?	05
Adoption and Impact of CTEM on Managed Service Providers	07
A Brief Expose Into Uni5 Xposure	08
Outcomes to Expect When Adopting CTEM	10
Strategic Recommendations for MSPs Implementing CTEM	11

Introduction

Facing resource limitations, complex IT infrastructures, and increasingly sophisticated cyber threats, many companies turn to MSPs for around-the-clock protection and cyber risk management. In 2022 alone, MSPs experienced an **82% growth rate,** marking the highest customer expansion within the technology and IT services sector. That year, their market size was valued at USD 14.48 billion and grew to USD 15.78 billion in 2023, exhibiting a CAGR of 8.98%.This significant CAGR highlights the value that enterprises place on MSPs for their expertise in providing continuous monitoring, advanced security measures, and risk management solutions. As a result of the growing demand for their services though, MSPs felt eerily similar pains as their customers.

According to a Coleman Parks research sponsored by N-able: "Fully **90 percent** of MSPs have suffered a successful cyberattack in the last 18 months." Being that they are the first-line defenders and guardians of various enterprise architectures, this statistic comes at no surprise. The challenges in combating these attacks are exacerbated by the need to manage diverse and complex client environments, lacking business context, non-interoperable tools, and the constant expectation to continuously adapt to the volume and sophistication of threats even when considering their own resource limitations. To solve these issues and to maintain integrity in their services as they grow, MSPs are turning to vendors for a solution that is integration friendly, scalable, responds proactively to threats, houses advanced security automation features, and has the ability to communicate risk in business terms. Moreover, MSPs are asking vendors how they meet the demands of a Continuous Threat Exposure Management (CTEM) program.

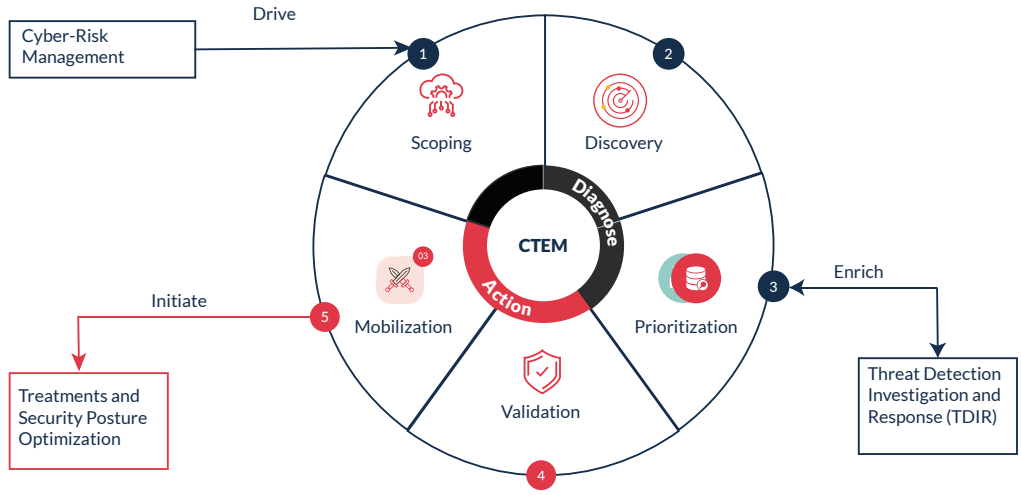
What is Continuous Threat Exposure Management?

Continuous Threat Exposure Management is first and foremost, a program. Created by Gartner Inc. in 2022, this new framework looks to combine and evolve traditional vulnerability management and threat hunting practices into a hybrid form that promotes threat-informed risk management and defense. It consists of a five-step process that outlines how to continually and consistently evaluate the visibility, accessibility and vulnerability of an organization's digital assets (Figure 1). To meet the program's demands and to assure reliability in reducing threat exposure, supporting tools must undertake both exposure assessment and cybersecurity validation (Figure 2).

The Five Step Process Simplified

The CTEM process, consisting of scoping, discovery, prioritization, validation, and mobilization, aligns cybersecurity efforts with business objectives.

