OMDIA UNIVERSE

Publication date:
16 Dec 2024

Author(s):
Andrew Braunberg, Principal Analyst
Eric Parizo, Managing Principal Analyst

Omdia Universe: Next-Generation SIEM Solutions (NG-SIEM), 2024–25

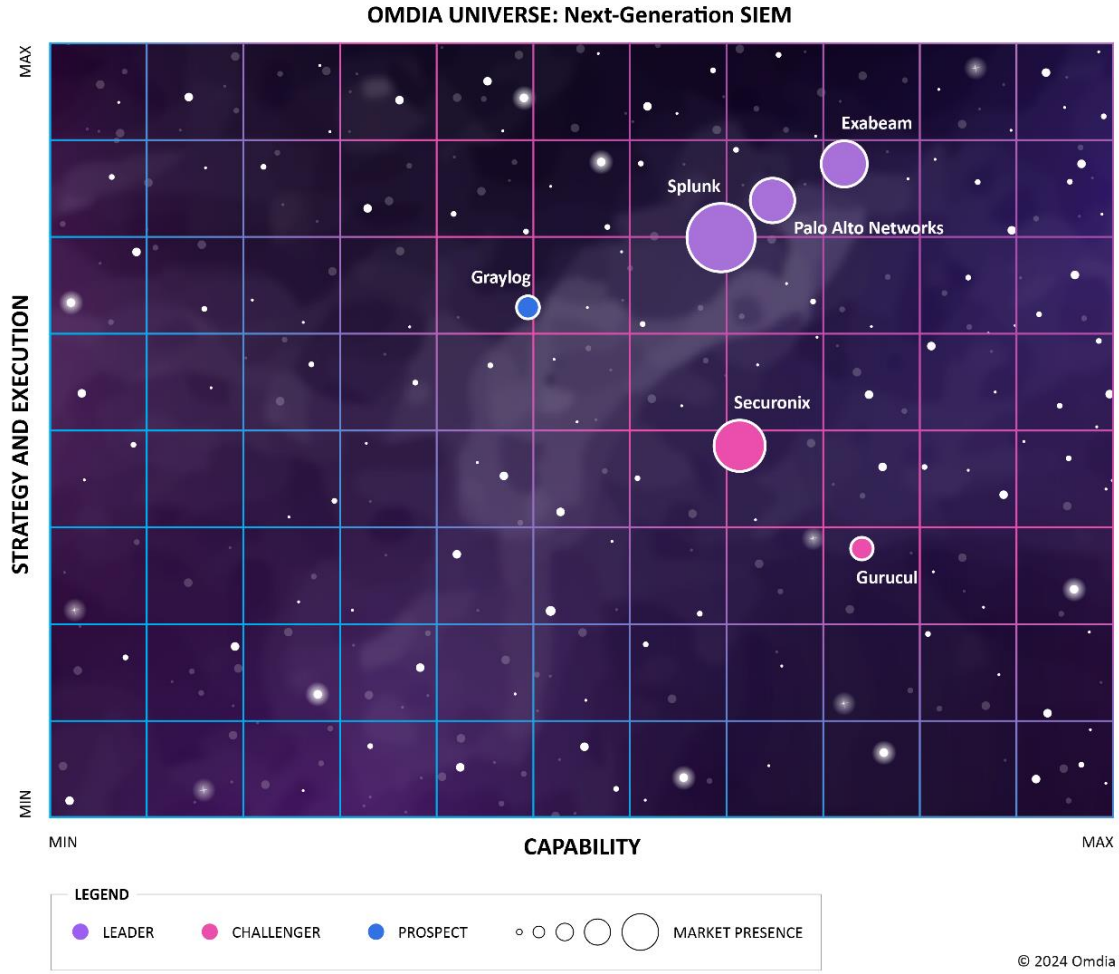
OMDIA

Summary

Catalyst

It has been 20 years since the emergence of security information and event management solutions, or SIEMs. These products have long served as the architectural centerpiece of enterprise security operations centers (SOCs), the primary tool for security analysts performing threat detection, investigation, and response (TDIR) operations. Despite widespread use, SIEMs have often been unable to fully deliver on expectations, a recurring theme since their introduction.

Figure 1: The Omdia Universe for NG-SIEM



Source: Omdia

Leading SIEM vendors have been in the process of deploying or migrating to a new generation of solutions for several years. Built for the cloud, these next-generation SIEMs (NG-SIEMs) can take in more types of data, apply built-in analytics, and manage the end-to-end process from detection to investigation and, finally, response. Furthermore, in the nearly three years since the first iteration of this report, significant

advancements have been made in other increasingly important areas, such as data engineering, artificial intelligence (AI), and automation.

This report profiles and ranks six NG-SIEM solutions, exploring the factors driving today's competitive landscape and providing insight for buyers as they look to successfully navigate the product evaluation, purchasing, and deployment lifecycle.

