

ENTHEC[®]

kartos[®]

External threat monitoring solutions

State, comparison and future

2	INTRODUCTION	
3	THE NEED TO MONITOR EXTERNAL THREATS	
6	TYPES OF EXTERNAL THREAT MONITORING SOLUTIONS	
8	• Threat Intelligence Solutions	
12	• External Attack Surface Management (EASM) Solutions	
16	• Digital Risk Management Solutions (DRPS)	
20	• Continuous Threat Exposure Management (CTEM) Solutions	
25	THE FUTURE OF THREAT PROTECTION	

INTRODUCTION

In an increasingly interconnected world, cybersecurity has become a strategic priority for organizations across all sectors. External threats, from malicious actors such as cybercriminals, industrial espionage groups, and nation-states, are constantly evolving, challenging traditional defenses and forcing companies to adopt more dynamic and proactive approaches.

External threat monitoring is a key strategy for anticipating attacks and minimizing the impact of potential security breaches.

External threat monitoring solutions enable organizations to **identify, analyze, and mitigate risks in real-time**, providing visibility into vulnerabilities, attack attempts, and potential breaches before they materialize. However, these tools present significant challenges, including the need for efficient integration with other security systems, effective alert management to reduce false positives, and adaptation to new attack vectors driven by emerging technologies such as artificial intelligence and quantum computing.

This whitepaper aims to **analyze the current state of external threat monitoring solutions**, comparing their features, capabilities, and limitations, while also exploring their future evolution in the context of enterprise cybersecurity. To this end, it will address key technologies such as threat intelligence, external attack surface management (EASM), digital risk assessment (DRPS), and innovative continuous threat exposure management (CTEM).

The need to monitor external threats

In today's digital environment, organizations face a constantly evolving threat landscape. The proliferation of cyberattacks, increasing vulnerabilities, and the sophistication of malicious actors have made security a constant challenge. Given this reality, continuous monitoring and management of exposure to external threats have become essential for companies seeking to minimize risks and ensure operational resilience.

EVOLUTION OF THE EXTERNAL THREAT LANDSCAPE

External threats have evolved significantly over the past few years. Attackers are no longer limited to exploiting known vulnerabilities; instead, they are employing advanced tactics, including the use of artificial intelligence, targeted ransomware, and highly targeted phishing.

Furthermore, the rise of the Internet of Things (IoT) and the migration to cloud environments have expanded organizations' attack surface, rendering traditional perimeter security insufficient.

Faced with this scenario, having a continuous monitoring strategy allows for rapid detection and response to potential threats. Technologies such as Threat Intelligence, Continuous Threat Exposure Management (CTEM), and event correlation platforms provide real-time visibility into an organization's security posture.

BENEFITS OF A CONTINUOUS MANAGEMENT STRATEGY

Early risk identification:

Continuous monitoring helps identify vulnerabilities before attackers can exploit them, thereby enhancing security. Advanced scanning and risk assessment tools enable the prioritization of critical issues and informed decision-making.

Reduction in response time:

Real-time threat detection solutions facilitate rapid response to suspicious activity, minimizing the impact of security incidents.

Regulatory compliance:

Regulations such as GDPR, ISO 27001, and NIST require organizations to maintain constant vigilance over their security. Implementing a CTEM strategy facilitates regulatory compliance and reduces the risk of penalties for non-compliance.

Improved decision-making:

Correlating external threat data with internal information provides a comprehensive view of risks. This allows security teams to adjust their protection strategy proactively.

DATA:

The incidence of attacks related to phishing, fraud, and scams increased three percentage points in 2023 compared to the previous year, representing the largest increase among the various threats.

*Identity Theft Resource Center (ITRC): 2023 Business Impact Report



Taking a proactive and consistent approach is essential to ensuring the integrity, confidentiality, and availability of digital assets.

- The threat landscape is changing rapidly. Cybercriminals evolve their tactics, techniques, and procedures at a dizzying pace, rendering static security measures quickly obsolete. Continuous monitoring enables **real-time threat detection**, allowing for the identification of potential attacks before they cause irreparable damage. This level of constant vigilance can only be achieved through the use of **advanced security analysis tools, artificial intelligence, and machine learning**. Proactive threat management involves not only detecting attacks but also anticipating them in advance. This consists of conducting regular risk assessments, continuously applying security patches, and training employees to recognize phishing and social engineering attempts.
- In this context, external threat monitoring technologies, such as Continuous Threat Exposure Management (CTEM), play a crucial role. **Monitoring enables organizations to continuously identify, assess, and mitigate vulnerabilities and exposures before attackers can exploit them.** These solutions provide real-time visibility into infrastructure weaknesses, prioritizing the most critical threats based on their potential impact.
- Integrating cyber surveillance solutions with SIEM and EDR is essential for achieving an effective and coordinated cybersecurity strategy. A SIEM collects and analyzes event logs from various sources within the infrastructure, enabling real-time data correlation. When integrated with external threat monitoring solutions, **visibility into risks across the attack surface is improved, and prioritized alerts can be generated based on the criticality of the detected vulnerabilities.** Furthermore, an EDR provides advanced endpoint monitoring and response capabilities, enabling organizations to react quickly to active threats. Connecting EDR with CTEM enhances mitigation capabilities by providing contextualized threat intelligence, allowing containment measures to be implemented before an attack escalates.

