Magic Quadrant for Exposure Assessment Platforms

10 November 2025 - ID G00808226 - 64 min read

By Mitchell Schneider, Dhivya Poole, and 1 more

Cybersecurity leaders must regularly assess their overall vulnerabilities and threat exposure as a key input to security architecture and operations planning. This research helps security teams evaluate exposure assessment platform vendors.

Strategic Planning Assumption

By 2027, organizations that integrate exposure assessment data into IT and business workflows will experience 30% less unplanned downtime from exploited vulnerabilities than those relying on isolated vulnerability management tools.

Market Definition/Description

This is the first version of the Magic Quadrant for Exposure Assessment Platforms. It replaces the **Market Guide for Vulnerability Assessment**.

Exposure assessment platforms (EAPs) continuously identify and prioritize exposures, such as vulnerabilities and misconfigurations, across a broad range of asset classes. They natively deliver or integrate with discovery capabilities, such as assessment tools, that enumerate exposures, like vulnerabilities and configuration issues, to increase visibility. EAPs use techniques like threat intelligence (TI) to analyze an organization’s attack surfaces and weaknesses, and prioritize treatment efforts for high-risk exposures by incorporating threat landscape, business and existing security control context. Through prioritized visualizations and treatment recommendations, EAPs help provide direction for mobilization, identifying the various teams involved in mitigation and remediation. EAPs are primarily delivered as self-hosted software or as a cloud service, and may use agents for exposure information collection.

Exposure assessment platforms (EAPs) discover, analyze and prioritize an organization's exposures, such as vulnerabilities, gaps in compliance, unmanaged assets and asset misconfigurations across organizational attack surfaces, including (but not limited to) external, internal, cloud and end-user. Continuous discovery and inventory of attack surfaces, involving verification of known assets and discovery of unknown threats, is a key step in an exposure management program to provide sufficient visibility. To improve prioritization and treatment efforts, EAP consolidates discovered exposures and prioritizes them based on exposure severity, asset criticality, business impact, likelihood of exploitation and the context of security controls. The results are consolidated into a central location to improve operational efficiency, indicated through risk scoring, trends, stats and other visualizations, such as visibility/accessibility of assets (e.g., via attack path), asset identification/ownership and remediation tracking. The core purpose of EAPs is to provide a better, consolidated view of high-risk exposures enabling organizations to take key proactive actions to prevent breaches.

Mandatory Features

The mandatory features for this market include the solution being able to:

- Natively deliver or integrate with discovery capabilities to uncover a wide range of assets from internal, external, cloud and end-user attack surfaces; and report on exposures across a variety of asset types. Asset sources include endpoints, network infrastructure, on-premises infrastructure, identity (e.g., entitlements), physical and virtual hosts, containers, Internet of Things (IoT) and operational technology (OT), and cloud platforms and applications.

- Prioritize discovered issues based on the accessibility, visibility and exploitability of the exposure. This includes applying asset context, threat intelligence and security control context.

- Enable mobilization by integrating into a wider set of IT service management systems, providing enhanced asset context and reporting.

Common Features

The optional capabilities for this market include:

- Extend discovery capabilities to digital assets and those artifacts being actively abused by external threat actors via native or third-party capabilities. Asset sources may include social media, surface/dark/deep web and digital supply chain.

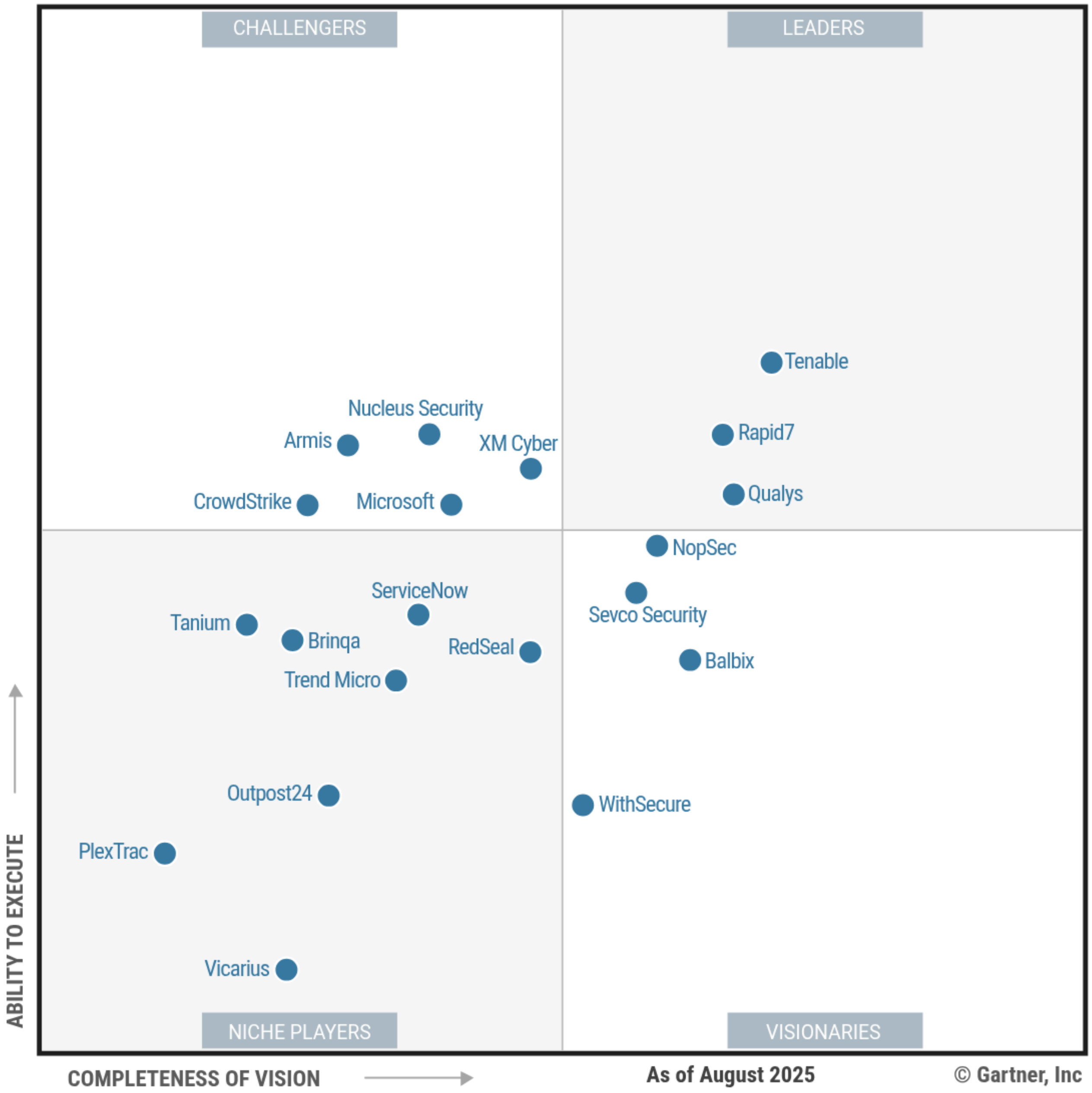
- Prioritize exposures through extended analysis of the accessibility and likelihood of exploitation via API flexibility to ingest additional non-native context. This may include the EAP solution performing attack path analysis and/or taking data/output from adversarial exposure validation such as breach and attack simulation (BAS).

- Enable faster remediation or mitigation through integration with IT risk management, IT operations, security operations solutions (e.g., security information and event management [SIEM], security orchestration, automation and response [SOAR]) and/or directly with controls (e.g., security posture management or automated security controls assessment solutions).

- Track the life cycle of exposures via a centralized, aggregated view supported with automated workflows.

Magic Quadrant

Figure 1: Magic Quadrant for Exposure Assessment Platforms



Gartner

Vendor Strengths and Cautions

Armis

Armis is a Challenger in this Magic Quadrant. Its Armis Centrix Cyber Exposure Management Platform is delivered as a SaaS solution, supporting on-premises and hybrid deployments to meet the needs of regulated and specialized environments.

Armis' operations are geographically diversified, with customer bases in North America, Europe, the Middle East, Africa, and Asia/Pacific. Its clients are primarily large enterprises and public sector organizations operating in sectors such as healthcare, manufacturing, transportation, and government. Over the past year, Armis has expanded its international footprint, supported by regional data centers, new channel partners, and local sales and support teams. Its tiered subscription licensing is based on asset volume, site count, and access to platform modules, such as asset intelligence, risk prioritization, and remediation orchestration.

Armis is enhancing its cyber-physical systems (CPS) protection capabilities with additional OT, IoT, and IIoT integrations (via the OTORIO acquisition), alongside improved AI-driven exposure detection and response (via Silk Security and CTCI acquisitions). Planned enhancements include improvements to its risk scoring engine and attack visualization, supporting broader exposure management across IT and OT environments.

Strengths

- **Strong partner ecosystem and demonstrated market growth:** Armis supports a strong partner ecosystem through its Armis Partner Experience (APEX) portal. It has expanded its customer base across a range of enterprise sizes, demonstrating flexibility in meeting diverse organizational needs and use cases.

- **CPS integration with native CAASM and ASCA capabilities:** Armis distinguishes itself with native support for exposure management domains, such as cyber asset attack surface management (CAASM) and automated security control assessment (ASCA). It extends to OT, IoT, and Internet of Medical Things (IoMT). Combined with FedRAMP Moderate certification, these capabilities differentiate it as a good option for highly regulated and operationally diverse sectors.

