

KuppingerCole Report

LEADERSHIP COMPASS

By **Alexei Balaganski**
January 20, 2022

Intelligent SIEM Platforms

This report is an overview of the market for modern, intelligent Security Information and Event Management (SIEM) platforms and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing SIEM solutions.



By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Introduction / Executive Summary	4
1.1 Highlights	5
1.2 Market Segment	6
1.3 Delivery Models	7
1.4 Required Capabilities	8
2 Leadership	11
2.1 Overall Leadership	11
2.2 Product Leadership	13
2.3 Innovation Leadership	15
2.4 Market Leadership	17
3 Correlated View	20
3.1 The Market/Product Matrix	20
3.2 The Product/Innovation Matrix	22
3.3 The Innovation/Market Matrix	23
4 Products and Vendors at a Glance	27
5 Product/Vendor evaluation	30
5.1 DNIF	32
5.2 Exabeam	35
5.3 FireEye	38
5.4 Fortinet	41
5.5 Gurukul	44
5.6 Huntsman Security	47
5.7 IBM	50
5.8 Logsign	53
5.9 ManageEngine	56
5.10 Micro Focus	59
5.11 Microsoft	62
5.12 NetWitness (RSA)	65

5.13 Securonix 68

6 Vendors to Watch 71

6.1 Chronicle / Google Cloud 71

6.2 Elastic 71

6.3 LogPoint 72

6.4 LogRhythm 72

6.5 Logz.io 72

6.6 Rapid7 73

6.7 Splunk 73

6.8 Sumo Logic 73

6.9 T-Systems 74

7 Related Research 75

Methodology 76

Content of Figures 82

Copyright 83

1 Introduction / Executive Summary

Security Information and Event Management (SIEM) solutions have dominated the enterprise security market for nearly two decades, and even nowadays they are still widely used to power security operations centers (SOCs) in large companies or managed security services for smaller ones.

At the beginning of the Digital Transformation era, when perimeter-focused tools like firewalls were no longer able to protect corporate networks, the scope of cybersecurity was gradually shifting towards threat detection. Back then, SIEM tools were hailed as the ultimate solution to all security challenges.

With centralized collection and management of security-related data across all corporate IT systems and a set of rules to identify known malicious activities in that stream of security events, the only thing that remained was to analyze each finding and respond accordingly. In addition to providing visibility into the overall security posture, SIEMs serve as a convenient tool for compliance reporting.

Unfortunately, it did not take long to realize that SIEM solutions were failing in delivering on their promises, with companies deploying them facing multiple obstacles and challenges. High deployment and operational costs, consistent failures to react to modern cyber threats in time, and, last but not least, the growing skills gap to staff the security teams needed for efficient security operations were the most common problems of legacy SIEM solutions.

Even with fairly simple rule-based detection capabilities, traditional SIEMs tend to generate an overwhelming number of alerts with a high percentage of false positives. Lacking any risk scores or other meaningful metrics for their impact, they make it very difficult to prioritize analysis. When it comes to analyzing a discovered incident, traditional SIEMs offer few automation capabilities and usually do not support two-way integration with security devices like firewalls and thus do not make forensic investigations any easier for analysts, since their job remains largely manual and time-consuming.

For years, organizations have been looking for better alternatives to replace their aging SIEMs. Some experts have even proclaimed that SIEM as a concept is no longer relevant, and they should give way to modern alternatives, such as XDR -- the emerging "Extended Detection and Response" technology. However, the SIEM market itself has also been constantly evolving in recent years, and modern products bear little resemblance to their ancestors.

Over the last decade or so, the security analytics market has undergone profound changes thanks to several groundbreaking technologies that emerged after the first generation of SIEM tools. These include such fundamental developments as Big Data frameworks, public clouds, and artificial intelligence, and machine learning. By incorporating these technologies into their products, as well as augmenting them with further new capabilities (such as user behavior analytics, intelligent decision support for analysts, sophisticated forensic tools, orchestration and automation for incident response, and so on), vendors can offer their customers substantially modernized, scalable and intelligent solutions and ensure that SIEMs

remain a core component of modern enterprise security architectures.

The market for these modern security intelligence and automation solutions continues to evolve, with solutions gaining new capabilities, merging previously standalone tools into integrated platforms, and, last but not least, changing names, definitions, and licensing policies. Some vendors continue to offer these capabilities as separate products or platform modules -- such as UEBA, SOAR, or even NDR -- while others deliver various capabilities under the single overarching "Next-Gen SIEM" banner.

Companies looking for an upgrade for their aging SIEM solution now have to face a tough task -- to look behind the alphabet soup of various security technologies, identify the most necessary capabilities that would address their specific requirements, and then choose a solution or a combination of solutions to modernize their security operations centers. Unfortunately, there is no universal recipe that would fit all possible customer sizes, industries, or geographies.

This Leadership Compass should be seen as an additional tool that can help you identify your requirements and map them onto capabilities offered by specific vendors, taking into consideration your scale, available skill set, and, of course, budget constraints.

1.1 Highlights

- SIEM solutions have dominated the enterprise security market for nearly two decades, but unfortunately, due to high operating costs and an increasing shortage of skilled security experts, traditional SIEMs can no longer keep up with the scale and sophistication of modern cybersecurity threats.
- The biggest shortcoming of legacy SIEM tools is their inability to deal with the overwhelming number of generated security alerts and to separate the relevant ones that need to be investigated from the useless statistical noise.
- Currently, the SIEM market is experiencing strong pressure from alternative approaches such as specialized security monitoring solutions for different attack surfaces (endpoints, networks, APIs, databases, etc.) and unified XDR solutions; however, SIEM solutions themselves continue to evolve, expand their coverage and address their historical challenges.
- Modern technologies like machine learning that powers behavior analytics, threat hunting, and remediation ensure that the usability and productivity of SIEM tools improves significantly
- Incorporation of advanced security orchestration, automation, and response (SOAR) capabilities either directly or via two-way API integrations ensures that forensic analysis and incident response can be automated to a high degree, reducing the time needed to react to a breach.

- The ongoing trend of delivering security solutions from the cloud affects SIEM platforms as well -- the support for cloud-based and hybrid deployments is available from every relevant vendor in this market.
- The number of fully-managed, cloud-only SIEM solutions offered as-a-Service continues to grow; smaller, agile and innovative startups and even some large veteran vendors like Microsoft opt for this approach.
- The market consolidation trend continues: capabilities like UEBA or SOAR, which just a few years ago were offered as standalone tools from independent vendors, are now increasingly integrated directly into SIEM products through acquisitions.
- Still, the market is far from reaching maturity and stagnation, this can be immediately observed in this Leadership Compass' findings: we have a healthy mix of large veterans and innovative startups among the leading SIEM offerings.
- The overall leaders in the Intelligent SIEM Platforms market are (in alphabetical order): Exabeam, FireEye, Fortinet, Gurukul, IBM, Micro Focus, Microsoft, NetWitness (RSA), and Securonix.

1.2 Market Segment

Traditional SIEMs have been introduced over 15 years ago as unified platforms for gathering, analyzing, and correlating security events from multiple sources to provide a centralized overview of all security-related events across the whole enterprise, alert the team of security experts, and provide tools for forensic analysis. For many companies, SIEMs serve as a focal point (if not the only component) of their Security Operations Centers (SOC).

As the size and complexity of corporate IT infrastructures continued to grow, even the enterprises that could afford the best expert teams realized that their existing tools face inherent limitations preventing them from efficiently reacting to cyberthreats. However, the emergence of breakthrough technologies like Big Data and Machine Learning (ML) has continuously driven innovation in the cybersecurity market throughout the last decade. New intelligent automation capabilities, whether integrated directly into newer SIEM solutions or augmenting the existing ones with new functions, ensure that security monitoring, forensic analysis, and incident response remain a core component of any modern cybersecurity architecture.

In this Leadership Compass, we are looking at the latest generation of SIEM solutions, which continue to evolve as general-purpose security management and intelligence platforms, incorporating innovative intelligence and automation capabilities. While we recognize that the market continues to expand, with other segments like SOAR emerging in parallel, we do observe the trend to incorporate these related capabilities into integrated yet modular and flexible platforms we consider the "next-generation intelligent SIEMs".

While some existing SIEM vendors have decided on the evolutionary development of their existing products, others opted for strategic acquisitions. Many smaller vendors and startups are focusing on specialized solutions to address specific critical problems of certain customers. The resulting multitude of various products made it very difficult not just for customers to find the right solution for their requirements, but also for analysts to predict their future development and event to rate the products against each other in a meaningful way.

In this Leadership Compass, we are focusing solely on universal security analytics solutions that conform to the following criteria:

- Collecting and parsing security data from multiple sources in various formats.
- Enriching collected data with additional context from external threat intelligence feeds.
- Applying Big Data analytics and machine learning algorithms to detect patterns and outliers in the collected data to identify previously unknown threats and suspicious activities.
- Providing built-in or tightly integrated tools for incident response and threat remediation.

As a result, next-generation security analytics solutions offer substantial improvements in both functionality and efficiency over traditional SIEMs:

- Performing real-time or near real-time detection of security threats without relying on predefined rules and policies.
- Correlating both real-time and historical data across multiple sources enables detecting malicious operations as whole events, not separate alerts.
- Dramatically decreasing the number of alarms by filtering out statistical noise, eliminating false positives, and providing clear risk scores for each detected incident.
- Offering a high level of automation for typical analysis and remediation workflows, thus significantly improving the work efficiency for security analysts.

1.3 Delivery Models

For over a decade, SIEM solutions have been primarily deployed on-premises, with a substantial investment required for both hardware and other infrastructure, as well as a team of skilled professionals to operate them. Unsurprisingly, operating a SIEM tool was an opportunity that only large enterprises or specialized managed security providers could afford.

However, with the growing scale, number, and complexity of enterprise networks and applications, even the

most powerful SIEM platforms could no longer keep up with the overwhelming amounts of security telemetry produced by all those systems. Unsurprisingly, modern SIEM solutions usually support deployments in cloud-hosted environments with varying degrees of shared management between customers and vendors or third-party MSSPs. However, even such products must still rely on a multitude of connectors, sensors, or APIs scattered across enterprise IT environments to collect and process security telemetry.

More recently, some vendors have begun offering their SIEM solutions as fully managed SaaS offerings, completely hiding the operational complexity from their customers. Unfortunately, these services, while offering massive improvements in usability and cost reduction, come with the usual potential challenges of the SaaS model that the customers must be aware of. These include compliance issues with regards to data residency and handling sensitive personal information, as well as limited customization options, potential latency and performance issues, and generally lower degree of control for the customer. And, of course, even fully cloud-based SIEM solutions must still collect security data from various on-prem sources, although this can also be partially simplified through cloud-native integrations with existing security tools (such as EDR, NDR, CSPM, etc.)

Additionally, organizations have to consider that many SIEM products have evolved not entirely organically but are the result of acquisitions or technology partnerships and are offered as suites of different products or services with different deployment options. This is especially relevant for capabilities heavily relying on machine learning (such as UEBA), which sometimes do not even support on-prem deployments. This essentially makes every SIEM deployment an inherently heterogeneous, distributed and hybrid, or even multi-cloud architecture project.

All these challenges make selecting the right SIEM solution even more complicated, especially for smaller companies. It is important to understand that a next-generation SIEM platform should not be considered just another security tool in a growing arsenal of security experts. On the contrary, the main reason for these solutions to emerge was to address the growing lack of skilled people in information security to use such tools to monitor, analyze, and respond to cyber threats.

As opposed to traditional SIEMs, next-generation solutions should not require a team of trained security experts to operate, relying instead on actionable alerts understandable even to businesspersons, a high degree of workflow automation, and ideally provide a complete end-to-end solution for a security operation center. Helping you to find the right balance between functional coverage, usability and efficiency, and budget constraints is the primary goal of this Leadership Compass.

1.4 Required Capabilities

We are looking for universal, extensible platforms that provide a holistic approach towards maintaining complete visibility and management of the security posture across the whole organization. Only by correlating both real-time and historical security events from logs, network traffic, endpoint devices, and even cloud services and enriching them with the latest threat intelligence data, it becomes possible to

identify previously unknown advanced security threats quickly and reliably, to be able to respond to them in time and thus minimize the damage.

Collection and efficiently storage of security events from various sources using Big Data technologies:

- Collecting and parsing system, application, service, or device logs in various formats.
- Capturing and analyzing network traffic information including packet capture, NetFlow, and similar technologies in real-time.
- Collecting security data directly from endpoints using agent-based or agentless methods.
- Providing integrations with various third-party sources of security events like firewalls, databases, application servers, etc.
- Providing integrations with cloud services to enable visibility into hybrid environments.

Real-time correlation across collected data using statistical algorithms and machine learning methods:

- Enrichment of collected data with business-related context information from various sources.
- Enrichment of collected data with current threat intelligence from external feeds.
- Detection of patterns and anomalies in security data, thus removing statistical noise and reducing false positives and other unnecessary alerts.
- Identification of multiple events from different sources as parts of a single security incident.
- Assignment of risk scores to each incident according to one or more predefined risk models.