Omdia view

Boiled down to its essence, the job of the SIEM is straightforward: gather security telemetry data (primarily streams of logging data) from a variety of internal and, often, external sources; identify and highlight the cybersecurity threats that matter; and facilitate rapid investigation and remediation. In practice, however, the scale and complexity of managing this lifecycle—and the many spots where it can go awry—have often left these solutions struggling to keep up with a dynamic threat landscape. This is where NG-SIEMs enter the picture. Unlike the SIEMs of the past, today's generation of solutions offers capabilities that are both broader and deeper, incorporating the power of cloud computing, the multifaceted threat detection capabilities of analytics, and the faster response and resolution afforded by orchestration and automation.

NG-SIEM has long been a fiercely competitive market segment, and Omdia's latest evaluation confirms that this remains true. It should be noted that the solution criteria of this NG-SIEM Omdia Universe are based on Omdia's vision for the long-term evolution of the NG-SIEM market segment. (See the report, *Fundamentals of Next-Generation Security Information and Event Management*; link in the ***Further reading*** section.)

The first NG-SIEM Omdia Universe report was released in 2021, and it was clear then that vendors still had a long way to go to meet Omdia's expectations and requirements for mature NG-SIEM solutions. In 2021, only one vendor exceeded our 50% solution capability threshold. To a large degree, Omdia has used the same criteria in this NG-SIEM evaluation. This time around, vendors have made significant strides in meeting market expectations for the breadth and depth of functionality, particularly in addressing the TDIR lifecycle. Today, five of the six participants exceeded the 50% solution capability threshold.

But there is still work to be done, and even market-leading vendors have areas that need continued attention. As a top example, vendors often still fall short with respect to response features, such as orchestration, automation, and evaluation.

Perhaps the most important takeaway from this report is that while Omdia identifies three market leaders, there is no such thing as a one-size-fits-all solution in the NG-SIEM market. The results demonstrate that the intense competition in this segment has driven vendors to invest heavily in product development, push the envelope in emerging capabilities areas that create meaningful differentiation, and be increasingly flexible regarding integration and pricing strategies.

Market definition

Omdia continues to consider the core functionality of SIEMs to include:

- Data collection
- Threat detection
- Threat response
- Reporting & management

However, to be considered as an NG-SIEM for this research, Omdia required vendors to demonstrate that their solutions met four baseline criteria:

- **Cloud native/cloud hosted:** The solution should be based on a purpose-built cloud native architecture, including storage. At a minimum, the solution's key components related to data collection and threat detection must be cloud hosted in one or more common infrastructure as a service (IaaS) environments.
- **Nontraditional telemetry support:** In addition to on-premises and cloud-based log ingestion support, the solution must also support the ingestion of a wide variety of threat intelligence, including indicators of compromise (IoCs). It should support other nontraditional telemetry sources, such as open database connections, hybrid cloud performance and latency metrics, and other emerging security metrics.
- **Native analytics:** The solution must offer built-in behavioral baselining and deviation detection, ideally with other machine learning (ML)-based detection mechanisms, to supplement traditional rules-based detection. The analytics capabilities should not require additional licensing.
- **Incident response/response enablement:** The solution should offer built-in incident response (defined by Omdia as threat incident response action enablement, orchestration, and automation features) to manage the entirety of the TDIR lifecycle quickly and efficiently from within the NG-SIEM.

Market dynamics

Since our previous report, Omdia has identified three emerging capabilities areas that were not specifically highlighted in our original evaluation criteria. They have been incorporated into this evaluation since they define the current market leaders:

- **Data engineering:** Omdia believes proprietary methods of data collection/forwarding, normalization, and enrichment are giving way to more customer-friendly open standards like the Open Cybersecurity Schema Framework (OCSF) and integrated multifunction security data lakes. We evaluate the extent to which NG-SIEM solutions are incorporating these capabilities.
- **AI:** Increasingly, Omdia believes AI, specifically generative AI (GenAI), will play a larger role in cybersecurity—particularly TDIR. We evaluate how the addition of AI-based capabilities to NG-SIEM solutions is increasing efficiency, decreasing cost, and improving outcomes.
- **Automation:** In the past three years, enterprises have begun to embrace automation—perhaps not because they are fully ready to do so, but because it is a necessity to keep pace with attacks while managing threats with limited resources. Omdia assesses the extent to which NG-SIEM solutions provide, enable, and facilitate successful automation to increase efficiency, decrease cost, and improve outcomes.

The landscape for NG-SIEM solutions consists of a variety of vendors, large and small, some well-established and others still largely unknown. This market is increasingly competitive, in no small part due to the meteoric rise of Microsoft's Sentinel NG-SIEM. The impact of this solution is being disproportionately felt in the mid-tier of the NG-SIEM market.