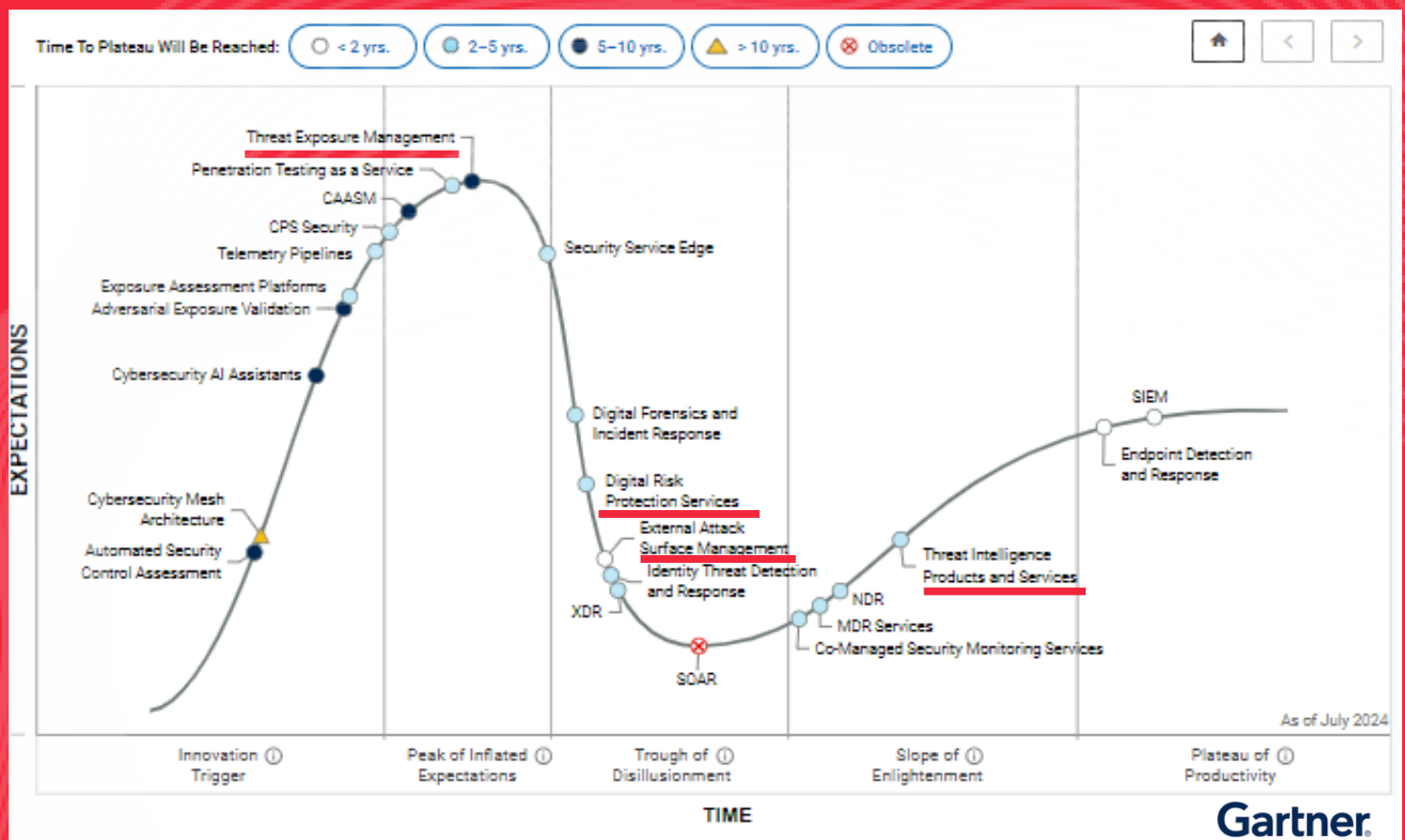
Types of external threat monitoring solutions

External threat monitoring encompasses a diverse set of solutions designed to detect risks that extend beyond the organization's perimeter. These tools vary in focus, scope, and level of automation, adapting to different needs and environments.

- Threat Intelligence Solutions
- External Attack Surface Management (EASM) Solutions
- Digital Risk Management (DRPS) Solutions
- Continuous Threat Exposure Management (CTEM) Solutions