Rich alerting and reporting functionality:

- Configurable dynamic dashboards for monitoring various aspects of corporate security and risk posture.
- A low number of alerts for discovered security incidents, ranked by risk scores.
- Actionable alerts enriched with business context and suggestions for remediation actions.
- Out-of-the-box reports for major industry compliance frameworks.

Forensic Investigation and incident management capabilities:

- On-demand access to all source and contextual security information related to an incident.

- Ability to pivot to related events, entities, or users for a better understanding of the impact.
- A high degree of automation with a large number of prepackaged risk models, policies, reports, and workflows tailored to a specific industry or market.
- Built-in or closely integrated incident response capabilities to initiate an orchestrated response as quickly as possible.

Integrations

- Integrations with 3rd party products and services to expand monitoring to applications, cloud services, security devices as well as support for standard protocols and APIs.
- Integrations with 3rd party security tools for automated threat mitigation: firewalls, identity management systems, cloud services, etc.
- Integrations with external threat intelligence feeds; support for industry standards like STIX/TAXII
- Integrations with own or 3rd party incident response solutions.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Compass. The Compass provides a comparison based on standardized criteria and can help identify vendors that shall be evaluated further. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of a pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

2.1 Overall Leadership

The Overall Leadership rating provides a consolidated view of all-around functionality, innovation, market presence, and financial position. However, these vendors may differ significantly from each other in terms of product features, platform support, and integrations. Therefore, we strongly recommend looking at all the leadership categories as well as each entry in chapter 5 to get a comprehensive understanding of the players in this market and what use cases they support best.

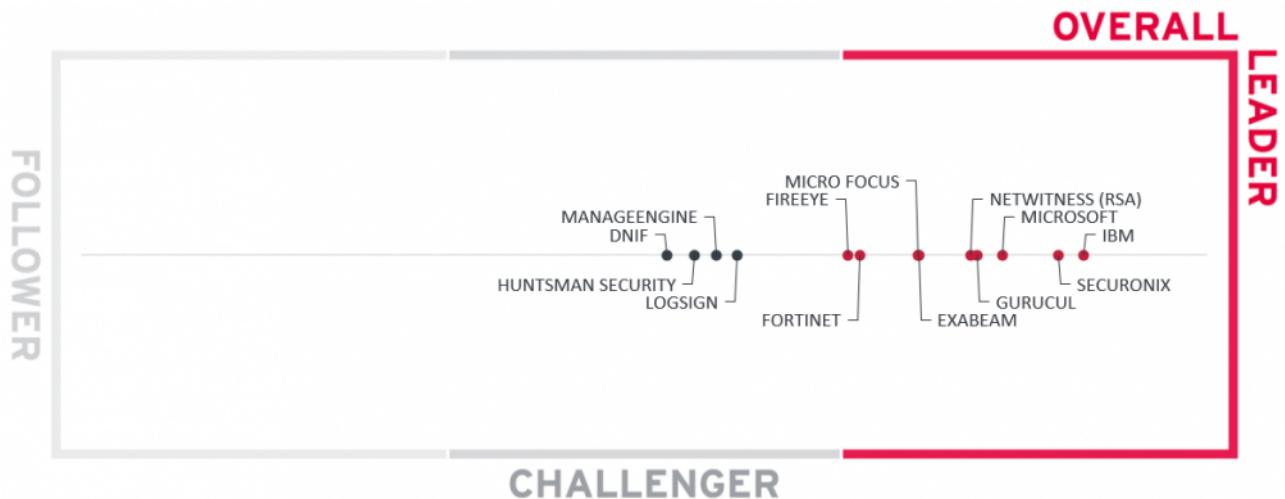


Figure 1: The Overall Leaders in the Intelligent SIEM Platforms market

Among the overall leaders among the Intelligent SIEM Platforms, we can find an interesting mix of both well-established solutions from veteran vendors like IBM QRadar, Micro Focus ArcSight, NetWitness (RSA), and Fortinet, modern cloud-native SaaS offerings from large companies like FireEye and Microsoft, as well as products from smaller but highly innovative companies like Exabeam, Gurucul, and Securonix. This indicates that the whole next-gen SIEM market is not yet fully matured, and still offers equal opportunities for success to vendors of any background. Whether looking for a sophisticated solution for a large enterprise or MSSP or a fully managed, easy-to-use SaaS offering, the overall leaders of our rating have you covered.

The rest of the vendors populate the Challenger segment. Please note that their current positioning does not imply any significant shortcomings in their products' capabilities. Rather, they might still be working on getting a more substantial market presence outside of their home region or perhaps simply not innovating enough to keep up with the changing market requirements.

There are no Followers in this rating.

Overall Leaders are (in alphabetical order):

- Exabeam
- FireEye
- Fortinet
- Gurucul
- IBM
- Micro Focus
- Microsoft
- NetWitness (RSA)

- Securonix

2.2 Product Leadership

The first of the three specific Leadership ratings is about **Product** leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services. In the Product Leadership rating, we look specifically for the functional strength of the vendors' solutions, regardless of their current ability to grab a substantial market share.

Among the product leaders, we can find the usual suspects - the large, well-established SIEM vendors that have been continuously expanding and improving their solutions for over a decade, including IBM, Micro Focus and NetWitness (RSA) - as well as equally large companies like Microsoft and FireEye, which joined the SIEM market much later, offering SaaS-based solutions natively designed for the cloud.

However, we can also observe several much smaller vendors among the leaders, which nevertheless are able to offer their solutions with comprehensive capabilities, flexible deployment options and lower operational complexity than the market giants. These include Exabeam with a highly modular general-purpose security management platform, Gurucul - one of the pioneers in behavior analytics technology powered by AI, and Securonix offering an integrated but extensible security operations and analytics platform.

The rest of the vendors populate the Challengers segment. Some, like ManageEngine, are established solution providers with broad portfolios of cybersecurity products and beyond, yet SIEM technology is not their strategic focus. Others are focusing on specific subsets of security analytics tools and are yet to expand their solutions to provide a uniform coverage of all capabilities we're focusing on in this report.

However, there are no Followers in the product leadership rating, which corresponds to the fair degree of maturity of the market segment compared to some of the more modern approaches to security analytics.



Figure 2: The Product Leaders in the Intelligent SIEM Platforms market

Product Leaders (in alphabetical order):

- Exabeam
- FireEye
- Fortinet
- Gurucul

- IBM
- Micro Focus
- Microsoft
- NetWitness (RSA)
- Securonix

2.3 Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements.

Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

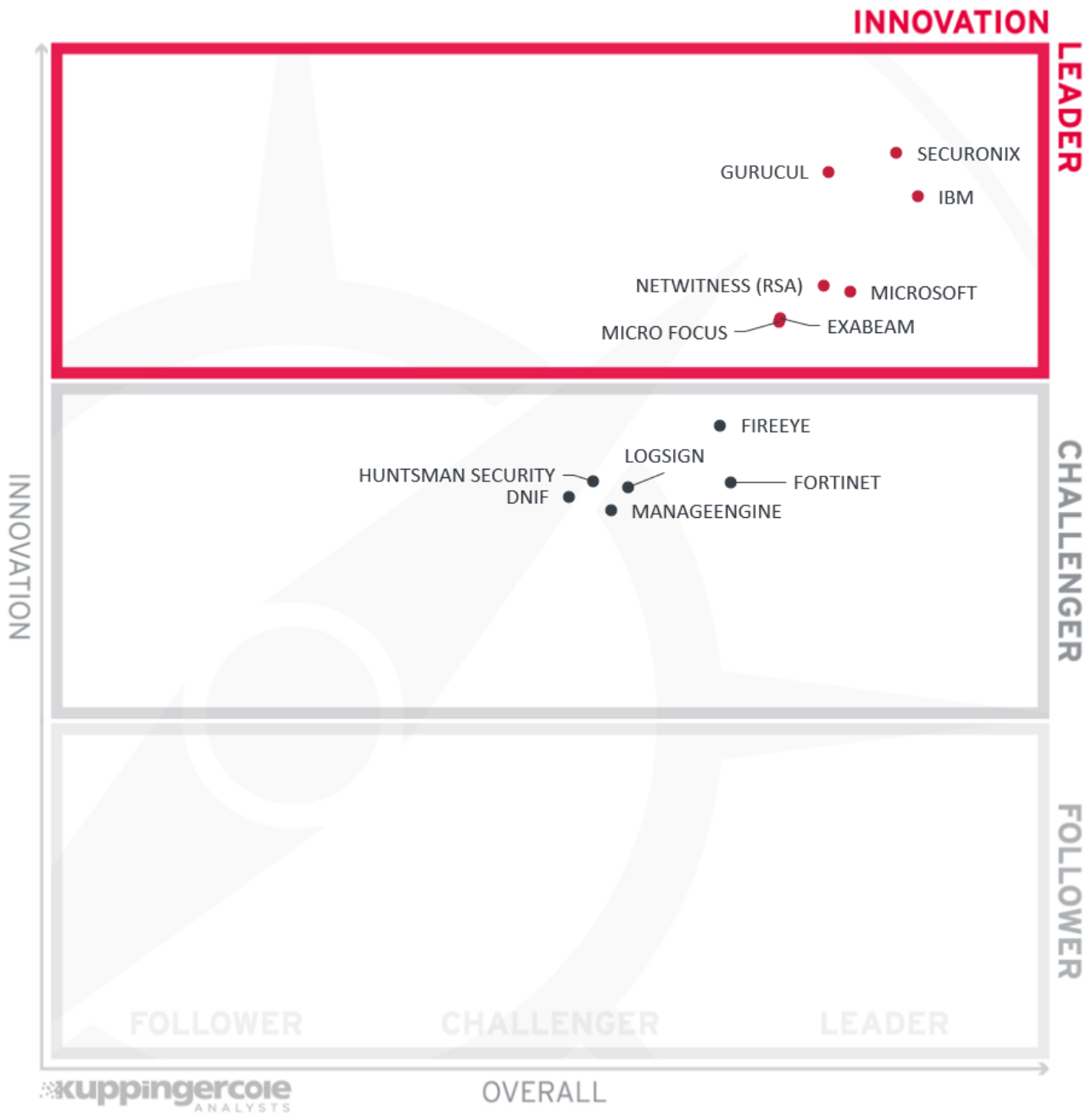


Figure 3: The Innovation Leaders in the Intelligent SIEM Platforms market

Our Innovation Leadership rating presents an interesting mix of both large and small vendors, indicating that the market still has potential for continued innovation even without massive R&D budgets and teams that only large companies can afford.

Veteran SIEM vendors like IBM, Micro Focus and NetWitness (RSA) continue to expand and improve their existing platforms by incorporating new capabilities (machine learning and cognitive technologies, security orchestration and automation, incident response, etc.) while other vendors, not having to deal with a substantial technical debt of "legacy architectures" can focus on improving scalability, performance and

usability of their tools.

Innovation Leaders (in alphabetical order):

- Exabeam
- Gurukul
- IBM
- Micro Focus
- Microsoft
- NetWitness (RSA)
- Securonix

2.4 Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, the size of deployments and services, the size and geography of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

Again, there is no surprise that all large veteran players can be found among the market leaders, including the likes of Microsoft and IBM, FireEye, Fortinet, Micro Focus, and NetWitness (RSA) -- all these vendors have massive worldwide presence and offer broad product portfolios beyond just SIEM solutions.

However, smaller and more specialized vendors like Exabeam and Securonix have also joined the Leaders segment. Despite having much smaller overall financial strength, they still have substantial customer bases in the SIEM market segment, even topping some of their much bigger competitors.

The rest of the vendors can be found in the Challengers segment: they are yet to reach the level of brand recognition and global market presence needed to join the leaders. Some of these companies are still primarily present in their home markets (like DNIF in India), for some, SIEM solutions only represent a small part of the overall portfolio (like ManageEngine with nearly 200 various software products), while others are still in their growth phase.

We have no Followers in the market leadership rating for intelligent SIEM solutions as well.