- **Customizable prioritization engine with data science flexibility:** Armis allows users to customize its exposure prioritization algorithms, enabling more tailored risk scoring based on the organization’s specific context.

Cautions

- **Premium pricing and feature tiering:** Armis’ asset- and feature-based pricing may be perceived as premium. Advanced capabilities such as behavioral analytics or extended integrations may require higher-tier licenses, which could introduce procurement complexity for budget-conscious organizations.

- **Limited native remediation and workflow automation:** Armis’ native remediation orchestration capabilities are less mature compared with those of other vendors in this research with built-in ticketing, patching, or workflow automation. Customers may need to rely on third-party tools to fully close the remediation loop.

- **Integration depth varies across ecosystem partners:** Armis' depth and functionality of IT, OT, and security platform integrations can vary. Some customers may require custom development or middleware to achieve full interoperability with security information and event management (SIEM), IT service management (ITSM), or cloud-native application protection platform (CNAPP) tools. This may limit Armis' appeal to buyers seeking a more unified exposure management strategy.

Balbix

Balbix is a Visionary in this Magic Quadrant. The Balbix Platform is delivered as a SaaS solution, supporting hybrid deployments that include on-premises components in regulated or air-gapped environments.

Balbix operates globally, with a primary North American base and expanding presence in Europe, the Middle East, Africa, and Asia/Pacific, serving mainly large enterprises and Fortune 1000 companies in sectors like financial, healthcare, and manufacturing. Its tiered SaaS subscription model is based on asset volume and access to advanced analytics, automation, and reporting features.

Balbix continues to invest in its risk-scoring algorithms, automated asset inventory, and real-time exposure prioritization. The company is advancing its bidirectional CNAPP, ITSM, and SIEM integrations, along with enhancing its predictive analytics.

Strengths

- **Dynamic risk scoring enables business-aligned risk quantification:** Balbix's key differentiator is its cyber risk graph, which dynamically maps assets, users, vulnerabilities, threats, and business impact. Customers report that Balbix's risk quantification features provide insights that are clearly differentiated from traditional vulnerability assessment technologies.

- **Exposure discovery, prioritization, and remediation workflow automation:** Balbix uses cybersecurity domain-specific AI models to automate asset discovery, normalize vulnerability data, and continuously assess exposure. Its analytics engine identifies likely attack paths and recommends prioritized actions, reducing manual triage.

- **Good fit for executive reporting and governance use cases:** Balbix offers customizable dashboards, scenario modeling, and risk forecasting, helping compliance (GRC) teams align cybersecurity with enterprise risk management strategies.

Cautions

- **Limited depth and maturity of bidirectional integrations:** Balbix's bidirectional capabilities are still developing and remain relatively limited compared with those of more mature EAPs. While ITSM and workflow management tool integrations are in production and API-based support for SOAR platforms is available, automation of remediation workflows may be constrained by integration depth and flexibility, potentially requiring manual effort in more complex environments.

- **Initial configuration requires strong data hygiene:** The effectiveness of Balbix's risk-scoring engine depends on high-quality data input. Organizations with incomplete asset inventories or inconsistent vulnerability feeds may face challenges during onboarding; however, Balbix applies inference and correlation to help complete inventories and provides telemetry dashboards to support data normalization.

- **Above-average pricing is prohibitive for cost-conscious budgets:** Balbix's pricing model, which scales with asset volume and access to advanced analytics, may be cost-prohibitive for midmarket organizations.

Brinqa

Brinqa is a Niche Player in this Magic Quadrant. Its Unified Exposure Management Platform is delivered primarily as a SaaS solution with support for hybrid deployments.

Brinqa's operations are geographically diversified, and its clients tend to be midsize to large enterprises across sectors such as finance, insurance, healthcare, consumer goods, and technology. Brinqa has increased its presence in North America and Europe over the past 12 months. Licensing is based on modular capabilities and asset tiers, with pricing aligned to the number of deduplicated assets with active findings.

Brinqa continues to invest in expanding its unified data model, enhancing automation and remediation workflows, and integrating AI to deliver deeper context for risk scoring and treatment guidance. Brinqa is expanding platform integrations, improving data quality, and developing AI and warehousing features to support better risk prioritization, streamlined workflows, and scalable exposure management.

Strengths

- **Contextual prioritization and workflow orchestration:** Brinqa's platform supports exposure management use cases by focusing on the most critical security issues, prioritizing risks based on relevant data and context, and streamlining the process of addressing those risks with tailored remediation workflows.

- **Focus on large enterprises:** Brinqa's go-to-market strategy and product roadmap are specifically designed for large, mature organizations, particularly those in regulated industries, with planned enhancements focused on scalability and compliance alignment.
- **Messaging and business alignment:** Brinqa effectively communicates its value proposition through use-case-driven messaging that resonates with both technical and executive stakeholders.

Cautions

- **Deployment complexity and onboarding variability:** Brinqa is typically selected by large enterprises with complex security environments, where deployments may take 45 to 60 days and involve structured onboarding or professional services. While many clients realize value early in the process, organizations with less intricate requirements may find Brinqa's flexibility more challenging to implement.
- **Limited bidirectional integrations:** Brinqa's current lack of bidirectional integrations — particularly with endpoint detection and response (EDR) and application security posture management (ASPM) platforms — may limit its ability to fully operationalize remediation workflows in complex environments.
- **Limited out-of-the-box remediation automation:** Brinqa offers fewer prebuilt remediation workflow integrations compared with some competitors, which may extend time to value for organizations seeking plug-and-play automation.

CrowdStrike

CrowdStrike is a Challenger in this Magic Quadrant. Its Falcon Exposure Management platform is delivered only as a SaaS solution.

CrowdStrike operates globally, with a strong presence in North America and growing adoption across Europe, Asia/Pacific, the Middle East, Latin America, and Japan. Its customer base primarily consists of midsize to large enterprises, particularly those leveraging the broader Falcon platform. Licensing follows a modular, subscription-based model, with pricing tied to endpoint coverage and available in bundled tiers.

CrowdStrike continues to invest in expanding its exposure management capabilities, including AI-driven and agentic risk-based vulnerability prioritization techniques and workflows, attack path analysis, network scanning, and integrations with third-party tools. These enhancements remain aligned with structured exposure management practices and broader enterprise security needs.

Strengths

- **Unified platform with broad native capabilities:** CrowdStrike's Falcon Exposure Management is tightly integrated into the broader Falcon platform (including its SIEM and SOAR), offering native capabilities across EDR, CAASM, external attack surface management (EASM), and security posture management for cloud, applications, data, and SaaS. This enables customers to consolidate point products, reduce tool sprawl, and benefit from seamless telemetry correlation across endpoint, identity, and cloud environments.

- **Threat intelligence and attack path contextualization:** The EAP integrates real-time native and third-party threat intelligence from a broad range of tracked adversaries and indicators of compromise (IoCs), enriching exposure data with adversary behavior and MITRE ATT&CK mappings. This contextualization enables risk-based prioritization and attack path analysis by aligning exposures with known tactics of threat actors.

- **Automation and remediation workflow depth:** CrowdStrike's Falcon Exposure Management offers a large number of prebuilt remediation workflows, automating ticketing and remediation actions using endpoint telemetry. The platform integrates with ServiceNow and Jira to enable coordinated remediation actions between security and IT teams.

Cautions

- **The cloud-only delivery model may limit deployment flexibility:** Falcon Exposure Management is a cloud-native SaaS offering, with FedRAMP High Authorization and DoD Impact Level 5 (IL5) compliance, but no on-premises deployment option. This may constrain organizations with strict data residency, regulatory, or air-gapped environment requirements.

- **Limited support for exposure management integrations:** While CrowdStrike offers native capabilities and platform integrations for various security use cases, its exposure-management-specific integrations — particularly in areas like EASM, CNAPP, and ASCA —

remain limited. Organizations seeking a more open, ecosystem-agnostic exposure management approach may require additional customization.

- **Lack of customization in prioritization models:** While the platform supports risk-based prioritization, clients cannot currently create custom exposure scoring models, limiting advanced users who want tailored prioritization logic.

Microsoft

Microsoft is a Challenger in this Magic Quadrant. Its Security Exposure Management solution is delivered only as a SaaS offering, activated via Microsoft Security licenses, and is accessible across multicloud environments.

Microsoft has geographically diverse operations at a global scale, with a broad customer base and steadily growing presence across enterprise environments. Most Security Exposure Management users are existing Microsoft customers, especially those using the broader Microsoft Defender ecosystem. Licensing is based on bundled Microsoft Security subscriptions (e.g., Microsoft 365 E5 Security), with Security Exposure Management included as a value-added capability rather than a stand-alone SKU.

Microsoft continues to expand its EAP capabilities by leveraging AI to support contextual remediation, broadening attack surface coverage (e.g., SaaS, OT, identity), and tightening integration with Microsoft Sentinel and third-party tools. It is also enhancing its attack path analysis and persona-specific reporting to support prioritization and remediation/mitigation workflows.

Strengths

- **Integrated exposure management capabilities:** Microsoft's EAP is part of the unified Defender ecosystem, offering native capabilities across EASM, CAASM, CNAPP, and OT security. It combines agentless and agent-based vulnerability discovery with authenticated and unauthenticated scans of unmanaged devices. The platform includes numerous reprioritize remediation workflows and integrates with third-party tools.