Omdia research data indicates that the annual SIEM revenue totals of the top three vendors (IBM, Microsoft, and Splunk) grew from $597m in 2021 to $916m in 2023, a CAGR of 24%. Meanwhile, the

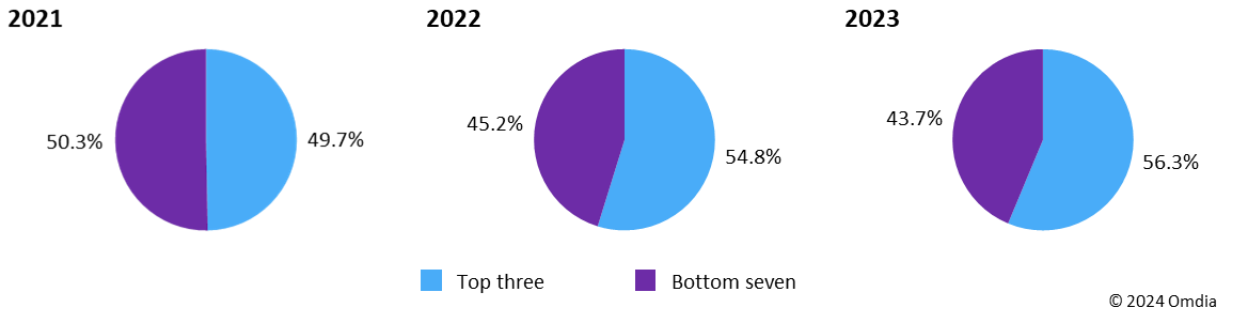
combined total revenue for the next seven vendors (3–10 in Omdia's rankings by revenue) grew from $604m in 2021 to $712m, a CAGR of just 9%. While still widely considered healthy growth, the data shows that the growth of the top three is far outpacing the rest of the top 10.

Omdia believes that in capturing an outsized share of market revenue, the top vendors—Microsoft in particular—have essentially squeezed the mid-tier, making growth prospects more challenging. This, in turn, is likely a key driver of the frenetic M&A activity in the NG-SIEM market over the past 12-plus months. This activity includes the following:

- Cisco's $28bn acquisition of Splunk in early 2024.
- AT&T's spinoff of its former AlienVault SIEM assets into LevelBlue in May 2024.
- Exabeam's merger with LogRhythm, also in May 2024.
- IBM's sale of its QRadar NG-SIEM and other assets to Palo Alto Networks in 3Q24.

Omdia expects this market upheaval to continue, with at least one to two additional mid-tier NG-SIEM vendors being acquired or otherwise exiting the market before the end of 2025.

Figure 2: SIEM market share percentage among top 10 vendors (by revenue), grouped by top three and bottom seven



Source: Omdia

Additionally, NG-SIEM continues to find itself competing with another rapidly advancing enterprise cybersecurity product segment: extended detection and response (XDR). The XDR market has moved past its peak of inflated expectations, and with a more seasoned view of the utility of the technology, it is clear where XDR and NG-SIEM will compete. Omdia believes that, ultimately, both will thrive. XDR focuses on specific threat types and outcomes with efficient, selective use of data and is often delivered as a managed service. NG-SIEM will serve as the preferred choice for large enterprises with expansive hybrid cloud environments, dedicated SOC teams, and specific, detailed compliance and reporting demands.

Figure 3: Vendor rankings in the NG-SIEM Universe

Vendor	Product(s) evaluated
Leaders	
Exabeam	Exabeam Security Operations Platform – Exabeam Fusion
Palo Alto Networks	Cortex XSIAM, Version 2.2
Splunk	Splunk Enterprise Security, Version 7.3.2 Splunk SOAR, Version: 6.2.2 Splunk Attack Analyzer, Version: 1.1.1 Splunk Asset and Risk Intelligence, Version: 1.0.0
Challengers	
Gurucul	Gurucul REVEAL NG-SIEM module
Securonix	Securonix Unified Defense SIEM (SaaS), Version 6.4
Prospect	
Graylog	Graylog Threat Detection and Response (TDIR) Platform

Source: Omdia

Market leaders

The scores achieved in this NG-SIEM Omdia Universe provide some encouragement that leading solutions continue to evolve, mature, and keep pace with market demand. Market leaders have demonstrated areas of competence that are impressive by any measure. On the other hand, each vendor, including market leaders, demonstrates a markedly unique set of core competencies, as well as shortcomings.

For example, Exabeam and Palo Alto Networks tend to excel more in the TDIR categories, while Splunk shines in the data engineering categories. This reality highlights how critical it is for customers to perform due diligence when assessing these solutions, including the leaders, to determine which aligns with their requirements and priorities.

Overall, Omdia has documented impressive improvements in capabilities since 2021, but in some areas, these solutions have yet to deliver on clear customer requirements. With respect to product capabilities, vendors generally struggle with the integration of security orchestration, automation, and response (SOAR) features. Three of six participants, including market leader Exabeam, delivered underwhelming scores in this category. Hence, there is no room for leaders to rest on their laurels and ample opportunity for challengers to gain ground.

Market challengers

From a feature and function perspective, there is not a huge delta between leaders and challengers in this year's NG-SIEM Omdia Universe. For example, Gurucul is very strong in almost all data engineering categories, while Securonix is market-leading in AI/ML support. Rather, the dividing line between leaders and challengers in this year's NG-SIEM Omdia Universe ran along the areas of market momentum and vendor execution. These metrics are determined by a combination of customer surveys and quantitative market analysis. As discussed, NG-SIEM is a particularly challenging market for midsize vendors, and both Gurucul and Securonix find themselves squarely in that tier.