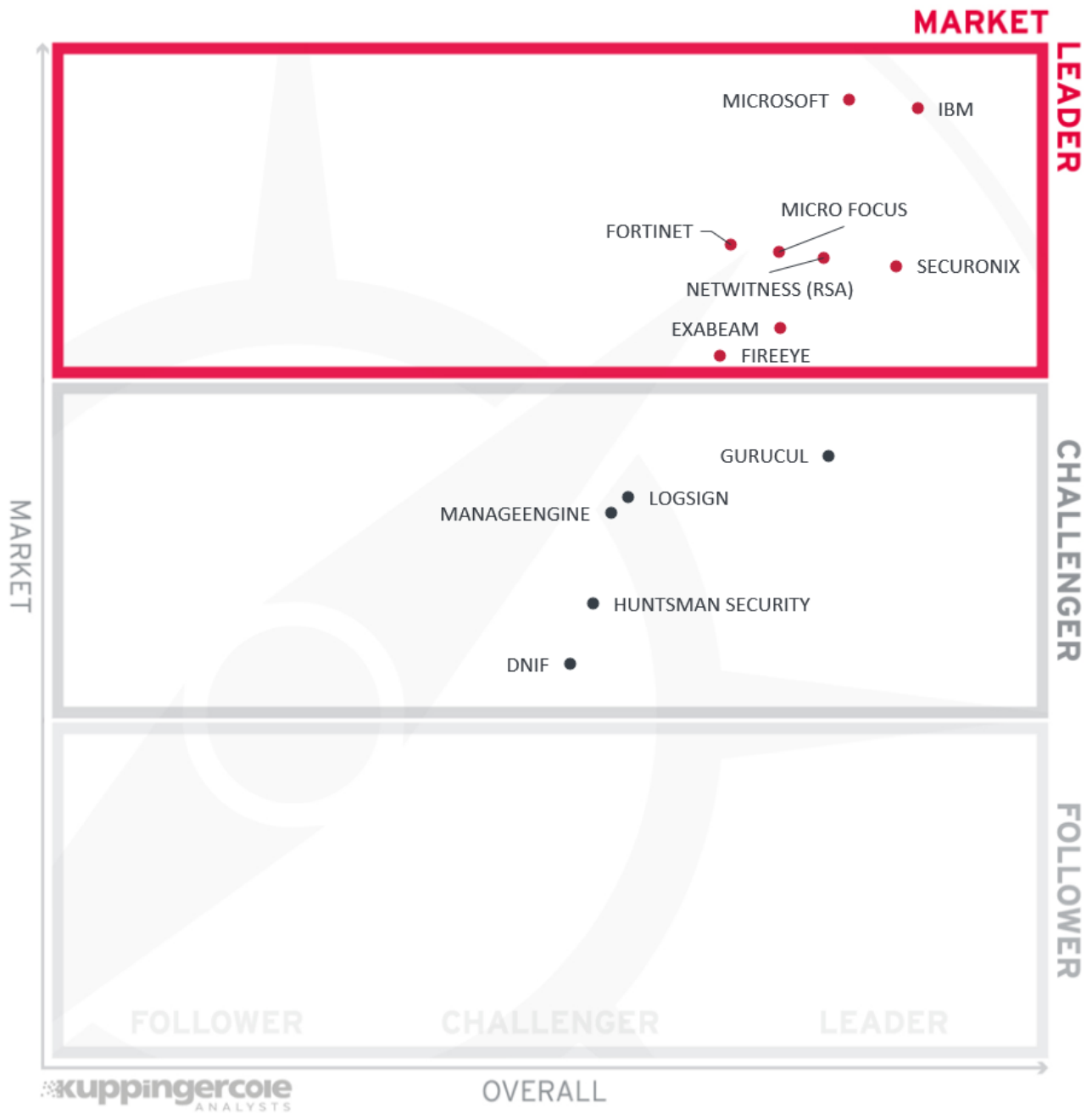


Figure 4: The Market Leaders in the Intelligent SIEM Platforms market

Market Leaders (in alphabetical order):

- Exabeam
- FireEye
- Fortinet
- IBM

- Micro Focus
- Microsoft
- NetWitness (RSA)
- Securonix

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.

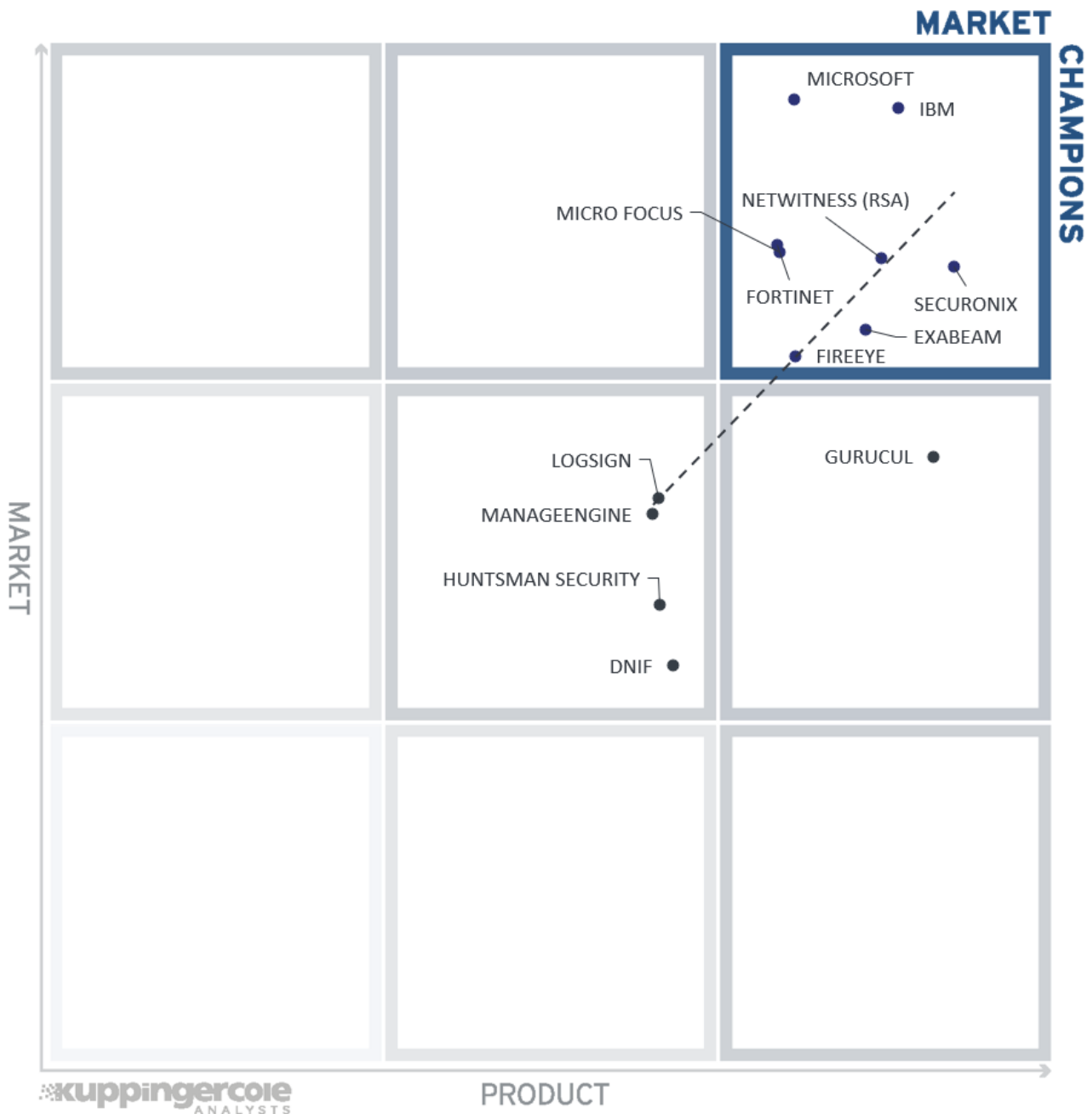


Figure 5: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership. All the vendors below the line are currently underperforming in terms of market share. However, we believe that each has a chance for significant growth.

In the Market Champions box, we observe most market leaders mentioned earlier - Microsoft and IBM, Micro Focus and NetWitness (RSA), as well as Securonix, Exabeam and FireEye. The only vendor that slipped into the top middle box is Fortinet, indicating that their strong market presence is owed to an extent

to other products from their portfolio.

Gurukul is the only vendor in the right middle box, indicating that their strong product capabilities are yet to win them substantial market share - a "hidden gem" of sorts.

The rest of the vendors can be found in the middle box, indicating average results both in product and market leadership - they clearly have the potential for future improvement.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we can see that the overall correlation between the product and innovation ratings is far from perfect, with many vendors appearing away from the dotted line. This is a strong indicator that the market continues to evolve, with different vendors favoring different functional areas and thus making their direct comparison somewhat complicated.

Among the Technology leaders we again observe a mix of large and small vendors, indicating that despite the traditional view of SIEM platforms as tools for large enterprises, one does not have to be one to be able to offer a capable and innovative product in this market.

The only vendor in the top middle box is FireEye, indicating that it is possible to deliver a functionally impressive SIEM platform even without implementing highly innovative "killer features". In fact, the absence of any vendors in the middle right box shows that, as opposed to many other, more modern market segments, it is impossible to develop a capable SIEM product based on killer features alone.

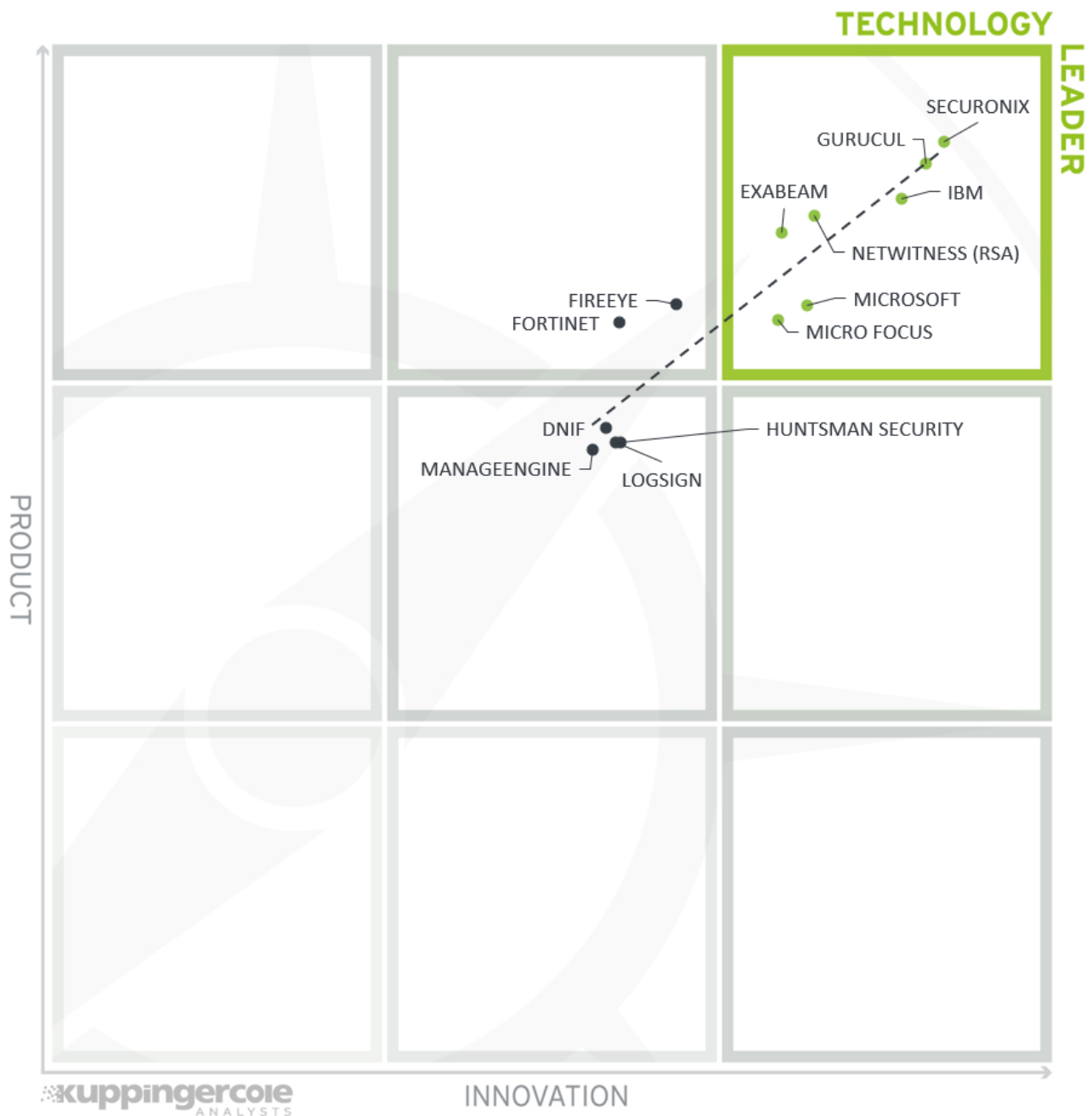


Figure 6: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, highly innovative vendors have a good chance of improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.



Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate while having less market share, and thus the biggest potential for improving their market position.

Once again, we can find all the usual suspects among the Big Ones, including Microsoft and IBM, Micro Focus and NetWitness (RSA), as well as Exabeam and Securonix. Gurucul appears in the middle right box, indicating their strong innovation rate that is yet to convert into market presence, while Fortinet and FireEye occupy the top middle box, demonstrating the opposite end of the spectrum.

The rest of the vendors can be found in the middle box, showing average innovation and market results.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other.