- **Data accessibility and external analytics support:** Microsoft Security Exposure Management provides graph-based attack path visualizations and supports data export via API. While its built-in prioritization model is not directly customizable, users can adjust prioritization through asset criticality settings, custom rules, and exceptions. For advanced use cases, data can be integrated with tools like Power BI or Jupyter for external analysis and custom prioritization logic.

- **Cross-team remediation support:** The EAP supports initiative and persona-specific reporting, integrates with Microsoft Sentinel and Intune, and offers AI-powered remediation guidance in multiple languages, addressing both technical and executive-level requirements.

Cautions

- **Roadmap execution:** While Microsoft has a roadmap for its EAP solution, many planned features are already common in competing platforms. The lack of a clear timeline and a reliance on incremental updates may limit differentiation.

- **Deployment model and dependencies:** The Security Exposure Management platform is delivered exclusively as a managed SaaS service, with no on-premises deployment option. This may not be suitable for organizations with strict data residency, regulatory, or infrastructure requirements. Additionally, heavy dependence on the Defender ecosystem could slow EAP-specific advancements.

- **Complexity in licensing and value clarity:** Microsoft's EAP solution is bundled within broader Microsoft Security offerings and not sold as a stand-alone product. This bundling may present challenges for security organizations specifically seeking to evaluate or acquire an exposure assessment platform independently.

NopSec

NopSec is a Visionary in this Magic Quadrant. Its Cyber Threat Exposure Management Platform is delivered exclusively as a SaaS solution.

NopSec's operations are geographically diversified, with a strong foothold in North America and a growing presence in Europe, the Middle East, Africa, and Asia/Pacific, supported by a direct and indirect go-to-market strategy. Its clients are primarily midsize to large enterprises. Licensing is based on a tiered SaaS subscription model, which includes bundled professional services, implementation support, and access to a dedicated customer success team.

NopSec continues to expand its capabilities in remediation orchestration and bidirectional integrations with technologies such as EDR, CNAPP, SIEM, and ITSM. NopSec aims to enhance contextual remediation guidance and persona-based reporting, as well as evolve its passive attack path modeling into active emulation to improve validation capabilities.

Strengths

- **Threat intelligence aggregation and risk scoring prioritization:** NopSec's platform integrates diverse threat intelligence feeds, aggregating a large number of sources into its risk-scoring engine. This supports contextualized prioritization based on attacker behavior, asset criticality, and control state, and reflects an approach that aligns with emerging threat-centric prioritization practices in exposure management.

- **Attack path visualization and remediation orchestration:** Users can visualize and analyze detailed attack paths, including security controls, vulnerability locations, and kill chain hops, across network, identity, EDR, and application layers. They can also initiate targeted remediation or exception workflows directly from the attack path view.

- **Remediation workflow automation and flexibility:** The platform provides out-of-the-box remediation workflows and customizable playbooks to automate and orchestrate remediation across IT, cloud, and applications, exception handling, and business unit routing for greater efficiency and accountability.

Cautions

- **Limited integration with security control optimization solutions:** NopSec's bidirectional integration capabilities are increasing. However, current limitations in native third-party integrations with adversarial exposure validation (AEV) and ASCA platforms may restrict full automation and closed-loop remediation in diverse environments. These gaps reflect a strategic focus on developing native AEV capabilities within the NopSec platform.

- **Cloud-only deployment model limits flexibility:** The platform has no on-premises deployment options. This may challenge organizations with strict data residency, sovereignty, or infrastructure control requirements, particularly in highly regulated or air-gapped environments.

- **Moderate global market penetration and brand visibility:** NopSec's customer base remains concentrated in North America, indicating a need for expanded efforts to support a global presence.

Nucleus Security

Nucleus Security is a Challenger in this Magic Quadrant. Its Nucleus Security Platform is delivered as a SaaS solution, with optional deployment in private, on-premises, air-gapped, or hybrid cloud environments, including AWS GovCloud (US) and Google Cloud Platform.

Nucleus Security operates globally, with a North American base and expanding presence in Europe, the Middle East, Africa, and Asia/Pacific. It mostly serves large enterprises and public sector clients, including federal agencies, Global 2000 companies, and managed security service providers. Licensing follows a tiered SaaS subscription model, including free implementation support and a dedicated customer success team.

Nucleus Security continues to enhance its bidirectional integrations across ASPM, EDR, CNAPP, and OT platforms, improve remediation workflows, and deepen its attack path modeling and validation capabilities. The company aims to make improvements in contextual remediation based on AI automation, expanded connector libraries, and automation frameworks.

Strengths

- **Integration framework supports public sector and enterprise use cases:** Nucleus Security's broad integration framework includes native support for CAASM, EDR, CNAPP, and ASPM platforms. Its FedRAMP-authorized deployment and alignment with frameworks like NIST SP 800-53 and CMMC make it well-suited for public sector and regulated enterprises.

- **Remediation workflow automation and customization:** The platform provides out-of-the-box remediation workflows and supports customizable playbooks, enabling automated remediation across IT, cloud, and application environments. Operational efficiency and accountability are enhanced by SLA tracking, exception handling, and business unit routing.

- **Channel-led global expansion and operational scalability:** Nucleus Security operates a 100% channel-led go-to-market model, with growth in Europe, the Middle East, Africa, and Asia/Pacific. The platform's ease of deployment and data-separated multitenancy make it well-suited for managed security service providers (MSSPs), M&A onboarding, agencies, and large enterprises seeking fast time to value.

Cautions

- **Missing advanced use cases:** Nucleus Security lacks broad native integrations with SIEM and ASCA platforms, which may limit automation and orchestration for organizations with mature security operations. This also reduces its support of full-spectrum continuous threat exposure management (CTEM) programs without a third party.

- **Limited orchestration capabilities:** Nucleus Security does not support direct, in-platform capabilities for remediation actions, which may limit end-to-end orchestration for organizations seeking fully integrated workflows.

- **Missing collaboration features:** Unlike many competitors, Nucleus Security lacks an integrated chat function for internal collaboration or GenAI chatbot support, which limits real-time communication and user assistance within the platform.

Outpost24

Outpost24 is a Niche Player in this Magic Quadrant. Its Outpost24 Exposure Management Platform is available as both an on-premises and a SaaS solution.

Outpost24's operations are mostly focused in North America, Europe, the Middle East, and Africa, and its client base is predominantly midsize enterprises. Outpost24 has increased its presence in Asia/Pacific and Latin America, primarily through partner-led initiatives. Licensing is based on a modular, asset-based subscription model, with separate pricing for capabilities such as vulnerability assessment and penetration testing as a service (PTaaS). Threat intelligence and digital risk protection are offered through a credit-based consumption model, allowing customers to scale their usage based on changing needs.

Outpost24 promises a steady evolution of its EAP, with ongoing investments in areas such as digital asset discovery (including discovery of the AI attack surface), threat intelligence, and AI-driven remediation guidance. The company is exploring the use of AI to enhance identification and prioritization across its digital risk protection capabilities. Its strategy emphasizes deepening and consolidating core capabilities, alongside plans to expand third-party integrations over time.

Strengths

- **Extensive out-of-the-box compliance reporting:** Outpost24 offers a higher number of compliance reports out of the box compared with its direct competitors in this Magic Quadrant. It is a certified Approved Scanning Vendor (ASV) by the PCI Security Standards Council, which may appeal to organizations in regulated industries seeking rapid alignment with PCI and other regulatory frameworks.

- **Digital risk protection services (DRPS):** The platform includes native DRPS and threat intelligence capabilities, enabling organizations to monitor for external exposures and threat activity — such as leaked credentials and brand impersonation — without relying on third-party tools. This is an advantage for security teams seeking integrated external visibility.

- **Built-in PTaaS:** Outpost24 provides PTaaS functionality, enabling customers to ingest and visualize penetration test and red team results and report them within the platform. This supports offensive security validation workflows that are often siloed in other solutions.

Cautions

- **Low market visibility and fragmented messaging:** Fragmented messaging and limited articulation of a unified exposure management narrative may lead to confusion around Outpost24's value proposition, requiring security leaders to invest additional effort to understand how the platform aligns with their needs. This is compounded by relatively low market visibility, which may reduce initial consideration during vendor evaluations.

- **Lack of CPS security and integration support:** Outpost24 lacks native OT security capabilities and cannot integrate with third-party OT security platforms, limiting its suitability for organizations with industrial control systems or critical infrastructure environments.

- **Gaps in more advanced exposure management domains:** While the platform supports native ingestion of CSPM data via its Cloudsec Scanner, it does not offer native capabilities or third-party integrations for CNAPP, AEV, or ASCA. This may restrict its ability to support advanced exposure management use cases.

PlexTrac

PlexTrac is a Niche Player in this Magic Quadrant. The PlexTrac for CTEM solution is delivered as SaaS, with self-hosted and air-gapped/federal deployment options.

PlexTrac primarily serves small and midsize enterprises, as well as service providers in North America, with a growing presence in Europe, the Middle East, Africa, and Asia/Pacific. Its clients are typically internal vulnerability management teams, as well as security consultancies and MSSPs focused on penetration testing, red teaming, and compliance-driven assessments. Licensing is based on a user-based subscription model, with modular access to features such as workflow automation, webhooks, and AI risk scoring.