Notable vendors

Several notable vendors are not included in this year's Omdia NG-SIEM Universe. In addition to supporting the functionality outlined above, to be included in this comparative report, Omdia also required that the solution be delivered as a standalone product. This requirement eliminated some otherwise eligible

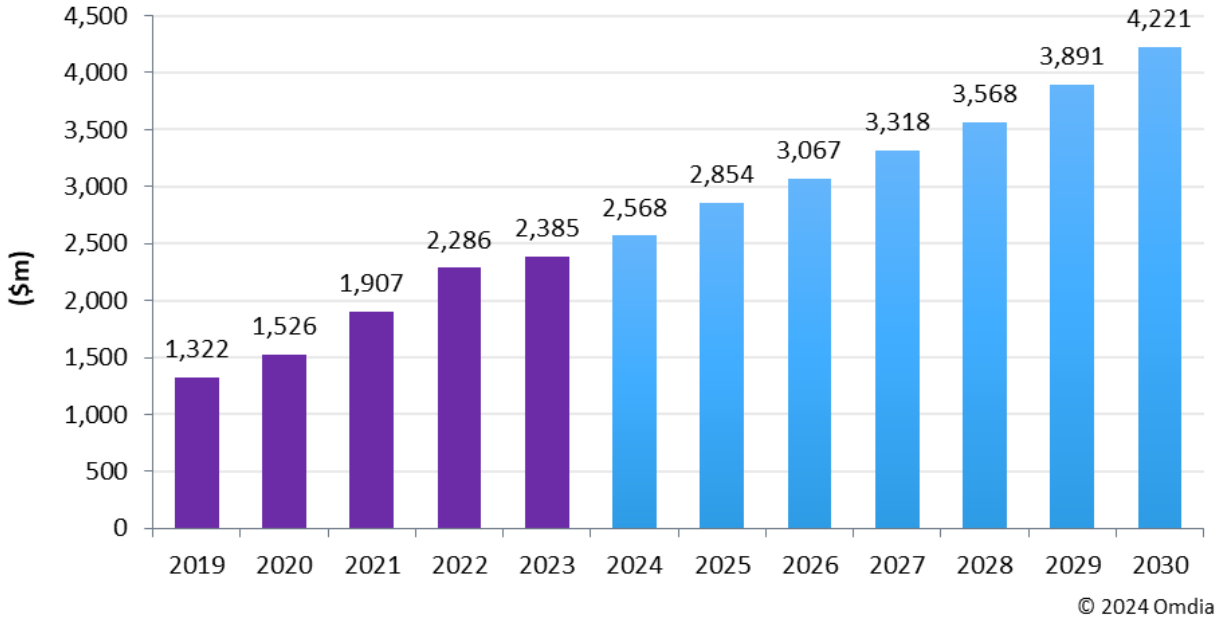
participants. For example, Omdia determined that CrowdStrike's Falcon Next-Gen SIEM product does not meet our definition of a standalone NG-SIEM, as it is dependent on either Falcon EDR or other third-party endpoint detection and response (EDR) functionality.

Other vendors considered for this research that were ultimately not included (or that declined participation) include Datadog, Devo, Elastic, Google Cloud, LevelBlue, Logpoint, Microsoft, OpenText, Sumo Logic, and Trustwave.

Market outlook

The SIEM market reached $2.454bn in annual revenue during 2023. Despite a slowed growth rate during 2023 versus recent previous years due to global economic conditions and longer buying cycles, Omdia anticipates strong growth throughout the most recent five-year forecast period as more enterprises migrate to NG-SIEM and take advantage of integrated analytics and SOAR capabilities. Omdia forecasts the global SIEM market will grow to $4.221bn in 2030.