These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Interoperability	Usability	Deployment	
DNIF						
Exabeam						
FireEye						
Fortinet						
Gurukul						
Huntsman Security						
IBM						
Logsign						
ManageEngine						
Micro Focus						
Microsoft						
NetWitness (RSA)						
Securonix						
Legend		critical	weak	neutral	positive	strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, in Table 2 we provide an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
DNIF	●	●	●	●
Exabeam	●	●	●	●
FireEye	●	●	●	●
Fortinet	●	●	●	●
Gurukul	●	●	●	●
Huntsman Security	●	●	●	●
IBM	●	●	●	●
Logsign	●	●	●	●
ManageEngine	●	●	●	●
Micro Focus	●	●	●	●
Microsoft	●	●	●	●
NetWitness (RSA)	●	●	●	●
Securonix	●	●	●	●
Legend	● critical	● weak	● neutral	● positive
				● strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For intelligent SIEM platforms, we look at the following categories:

- **Data Collection** - collection and efficient storage of security events from various sources using Big Data technologies is the original and primary goal of SIEM solutions. This includes parsing system, application, service, or device logs in various formats; capturing and analyzing network traffic information; collecting security data directly from endpoints using agent-based or agentless methods; as well as integrating with cloud services and other third-party sources.
- **Correlation and Enrichment** - identifying relationships between data from various sources in real-time using statistical algorithms and machine learning methods; adding business context information collected from other enterprise IT systems as well as incorporating threat intelligence from external feeds.
- **Threat Detection** - detecting patterns and anomalies in security data beyond the traditional rule-based approach. We expect modern intelligent SIEM solutions to be able to remove the statistical noise and reduce false positives without human intervention, by relying on techniques like behavior analysis or machine learning. Identifying security incidents across multiple events, assigning risk scores according to threat models and other methods of improving analyst productivity will lead to higher ratings.
- **Forensic Investigation** - providing on-demand access to all source and contextual security information relevant for an incident or proactive threat hunting; ability to pivot to related events or entities; automated forensic analysis supported with workflows, policies, and risk models tailored to specific industries or markets.
- **Incident Response** - built-in or closely integrated capabilities to initiate and orchestrate incident response process. Even though we cover specialized SOAR solutions in a separate Leadership

Compass, platforms that include these capabilities directly or through partnerships with third-party vendors get more favorable ratings.

- **Intelligence and Automation** - the primary advantage of next-gen intelligent SIEM platforms over traditional rule-based solutions is their ability to address the analyst fatigue and skills shortage through the high degree of intelligent automation. They should not require a team of trained security experts to operate, relying instead on actionable alerts, automated workflows, and ideally provide a complete end-to-end solution for a security operation center.
- **Compliance** - addressing regulatory compliance requirements is one of the primary use cases for modern SIEM solutions. Long-term security data retention, normalization and correlation across multiple IT systems, and rich visualization and reporting capabilities make SIEMs ideal tools for compliance audit and reporting. Solutions that provide out-of-the-box support for major regulatory frameworks will receive high ratings here.
- **Performance and Scalability** - modern SIEM platform must be able to keep up with the increasing number of systems and growing volumes of security telemetry, adapt to complex, distributed, large-scale deployment scenarios, and, of course, provide native support for cloud and hybrid scenarios.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some products may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations -- for example, for powering enterprise-grade security operations centers.

5.1 DNIF

DNIF is a security analytics vendor established in 2002 and based in Mumbai, India. Before 2017, the company operated in the managed detection and response business, gradually developing its own data analytics technology to power it. In 2017, the company has introduced DNIF HyperScale SIEM -- an integrated platform that's engineered to run security operations at a massive scale, suitable for large enterprises and MSSPs.

DNIF's solution combines SIEM, behavior analytics, orchestration, automation, and response capabilities in a single platform that's easy to deploy and operate without involving a team of engineers but is ready to deal with the petabyte-scale data collection to ensure complete coverage and full visibility into your company's security posture.

DNIF HyperScale SIEM has been specifically designed to democratize access to highly scalable security analytics capabilities even for companies lacking expertise and budget to operate a traditional enterprise SIEM and to ensure that organizations do not have to sacrifice security coverage to reduce operational costs. The underlying data lake has been designed from scratch for scale and performance and the SIEM platform offers integrated capabilities of traditional SIEM, UEBA, and SOAR solutions that can run on commodity hardware, has a flat learning curve and offers a large number of out-of-the-box content. The company also offers the platform as a fully managed service.

A major appeal of DNIF's solution is its substantially lower total cost of ownership compared to most other products in this market: this is especially valuable for companies with large-scale security operations. Several factors contribute to this: first of all, the platform's architecture allows it to ingest and process massive amounts of security data with an extreme compression ratio. Second, DNIF's licensing policy places no caps on the volume of stored data or the number of processed events per second, ensuring predictable, low operational costs. Finally, a free but unsupported Community Edition of the platform is available, with all functions unlocked.

Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ○
Deployment	● ● ● ● ●

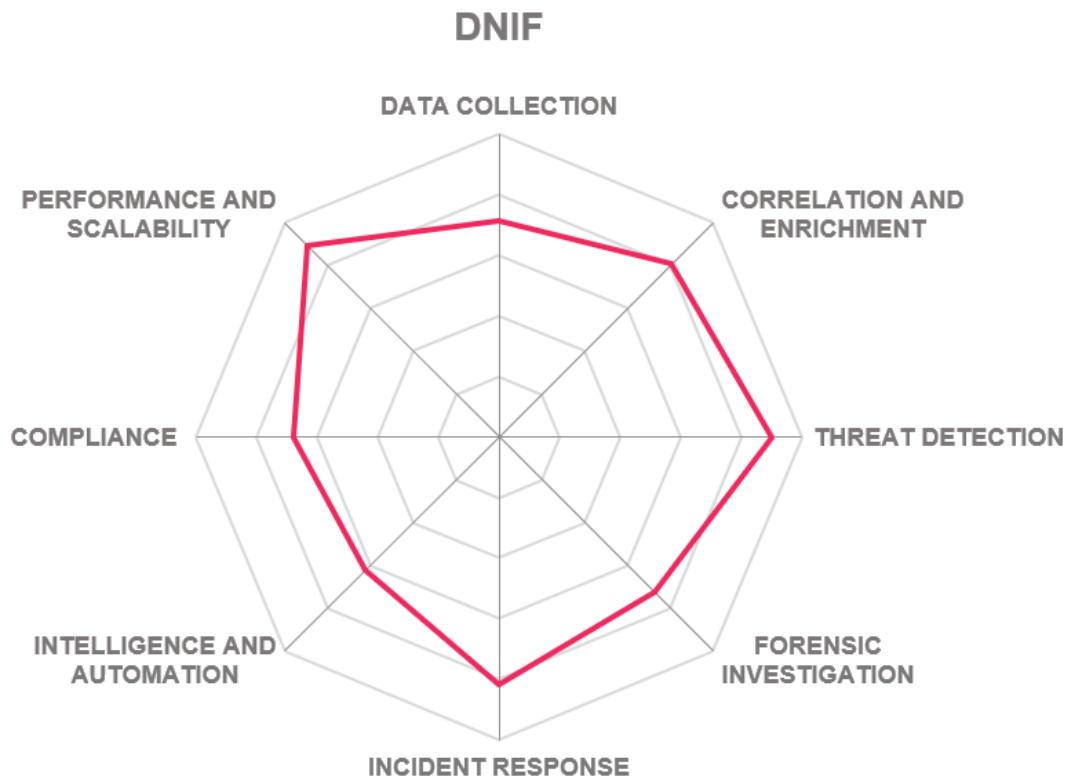


Strengths

- Architecture designed for petabyte-scale data collection and processing on commodity hardware
- Fully integrated, multi-tenant SIEM + UEBA + SOAR platform
- Uncapped device licensing model for unlimited storage and throughput
- Feature-complete Community Edition available at no cost

Challenges

- Very limited but growing market presence outside of India
- Capabilities beyond core SIEM are still fairly basic, planned for future releases
- Targeted primarily at large enterprise customers, might not be economical for small companies



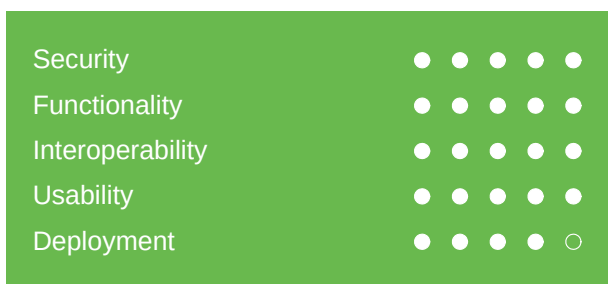
5.2 Exabeam

Exabeam is a privately-owned security analytics solution vendor headquartered in Foster City, CA. Founded in 2013 by a group of cybersecurity veterans from companies like Imperva, ArcSight, and Sumo Logic, the company's been focused on developing a smarter alternative to traditional SIEM platforms.

From its beginnings as a user and entity behavior analytics (UEBA) add-on to existing SIEMs, Exabeam has quickly evolved into a full-scale yet highly modular general-purpose security management platform, which can either completely replace an existing SIEM deployment or allow the customers to mix and match individual modules with 3rd party SIEM or SOAR products.

Exabeam Fusion is the latest incarnation of the company's unified security management platform. It combines the capabilities of SIEM and XDR solutions in a single architecture that's flexible and modular to support diverse use cases. Exabeam Fusion SIEM is essentially an amalgamation of the company's open XDR platform that provides threat detection, investigation, and response capabilities powered by behavior analytics and forensic automation and "traditional" SIEM functions like centralized storage for security data and compliance reporting. The company promotes a use-case-centric approach towards threat investigations by offering individual prepackaged content for different scenarios: external threats, compromised insiders, and malicious insiders.

Exabeam platform's modularity and flexibility make it particularly convenient for any company that's either looking for more intelligent and automated capabilities to augment their existing SIEM platform or to replace it completely without resorting to the "Rip and Replace" approach. Customers can mix and match individual modules for managing security information, advanced analytics, incident management, or threat hunting by integrating them with traditional SIEM platforms, case management systems, and other security tools and, as their requirements change over time, expand the coverage, eventually making Exabeam the central platform for their corporate SOCs.



Strengths

- Unified architecture that combines SIEM and XDR capabilities in a flexible, modular platform
- Supports on-prem, SaaS, or hybrid deployment scenarios
- Intelligent incident timelines powered by behavior analytics improve analyst productivity
- Integration of MITRE ATT&CK framework simplifies threat hunting and incident analysis, supports decision making

Challenges

- Market presence is overwhelmingly USA-centric
- Playbook automation is based on an OEM technology from a third-party vendor
- Collaboration tools in the platform are still quite limited, under active development

Leader in



EXABEAM



5.3 FireEye

FireEye is a cybersecurity vendor headquartered in Milpitas, California, USA. Founded in 2004, the company started with email and web sandboxing tools, but through growth and acquisitions they have added a wide range of cybersecurity products to their portfolio, including network, endpoint, and cloud security solutions, threat intelligence services, as well as FireEye Helix, a security operations platform.

For nearly a decade, the threat intelligence vendor Mandiant operated as a subsidiary of FireEye. In October 2021, McAfee Enterprise and FireEye announced that Symphony Technology Group (STG) had closed its sponsored acquisition of FireEye in an all-cash transaction totaling \$1.2 billion. This transaction completes the combination of McAfee Enterprise with FireEye. Mandiant and the combined McAfee Enterprise and FireEye company will continue to support customers post-closing with a joint reseller relationship, shared product telemetry and frontline threat intelligence.

Helix Security Platform is a unified SaaS security operations platform that allows organizations to take control of any incident from detection to response. It combines XDR and SOAR capabilities with real-time threat intelligence to augment, unify and simplify operations of multiple security products, including FireEye's own endpoint, network, email, and cloud security solutions, as well as over 600 third party tools via supported integrations. Helix Detect, the most recent addition to the platform, is a specialized lightweight edition of the platform targeted towards low midmarket customers.