PlexTrac is enhancing its exposure assessment capabilities with automated remediation tracking and contextual risk scoring. Its workflow-driven design fosters collaboration between offensive and defensive teams, accelerating remediation and enabling actionable reporting. Ongoing investments include deeper integrations with scanners, threat intelligence, and ticketing systems to streamline vulnerability ingestion, agentic AI recommendations, alert correlation, and remediation workflows.

Strengths

- **Workflow-centric platform for offensive and defensive collaboration:** PlexTrac serves a reporting and collaboration hub for red, blue, and vulnerability management teams, streamlining assessments, penetration tests, and remediation tracking, and reducing operational cycles due to workflow centricity.

- **Customizable assessment engine for GRC and technical testing:** PlexTrac's Assessments Module supports major frameworks (NIST, CMMC, ISO, CIS) and customizable questionnaires with up to 1,000 questions. This makes PlexTrac well-suited for security consultancies and MSSPs conducting GRC assessments and technical testing.

- **Ease of use:** PlexTrac emphasizes usability through an intuitive UI and a self-guided platform tour. This increases adoption and time to value for security teams and service providers, especially those with limited resources or technical expertise.

Cautions

- **Narrow scope:** PlexTrac is not yet focused on full-spectrum exposure management; instead, it prioritizes reporting, collaboration, and assessment management. Organizations needing unified asset discovery, risk quantification, and remediation orchestration may find PlexTrac better as a complementary tool than a stand-alone EAP solution.

- **Limited native capabilities:** PlexTrac lacks built-in asset discovery and vulnerability scanning, depending entirely on third-party tools for data ingestion. This limits real-time exposure visibility and native risk scoring, requiring external data normalization. Agentic AI features are available, but only to customers with SaaS-hosted deployments.

- **Bidirectional integration ecosystem and workflow automation gaps:** The platform has limited bidirectional integrations with key technologies (e.g., EDR, CNAPP, CAASM, SOAR, threat intelligence). It also lacks robust remediation workflow automation, offering only two out-of-the-box integrations and no native playbook testing or sharing capabilities.

Qualys

Qualys is a Leader in this Magic Quadrant. Its Enterprise TruRisk Platform serves as the foundation of Risk Operations Center (ROC) and includes modules such as VMDR, CSAM, and Policy Audit. It is delivered as a SaaS solution with optional on-premises deployment for specific use cases.

Qualys operates globally, with a strong presence in North America, Europe, the Middle East, Africa, and Asia/Pacific, serving large enterprises and government organizations in regulated industries like finance, healthcare, and critical infrastructure. Recent growth in Europe, the Middle East, Africa, and Asia/Pacific is driven by localized data centers and regional sales teams. Licensing is offered through modular and flexible asset-based SaaS subscription models, allowing customers to purchase bundles or interchangeable units.

Qualys is expanding exposure assessment through enhanced third-party integrations, AI-driven remediation, and its QFlow workflow automation platform. Qualys aims to include deeper OT and cloud-native support, broader compliance reporting, and continued innovation in risk-based vulnerability management.

Strengths

- **Comprehensive compliance and policy coverage:** Qualys offers one of the most extensive out-of-the-box compliance reporting portfolios in this research, supporting global frameworks that include NIST, PCI DSS, HIPAA, and ISO 27001. Its Policy Audit module integrates with the TruRisk platform, aligning vulnerability management with regulatory and governance requirements.

- **Scalable cloud architecture with global reach:** The Qualys Cloud Platform is built on a microservices architecture that supports dynamic scalability and global deployment. With data centers in all of the above-mentioned regions, and a strong presence in direct and indirect sales channels, Qualys is well-positioned to serve multinational enterprises and government entities with diverse infrastructure needs.

- **Patching and remediation orchestration:** Qualys clients can unify asset discovery, vulnerability prioritization, and orchestrate remediation workflows through its TruRisk platform and QFlow workflow automation engine. The platform supports third-party integrations for flexible patching, ticketing, and mitigation across hybrid environments.

Cautions

- **Limited differentiation in attack path modeling:** Qualys’ attack path modeling has limited asset coverage, potentially narrowing its support for mature CTEM programs without third-party augmentation.

- **Low market awareness of flexible licensing options:** While Qualys now offers flexible licensing that provides access to all platform modules and allows customers to swap units between products, market awareness of these options remains limited. As a result, some customers may not fully leverage the available flexibility and benefits.
- **Limited third-party integration:** Qualys' bidirectional integrations with third-party tools, particularly in areas such as EASM and ASCA, are limited. This may hinder organizations seeking a more open, ecosystem-agnostic approach to exposure management.

Rapid7

Rapid7 is a Leader in this Magic Quadrant. Its Exposure Command Platform is delivered as a SaaS solution, supporting on-premises scanning and hybrid environments.

Rapid7's operations are geographically diversified, with a strong presence in North America, Europe, the Middle East, Africa, and Asia/Pacific. Its customer base includes large enterprises and midmarket organizations across both public and private sectors. Rapid7's recent growth is supported by partner-led campaigns, regional events, and co-marketing initiatives. Licensing is based on a tiered subscription model, with options for standard and advanced packages.

Rapid7 is investing in the evolution of its remediation hub, leveraging the Noetic Cyber acquisition to enable AI-driven automated workflows. The platform is expanding full-stack integration with enhanced AppSec, cloud security, native and virtual patch management, and advanced remediation orchestration.

Strengths

- **Comprehensive remediation capabilities:** Rapid7 offers out-of-the-box remediation workflow with numerous prebuilt integrations and playbooks. These workflows benefit from many automations to quickly assign, track, and automate remediation tasks across common IT and ticketing systems.
- **Broad attack surface coverage:** The platform supports on-premises and cloud-native environments, with integrations across EASM, CAASM, CNAPP, ASPM, and OT. This enables comprehensive visibility and prioritization across diverse enterprise environments.

- **Strategic acquisition:** Rapid7's July 2024 acquisition of Noetic Cyber has already enhanced the platform with integrated automated discovery, asset classification, and LLM-based remediation guidance.

Cautions

- **Limited validation integrations:** Rapid7's lack of integrations with third-party AEV tools limits remediation and mobilization decisions, compared with competitors that offer diverse integrated validation capabilities. However, Rapid7 does offer continuous red teaming via its Vector Command managed service and ad hoc penetration testing through its services team.
- **Lack of orchestration capabilities:** Rapid7 lacks built-in orchestration features, such as automated impact analysis or configuration simulation, forcing organizations to rely on manual validation of any changes before deploying them fully.
- **Legacy perception:** Rapid7 is widely recognized by customers as a traditional vulnerability management vendor. This perception may lead security leaders to overlook its broader exposure assessment capabilities, requiring additional effort to understand the platform's full value proposition and strategic evolution.

RedSeal

RedSeal is a Niche Player in this Magic Quadrant. Its RedSeal Platform is delivered both as an on-premises and a SaaS solution.

RedSeal's operations are mostly focused in North America, and its clients tend to be large enterprises in regulated sectors such as government and critical infrastructure. RedSeal also has customers across Europe, the Middle East, and Asia/Pacific, and began targeting Latin America in early 2025. Licensing is based on the size of infrastructure and cloud workload; assets are not individually charged. Compliance checking is included, except for DISA STIG and CIS, which are offered at an additional cost.

RedSeal is investing in expanding integration across EASM, ASPM, TIPs, CAASM, ASCA, and AEV, although many of these integrations are still in the early stages and not yet bidirectional or available out of the box. Additionally, RedSeal promises enhancements such as threat actor modeling, environmental context to determine attack probabilities, expanding visibility into identity-to-asset relationships, and SaaS exposure assessment.

Strengths

- **Attack path simulation for exposure validation:** RedSeal's platform maps an organization's network and assets, overlaying vulnerability data and security configurations. The vendor refers to this process as a "digital twin." It supports in-depth analysis of potential exposures and integrates with EDR and ITSM tools to accelerate remediation.

- **Proven track record in complex environments:** With over two decades of experience supporting large-scale, hybrid enterprise and government environments, specifically in network security, RedSeal brings deep operational maturity and credibility to exposure modeling and network security posture management.

- **Security certifications and roadmap alignment with federal needs:** While not FedRAMP certified, RedSeal's on-premises solution is Common Criteria certified, FIPS 140-3 compliant, and listed on the DoDIN APL — a combination that might appeal to the preferences of many federal customers. RedSeal's current capabilities demonstrate responsiveness to evolving enterprise and federal priorities, including zero trust, OT security, and cloud exposure modeling.

Cautions

- **Limited visibility among exposure management buyers:** RedSeal, primarily recognized for its network security offerings, has limited visibility in exposure assessment shortlists and low brand awareness among prospective buyers in this market, with the federal government being a notable exception.

- **Gaps in remediation workflow automation:** RedSeal has limited prebuilt remediation workflows and lacks a low-/no-code interface for building or sharing playbooks, which may limit automation and operational efficiency for remediation teams.

- **Limited compliance reporting out of the box:** The platform includes a small number of compliance reports out of the box, which is low compared with other competitor offerings in this market, and may require additional customization to meet regulatory reporting needs.

ServiceNow

ServiceNow is a Niche Player in this Magic Quadrant. Its EAP is delivered through the Vulnerability Response (VR) module as part of the Security Operations suite, which is available as a SaaS solution, with on-premises deployment options.