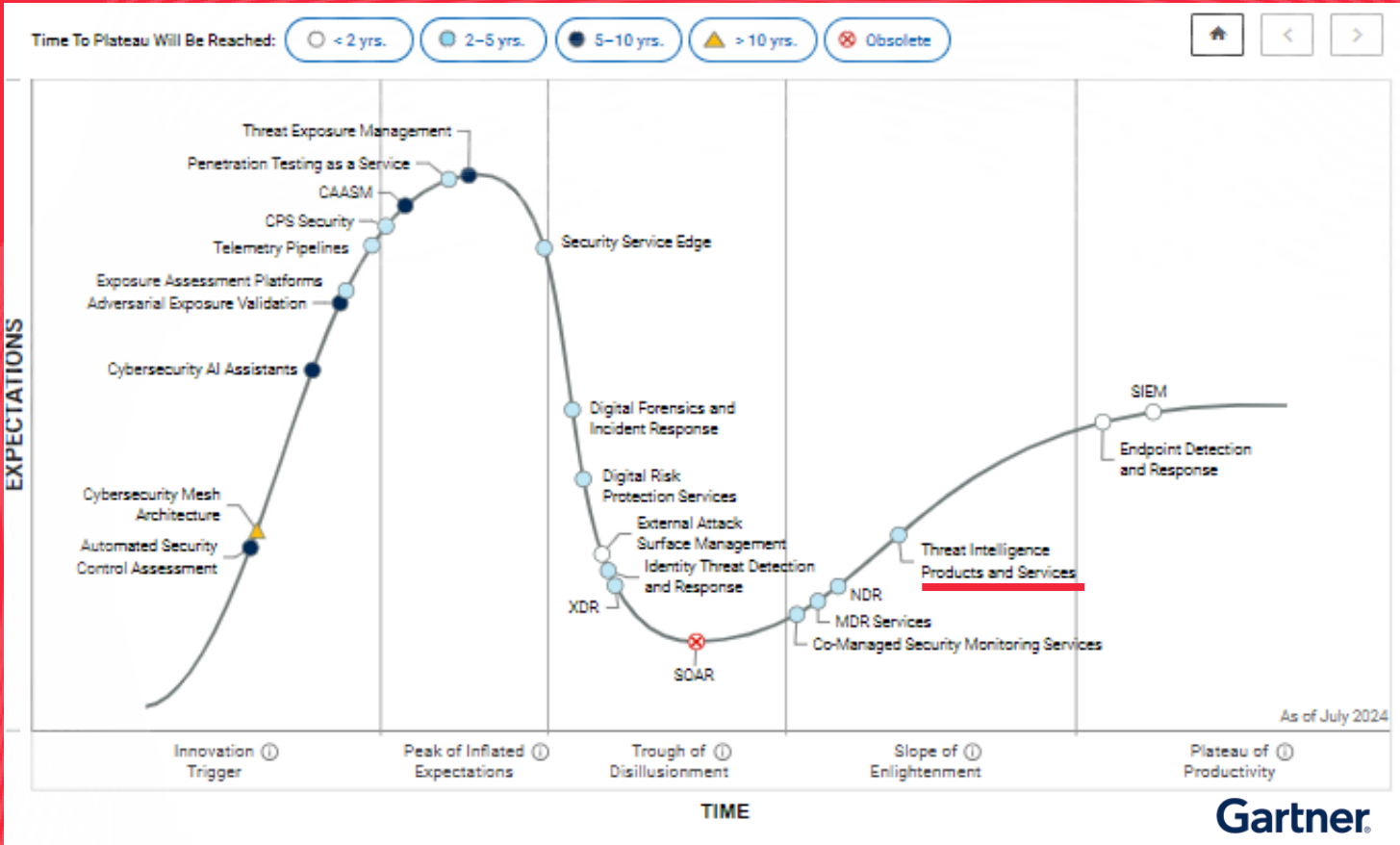
TYPES OF EXTERNAL THREAT MONITORING SOLUTIONS

Within the lifecycle of currently used cybersecurity tools, Gartner includes four external threat monitoring solutions:



- ⦿ Threat Intelligence Solutions
- ⦿ External Attack Surface Management (EASM) Solutions
- ⦿ Digital Risk Management Solutions (DRPS) Solutions
- ⦿ Continuous Threat Exposure Management (CTEM) Solutions

THREAT INTELLIGENCE



THREAT INTELLIGENCE

• What is it?

Threat intelligence is the process of collecting, analyzing, and utilizing information about potential or existing threats that may affect an organization. Its goal is to provide actionable data that helps improve cybersecurity and prevent attacks.

- Allows for understanding the threat environment, providing information about malicious actors, tactics used, exploited vulnerabilities, and potential targets.
- Helps identify patterns in previous attacks to anticipate future risks.

Strategic intelligence:

High-level information used by executives and security officers to make decisions about cybersecurity investments and protection policies.

Tactical intelligence:

Data on the tactics, techniques, and procedures (TTPs) used by attackers. This is useful for IT security teams managing infrastructure.

Operational intelligence:

Detailed information on ongoing attacks, malicious IP addresses, suspicious domains, and patterns of criminal activity on the network.

• How does it work?

Data collection:

Gathers information from a variety of sources, including threat databases, dark web forums, logs of previous attacks, and sensor networks.

Data analysis:

Applies artificial intelligence and machine learning algorithms to identify suspicious patterns.

Correlation of events:

Relates security events with known threat information to detect potential incidents.

Alert generation:

Notifies about suspicious activity trends or indicators of compromise (IoCs) that may pose a threat.

THREAT INTELLIGENCE

- **Advantages**

1. Identification of threat trends

Detection of threat trends by country and sector to adapt the strategy and resources to defend against them.

2. Reduction in incident response time and damage.

Thanks to the cybersecurity strategy developed based on data provided by Threat Intelligence, response times are reduced, and damage mitigation is strengthened.

3. Improved decision-making

With Threat Intelligence-driven data, organizations can better allocate resources and prioritize mitigation actions.

4. Protection against advanced threats

Cyberattacks are constantly evolving, and many sophisticated techniques identified by Threat Intelligence would go undetected by traditional defense systems.

5. Regulatory compliance

Facilitates compliance by providing visibility into threats and ensuring an effective response.

6. Cost reduction

Helps prevent financial losses from cyberattacks, reputational damage, and regulatory sanctions.