Available standalone or with the purchase of other FireEye's products, Helix serves as an integration point and a unified console to provide consistent visibility across multiple security tools and offers comprehensive next-gen SIEM capabilities along with security orchestration and threat intelligence. This approach ensures that the platform can be adopted extremely quickly without additional deployment efforts while enabling a future upgrade path for customers with a broad selection of on-prem and cloud integrations.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○



Strengths

- An integrated security operations platform combining XDR, SOAR, CTI capabilities with a next-gen SIEM
- Unified visibility and management across all FireEye security products
- Over 600 available integrations with third-party products
- A large number of curated analytics rules, updated daily
- Comprehensive support for MITRE ATT&CK framework

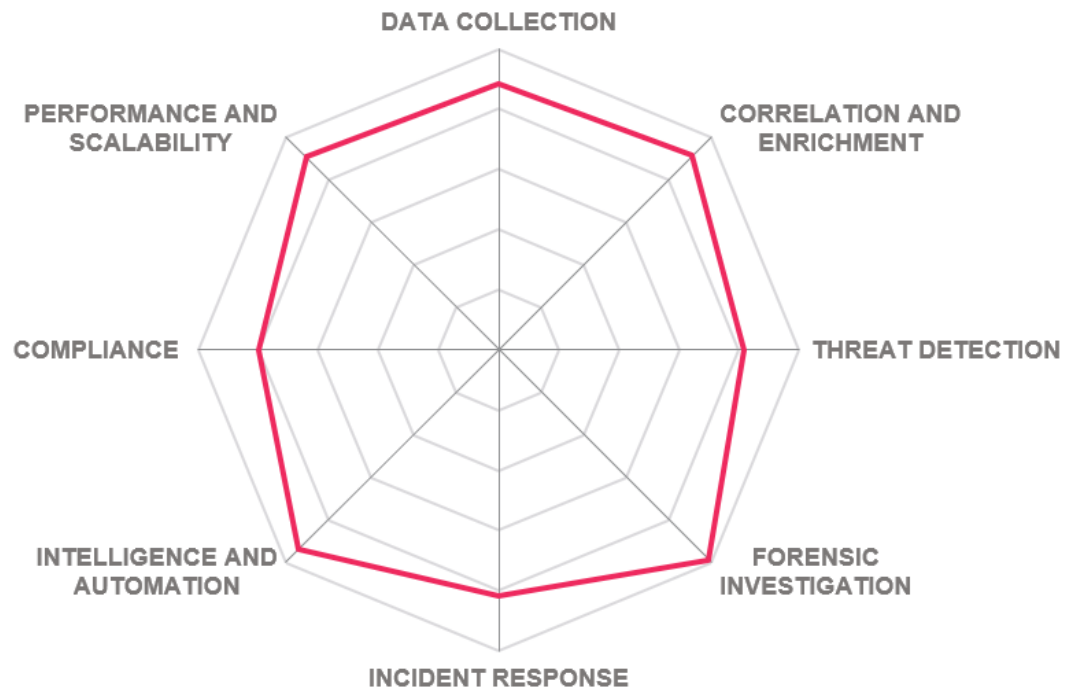
Challenges

- Available exclusively as a SaaS offering
- Decision support automation limited to tips and suggestions
- Future uncertainty regarding CTI services after separation from Mandiant

Leader in



FIREEYE



5.4 Fortinet

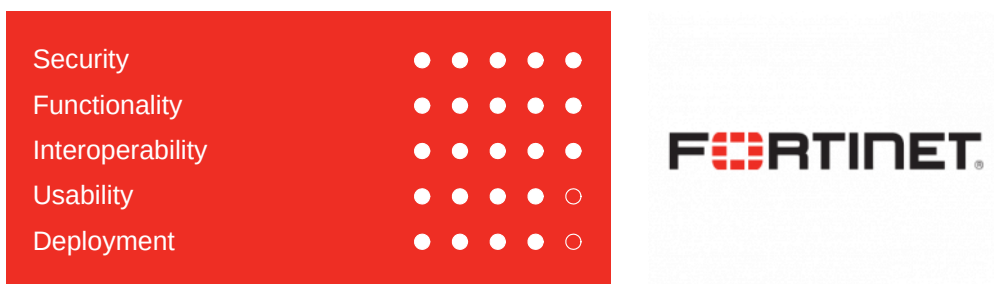
Fortinet is an American cybersecurity company with headquarters in Sunnyvale, California, USA. Established in 2000, it provides a wide range of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centers, enterprises, and distributed offices. Its solutions are integrated into the Fortinet Security Fabric.

As a part of its security operations portfolio, Fortinet offers a number of solutions that cover SIEM, SOAR and XDR capabilities, as well as more specialized tools for advanced security analytics and automation.

FortiSIEM is the company's security management solution that combines SIEM capabilities with user and entity behavior analytics (UEBA). It brings together visibility, correlation, and remediation for cyberthreats. Fortinet's Security Fabric concept ensures that the platform has access to various data sources beyond just security telemetry, enabling it to cross-correlate between analytics usually maintained in separate network and security operations centers in a single place.

Just like many other Fortinet's products, it is offered in the appliance form factor, either as hardware appliances or virtual machines for on-prem or public cloud deployment. To augment its capabilities, FortiSIEM supports multiple integrations with other products, both from Fortinet itself, as well as external security platforms, threat intelligence feeds, identity providers, and even data lakes.

Thanks to its form factor, integrated capabilities, and a broad range of out-of-the-box content, FortiSIEM enables quick deployment even for companies lacking the required operational expertise yet is able to offer a flexible upgrade path to support even the largest and most complex architectures for demanding enterprise customers.



Strengths

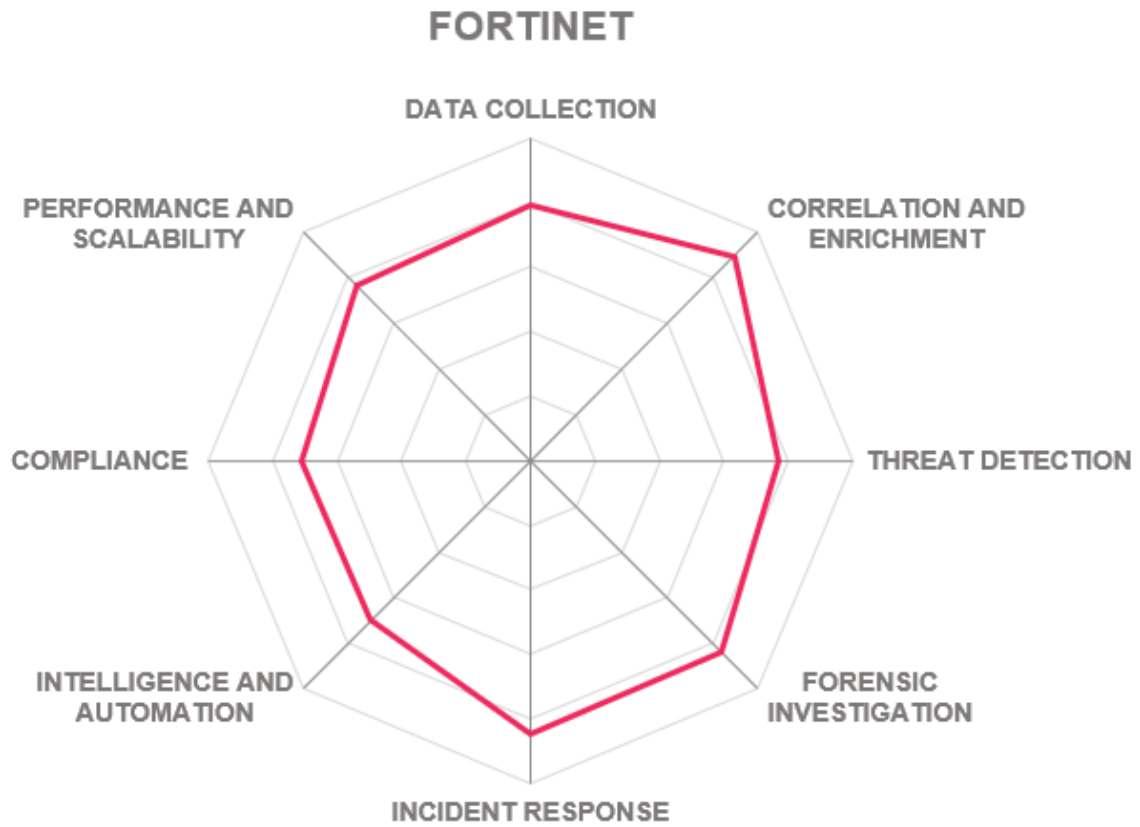
- Supports cross-correlation between network and security analytics
- Direct integrations with other Fortinet security tools
- Flexible, scalable deployment: supports hybrid complex architectures, MSSP-ready
- Asset management and monitoring with a built-in CMDB (or a 3rd party integration)
- A large number of out-of-the-box content to reduce time to value

Challenges

- Not available as SaaS, only as a managed solution hosted by an MSSP
- Built-in remediation functions are quite limited, require FortiSOAR for advanced use cases
- Dated, overloaded UI

Leader in





5.5 Gurukul

Gurukul is a privately held software vendor headquartered in El Segundo, California, USA. Founded in 2010, the company provides a range of security, identity, and fraud analytics solutions and services unified into a single Security and Risk Analytics platform.

One of the pioneers of behavior analytics technology powered by machine learning, Gurukul is able to offer a universal enterprise risk analytics solution that is agnostic both to specific business applications and underlying big data platforms. On this foundation, the company offers a broad portfolio of products ranging from SIEM, UEBA, and XDR to fraud prevention and even Zero Trust security.

Gurukul Analytics-Driven SIEM is a versatile next-generation SIEM platform powered by the company's Risk Analytics platform. Gurukul's vendor-agnostic approach towards data collection and management allows the company to design a SIEM solution that can offer much more sophisticated and configurable analytics without the technical debt of legacy platforms. In fact, Gurukul was among the first vendors to design a SIEM solution entirely with real-time ML-powered security analytics based on a uniform entity model, dynamic risk scores and detection models completely customizable with a provided Gurukul STUDIO tool.

On top of this foundation, Gurukul provides a full set of threat detection, forensic investigation, and incident response capabilities in an integrated, yet modular offering. With an impressive range of built-in content - ingestion pipelines, dashboards, reports, threat models, etc. - Gurukul is nevertheless able to offer an unprecedented level of flexibility in deployment and customization of its platform for any customer.

The company's biggest challenge is perhaps to find the way of establishing a more prominent presence for itself in the SIEM market - until now it remains relatively unknown, especially outside the US.

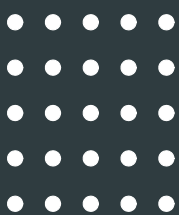
Security

Functionality

Interoperability

Usability

Deployment



GURUCUL

Strengths

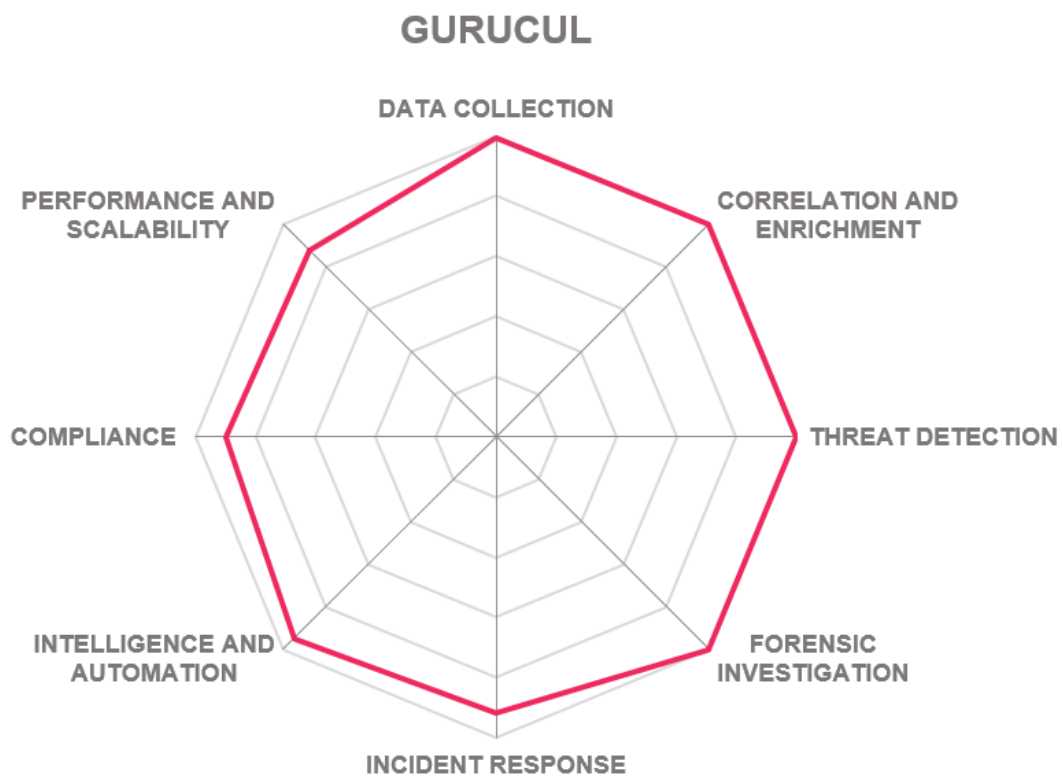
- Universal risk analytics engine for multiple use cases: network, identity, fraud, etc.
- Vector-agnostic data lake and data pipelines architecture
- A broad range of deployment options: on-prem, hybrid, all major clouds
- Gurucul STUDIO for designing and tuning own analytics models
- Individual capabilities available as optional modules according to customer needs

Challenges

- Recognition as a SIEM vendor is still low, needs more time to improve
- Licensing model with multiple add-on modules might be confusing for some users

Leader in





5.6 Huntsman Security

Huntsman Security is a privately owned cyber security software company based in Sydney, Australia. Founded in 1999, the company has additional offices in Great Britain, Japan, and the Philippines. Huntsman Security's customer base comprises government agencies and other public sector companies, as well as critical infrastructure, telecommunications, and managed security service providers.