ServiceNow operates globally, with a strong presence in North America and established customer bases in Europe, the Middle East, Africa, and Asia/Pacific. Its VR module is primarily adopted by large enterprises, especially in highly regulated and security-conscious industries. ServiceNow has increased its market presence through active marketing and a strong partner ecosystem, including VR-specialized partners. Licensing uses a tiered subscription model (Standard, Professional, Enterprise) where pricing is based on the number of devices, with higher tiers offering broader integration and orchestration features.

ServiceNow continues to expand its exposure management capabilities through planned enhancements, including broader integration coverage across cloud, application, and mitigation technologies, as well as improvements to the user experience through embedded AI assistants and workflow automation.

Strengths

- **Platform familiarity:** ServiceNow's exposure assessment platform integrates with its ITSM and CMDB (separate products), facilitating adoption and integration for existing ServiceNow customers, reducing friction in deployment and operationalization.

- **Enhanced exposure response:** ServiceNow's VR module benefits from the platform's broad integration ecosystem, allowing organizations to customize exposure assessment workflows across security and IT domains using apps available in the ServiceNow Store.

- **Strategic acquisitions:** ServiceNow has integrated capabilities from acquisitions — such as Passage AI and Element AI — into its exposure management workflows. These additions support contextual workflow automation, remediation planning, and compliance tracking within exposure management processes.

Cautions

- **Lack of attack path analysis:** ServiceNow does not offer native attack path analysis capabilities, a feature that is increasingly standard in this market. While integration with AEV tools is possible, the absence of built-in attack path mapping may limit visibility for some organizations.

- **No native threat intelligence feed:** Unlike others in this market, ServiceNow does not provide native threat intelligence out of the box. Customers must provide and integrate their own threat intelligence sources, which may require additional integration and tuning effort and cost.

- **Security control prioritization requires an additional module:** ServiceNow's exposure prioritization based on security controls requires the separate Security Posture Control module, which is sold from the Vulnerability Response offering. This limits the prioritization depth for customers using only the core VR module.

Sevco Security

Sevco Security is a Visionary in this Magic Quadrant. The Sevco Exposure Assessment Platform is delivered as a SaaS solution, supporting hybrid environments through API-based integrations.

Sevco Security primarily operates in North America, with a small but growing Europe, Middle East, Africa, and Asia/Pacific presence through MSSP partnerships and targeted enterprise engagements. Its clients are midsize to large enterprises, service providers, and consultancies. Licensing is based on a tiered SaaS subscription model, priced according to asset volume and access to modules such as asset inventory, vulnerability correlation, and remediation tracking.

Sevco Security is investing in capabilities to enhance asset contextualization, prioritization, and autonomous remediation. Planned developments include native ASCA capabilities and integrations with AEV platforms to support broader exposure management use cases.

Strengths

- **Unified asset graph:** The Sevco platform leverages an asset graph that correlates and provides contextualization for devices, users, software, vulnerabilities, and security controls. This enables precise exposure mapping and prioritization, which is particularly valuable for organizations seeking to unify fragmented asset inventories across hybrid environments.

- **Remediation playbook library:** Sevco Security offers extensive automated remediation workflows with automated asset ownership assignments, ticketing integration, and structured exception handling to track false positives and exception requests — supported by accurate vulnerability validation.

- **Lightweight deployment with broad ecosystem compatibility:** Sevco Security's primary sources for data collection are third-party tool integrations, including EDR, CMDB, and vulnerability scanners, which makes it easy to plug the platform into existing infrastructure.

Cautions

- **Hybrid deployment options limit flexibility:** Sevco Security does not support on-premises deployment, other than some API integrations for tools that already exist within those hard-to-reach environments. This may present a barrier for organizations with strict data residency, sovereignty or air-gapped infrastructure requirements — particularly in government or critical infrastructure sectors.
- **Limited third-party bidirectional integrations:** The platform does not offer some of the bidirectional integrations that the leading vendors provide, such as CAASM, ASCA, AEV, and SOAR.
- **Low market visibility outside North America and regional imbalance:** Gartner does not see Sevco Security shortlisted for EAP in Europe, the Middle East, Africa, Asia/Pacific, or Latin America. The vendor offers limited sales and support presence in these regions.

Tanium

Tanium is a Niche Player in this Magic Quadrant. The Tanium Risk & Compliance solution is delivered both as an on-premises and SaaS solution, and it offers support for real-time endpoint monitoring.

Tanium's operations are geographically diversified, with the vendor primarily operating in North America and experiencing growing adoption across Europe, the Middle East, Africa, and Asia/Pacific, supported by its partner ecosystem and global channel strategy. Its clients tend to be large enterprises and government organizations. Licensing is based on an endpoint-based subscription model, with pricing tiers aligned to the scale of deployment.

Tanium is continuing to expand its capabilities in automating patching and remediation workflows and enhancing its integration with Microsoft and ServiceNow ecosystems. Tanium aims to expand visibility across attack surfaces, enhance compliance reporting, and improve prioritization.

Strengths

- **Endpoint and IT operations integration:** Tanium's exposure management capabilities are tightly integrated with its endpoint management, patching, software deployment, and device configuration. This integration enables improved visibility, patch orchestration, and compliance assessments across large enterprise environments.

- **Automated remediation:** Tanium offers automation playbooks that implement prioritized recommendations, informed by industry benchmarks such as CIS. It offers phased rollouts of remediation and patches to better control the potential impacts on the infrastructure.

- **Operational dashboards:** Tanium provides real-time visibility into autonomous activities, supporting teams who want to monitor, diagnose, plan, and remediate issues. Its role-based access control (RBAC) features allow teams to tailor levels of automation, balancing autonomous response with human oversight as needed.

Cautions

- **Limited third-party integration ecosystem:** Tanium's EAP is primarily designed to operate within its own ecosystem, with bidirectional integrations focused on asset inventory. While out-of-the-box integrations exist for select platforms, coverage across adjacent security domains — including EDR, ASPM, EASM, CAASM, OT, CNAPPs, and TIPs — remains limited, which may hinder interoperability in heterogeneous environments.

- **Narrow exposure validation capabilities:** The Tanium platform maintains a focus on posture and compliance, with only foundational support for threat-intelligence-driven exposure management. Capabilities such as AEV and attack path analysis are limited, particularly beyond endpoint lateral movement.

- **Modest visibility among exposure management buyers:** Tanium, primarily recognized for its endpoint and IT operations solutions, is still developing differentiation in the exposure assessment market. Its messaging and capabilities largely appeal to its existing customer base, resulting in modest visibility and competitiveness in dedicated exposure assessment platform evaluations among prospective buyers.

Tenable

Tenable is a Leader in this Magic Quadrant. Its Tenable One Platform is available both as an on-premises and as a SaaS solution.

Tenable's operations are geographically diversified, with a good overall presence across North America, Europe, the Middle East, Africa, Asia/Pacific, and Latin America. Its clients tend to be large enterprises across all industries, such as finance, healthcare, and government. Over the past year, Tenable has increased its presence in Europe, the Middle East, Africa, and Asia/Pacific, supported by a robust partner ecosystem and global channel strategy. Licensing is based on a subscription model, with pricing aligned to asset coverage and platform capabilities.

Tenable continues to invest in expanding its exposure assessment capabilities through strategic acquisitions (e.g., Vulcan Cyber and Eureka Security). The company is also enhancing its platform with improved prioritization, automated remediation, and broader attack surface coverage, including cloud, OT, and SaaS environments.

Strengths

- **Broad attack surface coverage:** Tenable One is a well-integrated platform that spans traditional IT, identity, cloud, OT, and container environments. Its native capabilities include asset visibility, vulnerability prioritization, asset and identity relationship mapping, and contextual risk scoring across a wide range of attack surfaces.
- **Strong market presence:** Tenable's early adoption of exposure management concepts, combined with its robust partner ecosystem and channel-first sales model, has contributed to it being a dominant player in the exposure assessment space. Its global reach and consistent customer acquisition across enterprise segments reflect a mature go-to-market strategy and operational scalability.
- **Integrated threat intelligence and exposure analytics:** Tenable uses multiple threat intelligence sources to assess exploit likelihood and prioritize vulnerabilities with real-world impact. This capability, combined with native support for CVSS v4.0, EPSS, asset criticality, business impact, attack path analysis, and control posture, enhances Tenable's ability to surface emerging exposures early.

Cautions

- **Limited customization:** Tenable users cannot currently modify or create custom models for prioritization. This may limit flexibility for organizations seeking to tailor risk models to their unique operational or compliance needs.
- **Gaps in remediation playbooks:** The Tenable One Platform offers limited native remediation playbooks and lacks the ability to simulate the impact of configuration changes or test remediation workflows. This may hinder a user's ability to make quick decisions on remediations.
- **On-premises deployment complexity:** Tenable's on-premises capabilities are more limited than its SaaS offering, and some integrations — particularly for remediation and

automation — require professional services or custom development, increasing time to value for complex environments.

Trend Micro

Trend Micro is a Niche Player in this Magic Quadrant. Its Vision One Cyber Risk Exposure Management (CREM) Platform — previously Attack Surface Risk Management — is delivered as a SaaS solution, with an available on-premises version.

Trend Micro primarily services midsize to large enterprises globally, often existing customers, but has increased its presence in major global regions over the past 12 months, primarily through indirect channel partners and supported by marketing initiatives. Licensing is based on a tiered, per-device or per-cloud-account subscription model depending on the bundle offering: Core, Essentials, or Cloud Risk Management.