Continuous Threat Exposure Management



Source: Gartner

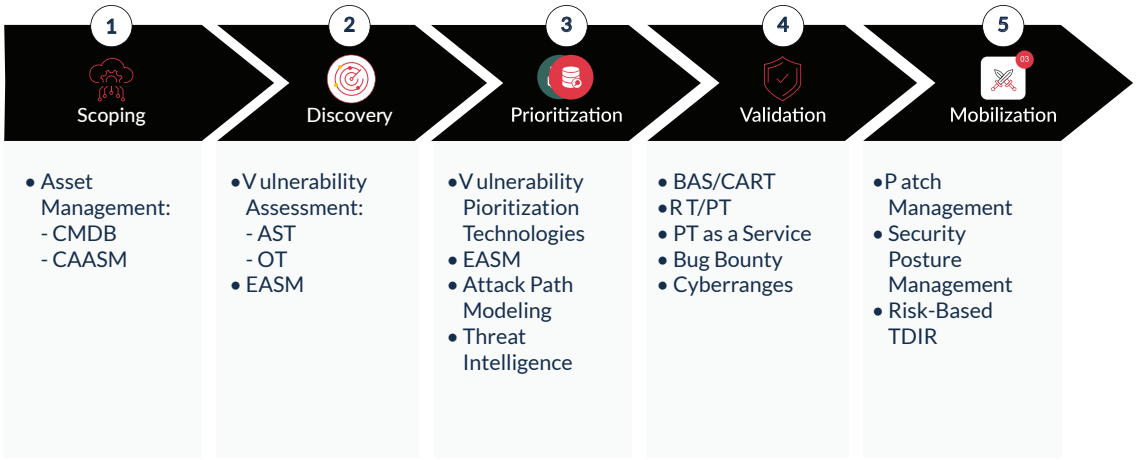
Figure 1

1. **Scope** involves identifying what is important to the business, including an expansive asset estate and vulnerability intelligence.
2. **Discover** goes beyond identifying vulnerabilities to include misconfigurations, poor responses, and hidden risks.
3. **Prioritize** focuses on the most critical threats based on urgency, severity, available controls, risk appetite, and business impact.
4. **Validate** involves testing potential attacks and assessing the effectiveness of monitoring and control systems through simulations or emulations.
5. **Mobilize** fosters cross-team collaboration and accountability, integrating CTEM with organizational workflows to ensure effective and timely remediation actions.

This process aims to continuously manage and mitigate threat exposures by aligning security efforts with business priorities, ensuring comprehensive risk assessment, and fostering effective remediation through cross-team collaboration. By integrating CTEM, MSPs and MSSPs can offer more effective and actionable threat management solutions, reduce diagnostic fatigue, and ensure that remediation efforts are aligned with clients' risk appetites and business objectives.

Exposure Assessment & Cyber Validation

Technologies Supporting Exposure Management



Source: Gartner

AST = application security testing; BAS = breach and attack simulation; CAASM = cyber asset attack surface management; CART = continuous automated red teaming; CMDB = configuration management database; EASM = external attack surface management; IO = infrastructure and operations; PT= penetration testing; RT = red teaming; TDIR = threat detection and incident response

Figure 2

Exposure Assessment (Steps 1,2,3,5)

Exposure Assessment involves evaluating the breadth and depth of an organization's potential vulnerabilities and weaknesses. This process extends beyond identifying traditional software vulnerabilities to include misconfigurations, counterfeit assets, and poor responses to phishing attempts. It encompasses a comprehensive view of all possible exposure points, considering the various ways an attacker could exploit them. The goal is to understand the full scope of risk by examining all digital and physical assets, and identifying how these exposures could impact the organization. This assessment informs prioritization efforts, ensuring that security resources are focused on the most critical and exploitable threats.

Cyber Validation (Steps 3,4)

Through 2026, more than 40% of organizations, including two-thirds of midsize enterprises will rely on consolidated platforms or managed service providers to run cybersecurity validation assessments. Cyber Validation refers to the process of verifying how effectively an organization's security measures can detect and respond to potential attacks. This involves conducting controlled simulations or emulations of attacker techniques to see how well the existing security controls and monitoring systems perform in real-world scenarios. Validation ensures that the identified threats and vulnerabilities are not only theoretical but have practical implications that can be tested and measured. This step helps organizations assess the likely success of attacks, estimate the potential impact, and confirm that their remediation and response processes are adequate and effective. Cyber validation provides evidence to stakeholders about the efficacy of their security posture and the practical resilience of their defenses.