The company's security portfolio is focused on security monitoring and vulnerability reporting capabilities, offering an integrated threat detection and security analytics platform with integrated SOAR capabilities and compliance reporting, primarily targeted at governments, large enterprises, and MSSPs.

Huntsman Enterprise SIEM is a cybersecurity analytics platform designed to provide a complete threat detection, incident management, and actionable reporting system. It combines the capabilities of a SIEM (collection, correlation, and analysis of activity, system, and network data with compliance reporting) and behavioral anomaly detection to identify unknown threats or suspicious activities. In addition, it includes an optional add-on with security orchestration and automation functions to support rapid decision-making during threat investigation and remediation workflows.

Designed with a strong focus on large enterprises and government agencies, the solution incorporates multiple functions to streamline SOC operations, supporting large teams working in shifts. Multi-tenant architecture and flexible licensing simplify deployment and operations for managed security service providers.

Together with Huntsman Security's solution for policy compliance and vulnerability management, the company's SIEM platform can provide a complete foundation for an enterprise-grade security operations center, both for on-prem or managed deployment. The platform is favored by government agencies, large enterprises, and service providers for its fully multitenant architecture and the ability to accommodate extremely high event throughputs.

Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○



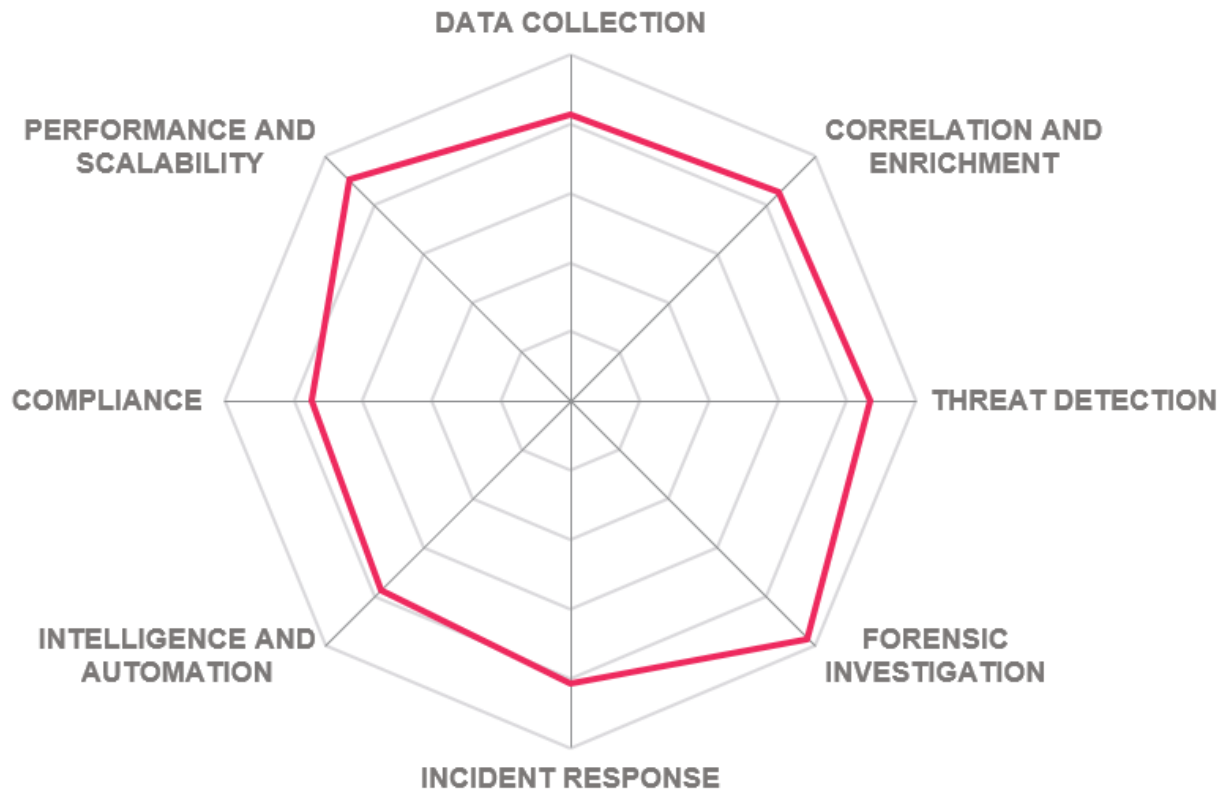
Strengths

- Platform designed for governments, large enterprises, and MSSP deployments
- Incorporates XDR and SOAR capabilities
- Broad support for cloud connectors to monitor cloud and SaaS environments
- Native visual app for high-performance threat investigations
- Real-time MITRE ATT&CK heatmap to identify ongoing attacks

Challenges

- Not available as SaaS, only as a managed deployment
- Limited market presence outside of the APAC and EMEA regions
- Multiple standalone UIs for different management aspects

HUNTSMAN SECURITY



5.7 IBM

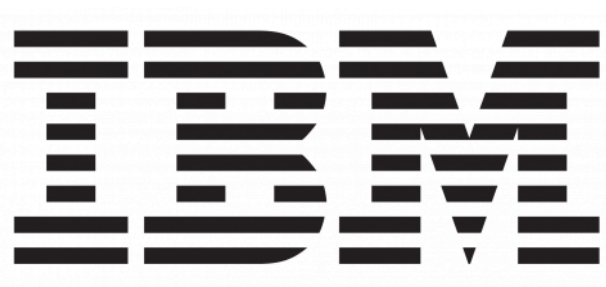
IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. With over 100 years of history, IBM has evolved from a computing hardware manufacturer towards offering a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and, of course, information security.

The company's security solutions portfolio is built around the integrated security analytics platform known as QRadar. Originally conceived as a traditional network security tool, QRadar has evolved into a full-featured security intelligence solution that does not just provide visibility into security events, but eliminates false positives, delivers actionable insights, and helps to identify, investigate, and mitigate the riskiest threats as quickly as possible.

IBM Security QRadar is an integrated security intelligence platform that unifies log management, SIEM, UEBA, NTA, and SOAR capabilities. A result of nearly 20 years of evolution, the platform has grown into a massive open technology ecosystem with hundreds of available 3rd party integrations. QRadar itself ships with hundreds of pre-built security use cases and other apps and content packs. The QRadar Use Case Manager (UCM) is specifically designed to help simplify the deployment and management of analytics. UCM enables users to visualize their detection coverage for each MITRE ATT&CK technique based on the data sources collected and the analytics that are deployed.

The multitude of capabilities and functions included in the platform cover every stage of the threat detection, investigation, and response process. Advanced cognitive technologies provided by IBM Watson AI provide dramatic improvements in analyst productivity and enable quick response to cyberthreats. IBM's ongoing initiative to incorporate QRadar into the Cloud Pak for Security platform ensures that the company's SIEM solution remains relevant and modernized 15 years after its initial launch.

Security	●	●	●	●	●
Functionality	●	●	●	●	●
Interoperability	●	●	●	●	●
Usability	●	●	●	●	●
Deployment	●	●	●	●	○



Strengths

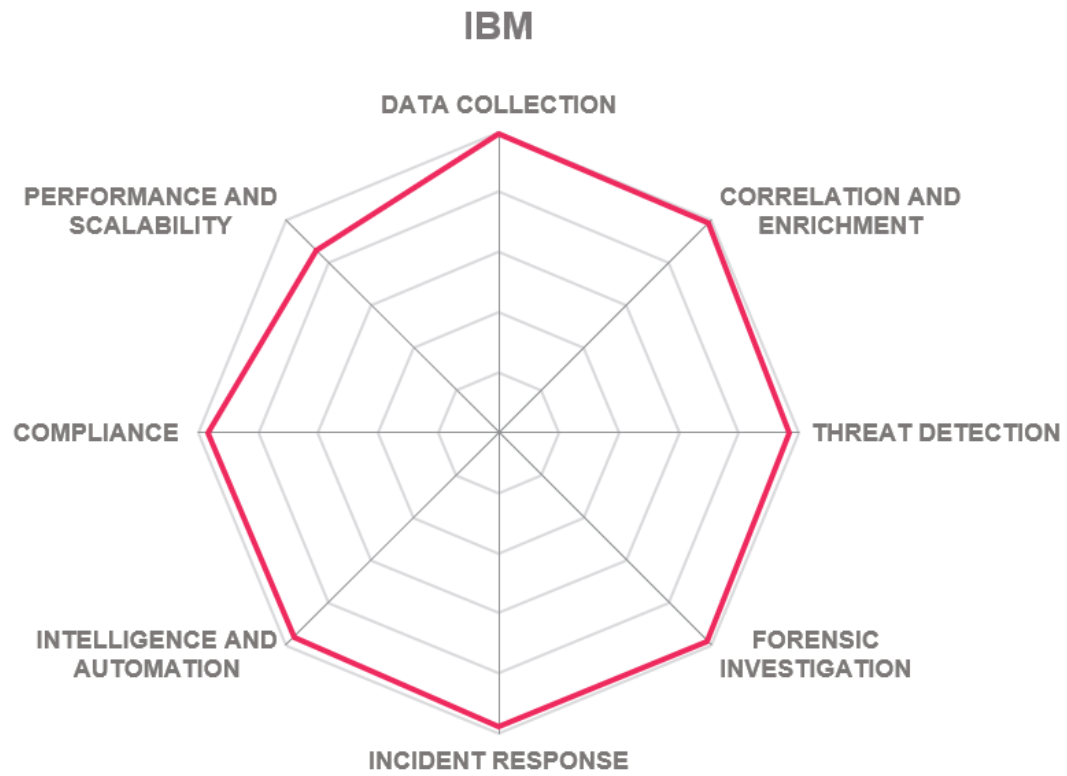
- A completely integrated platform covering all aspects of security analytics, automation, and response
- Massive technology ecosystem with hundreds of available integrations
- Tight integration with the X-Force threat intelligence platform
- IBM's cognitive technologies to augment investigations and remediations
- Use Case Manager to simplify deployment and management of analytics

Challenges

- The ongoing migration to the Cloud Pak for Security platform might introduce additional challenges
- A complicated licensing model can make contract planning difficult for some organizations
- Lack of consistent UI across different modules

Leader in





5.8 Logsign

Logsign is a software company focusing on the development of automation-driven cybersecurity solutions, specializing in security data collection, intelligence, and management. Established in 2010, the company has its origins in Istanbul, Turkey but is now headquartered the Hague, Netherlands with an additional office in San Francisco, California, USA.

Logsign's primary products are next-generation SIEM and SOAR solutions, augmented by an integrated threat intelligence service with 40+ feeds. Based on this technology platform, the company offers a range of co-managed security services as well as a network of MSSPs.

Logsign SIEM provides full visibility and control of all security telemetry across on-prem and cloud sources by allowing analysts to collect and store unlimited data, detect and investigate threats, and respond quickly. The company places a strong emphasis on quick and easy deployment and onboarding by providing a large number of built-in integrations and a free plugin service for automatic parsing of unstructured data.

To automate incident investigation and remediation, Logsign has recently expanded into the security orchestration, automation, and response market as well, offering a separate SOAR product that complements their existing SIEM offering. Without it, Logsign SIEM offers basic notification and remediation functions.

Logsign's security data lake is powered by Lucene search, providing quick and convenient access to any stored event, facilitating threat hunting with real-time data enrichment. By adding business context and threat intelligence to search results on the fly, the product helps analysts to work more productively. Hundreds of built-in alerts, dashboards and reports provide full visibility into the current and historical security posture; access to individual visualizations can be limited by a role or location.

For a relatively small company, Logsign offers a surprisingly feature-complete security analytics solution, which is nevertheless very quick and easy to deploy and operate. With its affordable pricing, it can be especially recommended for smaller organizations.