THREAT INTELLIGENCE

• Threat Intelligence vs. the rest

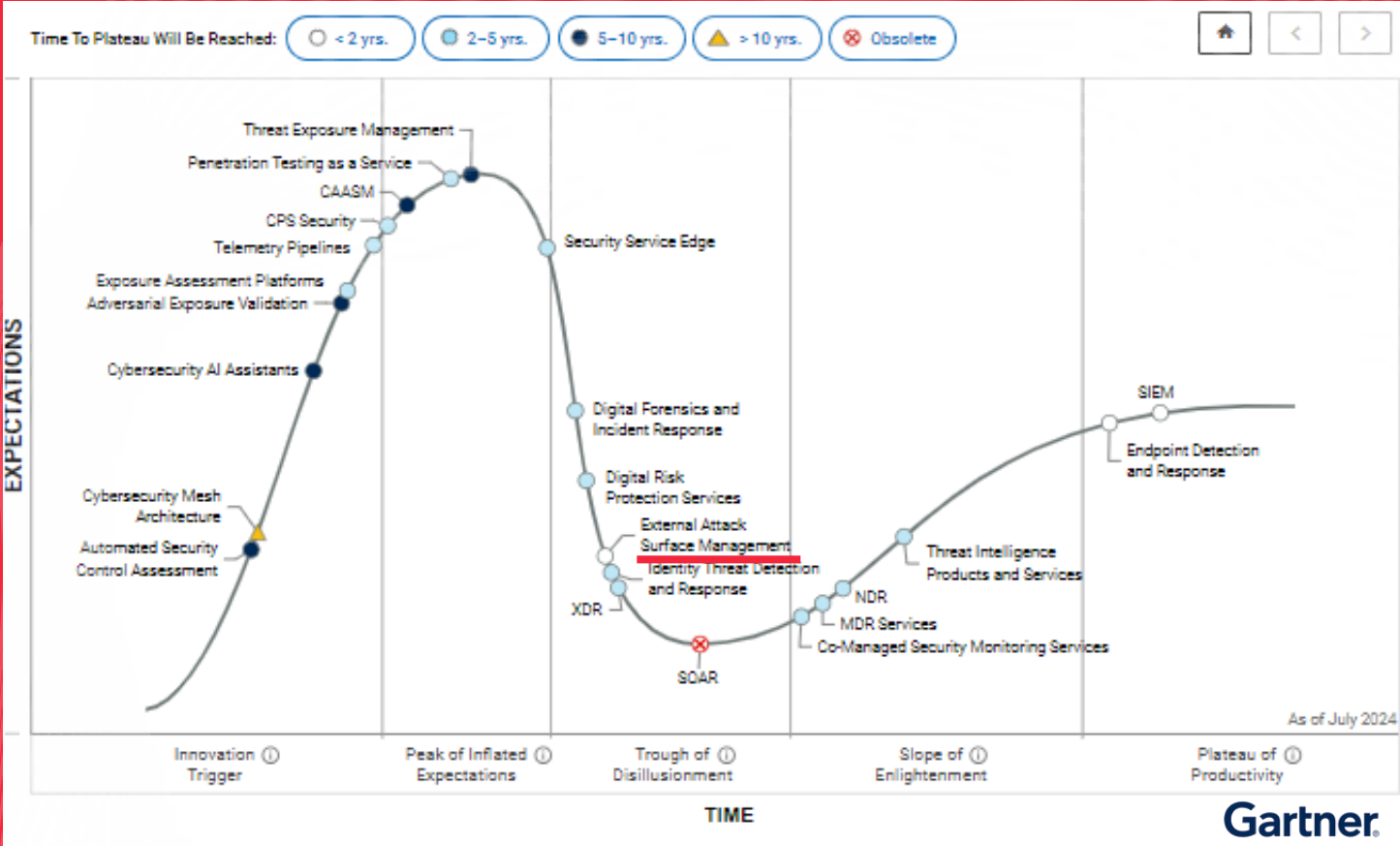


- A cross-cutting tool that provides real-time information on attacks worldwide and by sector.
- Good for understanding the overall state of the cybersecurity environment and designing strategies.



- It does not provide information about ongoing risks or attacks on a specific organization.
- Poor for the immediate and ongoing protection of the organization against its own ongoing risks.

EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)



EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)

• What is it?

The external attack surface includes all of an organization's digital assets that are accessible from the internet. This includes websites, cloud servers, APIs, domains, IP addresses, and other connected systems that cybercriminals can potentially exploit.

- Helps organizations discover, assess, and manage exposed assets, enabling them to mitigate risks before attackers can exploit them.
- Provides real-time visibility into external assets, allowing vulnerabilities to be prioritized for improved security.

• How does it work?

Digital Asset Discovery:

Automatically identifies all of the organization's digital assets, including those that are unknown or unmanaged.

Scans domains, subdomains, IP addresses, web applications, and exposed APIs.

Vulnerability analysis:

Evaluates detected assets for security vulnerabilities, misconfigurations, or outdated software.

Applies ethical hacking methodologies and automated penetration testing to identify risks.

Continuous monitoring:

Scans in real time to detect changes in the attack surface, such as the appearance of new assets or accidental exposures.

Alerts on new risks for rapid mitigation.

Risk assessment and prioritization

Utilizes risk analysis algorithms to categorize threats based on their level of criticality.

Allows organizations to focus on the most serious and urgent problems.

EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)

• Advantages

1. Greater visibility over the attack surface

A complete and up-to-date overview of Internet-accessible systems, including those that may have been forgotten or mismanaged.

2. Early detection of vulnerabilities

Preventing incidents such as ransomware attacks, data theft, or unauthorized access to critical systems.

3. Reducing the risk of cyberattacks

Reducing the chances of cybercriminals exploiting security flaws.

4. Regulatory and normative compliance

The latest cybersecurity regulations require organizations in sensitive sectors to properly manage their attack surface.

5. Optimizing the security team's time and resources

Automation of otherwise time-consuming tasks, such as asset mapping and vulnerability detection.