Adoption and Impact of CTEM on Managed Service Providers

All organizations using CTEM will be three times less likely to suffer breaches by 2026, showcasing its effectiveness in improving security posture and reducing risks.

Earlier, we spoke to why customers turn to MSPs to alleviate them of certain cybercare burdens. Resource constraints and limited budgets are why they turn to MSPs, though the problems MSPs inherit are not often any different than what customers offload. Both alike are struggling with consolidating and correlating security findings and threat intelligence from various platforms, as well as in applying business risk context to all results. This miscalculation impedes their ability to accurately assess an overall risk posture and effective remediation strategies. Worse yet, due to non-interoperable tools and the sprawl of risk score results, the risk calculation task is undertaken manually where long .csv files, wordy reports, and external test outcomes are labored upon for more hours than deserving. Threat actors thrive on our inefficiencies and oversight. For proactive, threat-informed defense we must enact smart automation to where human errors are most likely to lead to security breaches. Otherwise, such mistakes become the MSPs' burden to manage and rectify, potentially damaging their reputation and client trust.

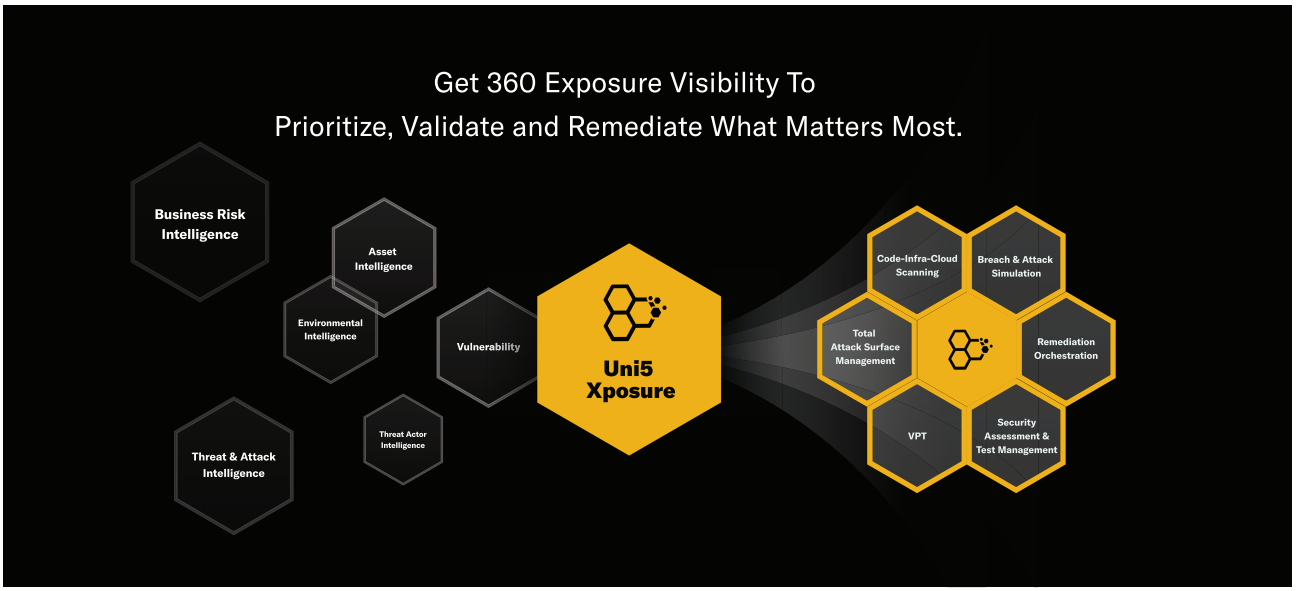
To address these pains, MSPs would benefit from a cost-effective and consolidated solution that offers smart automation—where risks are automatically normalized across different environments, and remediation intelligence is enriched and prioritized continuously. Such a solution should promote Continuous Threat Exposure Management by purpose, and not just by branding. We believe this solution to be Uni5 Xposure.