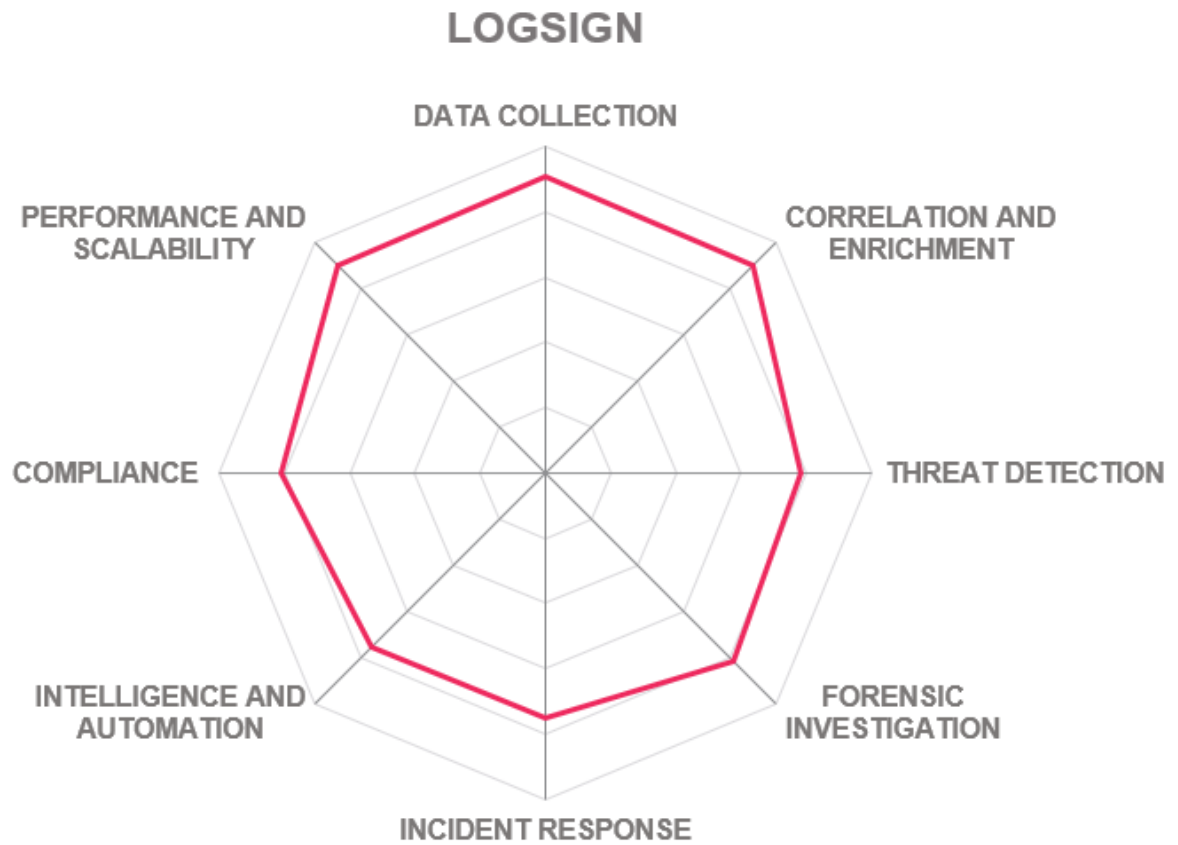
Security	●	●	●	●	○
Functionality	●	●	●	●	○
Interoperability	●	●	●	●	●
Usability	●	●	●	●	●
Deployment	●	●	●	●	○

Strengths

- Cluster architecture with unlimited scalability and high availability
- Unlimited log collection and usage
- 400+ built-in integration with a free unstructured data parsing service
- Clean, highly visual, easy to use UI
- Flexible and affordable pricing model

Challenges

- Not yet available as a SaaS offering
- Small but growing presence outside of the EMEA region
- Range of automation capabilities is limited without a separate SOAR product



5.9 ManageEngine

ManageEngine is the enterprise software division of Zoho Corporation, an international software development company. Founded in 1996, Zoho Corporation currently offers hundreds of applications to over 50 million customers worldwide. ManageEngine offers solutions for different markets including IT service and IT operations management, with IT security remaining a strong priority since the initial years.

Headquartered in Pleasanton, California, USA with development and operations happening out of Chennai, India, ManageEngine provides over 180,000 customers around the world with over 100 solutions for managing IT operations for endpoints, servers, networks, and the cloud, as well as security tools for desktops and mobile devices.

ManageEngine Log360 is an integrated solution for log management and network security monitoring. In a fashion that reflects the company's design philosophy, Log360 is in fact not a single product, but a suite of multiple specialized tools integrated into a single management console and covered by a flexible licensing policy. Positioned by the vendor as a SIEM solution, Log360 might not reach full feature parity with enterprise-grade SIEM products from market-leading vendors, but where it lacks in "traditional" SIEM capabilities, it can compensate by providing a multitude of additional security and compliance features.

In a way, the product defies classification. It incorporates so many additional capabilities for both proactive and reactive analysis of an organization's security posture across all layers of its IT infrastructure, that it can just as easily be classified as an Endpoint Detection and Response (EDR), Data Loss Prevention (DLP) or even a SOAR product. Where Log360 lacks in certain functions compared to dedicated enterprise SIEM or SOAR solutions, it compensates with a broad range of additional (and very useful) security and compliance features, which are incorporated into a convenient unified management console with impressive out-of-the-box reporting capabilities.

Currently ManageEngine is focusing more on its cloud SIEM offering called Log360 Cloud. While Log360 Cloud does not yet have all the features of Log360 on-premises, the company is making efforts to bring feature parity within the next few months.

Security	●	●	●	●	○
Functionality	●	●	●	●	○
Interoperability	●	●	●	○	○
Usability	●	●	●	●	●
Deployment	●	●	●	●	○

ManageEngine

Strengths

- Tightly integrated suite with a single UI and cross-correlation capabilities
- A broad range of supported security event sources, agent-based and agent-less modes, integrations with 3rd party tools
- Incorporates non-event data for improved correlation and risk assessment
- Complements SIEM features with EDR, DLP, SOAR capabilities
- Easy to deploy and operate, affordable and flexible licensing (not volume-based)

Challenges

- Grouping events into attack timelines is largely rudimentary, not on par with next-gen SIEM products
- Workflows primarily focus on remediation (as opposed to modern SOAR products)
- Cloud-based offering still in development, has not yet reached feature parity with the on-prem solution

MANAGEENGINE



5.10 Micro Focus

Micro Focus is a British multinational software company headquartered in Newbury, UK. A large veteran player in the IT market, the company has been offering a broad range of enterprise software products and consulting services since 1976. The company is known for its long history of acquisitions, holding ownership in product lines of such vendors as Attachmate, NetIQ and Novell.

In 2017, Micro Focus completed the spin-merger with the software business of Hewlett Packard Enterprise, which, among other assets, gave it ownership over ArcSight, one of the pioneering security analytics and intelligence platforms. Recently, Micro Focus acquired Intersect and AT&T Labs, integrating their UEBA and SOAR technologies into the ArcSight platform.

The ArcSight brand has existed since 2000, predating even the notion of "SIEM" and essentially making it one of the earliest enterprise security analytics platforms. Going through an uneasy history of acquisitions, ArcSight nevertheless continued to maintain its high level of brand recognition. Currently, the product is a part of CyberRes, a line of business within Micro Focus with one of the largest solution portfolios for cybersecurity and business resiliency.

ArcSight is being actively modernized and expanded to fulfill the strategic vision of the industry's first layered security analytics platform and to reestablish the brand as the market standard it once was considered. Currently it is being offered as a complete end-to-end security operations solution, including SIEM, UEBA, SOAR, and Threat Hunting capabilities, on a unified platform with common storage, a shared data model, and a unified interface.

From the licensing perspective, the platform comprises three base components: Enterprise Security Manager (SIEM), Recon (threat hunting, investigation, and log management) and Intelligence (ML-powered behavior analytics). ArcSight's SOAR solution is included with each of these components for no additional charge. Also included is ArcSight's unifying UI, ArcSight Fusion, which provides a centralized location for the Security Operations Center to monitor activity collected by each ArcSight component (ESM, Recon, and Intelligence).

A strategic modernization program that aims to completely unify all ArcSight components into a single end-to-end security operations platform is currently underway, with higher-level integrations between these components already available.

Security	● ● ● ● ○
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○



Strengths

- Complete unified SecOps platform with a full range of detection, investigation, and response capabilities
- SOAR functionality natively integrated, provided at no extra cost
- Massive library of use cases covered out of the box
- Advanced threat analytics to help analysts with decision support
- Data security and privacy controls for regulatory compliance

Challenges

- Architecture modernization is still work in progress, might lead to inconsistencies in deployment
- Connector library for cloud services is somewhat limited, inconsistent between cloud service providers

Leader in



MICRO FOCUS



5.11 Microsoft

Microsoft is a multinational technology company headquartered in Redmond, Washington, USA. Founded in 1975, it has risen to dominate the personal computer software market with MS-DOS and Microsoft Windows operating systems. Since then, the company has expanded into multiple markets like desktop and server software, consumer electronics and computer hardware, mobile devices, digital services, and, of course, the cloud. Microsoft is the world's largest software company and one of the top corporations by market capitalization.

Microsoft Sentinel, until recently known as Azure Sentinel, is a cloud-native SIEM and SOAR platform that delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Thanks to its multiple native integrations into Azure cloud services, Microsoft's endpoint management and security tools, and threat intelligence, Sentinel offers an unprecedented degree of efficiency and ease of deployment compared to any competing SIEM solution, even the SaaS-based ones. On the other hand, Microsoft offers substantial freedom of customization for the platform, by allowing customers to integrate other Azure services, enabling advanced analytics and threat hunting, own machine learning models, custom automations, external threat intelligence, etc.

Built with Azure Logic Apps, Microsoft Sentinel's automation and orchestration solution provides an extensible architecture that enables scalable automation as new technologies and threats emerge. With over 200 available connectors, Sentinel playbooks can integrate with Azure services, as well as with 3rd party ticketing systems, collaboration platforms, and custom APIs. Although built-in investigation tools are still in preview, customers can use the Azure Synapse platform for advanced analytics and threat hunting. A large user community offers numerous custom resources to extend and augment the platform.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○



Strengths

- Fully managed, cloud-native, massively scalable security analytics platform with UEBA, SOAR capabilities
- Native integrations with Microsoft's endpoint and cloud security tools, threat intelligence
- Custom analytics with Azure Synapse (for threat hunting, etc.)
- Content Hub with over 100 pre-packaged solutions from Microsoft, partners, and community
- Support for data residency regulations

Challenges

- Only available as a SaaS offering in the Azure cloud
- Yet to develop an ecosystem of third-party integrations comparable to leading competitors
- Only volume-based pricing is available

Leader in



MICROSOFT



5.12 NetWitness (RSA)

RSA Security is a computer and network security company headquartered in Bedford, Massachusetts, USA. Founded in 1982 by Ron Rivest, Adi Shamir, and Len Adleman -- the developers of the RSA public-key cryptography algorithm, the company had a complex history of acquisitions. In 2006, RSA was itself acquired by EMC Corporation and since 2016 it was a subsidiary of Dell Technologies. In 2020, the private equity firm STG acquired RSA from Dell and the company once again operates as an independent business, one of the largest cybersecurity and risk management organizations.

Although RSA is perhaps best known for its SecurID identity platform, security analytics represents a major part of its portfolio. RSA NetWitness platform is a SIEM and Open XDR platform that combines visibility, analytics, and automation in a single solution that can power any organization's security operations center. Originally an independent company, NetWitness became part of RSA in 2011.

The NetWitness Platform is a comprehensive threat detection and response product featuring rich data analysis, advanced analytics, incident response, compliance, threat intelligence, and investigation capabilities. It can collect and correlate log, network, endpoint, IoT, and cloud security data into actionable insights to help detect, analyze, and remediate both known and unknown threats.

The platform enables both SIEM and XDR use cases in a combined solution that RSA calls "Evolved SIEM", implementing major capabilities usually found in EDR, NDR, UEBA, SOAR, and CTI products. These cover both detecting anomalies and malicious activities with the help of machine learning and threat intelligence across different IT environments, as well as orchestration and workflow management for forensic investigation and incident response.

As a highly integrated and unified platform, NetWitness is a solution best suited for large enterprises looking for a security operations solution from a single vendor. Despite potential challenges with initial deployment, the platform is able to deliver true end-to-end detection, investigation, and response coverage across endpoints, networks, and the cloud.

Security	●	●	●	●	●
Functionality	●	●	●	●	●
Interoperability	●	●	●	●	●
Usability	●	●	●	●	○
Deployment	●	●	●	●	○



Strengths

- Integrated platform for log, network, endpoint, cloud, and IoT security analytics and automation
- Flexible deployment models (including multiple hybrid options)
- Advanced security insights by correlating network, endpoint, and log events accelerate investigations
- Data sovereignty and data protection controls for regulatory compliance
- Fully unified modern UI

Challenges

- Not all components are currently available as SaaS offerings
- Complex architecture with multiple components most likely requires service engagements to be successful
- The number of native cloud integrations is limited

Leader in



NETWITNESS (RSA)



5.13 Securonix

Securonix is a privately held security analytics solution vendor headquartered in Addison, Texas, USA. Founded in 2008 by a team of seasoned experts in information security, risk management, and identity compliance, the company brought their first product to the market in 2011 and has been growing steadily ever since.

The company currently has over 750 employees across North America, EMEA and APJ and a large global partner network. With a strong focus on developing a healthy technology ecosystem, Securonix provides a substantial number of integrations with different security solutions and maintains strategic partnerships with large integrators and consulting companies.