6. Integration with other cybersecurity tools



It can be integrated with other security platforms, such as firewalls, threat intelligence tools, and intrusion detection systems (IDS/IPS), enabling a more coordinated and effective defense.

7. Proactive response to security incidents

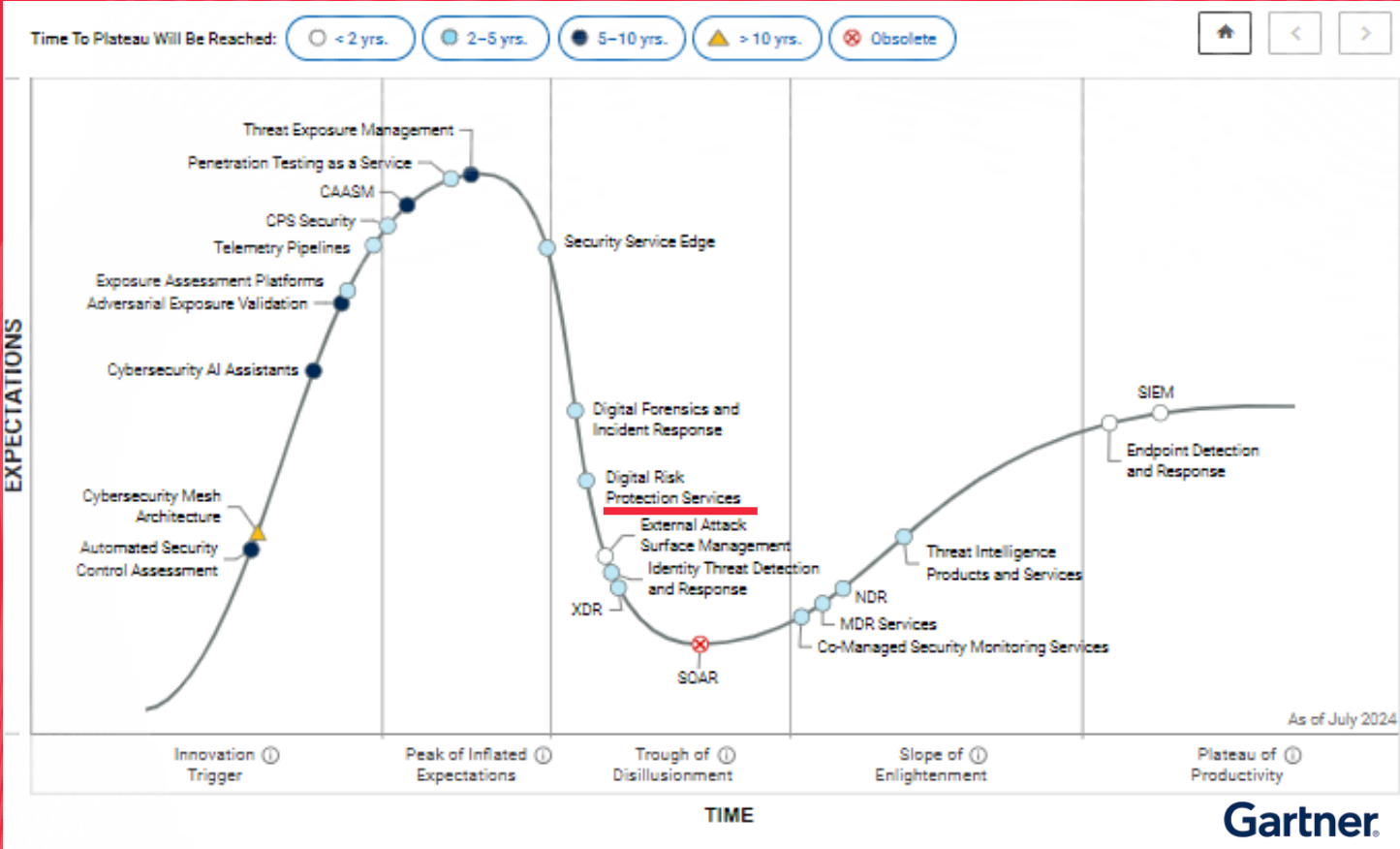
Organizations can act proactively to address potential threats, rather than reacting after an attack occurs.

EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)

- **EASM vs. the rest**

	<ul style="list-style-type: none">• Analyzes holes and vulnerabilities that exist in the physical elements of a company's infrastructure, such as exposed servers, websites, networks, or Internet-facing elements, which could lead to a cyberattack.• Analyzes and prioritizes the risks and which elements are most susceptible to attack or exploitation by cybercriminals.• In some cases, through integration with third parties or even their own technology, can offer mitigation and remediation functionalities.
	<ul style="list-style-type: none">• Generally works in an intrusive way, since they are internal tools that monitor the external surface from within.• Its capabilities are limited to locating perimeter infrastructure failures.

DIGITAL RISK MANAGEMENT (DRPS)



DIGITAL RISK MANAGEMENT (DRPS)

• What is it?

The external attack surface includes all of an organization's digital assets that are accessible from the internet. This includes websites, cloud servers, APIs, domains, IP addresses, and other connected systems that cybercriminals can potentially exploit.

- Helps organizations discover, assess, and manage exposed assets, enabling them to mitigate risks before attackers exploit them.
- They provide real-time visibility into external assets, allowing vulnerabilities to be prioritized and improving security.

• How does it work?

Digital Asset Discovery:

Automatically identifies all of the organization's digital assets, including those that are unknown or unmanaged.

Scans domains, subdomains, IP addresses, web applications, and exposed APIs.