A Brief Expose Into Uni5 Xposure

As MSPs implement Continuous Threat Exposure Management (CTEM) programs, Uni5 Xposure by Hive Pro supports and enhances these efforts. This platform is purpose-built to meet CTEM and not a bolt-on solution, thus meeting the demands of threat-informed defense with integrity.

Uni5 Xposure provides comprehensive end-user asset intelligence, vulnerability information, threat intelligence, exposure classification across all findings, and a means to test and strengthen compensatory controls. By involving these features, Uni5 Xposure is able to assess the risks incurred from asset exposure, whether or not compliance requirements are being met, the lifecycle status of open risks, and the efficacy of security controls in action. Further, Uni5 Xposure excels in seamless integration across multiple scanners, incident logging, reporting, risk management and detection tools with a friendly API. By combining heterogeneous sources for security findings with the findings of 6 built-in scanners from code to infrastructure and cloud, total attack surface visibility is assured.

All-in-all, at Hive Pro, we consider Uni5 Xposure to be the glue for your security tools–an overarching data plane for all findings that serves as the foundation for proactively reducing the risks most likely to be exploited.



The Details

Advanced Threat Detection and Prioritization

AI-driven risk scoring, incorporating vulnerability attributes like exploitability, dark web discussions, and active exploitation. Threat actor monitoring providing predictive insights.

Simulation-Based Attack Path Analysis

Attack simulations in a secure, sandbox environment to enable MSPs to identify high-risk exposure points, gaps in security coverage and remediation priorities. MITRE ATT&CK Mapping to highlight attack paths.

Seamless Integration with Ticketing Service Management Platforms

Integration with platforms like ServiceNow, Jira and more to streamline incident management and response workflows, validate patches and fixes, track exceptions and update risks.

Comprehensive Database Access

With over 229,000 CVEs, insights on 270+ threat actors, enriched IoC intelligence, and 1,000+ threat advisories, Uni5 Xposure equips MSPs with extensive threat intelligence, enabling prompt and informed responses to vulnerabilities.

Continuous Improvement and Customization

The platform supports continuous updates and customization, allowing MSPs to tailor it to their specific needs and evolving threat landscapes, maintaining its effectiveness.

Outcomes to Expect When Adopting CTEM

Reduced MTTD and MTTR

Adopting Continuous Threat Exposure Management (CTEM) enables Managed Service Providers (MSPs) to significantly enhance their threat detection and response capabilities, thereby reducing the mean time to detect (MTTD) and mean time to respond (MTTR) to threats. By leveraging advanced threat detection and AI-driven risk scoring, CTEM allows MSPs to identify potential threats more quickly and accurately, decreasing the MTTD. Faster detection leads to quicker remediation actions, thus significantly lowering the MTTR. This rapid response minimizes potential damages and ensures that threats are addressed effectively, preventing them from escalating into more severe incidents. The ability to provide comprehe no nsive visibility into assets and exposures further enhances the MSPs' capacity to manage and secure their clients' environments. This visibility, coupled with real-time threat intelligence, ensures that MSPs can maintain continuous monitoring and respond to threats around the clock, thereby strengthening their 24/7 security capabilities.

Operational Effiency and Reduced Costs

CTEM also optimizes resource utilization, leading to improved operational efficiency. By automating and streamlining security tasks, MSPs can manage complex environments more effectively, reducing the burden on their teams and allowing for a more strategic allocation of resources. This proactive risk management approach focuses on mitigating the most critical threats, ensuring that security efforts are directed where they are most needed. Additionally, the deep analytics provided by CTEM offer strategic security insights, enabling informed decision-making and strategic planning. These enhancements not only bolster security operations but also increase client trust and retention by proactively protecting clients' assets and building stronger relationships through reliable and efficient service delivery.

Meeting Those Outcomes with Uni5 Xposure

Uni5 Xposure by Hive Pro enhances CTEM outcomes by providing advanced threat detection and AI-driven risk scoring, reducing MTTD and MTTR. This platform quickly identifies and prioritizes threats, enabling faster remediation and minimizing potential damage. It offers comprehensive visibility into assets and exposures, combined with real-time threat intelligence, ensuring continuous 24/7 monitoring and response capabilities. By automating and streamlining security tasks, Uni5 Xposure optimizes resource utilization and enhances operational efficiency, reducing team burden and allowing for strategic resource allocation. Additionally, its deep analytics provide strategic security insights, supporting informed decision-making and planning, which boosts client trust and retention through proactive asset protection and efficient service delivery.