Figure 4: Global NG-SIEM market forecast, 2019–30

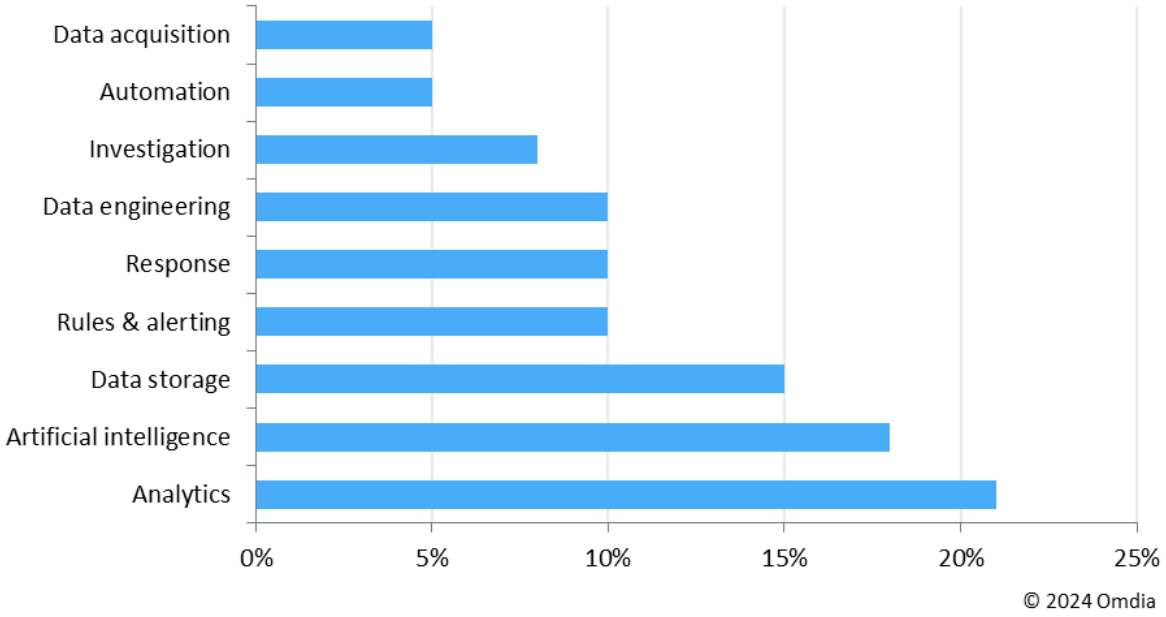


Source: Omdia

Market drivers

Omdia's 2024 Cybersecurity Decision-Maker Survey asked organizations which NG-SIEM features currently had the most influence on buying decisions. As seen in **Figure 5**, among respondents with more than 2,500 employees, analytics, AI, and data storage were the most important features.

Figure 5: Which next-generation SIEM (NG-SIEM) feature is most likely to positively influence your next purchasing decision (respondent organizations with more than 2,500 employees)?



Source: Omdia

There is one additional emerging success criterion that Omdia believes is widely overlooked, especially in what is becoming the age of cybersecurity platforms. That criterion is flexibility. While consolidating capabilities around a single vendor's security operations (SecOps) platform may make sense for various reasons, NG-SIEM purchasing influence is consolidating around the role of the security architect within enterprise buying teams. This role is increasingly responsible for ensuring a solution meets the needs of all the other stakeholders and their unique use cases.

To meet the needs of an increasingly diverse set of stakeholders, security architects value one thing above all others: flexibility. The ability to ingest data in an open format of the customer's choice, store data in various locations based on business requirements, federate search across multiple data lake houses and instances, and support the niche feature demands of everyone from threat hunters to chief information security officers are all reasons why it may not be a consolidated platform approach that ultimately rules NG-SIEM. Rather, a modular, bring-your-own-building-block approach to NG-SIEM may be gaining favor. It would be ironic if the winning strategy for NG-SIEM five years from now is not about building up platforms but about breaking out capabilities. Omdia believes savvy vendors that pursue this approach will likely find themselves well-received in the NG-SIEM market of the not too distant future.

Competitive landscape

The global NG-SIEM market remains healthy, growing, and remarkably competitive. But the dynamics of the SIEM market have changed dramatically in the past several years. As noted, that change is largely driven by one vendor: Microsoft. Per previous research published in Omdia's *Enterprise Cybersecurity Operations (SecOps) Market Tracker – 2H23 Analysis*, the software giant is now the top partner—or top competitor—for most of the major vendors and/or providers in SecOps, including NG-SIEM. This new competitive dynamic has been the primary driver of the rash of M&A activity in the NG-SIEM space. However, given the segment's breadth of capabilities and the broad set of customer demands, Omdia remains confident that there remains room for an abundance of top-tier competitors, as well as startups and other niche vendors that deliver disruptive capabilities and find innovative ways to meet customers' requirements.