Vulnerability analysis:

Evaluates detected assets for security vulnerabilities, misconfigurations, or outdated software.

Applies ethical hacking methodologies and automated penetration testing to identify risks.

Continuous monitoring:

Scans in real time to detect changes in the attack surface, such as the appearance of new assets or accidental exposures.

Alerts on new risks for rapid mitigation.

Risk assessment and prioritization

Utilizes risk analysis algorithms to categorize threats based on their level of criticality.

Enables organizations to focus on the most pressing and urgent issues.

DIGITAL RISK MANAGEMENT (DRPS)

• Advantages

1. Early threat detection

Enables organizations to identify risks before they are exploited, thereby reducing the impact of attacks and enhancing their ability to respond effectively.

2. Protection against data breaches

Helps detect stolen credentials, compromised sensitive information, or leaked databases, enabling rapid action to protect the organization.

3. Reducing the risk of fraud and phishing

Helps detect fraudulent websites and fake accounts seeking to deceive customers and employees.

4. Protection of the company's reputation

Controls the organization's image in the digital environment, preventing disinformation attacks or impersonation that could damage its reputation.

5. Improving corporate resilience to attacks

Helps strengthen the company's resilience to cyberattacks.

6. Regulatory and normative compliance



Facilitates legal compliance by detecting security incidents and generating risk reports.

7. Integration with other security systems

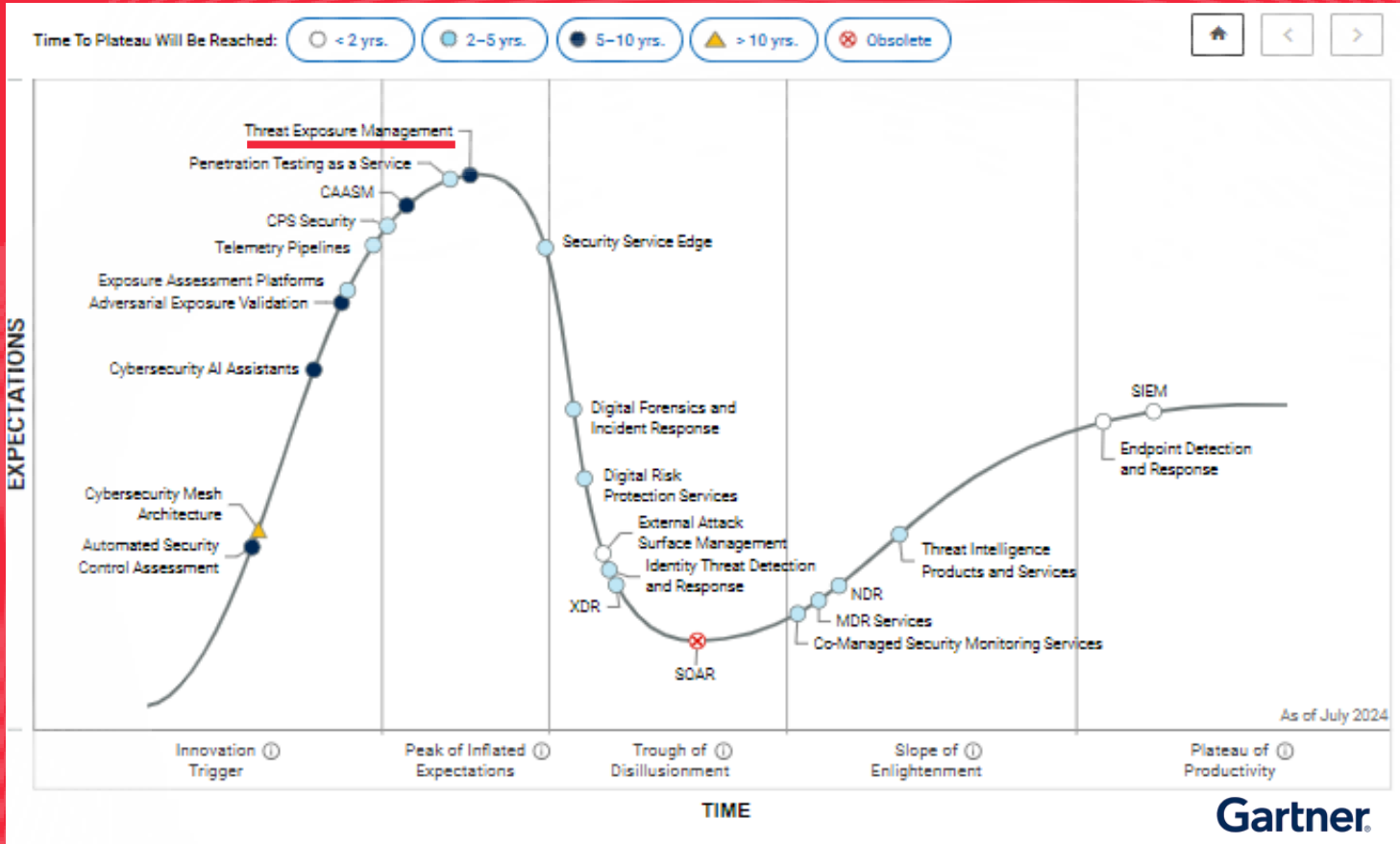
It can be integrated with Threat Intelligence, SIEM, and incident response platforms, improving threat detection and mitigation capabilities.