Trend Micro has invested in GenAI-powered features for enhanced risk prioritization and remediation, including tools to highlight top risks, analyze exploitable attack paths, and streamline mitigation planning. Development priorities include simulation-based risk modeling to validate remediations before deployment, as well as enhancements to executive-level visibility and third-party integration breadth.

Strengths

- **Cohesive native ecosystem integration:** Deep integration across Trend Micro's security portfolio provides unified telemetry, coordinated control deployment (e.g., intrusion prevention system [IPS] rules), and consistent risk scoring across layers. This reduces integration overhead and improves detection-to-response efficiency for existing customers.

- **Cloud-native scalability with unified management:** Trend Micro supports cloud-native, hybrid, and on-premises deployments — including sovereign and private cloud use — with centralized management and automated updates. This reduces operational overhead for organizations with diverse infrastructure.

- **Channel-led global reach:** Trend Micro's nearly 100% channel-led go-to-market model ensures broad global reach and scalability through a vast partner network. This supports consistent customer acquisition while allowing an internal focus on innovation and partner enablement.

Cautions

- **Standardization of risk scoring models:** Trend Micro's EAP does not allow users to modify or create custom risk-scoring algorithms or substitute third-party scoring engines. While this design supports consistency, benchmark integrity, and auditability, it may limit flexibility for organizations with advanced risk modeling requirements or preferences for tailored scoring approaches.
- **Limited bidirectional integrations with third-party platforms:** Trend Micro lacks bidirectional integrations with several key third-party systems, including CMDB, ASPM, EASM, CAASM, OT, CNAPPs, ASCA, and AEV platforms. This limits asset context enrichment, exposure validation across diverse environments, and automated remediation workflows with external telemetry, potentially impacting data quality and operational efficiency.
- **Lower availability of regionalized interface options:** The CREM Platform's user interface is only available in English and Japanese, even though it has a presence across all major regions and support in 60+ countries. This limited language support may hinder adoption or usability in multilingual organizations seeking localized experiences.

Vicarius

Vicarius is a Niche Player in this Magic Quadrant. Its vRx platform is delivered as a SaaS solution, supporting agent-based deployment and optional integrations for hybrid environments.

Vicarius' operations are geographically diversified, and its clients tend to be midsize to large organizations across sectors such as retail, healthcare, and manufacturing. Over the past 12 to 18 months, Vicarius has increased its presence in North America and Europe, supported by strategic partnerships and a growing channel ecosystem. Licensing is based on a per-asset model, with flexible packaging that includes patch management, prioritization, and remediation orchestration capabilities.

Vicarius is investing in automated security control assessment and GenAI-driven remediation guidance, including its proprietary "VulnGPT" engine and zero-day binary analysis tool for patchless protection. The company is also expanding its integrations with EDR, ITSM, and SOAR platforms to streamline policy-driven workflows and reduce time to remediation.

Strengths

- **Code-level security control assessment via binary analysis:** Vicarius differentiates itself with a proprietary zero-day binary analysis engine that detects control violations at the code level. This enables early identification of vulnerabilities and supports “patchless protection” workflows, offering a unique approach to mitigating risk in environments where traditional patching is not feasible.

- **GenAI-powered remediation guidance with VulnGPT:** The vRx platform integrates VulnGPT, a GenAI engine trained on Vicarius’ proprietary “fix” database. This provides tailored remediation recommendations based on runtime telemetry, asset context, and threat intelligence — enhancing decision making and accelerating response.

- **Flexible deployment and integration model:** vRx is cloud-agnostic and supports both SaaS and self-hosted deployments, with lightweight sensors and API-based integrations across EDR, ITSM, and SOAR platforms. This flexibility allows Vicarius to serve a wide range of customer environments, from cloud-native startups to compliance-driven enterprises.

Cautions

- **Limited native language support:** The platform currently supports only one native language (English), which may limit usability for global organizations requiring multilingual interfaces or localized workflows.

- **Early-stage ecosystem and marketplace maturity:** Compared with more established vendors in this research, Vicarius offers a smaller library of prebuilt integrations and automation playbooks. This may require additional customization effort for organizations seeking rapid time to value through orchestration.

- **Customization requires vendor collaboration:** While vRx supports prioritization customization, it often requires collaboration with Vicarius’ customer success team. This may limit self-service flexibility for organizations that prefer to independently tailor risk models and scoring logic.

WithSecure

WithSecure is a Visionary in this Magic Quadrant. Its Elements Exposure Management (XM) solution is a component of its broader Elements Cloud security platform and is delivered as a SaaS solution, with options for on-premises scanning (endpoint protection agents and network scanners).

WithSecure's operations are primarily focused in Europe, particularly in the Nordic market, and its clients tend to be midsize to large enterprises, especially in regulated sectors such as government, healthcare, and finance. Over the past 12 months, WithSecure has increased its presence in Europe and Asia/Pacific, supported by its participation in the AWS European Sovereign Cloud initiative and regional compliance campaigns, such as the Network and Information Security Directive (NIS 2). Licensing is based on a subscription model, available in both monthly and annual terms. Pricing tiers are aligned to user count and deployment scale, and include maintenance, basic support, and training resources.

WithSecure is expanding its GenAI capabilities to deliver advanced, context-driven remediation guidance and locally tailored recommendations, while broadening integrations and compliance frameworks.

Strengths

- **Integrated assessment and validation capabilities:** WithSecure's Elements XM platform combines native AEV through heuristic exposure hunting with integrated ASCA. It also includes CAASM functionality to enrich asset context and visibility. These capabilities collectively support continuous exposure discovery, prioritization, validation, and response across hybrid environments.

- **Strong European compliance and localization:** WithSecure is a launch partner for AWS European Sovereign Cloud, complies with GDPR, and offers multilingual support, making it well-suited for the European public sector and regulated industries.

- **AI-driven remediation guidance:** The platform leverages the built-in Luminen GenAI assistant to provide persona- and region-specific remediation guidance in 11 languages, enhancing usability and operational efficiency for global teams.

Cautions

- **Limited customization and external enrichment:** WithSecure's risk-scoring engine leverages proprietary threat intelligence and algorithms optimized for midsize, resource-constrained organizations. While effective out of the box, this model restricts customers from customizing prioritization logic, incorporating organization-specific risk factors, or integrating third-party threat intelligence. As a result, the platform may lack the flexibility required by organizations with advanced or highly tailored risk management needs.

- **European-centric focus and partner ecosystem:** WithSecure's strong alignment with European standards and a partner network primarily concentrated in Europe may limit its ability to support non-European regulatory frameworks, certifications, and localized expertise. This regional focus could reduce its appeal for organizations with global operations or U.S.-centric compliance requirements.

- **Limited prebuilt integrations and automation:** WithSecure's platform offers a narrow range of prebuilt integrations for remediation and response, and its automation capabilities are restricted to predefined options. The lack of deep integration and full workflow customization may require organizations to invest in custom development via its API-first model to achieve broader interoperability and automation.

XM Cyber

XM Cyber is a Challenger in this Magic Quadrant. Its Continuous Exposure Management Platform is delivered as a combination of on-premises sensors, cloud APIs, network scanners, and a SaaS management console.

XM Cyber operates globally; however, most of its clients are located in Europe, the Middle East, and Africa (EMEA), and are most commonly large enterprises. Smaller clients are most commonly delivered through value-added reseller partners, rather than being delivered directly. XM Cyber is expanding in North America through routes including partnerships with Accenture, ServiceNow, and Google, and in Asia/Pacific and Japan through a partnership with SoftBank. Licensing is based on environment size, with on-premises deployments priced by number of servers and workstations, and cloud deployments priced by number of workloads and Kubernetes clusters.

Recent acquisitions in ASCA (Cyber Observer) and CDR (Confluera) have expanded XM Cyber's platform capabilities. Future investments include enhancements to prioritization, contextualization and scanning techniques, and ingestion of third-party threat intelligence sources.

Strengths

- **Customer enablement through maturity model and value estimation tools:** XM Cyber provides resources such as a structured maturity model and a value estimation tool to help organizations transition from traditional vulnerability management to exposure management. These tools support a contextual understanding of exposures and help estimate potential risk reduction, aiding investment justification and executive alignment.

- **Exposure management service:** XM Cyber offers a managed Exposure Management Service (EMS), delivered directly or through partners, providing remediation expertise and operational support for organizations that may have limited internal resources or specialized exposure management capabilities.

- **Operational maturity and enterprise fit:** The platform is designed to support large, complex environments and can be deployed on-premises, in the cloud, or in sovereign cloud environments such as STACKIT. This deployment flexibility helps meet the operational and compliance needs of global enterprises, particularly in regulated sectors — such as those required to comply with standards like ISO, NIST, and CIS.

Cautions

- **Limited visibility but developing traction in North America:** XM Cyber has a strong presence in EMEA, and while its customer base and visibility in North America are growing — supported by strategic partnerships, increased investment, and a tailored regional roadmap — this geographic imbalance may still affect its competitive positioning and perception among North American enterprises.

- **Customization constraints in prioritization logic:** XM Cyber does not allow users to modify or create custom algorithms for prioritization. While users can refine scenarios and manage exclusions to tailor risk scoring to their environment, the lack of algorithm-level customization may limit flexibility for organizations seeking deeper control over prioritization logic.

- **Gaps in CPS integration and coverage:** XM Cyber can identify exposures in OT, IoT, and legacy environments without sensors, but lacks direct, bidirectional integrations with OT security technologies. It does not explicitly address industrial control systems and has indicated plans to integrate with vendors such as Claroty and Nozomi, which limits its current applicability in OT-heavy environments.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

As this is a new Magic Quadrant, no vendors were added.