Vendor analysis

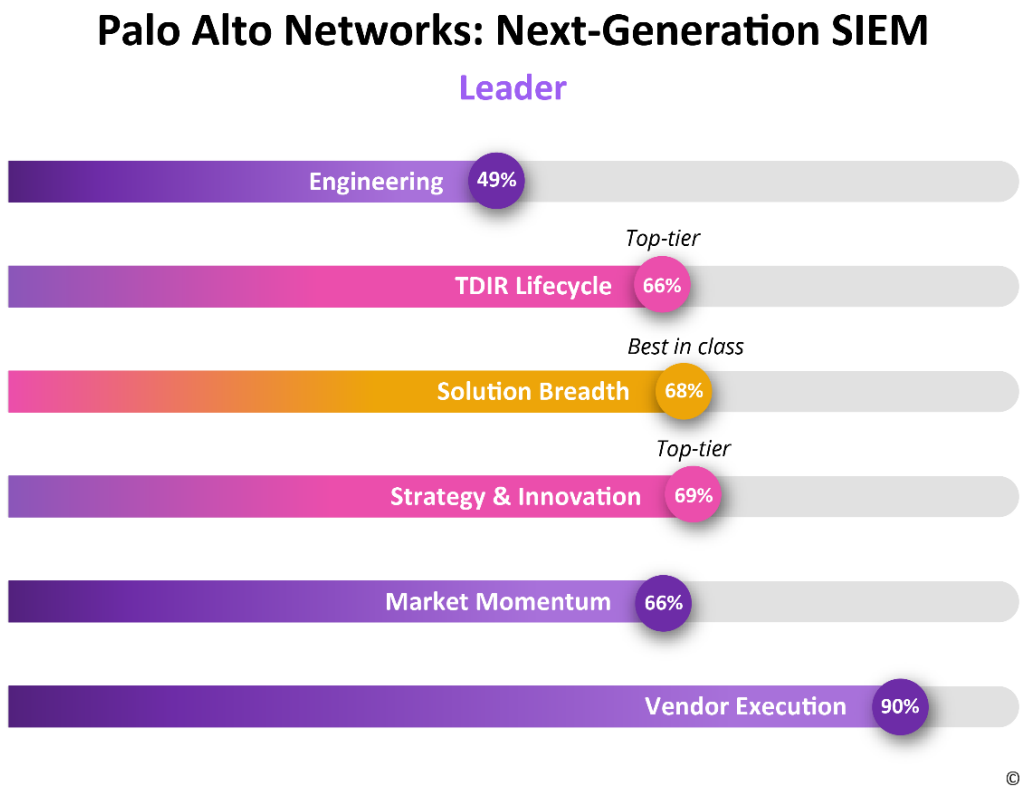
Palo Alto Networks (Omdia recommendation: Leader)

Table 1: Palo Alto Networks solution profile

Product name	Cortex XSIAM, Version 2.2
Target market	Americas (North America, Latin America & the Caribbean), Europe (Western, Eastern), Asia (Central, Southern, Oceania, Eastern & South-Eastern Asia), and MEA (Middle East and Africa)
Number of customers	n/a
Key customers	Vendor declined to provide

Source: Omdia

Figure 9: Omdia Universe ratings—Palo Alto Networks



Source: Omdia

Palo Alto Networks should appear on your shortlist if:

- A top priority is a solution that can drive a heavily automated TDIR lifecycle.
- The customer wants a solid solution across the board that is backed by a top-tier vendor.
- The customer is driving toward a Palo Alto Networks-centric platform approach.

Market position overview

Palo Alto Networks is relatively new to the NG-SIEM segment, but a series of bold moves and rapid advancement of its capabilities, particularly in automation, have earned the vendor a leader position in this Omdia Universe. Palo Alto Networks was founded in 2005 by cybersecurity industry legend Nir Zuk, who serves as the company's chief technology officer. An early developer of next-generation firewalls (NGFWs), today Palo Alto Networks has one of the broadest enterprise product portfolios in the cybersecurity industry. Its SecOps platform, Cortex, includes several products: Cortex XDR, Cortex XSOAR, Cortex Xpanse (attack surface management), and its NG-SIEM solution, Cortex XSIAM. The company recently completed its bombshell acquisition of several cybersecurity assets from IBM, including its QRadar NG-SIEM (excluding the appliance version). Palo Alto Networks intends to migrate QRadar customers to XSIAM over time.

Technology details

Palo Alto Networks has been strategic in building out its NG-SIEM functionality, which debuted in 2022, through acquisition and internal development. Acquisitions that contributed to the Cortex XSIAM include Cyvera (endpoint security, 2014), LightCyber (UEBA, 2017), Secdo (EDR, 2018), Demisto (SOAR, 2019), Crypsis (incident response, 2020), and Expanse (attack surface management, or ASM, 2020). Cortex XSIAM has already achieved admirable technological breadth compared to competitors. In Omdia's evaluation, the company scored particularly well in the areas of detection and alerting and case investigation.

Data collection details

Cortex XSIAM collects data directly from cloud and on-premises sources with a mix of agents and virtual machines (VMs), as well as from Palo Alto Networks' Strata NGFWs. Cortex XSIAM supports OOTB parsing and normalization of approximately 200 different data sources and supports more than 250 total OOTB connectors, among them more than 150 that use APIs for sources such as Azure, Google Cloud Platform (GCP), Okta, and Dropbox. API protocols include, among others, REST, Socket, GraphQL, and SOAP, and data can be collected and stored in any format. Queries are typically executed using the XSIAM Data Model.

Cortex XSIAM runs on GCP, with data stored in BigQuery. Default hot data retention is 31 days for raw data, 180 days for alerts and incidents, and 365 days for forensic artifacts (with a separate license). All customer data is stored in GCP in the same location as the XSIAM environment. Cortex XSIAM can query external data repositories if needed, but because of the nature of analytics and detection capabilities, it is not recommended nor generally supported by the company. Cortex XSIAM is delivered as a software as a service (SaaS) solution, which provides architectural advantages with respect to scale, and resources can be extended quickly and flexibly. For example, the Cortex Broker VM for local log collection allows for 80,000 EPS per broker (each virtual broker generally includes eight virtual cores at 10,000 EPS each) and can be scaled with clusters of brokers, as well as adding additional resources on brokers.