DIGITAL RISK MANAGEMENT (DRPS)

• DRPS vs. the rest

	<ul style="list-style-type: none">• Protects digital assets, i.e., the organization's information that is exposed outside its perimeter and visible to third parties.• Evaluates brand risk, check for leaked information, credentials, or data, including gaps and errors that can be seen from the outside.• In many cases, it also allows for monitoring information about people of interest, whether VIPs, executives, or relevant people within the company.
	<ul style="list-style-type: none">• It does not cover the location of existing gaps in the physical elements of the company's infrastructure or the inventory of assets and systems that are exposed to the outside world.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)



CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

• What is it?

Continuous Threat Exposure Management (CTEM) is a security approach that enables organizations to assess and reduce their attack surface continuously.

- Allows to maintain a real-time view of vulnerabilities and risks, enabling you to respond more quickly and efficiently to emerging threats.
- Not only seeks to detect security flaws, but it also helps prioritize and manage vulnerability remediation based on their potential impact.

• How does it work?

1. Identification of exposed assets

Continuously scans and analyzes the organization's digital assets.

Detects systems, applications, and services that cybercriminals could exploit.

2. Vulnerability assessment

Identifies security flaws, misconfigurations, or exposed credentials in software.

Uses threat intelligence to determine which vulnerabilities are most likely to be exploited.

3. Risk prioritization

Classifies vulnerabilities based on their level of criticality and probability of exploitation.

Provides actionable recommendations to remedy the most urgent risks.

4. Real-time monitoring and response

Detects new risks continuously, without the need for scheduled audits.

Takedowns and real-time alerts to security teams about findings and changes in threat exposure.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

• Advantages

1. Unification of several monitoring solutions into one

Simplifying vulnerability monitoring and management processes by unifying cybersecurity capabilities such as EASM, DRPS, scoring, third-party monitoring, and VIP protection into a single tool.

2. Continuous evaluation of the attack surface

Constant and updated view of exposure to threats, including those in the value chain.

3. Prioritization of critical threats

Helps prioritize the most dangerous risks based on their potential impact and likelihood of exploitation.

4. Reduction in incident response time

Allows acting more quickly to mitigate risks, reducing the time a vulnerability remains exposed.

5. Integration with other security tools

Integration with incident management, threat intelligence, and forensic analysis systems improves coordination in attack response.

6. Reducing the risk of security breaches

Helps prevent security incidents before they occur.

7. Adaptation to new threats

Enables businesses to adapt in real-time to new attack tactics and exploitation techniques, and monitor their impact on corporate security.

8. Regulatory compliance and security audits



Facilitates compliance with cybersecurity regulations by providing detailed, real-time reports on organizations' risk management and vulnerability mitigation.

9. Focus on business impact

Enables aligning cybersecurity strategy with business objectives, facilitating risk prioritization, and addressing specific vulnerabilities. This approach considers the potential impact on the business, the likelihood of an attack, and which parts of the company would be affected.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

- **CTEM ahead of the rest**

	<ul style="list-style-type: none">• Integration of all the above types of tools to achieve automated, continuous, real-time monitoring focused on business criteria.• Ability to continuously, automatically, and in real time monitor the external attack surface, digital risk, third-party risk, the protection of key people within the organization, internal and third-party compliance, as well as the impact of artificial intelligence.• Allows organizations to prioritize risks and address specific vulnerabilities and problems, taking into account not only technical criteria but also business criteria.
	<ul style="list-style-type: none">• Short time on the market and few manufacturers offering this type of tools.• Limited awareness of this advanced technology among corporate cybersecurity teams.• Constant technological innovation to avoid becoming obsolete.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