Dropped

As this is a new Magic Quadrant, no vendors were dropped.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, each vendor must:

- Demonstrate global presence and features/scale relevant to enterprise-class organizations:
  - The exposure assessment platform (EAP) offering must have generated at least $20 million in annual revenue, combined with a customer count growth rate of at least 50% during the 12 calendar months prior to its receipt of Gartner’s Magic Quadrant welcome packet (21 April 2025).

Or:

- The EAP offering must have at least 200 paying, production (non-beta test) customers in at least two or more geographic regions (Asia/Pacific, Europe, the Middle East and Africa, Latin America or North America).
- Demonstrate minimum signs of a global presence; evidence of having at least 25 production customers outside its home region (the Americas, Europe, the Middle East and Africa, or the Asia/Pacific region).
- Provide 24/7 global technical support available on multiple continents.
- Be actively participating in the market via selling/marketing to enterprise customers.
- Be actively developing new features and capabilities around the management and reduction of vulnerabilities and other exposures.

In addition, each vendor must feature in the Customer Interest Indicator (CII) defined by Gartner for this Magic Quadrant. Data inputs used to calculate the CII for EAP include a balanced set of measures:

- Gartner end-user inquiry volume per vendor
- **Gartner.com** search data
- Gartner Peer Insights competitor mentions
- Google trends data
- Web traffic analysis

In terms of features, each vendor must:

- Provide dedicated EAP capabilities that were generally available (GA) as of 1 January 2024. GA means the product or service is widely available to all customers for purchase through normal sales channels.
- Deliver asset and attack surface discovery capabilities natively to uncover a wide range of assets, including, at minimum, IT servers and workstations (hardware, software, physical, virtual), OT/IoT, applications (e.g., applications based on their fully qualified domain name [FQDN] or collection of FQDNs that make up an application), identity, internet-facing systems, and cloud workloads.

And/or:

- Have direct integration with, or API access to, other security appliances for dynamic discovery of assets and their riskiest exposures (e.g., EDR, EASM, CNAPP, VA, and DRPS).
- Enumerate a range of the prioritized exposures, including vulnerabilities and misconfigurations.
- Normalize the asset inventory relevant to attack surface management by deduplicating and aggregating raw data from various disparate data sources.
- Prioritize vulnerabilities, misconfigurations, security control gaps, and other exposures based on severity (e.g., vendor score and CVSS), exploitability (e.g., vulnerability intelligence/EPSS), and potential impact (e.g., asset context and business impact).

- Have the ability to leverage threat intelligence to provide context and reprioritize findings.

- Have the ability to ingest security control context to enhance prioritization around asset accessibility and/or feasibility of attack.

- Provide a role-based and centralized management console for administration and reporting, including the status of the identified exposures categorized by severity, impacted assets, remediation status, and business unit, approved exceptions, and trends.

- Provide secure APIs to enable full access to exposure data, platform capabilities, and integrations with third parties.

- Provide action plans on the mitigation of prioritized threats, as well as the remediation workflow or integration with ticketing systems, incident response tools, and TDIR-capable solutions, such as SIEM solutions.

- Have out-of-the-box reporting options for compliance, control frameworks, defined security policies, and benchmark assessments aligned to both industry and organizational requirements, and multiple roles such as technical resolvers and C-level executives.

Excluded from consideration were:

- Exposure assessment and prioritization capabilities solely focused only on specialized environments, such as cyber physical systems (CPS) [e.g., Internet of Things (IoT) and operational technology (OT) devices], applications and cloud.

- Solutions where discovery (via native or integration) capabilities are limited to less than three types of attack surfaces (internal, external, cloud, end user, and digital).

- Vendors that were not the original manufacturer of the EAP product. This includes software original equipment manufacturers (OEMs), resellers that repackage products that would qualify from their original provider, carriers, internet, and other service providers that offer managed services, such as managed security services providers (MSSPs) or managed detection and response (MDR) providers.

Honorable Mentions

There are many vendors in the exposure assessment platform (EAP) market. Of these, over 50 were surveyed. Twenty met the inclusion criteria and were selected for evaluation in this Magic Quadrant. However, the exclusion of a provider does not mean that the vendor lacks viability. The following are noteworthy vendors that either did not meet all inclusion criteria or were not selected to be surveyed. These vendors could be appropriate for clients, contingent on requirements:

- **Axonius:** Axonius applies asset-centric analysis to identify coverage gaps and misconfigurations that contribute to exposure risk. Its normalization of asset data and integration breadth may appeal to organizations seeking to improve exposure visibility and hygiene through existing CAASM workflows. Axonius expanded its offering, adding dedicated EAP capabilities in April of this year, after this Magic Quadrant's research kicked off, and thus was not selected to be surveyed as part of this Magic Quadrant process.

- **Hive Pro:** Hive Pro's Uni5 Xposure platform combines third-party — as well as first-party — asset, code, infrastructure, and cloud scanning data with threat intelligence and adversarial validation to prioritize exposures based on real-world risk. It may suit organizations seeking to align remediation efforts across teams by integrating detection, validation, and response into a single workflow. Hive Pro did not meet the minimum criteria for market presence or scale for inclusion in this Magic Quadrant.

- **Reveald:** Reveald uses simulation-based analysis to model attack paths and identify exploitable exposures by creating a digital representation of the environment. This approach may appeal to organizations seeking to reduce remediation scope by focusing on exposures that enable real-world attacker movement across hybrid infrastructure. Reveald did not meet the minimum criteria for market presence or scale for inclusion in this Magic Quadrant.

- **Zafran:** Zafran focuses on reducing risk by identifying and remediating the small subset of vulnerabilities that are exploitable within an organization's specific environment, factoring in the configuration of existing tools and risk context, such as internet exposure, runtime presence, and active threats. Zafran further helps take action by deploying control-based mitigations and auto-assigning remediation tickets to the right owners. This approach may suit organizations aiming to optimize remediation efforts and security investments by narrowing focus to high-impact exposures. Zafran did not meet the minimum criteria for market presence or scale for inclusion in this Magic Quadrant.

- **Zscaler:** Zscaler Unified Vulnerability Management (UVM) correlates vulnerability data with threat intelligence, identity, asset context, user behavior, and business processes across cloud and on-premises environments to support risk-based prioritization. Its data normalization and correlation, customizable scoring, and workflow automation may appeal to organizations — particularly existing Zscaler clients — seeking to align remediation with operational priorities while leveraging existing security investments through broad tool integrations. Zscaler did not meet the minimum criteria for market presence or scale for inclusion in this Magic Quadrant.

Evaluation Criteria

Ability to Execute

Product/Service: This criterion evaluates a vendor's ability to provide product functions in core EAP areas, such as the ability to continuously discover organizational assets, identify multiple attack surfaces, perform enumeration prioritization, support treatment workflow integrations, and generate reports to support business, compliance, and audit needs.

Overall Viability: This criterion includes an assessment of a vendor's financial health, the financial and practical success of its overall company, the likelihood that it will continue to invest in EAP technology, as well as the EAP's contribution to revenue growth.

Sales Execution/Pricing: This criterion evaluates a vendor's success in the EAP market and its capabilities in presales activities. Considerations include the size and growth of its EAP revenue and installed base, flexibility of pricing models, its presales support, and the distribution and inclusivity of its sales channel. The level of interest and reviewed experiences from Gartner clients is also considered.

Market Responsiveness/Record: This criterion evaluates the delivered features and alignment to client demand for adjacent EAP capabilities, as well as the track record of delivering new and differentiated functions in line with the changing needs of the market. Considerations include support for multiple attack surfaces: internal, external, cloud, end user, and digital.

Marketing Execution: This criterion evaluates a vendor's EAP market messaging in light of Gartner's understanding of customers' needs. Promotion of the brand, increasing awareness of products, and influence on the EAP market are evaluated, in addition to Gartner client level of interest.

Customer Experience: This criterion evaluates product and service experience in production environments. Included are ease of deployment, operation, administration, stability, scalability, and vendor support capabilities. This criterion is assessed on the basis of analysis of feedback received via Gartner's client inquiry service, reviews on Gartner's Peer Insights forum, and other interactions with Gartner clients that are using, or have completed competitive evaluations of, a vendor's EAP offering.

Operations: This criterion evaluates a vendor's resources for developing the EAP product (research and development), tenure, and stability of its product leadership teams, and its overall organizational structure.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	High
Operations	Medium

Source: Gartner (November 2025)

Completeness of Vision

Market Understanding: This criterion evaluates a vendor’s ability to understand buyers’ emerging needs, their market competitors, and how to communicate solutions effectively. EAP vendors that show the highest degree of market understanding can identify how technology and change in ways of working will translate into modern security operations requirements, while also meeting the business risk and ROI reporting needs of organizations.

Marketing Strategy: This criterion evaluates a vendor’s ability to communicate the value and competitive differentiation of its EAP offering.

Sales Strategy: This criterion evaluates whether a vendor has a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. Also taken into consideration are partners that extend the scope and depth of market reach, expertise, technologies, services, and their customer base.

Offering (Product) Strategy: This criterion evaluates a vendor’s approach to product development and delivery, with an emphasis on how well functionalities and features correspond to current requirements. Development plans during the next 12 months are also evaluated.