Threat detection details

Cortex XSIAM employs multiple discrete analytics engines designed to handle diverse data types and behavioral patterns. These engines include UEBA, ML-driven detection, threat intelligence correlation, and a rules engine. The solution uses ML models to build baselines of normal behavior across various data

sources, such as endpoint activity, network traffic, and user behavior. These baselines are then used to identify anomalies and potential threats in real time. Cortex XSIAM Analytics baselines all data ingested for profiling, entity classification, detection, and automation. The analytics engine supports both first- and third-party data from endpoints, SaaS, cloud infrastructure, network, and event log sources. AI and ML are used for entity classification, threat detection and prevention, and scoring and automation. Cortex XSIAM comes with thousands of OOTB rules, the vast majority of which are based on ML and the profiling of entities. The solution supports several options for querying data:

- Free-text search on all data
- A structured search using a wizard called Query Builder
- Via the XQL query language
- With an embedded Jupyter Notebook using Python

Threat response details

Cortex XSIAM extracts data from each alert to determine data origin, users/host/entities involved, artifacts and IoC observed, source of alerts, and suggested automation actions. Visualizations include an attack path mapping and a timeline view available at the case level. All data is available for drilling down and pivoting without leaving the case dashboard. XSIAM employs incident response prioritization, using ML to create a score for each incident (between 1 and 100). Palo Alto's XSOAR solution is embedded in Cortex XSIAM, which makes available 1,000 integrations and thousands of playbooks OOTB. Users can edit and tune playbooks or create playbooks with no-code or code options. Cortex XSIAM supports full automation in response to alerts and incidents, semi-automation (actions are recommended and triggered upon analyst confirmation), or manual response. Users can customize triggers and pick from canned response actions for common use cases such as ransomware, insider threats, and data leakage. XSIAM's playbook creation feature allows for the codification of processes and workflows. Full customization of playbooks is supported, and existing playbooks can be modified as required. Playbooks can also be nested within other playbooks so that dependent processes can be leveraged across different scenarios.

XSIAM offers one of the industry's most advanced AI copilot offerings, with a vast array of capabilities supporting investigation and response. Copilot also suggests relevant XQL queries with embedded parameters based on the user prompt so the queries can run without analyst input. It can recommend relevant playbooks to automatically remediate and resolve incidents, suggest investigation steps based on the user prompt, and assist with advanced data queries.

Palo Alto Networks has also done a particularly good job of integrating XSOAR into the XSIAM platform. XSIAM comes OOTB with more than 1,000 integrations and thousands of playbooks, and users can tune, customize, or create playbooks with no-code or code interfaces. The solution also supports robust automation capabilities in response to alerts and incidents.

Reporting & management details

Cortex XSIAM comes with multiple OOTB reports and dashboards. Palo Alto Networks has made progress in meeting table stakes compliance use cases with its reporting but still lacks the mature reporting offered by established rivals. Users can customize existing reports and create new reports with visualizations and designs for various audiences, both senior and technical/operational. XSIAM includes content packs, which provide onboarding technology and content in support of standard tasks such as data, parsing, normalization, and integration. Ongoing system management is also enabled through intelligence health

monitoring to better understand normal communication and alerting patterns and to flag abnormal behavior. This health monitoring can support incident response and XSIAM performance management.

Strategy and roadmap

For the past several years, Palo Alto Networks' strategy has been to build and bring to market a set of broad, integrated platforms featuring best-of-breed cybersecurity solutions. The thinking of CEO Nikesh Arora has been to "land" new customers with one of its SecOps solutions, such as its popular XSOAR orchestration product, and "expand" by later selling other pieces of its Cortex portfolio, featuring SecOps offerings in addition to SOAR, including XDR, Xpanse, and the XSIAM.

When Palo Alto Networks introduced Cortex XSIAM two years ago, it was billed as the new centerpiece for Cortex, positioning it as an autonomous SecOps platform. In early 2023, an Identity Threat Detection and Response (ITDR) module was introduced, setting the stage for the release of a considerably matured XSIAM 2.0 later that year.

Additional upgrades were announced in May 2024, including support for a Bring Your Own Machine Learning (BYOML) framework that empowers custom ML models for tailored security solutions, a broader partnership with IBM in support of delivering AI-power outcomes, and expanded cloud detection and response capabilities.

Then, in September 2024, Palo Alto Networks shocked the world with the acquisition of IBM's QRadar SaaS assets, instantly gaining the technology and customers. The company has stated its intention to migrate QRadar SaaS customers to XSIAM, but the timeline for doing so and other related details are unclear. Also that month, Palo Alto Networks announced an expanded partnership with Red Canary to offer Managed XSIAM.

Palo Alto Networks has mapped out an aggressive adoption plan for AI technology. Areas of current interest include the use of ML for creating behavioral threat protection rules, a new module that provides shellcode AI protection (based on supervised learning that leverages decision trees, weak supervision, and proprietary ML algorithms), and AI-powered email security, which leverages LLMs to identify social engineering attacks.