The Securonix Security Operations and Analytics Platform provides a truly advanced security analytics technology for collecting, analyzing, and visualizing a wide range of business and security information and converting it into actionable intelligence. What positions Securonix apart of many other players in this market is the platform's extensibility, a comprehensive set of out-of-the-box contents, and a broad range of connectors and integrations with third-party identity management and security products. On this foundation, the company offers a number of solutions with SIEM, UEBA, SOAR, NDR and XDR capabilities.

The Securonix Next-Generation SIEM combines log management, user and entity behavior analytics, and security incident response into a complete, end-to-end security operations solution. Powered by advanced analytics, behavior detection, threat modeling, and machine learning, it provides a complete range of capabilities to address the requirements of every demanding customer. Securonix's agility and competitive pricing make them a worthy choice for potential customers ranging from small businesses to the largest enterprises in regulated industries.

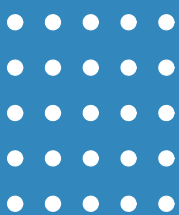
Security

Functionality

Interoperability

Usability

Deployment



Strengths

- A unique open platform architecture focused on extensibility and deployment flexibility
- Support for hybrid, multi-cloud, and “bring your own cloud” environments
- Comprehensive privacy-enhancing and data protection controls to ensure regulatory compliance
- Large number of out-of-the-box connectors and integrations through the Securonix Fusion partner network
- Analytics Sandbox for testing content without impact on production processes

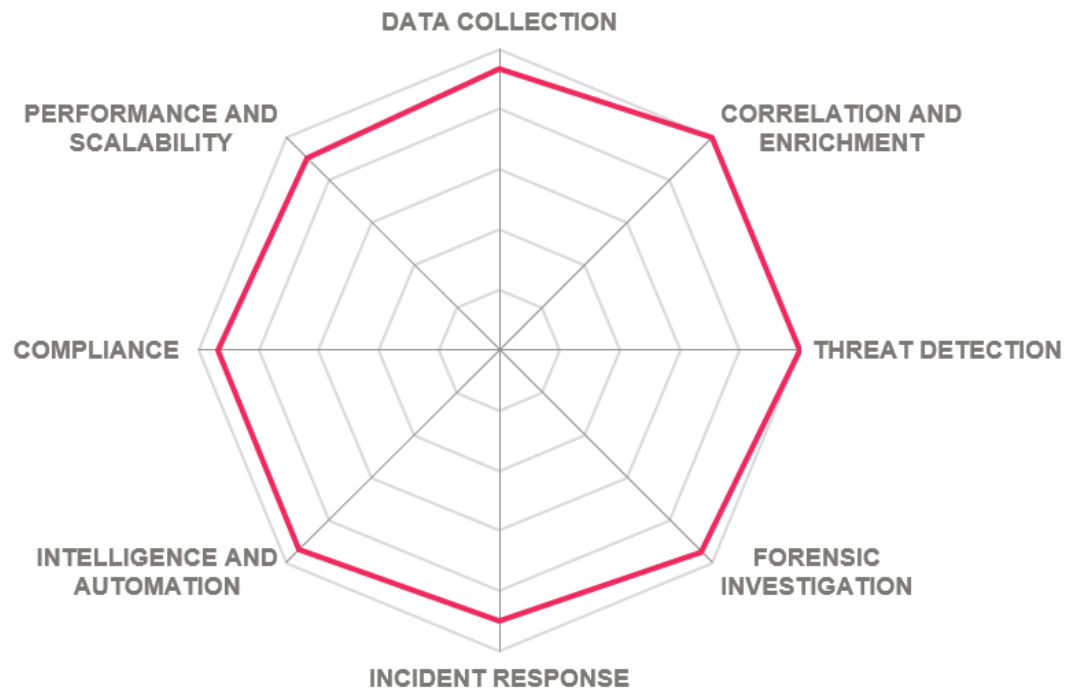
Challenges

- Cloud-first focus; on-prem deployments can be complicated for some users
- Incident resolution tools not quite on par with investigative capabilities
- Some product- or industry-specific content is only available

Leader in



SECURONIX



6 Vendors to Watch

Aside from the vendors covered in detail in our rating, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors that do not fully fit into our definition of the market segment or are not yet mature enough to be considered in this evaluation. We provide short descriptions of these vendors and their respective products below.

6.1 Chronicle / Google Cloud

Chronicle Security is a cybersecurity analytics company based in Mountain View, California. Founded in 2018 as a company within Alphabet, the company is now part of Google Cloud. Established with a vision to create a security analytics platform with unlimited scalability and intelligent automation, Chronicle harnesses Google Cloud's infrastructure to offer a cloud-native analytics platform for managing security data at a petabyte scale. The company also operates the popular malware scanning service VirusTotal.

Why worth watching: although Chronicle is not positioned as a SIEM platform, it does offer all the features typically found in one: ingesting, retaining, and analyzing massive amounts of network and security telemetry from a variety of sources. The platform provides enterprise customers with private containers for securely storing this data in the Google Cloud and enriching and correlating it with third-party threat intelligence. On top of this, Chronicle offers a range of tools for incident investigation, threat hunting, and attack detection. In January 2022, Google has acquired Siemplify, a leading SOAR vendor - the company plans to integrate its capabilities directly into Chronicle to further automate security operations.

6.2 Elastic

Elastic is a software company headquartered in Mountain View, California. Founded in 2012, Elastic is primarily known as the developer of the popular open-source Elastic Stack, which combines the Elasticsearch search engine and Kibana data visualization framework with powerful data ingestion and processing capabilities. Elastic offers a broad range of products and services for such applications as enterprise search, business analytics, infrastructure monitoring, application performance management, and others. Since 2019, Elastic offers its own vertically integrated security solution.

Why worth watching: Elastic Security is a solution that combines security information and event

management (SIEM), endpoint protection (EPP) with threat hunting, cloud monitoring, and more - including fraud detection and continuous monitoring for compliance - built upon the Elastic Stack. Built on a proven, flexible, and distributed open-source foundation, it represents an update of the aging "traditional SIEM" concept free from technical debt and ready for massive cloud-native scalability.

6.3 LogPoint

LogPoint is a multinational software company originally founded in 2003 in Copenhagen, Denmark. At present, the company has global presence with multiple offices across Europe, North America and Asia, with the US headquarters in Boston, MA. LogPoint offers a modern SIEM platform with behavior analytics capabilities, complemented by a tightly integrated SOAR solution. An additional product is offered to integrate SAP environments into SIEM.

Why worth watching: LogPoint is notable for offering a complete solution combining SIEM, UEBA and SOAR from a single hand, making it easy to implement and maintain. Its native multi-tenant capabilities and support for distributed deployments make it especially appealing to large enterprises with complex requirements, as well as to MSSPs. The company's European roots are clearly visible in the solution's strong focus on privacy and data protection according to regulations like GDPR.

6.4 LogRhythm

LogRhythm is an information security company based in Boulder, Colorado, USA. The company was founded in 2003 by a pair of veteran IT experts with a goal of addressing the growing need for log and event management solutions. With offices in all geographic regions, LogRhythm has a substantial global presence, further supported by a massive network of MSSP partners around the world. Currently, the company offers a broad portfolio of security solutions beyond log management, including SIEM, UEBA, SOAR, as well as NDR and XDR products.

Why worth watching: LogRhythm provides a unified security intelligence platform combining next-generation SIEM, log management, network and endpoint monitoring and forensics with full threat lifecycle management and response orchestration. By strongly focusing on delivering out-of-the-box experience and providing a modular solution with preconfigured hardware appliances or a managed cloud-based service, the company can address the requirements of smaller enterprises and many SMB companies yet scale up to the most demanding large enterprise deployments.

6.5 Logz.io

Logz.io is a provider of cloud-native observability and security solutions founded in 2014 in Tel-Aviv, Israel. From the very start, it had a strong vision of completely reinventing the legacy log management and SIEM tools. The team has designed its platform as a universal solution for both DevOps and security specialists, based on a cloud-native architecture and powered by multiple open-source technologies.

Why worth watching: Logz.io Cloud SIEM is a cloud-native security monitoring and analytics platform with a multi-cloud, multi-tenant architecture and unlimited scalability. In a way, the company offers a SIEM solution completely without the technical debt of legacy tools. With an API-first approach, it is suitable for companies that want to integrate SIEM functionality into existing toolchains.

6.6 Rapid7

Rapid7 is a cybersecurity vendor based in Boston, Massachusetts, USA. Established in 2000, the company now offers a broad range of cybersecurity products and services, with the majority of its portfolio built upon the unified, cloud-native Insight platform. These include but not limited to vulnerability management, application and cloud security, threat detection and response, threat intelligence, and security orchestration and automation.

Why worth watching: with the Rapid7's Insight Platform, customers have an unmatched degree of flexibility of combining multiple security solutions according to their current requirements, yet expand as their needs grow, still maintaining uniform visibility, management and analytics across all products. For smaller customers experiencing skill shortage, Rapid7 offers a number of managed security services as well.

6.7 Splunk

Splunk is an American technology company headquartered in San Francisco, California, USA. Since 2003, the company produces solutions for searching, monitoring, and analyzing any kinds of machine-generated data. With its worldwide market presence and a strong ecosystem, Splunk is often considered a de facto standard for operational analytics and intelligence solutions. Since 2009, the company offers Splunk Enterprise Security - a dedicated security analytics platform.

Why worth watching: Splunk's strong market visibility makes it the first choice for any kind of operational or security analytics for many organizations, especially when a large number of readily available integrations, applications and APIs are required. The company's technology ecosystem is unmatched by any competitor.

6.8 Sumo Logic

Sumo Logic is a cloud-native data analytics company based in Redwood City, California, USA. Founded in 2010, the company focuses on developing and operating an elastic cloud platform for collecting and analyzing enterprise log data. Sumo Logic offers a range of operational, security, and business intelligence solutions that are entirely cloud-based and maintenance-free.

Why worth watching: the company's Cloud SIEM solution is, as the name implies, an entirely cloud-based SaaS offering with a flexible pricing model and unlimited scalability. The solution's multi-tenant architecture allows customers to benefit from the "crowd wisdom" via anonymized threat analytics and recommendations.

6.9 T-Systems

T-Systems is a large IT services and consulting company headquartered in Frankfurt, Germany, founded in 2000 as a subsidiary of Deutsche Telekom. It is one of the largest European IT service providers operating in more than 20 countries. The company's Security division offers a complete managed Security Operations Center package for enterprise customers, which is powered by Magenta Security Analytics System, a security analytics platform developed specifically for managed security services.

Why worth watching: Magenta Security Analytics is the platform that powers DT/T-System's managed cyber defense service portfolio. Designed to address the requirements of the largest enterprises in highly regulated industries, it completely hides the operational complexity from the customers and ensures strict compliance with regulatory frameworks like GDPR.

7 Related Research

[Market Compass: SOC as a Service - 80287](#)
[Leadership Compass: Security Orchestration Automation and Response \(SOAR\) - 80016](#)
[Leadership Compass: Network Detection and Response - 80126](#)
[Leadership Brief: Find Your Route from SIEM to SIP and SOAR - 80008](#)
[Leadership Brief: Responding to Cyber Incidents - 80209](#)
[Leadership Brief: Incident Response Management - 80344](#)
[Leadership Brief: Security Fabric: A Methodology for Architecting a Secure Future - 80476](#)
[Architecture Blueprint: Architecting your Security Operations Centre - 72551](#)
[Executive View: ManageEngine Log360 - 80141](#)
[Executive View: Elastic Security - 80152](#)
[Executive View: Exabeam Security Management Platform - 80001](#)
[Executive View: IBM Cloud Pak for Security - 80172](#)
[Executive View: IBM QRadar Security Intelligence Platform - 72515](#)
[Executive View: Securonix Cloud SIEM and UEBA - 79035](#)
[Executive View: Logsign SOAR - 80555](#)
[Executive View: LogRhythm Security Intelligence Platform - 72517](#)
[Master Class: Incident Response Management](#)
[Analyst Chat: The Alphabet Soup of Security Analytics](#)
[Analyst Chat: The SOCaaS Market Segment - A First Look](#)
[Analyst Chat: How the Cybersecurity Market Is Evolving](#)

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- ****Security**
- **Functionality**
- **Deployment**
- **Interoperability**
- **Usability****

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive

Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive

Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak

Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical

Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Figure 1: The Overall Leaders in the Intelligent SIEM Platforms market

Figure 2: The Product Leaders in the Intelligent SIEM Platforms market

Figure 3: The Innovation Leaders in the Intelligent SIEM Platforms market

Figure 4: The Market Leaders in the Intelligent SIEM Platforms market

Figure 5: The Market/Product Matrix

Figure 6: The Product/Innovation Matrix

Figure 7: The Innovation/Market Matrix

Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.