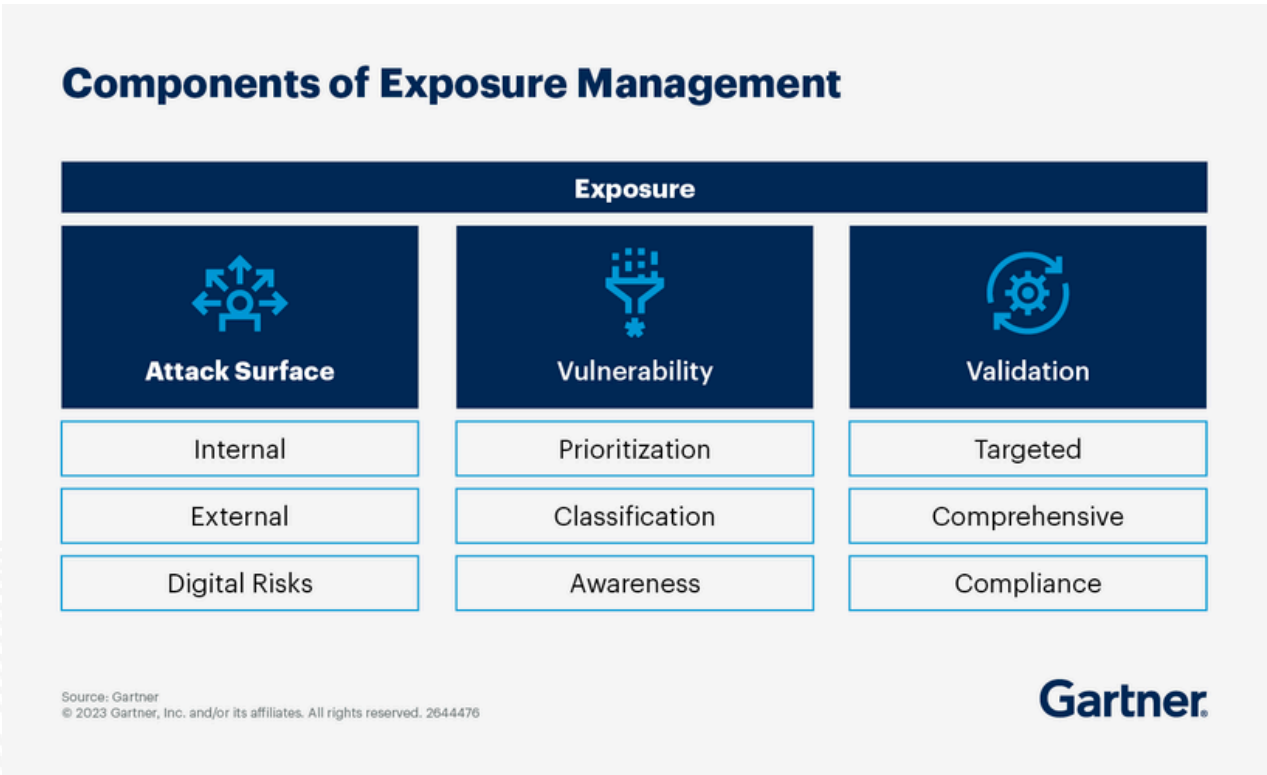
- Gartner on CTEM

Gartner highlights **Continuous Threat Exposure Management (CTEM)** as a [key trend in cybersecurity](#). Its approach enables organizations to continuously assess the accessibility, exposure, and exploitability of their digital and physical assets. Unlike traditional periodic assessments, CTEM provides a constant, up-to-date view of vulnerabilities, facilitating a more agile and effective response to potential threats.

Gartner emphasizes that with the expansion of digital attack surfaces and the influence of AI in the execution of cyberattacks, traditional cybersecurity models focused on patching and securing physical systems and self-managed software are no longer sufficient. CTEM offers a comprehensive and proactive approach that is needed today.

Furthermore, Gartner predicts that **by 2026, unpatched attack surfaces will have grown to represent more than half of the enterprise's overall attack surface**. Therefore, traditional vulnerability management programs will be unable to keep up, and organizations that prioritize CTEM-based security investments are expected to be three times less likely to suffer a security breach.

For all these reasons, Gartner believes that the adoption of CTEM and the use of the necessary monitoring solutions is essential for organizations to maintain a strong and proactive security posture against emerging cyber threats.



The future of threat protection

The cybersecurity landscape is constantly evolving, and organizations must adapt to effectively protect against external threats.

The future of protection against threats

1. AI and machine learning

The application of artificial intelligence (AI) and machine learning (ML) in cybersecurity poses a risk, but it is also revolutionizing the way organizations detect and respond to threats. These technologies allow large volumes of data to be analyzed to identify patterns and anomalies that indicate malicious activity, facilitating a more proactive and efficient response.

2. Zero Trust Approach

The Zero Trust security model, based on the principle of "never trust, always verify," will continue to gain traction. This approach implies that no entity, whether internal or external, is considered trustworthy by default. Every access request must be authenticated and authorized, which helps prevent internal and external threats.

3. Increase in supply chain attacks

An increase in attacks targeting supply chains is anticipated. Cybercriminals are looking for vulnerabilities in suppliers or partners to infiltrate target organizations. This underscores the need for more rigorous risk management and greater oversight of third parties to ensure security throughout the supply chain.

4. Expansion of the Attack Surface

With digitalization and the adoption of emerging technologies, organizations' attack surface is expanding. This includes IoT devices, cloud environments, and remote systems, which require more comprehensive and up-to-date security strategies to protect all potential entry points.

5. Post-Quantum Cryptography

The advent of quantum computing poses challenges for current cryptographic methods. Organizations will need to prepare by adopting post-quantum cryptography techniques to protect their data against potential future threats stemming from this emerging technology.

6. Spain as an emerging leader

Spain is positioning itself as an emerging leader in cybersecurity in Europe, thanks to significant investments and the development of specialized talent focused on the design of advanced strategic cybersecurity solutions and tools.

Kartos Corporate Threat Watchbots is the CTEM platform developed by Enthec that locates exposed corporate information and vulnerabilities that can be exploited to execute an attack, allowing organizations to protect themselves and improve their defenses.

CyberIntelligence

To discover latent vulnerabilities

Identify open and exposed company information and vulnerabilities on the Internet, the Deep Web, the Dark Web, and social media. Identify phishing campaigns, fraud and scams, CVEs, and DNS health. Identify leaked passwords and credentials, documentation, or databases.

Cybersecurity

To keep digital assets safe

Expand your cybersecurity strategy beyond the corporate IT perimeter. Brand, domain, and subdomain protection. Corporate email protection. Ransomware protection. Web security and threat remediation.

Scoring

To increase the security score

Corporate and third-party cybersecurity score based on objective, real-time data.

Compliance

To comply with current regulations

Corporate and third-party compliance based on objective, real-time data. ISO 27001. PCI-DSS.

WHY CHOOSE KARTOS

- Automated, non-intrusive and continuous monitoring.
- 5 tools in one: EASM, DRPS, Scoring, Third-Party Risk, and VIP Protection.
- Real-time alerts on open and exposed vulnerabilities.
- Elimination of false positives in search results thanks to Kartos Context Tags, which use internally developed AI.
- Without back doors, all the technology used by Kartos is developed internally and does not depend on third-party applications for its operation.
- To get started, Kartos just requires entering the domain to monitor. No implementation is required within the organization's IT system.
- Annual license price fixed.

#WeAlreadyKnow

ENTHEC[®]



@enthec



@enthecsolutions

kartos[®]