Opportunities

Palo Alto Networks underperformed versus competitors in Omdia's engineering categories: data management, integration, and architecture. This is in part because the solution has only been in the market for a little over two years, and the vendor simply has not had time yet to build many of the backend customizations that its rivals have spent years perfecting.

However, this is also, in part, strategic. XSIAM is designed to be the centerpiece of a Cortex SecOps platform that takes data in from and facilitates response to its other Cortex solutions in a highly automated fashion. Hence, certain areas where the solution is lacking, such as purpose-specific visibility agents, support for data lake houses, and federated analytics, are because the adoption of the Cortex platform is meant to either facilitate those capabilities or make them unnecessary. Still, Omdia sees a broad opportunity for Palo Alto Networks to improve the third-party interoperability of XSIAM.

Palo Alto Networks gets credit for a low-touch data storage system designed for ease of use with minimal configuration. However, its retention policies are industry standard minimums, and the lack of granularity regarding performance metrics and retrieval/restoration time suggests an offering that has yet to mature. As noted, the company discourages the use of federated storage, stating that the practice has a negative effect on data availability, performance, accuracy, and integrity. The solution also uses a proprietary data

format called XSIAM Data Model (XDM) with no standards-based support, but the company claims that OCSF support is on its product roadmap.

AI and ML are used effectively for entity classification, threat detection and prevention, scoring, and automation. The product leverages multiple patented unique AI approaches to improving cybersecurity use cases, and the flexibility of the solution is impressive; for example, users can customize their own AI models.

XSIAM also delivers above-average granularity and flexibility in approaches and methods for threat hunters, with some caveats tied to the default hot storage package. When hunting across cold storage locations, which threat hunters often desire to query historic data for newly discovered IoCs, data is automatically re-warmed. Yet, the data requires the consumption of additional compute units, which can be costly. As such, customers will need to weigh the cost of cold storage compute units versus purchasing longer hot storage retention for threat hunting.

Palo Alto Networks has taken considerable care in making its solution easier to deploy and use. The solution delivers a strong go-to-market value proposition that leans into its strengths (entirely cloud-based, heavily AI-driven, empowering organizations to advance automation). But it is telling that all customers Omdia surveyed have "opted" to use professional services for deployment and configuration, suggesting the solution has many of the same complexities as its more established rivals.

Omdia analysis

Omdia was pleasantly surprised by Palo Alto Networks' XSIAM. Despite being the newest NG-SIEM on the market, the solution's capabilities have been rapidly advanced, already boasting TDIR lifecycle management capabilities—from detection and alerting through to remediation response actions—that equal or surpass nearly every other competing solution.

It cannot be emphasized enough that XSIAM was built to enable organizations to take an automation-first approach to TDIR: gathering data, conducting queries, summarizing results, and even suggesting response options. The company asserts that with the full complement of supporting solutions, Palo Alto Networks customers can automate away all but a handful of daily threat incidents.

The product needs maturing in its engineering capabilities, and it remains to be seen whether the breadth of TDIR automation promised in the current version of the solution can meet expectations. But for enterprises centering on Palo Alto Networks' Cortex platform, XSIAM is a strong and obvious choice.

More broadly, though expanding its platform ambitions is a top strategic priority for the company, being a top-tier NG-SIEM solution means accepting that third-party integration will always be a key customer requirement. Winning over large enterprises consistently will require a greater focus on data integration capabilities and demonstrating a commitment to playing its part within the industry-wide cybersecurity solution ecosystem. The fact that current XSIAM customers tend to be cost-conscious suggests that Palo Alto Networks' platform strategy is beginning to resonate with its target audience.

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and Omdia's enterprise insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Vendors are interviewed, and in-depth briefings are provided on current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

Omdia has closely tracked the emergence and rapid evolution of the NG-SIEM segment. Inclusion criteria were largely dictated by Omdia's own research, including, but not necessarily limited to, the following:

- The product(s) submitted for consideration must have been generally available at the time which Omdia's research was initiated, no later than June 1, 2024. The product(s) did not have to be available in all markets globally or any specific geographic regions or subregions as defined by Omdia.
- The product(s) submitted for consideration must meet the four baseline criteria for inclusion mentioned above. The product(s) do not necessarily have to be named/branded as NG-SIEMs in technical documentation for public-facing marketing materials.
- The product(s) submitted for consideration must generate a minimum annual revenue of $10m, as determined through publicly available information, vendor-provided information, or Omdia research.
- The product(s) submitted for consideration must have active customers, as demonstrated by the vendor. A minimum number of customers established by Omdia must provide customer experience survey data to Omdia in the form of surveys fielded by Omdia or its research partner.

Further reading

Fundamentals of Next-Generation Security Information and Event Management (July 2021) *Cybersecurity Decision-Maker Survey 2024: Enterprise Cybersecurity Operations (SecOps)* (September 2024)

Enterprise Cybersecurity Operations (SecOps) Market Tracker – 2H23 Analysis (December 2023)

Authors

Andrew Braunberg, Principal Analyst, SecOps

Eric Parizo, Managing Principal Analyst, SecOps

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com