Vertical/Industry Strategy: This criterion evaluates a vendor’s performance in specific industries and strategy to support EAP requirements specific to industries and their unique attack surfaces/exposures.

Innovation: This criterion evaluates a vendor’s development and delivery of EAP technology that is differentiated from that of its competitors. We consider product capabilities and customer use in areas such as attack surface management, enhanced prioritization, including security control enrichment, and expanded uses of generative AI, including but not limited to diagnostics, remediation recommendations, and reporting.

Geographic Strategy: Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of their sales and support strategies for those regions, as well as product features to support local and regional compliance requirements (e.g., product localization and points of presence in different geographies).

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (November 2025)

Quadrant Descriptions

Leaders

Leaders in the EAP market are vendors demonstrating strong momentum in both sales and market visibility. They consistently deliver tightly integrated solutions with advanced capabilities for identifying, quantifying, and prioritizing threat exposures. Their product strategies align with the evolving demand for intuitive, high-impact features that support threat exposure management initiatives. These vendors also invest in long-term innovation, ensuring their platforms remain relevant as organizational security needs mature. Leaders typically have strong sales and distribution networks, a diversified presence across industries and regions, and a clear vision for how EAPs fit into broader security operations and exposure management strategies.

Challengers

Challengers in the EAP market often provide solutions that are more narrowly focused or less fully integrated, which may not yet encompass the advanced capabilities or evolving practices seen in more mature exposure management approaches. While they may not lead in product innovation, they often maintain strong market presence through established sales channels, partnerships, or brand recognition. Challengers tend to appeal to organizations with existing relationships or those prioritizing vendor familiarity over feature depth or platform maturity.

Visionaries

Visionaries in the EAP market are recognized for their technical innovation or unique product approaches, but may lack the execution track record, market visibility, or organizational scale of more established vendors. While their platforms often introduce forward-looking capabilities, they may have limited sales channels or strategic partnerships. Visionaries can be a good fit for organizations seeking innovative features, but buyers should carefully assess long-term viability and be mindful of potential business disruption, especially if the vendor becomes an acquisition target.

Niche Players

Niche Players in the EAP market typically offer capable solutions focused on specific use cases, industries, or regions. While they may excel in certain technical areas, they often lack the broader market presence, resource scale, or strategic vision seen in other categories. Niche Players can be a strong fit for organizations whose needs align closely with the vendor's focus, but may be less suitable for buyers seeking comprehensive or widely supported platforms.

Context

EAPs continuously identify and prioritize exposures — such as vulnerabilities, misconfigurations, and security controls gaps — by mapping them to potential attack paths within a business risk context. EAPs integrate with discovery tools and asset inventories to centralize visibility, and they facilitate remediation through integrations with ticketing and patching systems. These platforms are delivered as software-based solutions, often with support for hybrid environments, including on-premises, cloud, and containerized assets.

Data from Gartner client inquiries and market observations indicate that EAP adoption is most common among large enterprises with mature security operations and a strategic focus on CTEM. However, vendors are increasingly targeting midsize organizations by offering more accessible, integrated, and automated solutions that reduce operational overhead and improve exposure visibility.

Gartner expects the EAP market to grow steadily over the next few years, driven by the increasing complexity of cloud environments and the accelerating use of AI, which are amplifying the scale and impact of exposures — potentially at an exponential rate. As organizations face an expanding and increasingly complex attack surface, EAPs will play a critical role in unifying exposure management and other security operations practices. By contextualizing exposures with asset criticality, threat intelligence, security control context, and business impact, EAPs enable organizations to prioritize remediation efforts more effectively and reduce the likelihood of breach.

Market Overview

Exposure assessment platforms (EAPs) are a foundational capability for organizations seeking to continuously discover, analyze, and prioritize exposures across their entire attack surface. As the EAP market remains nascent and continues to evolve through the convergence of multiple adjacent capabilities, Gartner observes that foundational features, such as native scanning, remain highly valued. This is reflected in the positioning of historically strong vulnerability assessment vendors in this year’s Magic Quadrant. However, the pace of innovation is accelerating, and Gartner expects today’s Leaders to be increasingly challenged by competitors offering differentiated approaches to exposure discovery, prioritization, and operationalization.

EAPs are designed to unify visibility across internal, external, cloud, and end-user environments, and are increasingly integrated into broader CTEM programs.

Although still forming, the global EAP market is showing early signs of momentum, fueled by the rising volume and complexity of exposures, the convergence of vulnerability and attack surface management, and growing demand for contextualized, risk-based prioritization. While machine learning has long supported prioritization models — such as EPSS and vendor-specific scoring — recent enhancements reflect incremental improvements rather than transformative innovation. Latest AI technique advancements, including generative and agentic approaches, are beginning to emerge in downstream phases such as remediation, where they support tasks such as guided response planning and automated playbook generation. Vendors that differentiate themselves tend to have a native emphasis on exposure assessment and offer well-developed integration capabilities that support broader security workflows, helping teams more effectively prioritize, assign, and remediate exposures within their existing operational context.

At its core, an EAP enables an organization to identify and prioritize exposures — such as vulnerabilities, misconfigurations, and unmanaged assets — based on exploitability, existing security controls, asset criticality, and business impact. Furthermore, vendors are rapidly expanding capabilities to include attack path analysis, integration with AEV, and support for digital supply chain and external threat surface discovery.

Some EAP vendors emphasize deep contextual analysis and flexible integrations, appealing to mature security teams that require granular control over prioritization logic and remediation workflows. These solutions often support advanced use cases such as threat-informed defense, asset ownership mapping, and life cycle tracking of exposures. However, this flexibility can come at the cost of ease of deployment and operational simplicity.

Other vendors focus on delivering streamlined, outcome-driven platforms that emphasize automation, intuitive dashboards, and rapid time to value. These solutions are particularly attractive to organizations with lean security teams or those early in their CTEM maturity journey, offering centralized visibility and simplified remediation workflows.

Recent Trends in the EAP Market

Gartner observes several key trends shaping the evolution of the EAP market:

- **Expanded discovery scope:** Vendors are extending discovery capabilities to include unmanaged assets, digital supply chain components, and external-facing infrastructure, either natively or through integrations with third-party CAASM and EASM tools.

- **Contextual prioritization:** EAPs are increasingly incorporating threat intelligence, asset ownership, and compensating control data to refine prioritization beyond CVSS scores.

- **Attack path and adversarial testing integration:** Some platforms now offer native or integrated attack path analysis and ingest outputs from AEV tools to validate exposure risk.

- **Exposure life cycle coverage:** Exposure life cycle tracking — including ownership assignment, remediation status, and SLA monitoring — is becoming a standard feature.

- **Cloud-delivered architectures:** Many vendors are delivering EAPs as cloud-native platforms, enabling scalability and integration with modern DevSecOps pipelines and hybrid environments.

- **Operational and SOC enrichment:** EAPs are increasingly integrated with ITSM, SOAR, and SIEM platforms to support automated remediation and incident response workflows.

Vendor Differentiation

Gartner identifies three broad categories of vendors operating in the EAP market:

- Exposure aggregators that build their platforms around comprehensive exposure data aggregation, advanced analytics, and business context, offering strong integration and automation capabilities.

- Vulnerability assessment vendors that are evolving their products to include exposure assessment features, sometimes repurposing legacy technologies to address the growing demand for risk-based prioritization and unified visibility.

- Large security providers that deliver EAP functionalities as part of their product suite/portfolio, often leveraging existing data sources and workflows to provide exposure management alongside other security operations tools.

The EAP market emerged from vulnerability assessment and adjacent capabilities such as vulnerability prioritization technology (VPT), external attack surface management (EASM), cyber asset attack surface management (CAASM), and breach and attack simulation (now combined with automated pentesting as adversarial exposure validation [AEV]). These capabilities have since converged or complemented each other to form the EAP market. The EAP Magic Quadrant reflects this evolution and evaluates vendors against criteria aligned with real-world exposure management needs.

Acronym Key and Glossary Terms

AEV	adversarial exposure validation

ASCA	automated security control assessment
ASPM	application security posture management
CAASM	cyber asset attack surface management
CDR	cloud detection and response
CIS	Center for Internet Security
CMDB	configuration management database
CMMC	Cybersecurity Maturity Model Certification
CNAPP	cloud-native application protection platform
CPS	cyber-physical systems
CTEM	continuous threat exposure management
CVSS	Common Vulnerability Scoring System
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide
DoD	Department of Defense
DoDIN APL	Department of Defense Information Network Approved Products List
DRPS	digital risk protection services
EAP	exposure assessment platform

EASM	external attack surface management
EDR	endpoint detection and response
EPSS	Exploit Prediction Scoring System
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
GRC	governance, risk, and compliance
HIPAA	Health Insurance Portability and Accountability Act
IoC	indicator of compromise
IoMT	Internet of Medical Things
IoT	Internet of Things
IPS	intrusion prevention system
ISO	International Organization for Standardization
ITSM	IT service management
LLM	large language model
M&A	mergers and acquisitions

MSSP	managed security service provider
NIST SP	National Institute of Standards and Technology Special Publication
OT	operational technology
PCI DSS	Payment Card Industry Data Security Standard
PTaaS	penetration testing as a service
RBAC	role-based access control
SIEM	security information and event management
SLA	service-level agreement
SOAR	security orchestration, automation and response
TDIR	threat detection, investigation, and response
TIP	threat intelligence platform
VA	vulnerability assessment

⊕ Evaluation Criteria Definitions

information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.