Strategic Recommendations for MSPs Implementing CTEM

For successful CTEM implementation, MSPs should focus on developing robust exposure management maturity models, leveraging advanced technologies, and ensuring thorough staff training. A proactive approach is essential for maintaining a high level of security readiness and effectively protecting clients from emerging threats.

To successfully implement CTEM, MSPs should:

Develop a Robust Framework

Build an exposure management maturity model that includes proactive security measures, ensuring a structured approach to continuous threat assessment and remediation.

Leverage Advanced Technologies

Adopt integrated platforms like Uni5 Xposure, which support continuous monitoring, advanced threat detection, AI-driven risk scoring, and automated response capabilities. These technologies will help reduce MTTD and MTTR, ensuring rapid and effective threat management.

Focus on Training and Awareness

Ensure that staff are well-trained in proactive security measures and the use of supportive tools. Regular training sessions and updates on the latest threat landscapes and response strategies are crucial for maintaining an informed and prepared team.

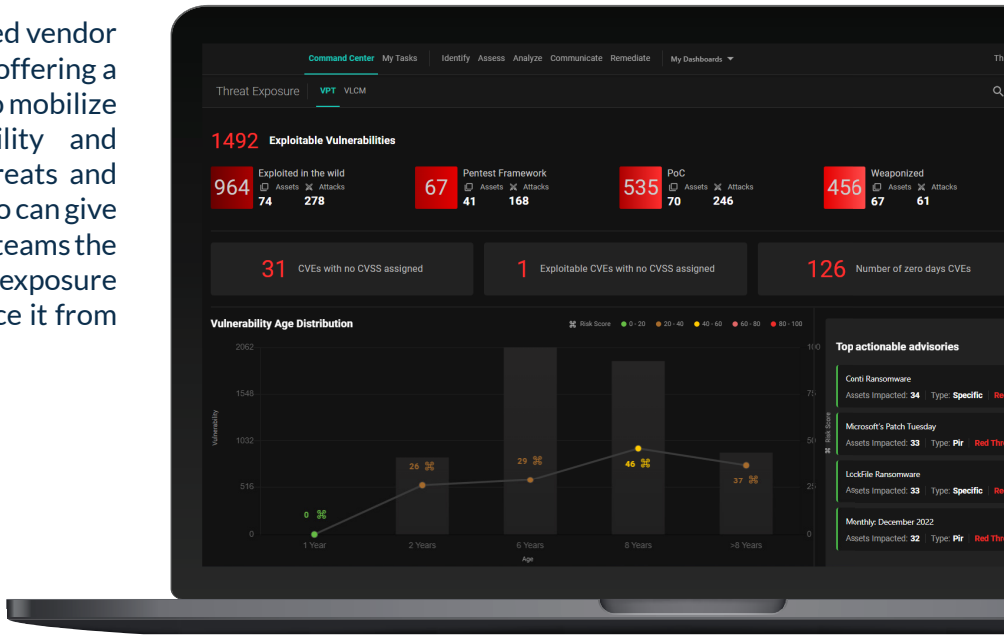
By shifting towards Continuous Threat Exposure Management, MSPs can significantly enhance their cybersecurity offerings, providing better protection for their clients. This proactive approach not only improves security efficacy but also allows MSPs to offer differentiated services, fostering greater client trust and driving business growth. Implementing CTEM effectively positions MSPs as leaders in advanced cybersecurity practices, capable of managing complex and evolving threat environments.

For more information about how we work with MSPs and MSSPs, please visit:
https://www.hivepro.com/partner-program/

About Hive Pro

Hive Pro is a recognized and trusted vendor in Threat Exposure Management, offering a purpose-built platform designed to mobilize comprehensive asset, vulnerability and threat intelligence to prevent threats and remediate high-risks. Only Hive Pro can give Security, IT, Business, and DevOps teams the full spectrum of their cyber threat exposure and the means to actionably reduce it from one interface.

Learn more at www.hivepro.com



Get in Touch

Hive Pro Inc. | info@hivepro.com | www.hivepro.com

Book a Demo

Read our Blog