SIEM Buyer's Guide

In today's globalized, digital economy, it's essential to monitor and guard your company's data against increasingly advanced cyber threats.

This is getting increasingly complicated by security skill shortage and alert-fatigue caused by too many security tools. Today's next-gen SIEM solutions enable your company to react quickly and precisely in the event of a threat or data leak. A next-gen SIEM solution provides management, integration, correlation, and analysis in one place, making it easier to monitor and troubleshoot your IT infrastructure in real time from one single interface.

chess LOGPOINT

TABLE OF CONTENTS

What is SIEM?

Security incident and event management (SIEM) is a tool that provides monitoring, detection and alerting of security events or incidents within an IT environment. It provides a comprehensive and centralized view of the security posture of an IT infrastructure and gives enterprise security professionals insight into the activities within their IT environment.

SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices, such as firewalls and antivirus. The software then identifies, categorizes and analyzes incidents and events. The SIEM analysis delivers real time alerts, dashboards or reports to several critical business and management units.

The modern SIEM scales with your infrastructure requirements and improve capabilities for external and internal threat discovery and incident management. According to Gartner, this includes targeted attack detection, user activity monitoring, application activity monitoring, profiling and anomaly detection, threat intelligence, effective analytics and incident response features to mention a few.

Next-gen SIEMs provide extensive machine learning and anomaly detection capabilities, for advanced threat detection. This ultimately can assist your security team to increase their effectiveness and reduce the resources required to run security operations – which is important in a time where there's a shortage of security skills and an ever-increasing number of alerts.

In a nutshell, SIEM allows IT teams to see the bigger picture by collecting security event data from enterprise applications, the cloud and core infrastructure to learn exactly what goes on within the enterprise – creating value from the sum of data which is worth much more than the individual pieces. A single alert from an antivirus filter may not be a cause of panic on its own, but if it correlates with other anomalies, e.g. from the firewall at the same time, this could signify that a severe breach is in progress.

The need for SIEM

In the globalized, digital economy, it's essential that enterprises monitor and guard their data to protect themselves from increasingly advanced cyber threats. Chances are, your company has more data to collect and analyze than ever before. In fact, according to IDC's Data Age 2025 study[1], the global datasphere will grow to 163 zettabytes (a trillion gigabytes) by 2025, which is ten times the 16.1 zettabytes of data generated in 2016.

Organizations today must be attentive about investing in the right cyber expertise to thwart potential threats. While there have been investments in education and skills training, the cybersecurity skills gap is getting wider. In 2015, Frost & Sullivan forecasted a 1.5 million worker shortage by 2020. In the most recent report [2], that figure was revised to a 1.8 million worker shortage by 2022.

To counter this skills gap, organizations must invest in the right technological capabilities to counter the alert-fatigue and overload of security tools. This is where next-gen security information and event management (SIEM) solutions come into play by having great integrations, Machine Learning and AI to automate many of the tasks that companies cannot hire people to take on.

Today's next-gen SIEM solutions enable companies to react quickly and precisely in the event of a threat or data leak. A next-gen SIEM solution provides collection, classification, detection, correlation and analysis capabilities in one place, making it easier for teams to monitor and troubleshoot IT infrastructure in real-time. Without a SIEM solution, security analysts must go through millions of non-comparable and siloed data for each software application and security source. In short, SIEM solutions can improve simplicity, efficiency and accuracy.

Benefits of a next-gen SIEM solution

SIEM solutions have been around since 2005, but as the threat landscape evolves to one that involves new levels of sophistication and heightened numbers of attacks, the criteria for an effective solution has too evolved. Companies today must be able to monitor activities that can lead to potential threats in real time, meaning they require solutions that can pinpoint a larger variety of threats even faster and more accurately than ever before.

1 IDC Data Age 2025 study pdf
2 Europe-GISWS-Report. pdf

At the same time the amount of federated collaboration in organizations has dramatically increased, degrading the well-defined security perimeter and exposing a larger threat surface than ever before, Consequently, network infrastructure is growing in complexity and size, and at the same time the number of business "pains" that can arise from a breach is increasing. This is a key development in making a next-gen SIEM a crucial element in enterprise cybersecurity.

In addition, the shortage of security analysts caused by the "cybersecurity skills gap" with the knowledge and skills makes it difficult to keep pace with the evolution of cyber threats and increasingly stringent compliance demands. Security operations teams are struggling to keep up with the deluge of security alerts and must rely on manually created and maintained document-based procedures for operations. To counter these obstacles, many organizations over the years have implemented SIEM solutions.

For years, SIEM solutions have been implemented to help security and IT teams analyze security alerts in real-time, though many legacy SIEM solutions lacked the ability to gather and analyze large amounts of data from a variety of sources. In addition, SIEM solutions of the past could not scale with an organization as it its needs grew.

Fortunately, the new era of digitalization and machine learning is creating new possibilities for SIEM solutions to make a big impact on businesses across industries. To establish an effective cybersecurity program, a next-gen SIEM solution is a must-have for businesses large and small. Today's businesses need a solution that can unify, simplify and automate security workflows to enable better information-sharing and incident prevention procedures. The key benefits of a next-gen SIEM include:

Better threat detection and response

As cyber threats continue to expand and increase, businesses that can complete analysis of security events quickly and more accurately, will have a competitive advantage. A next-gen SIEM solution provides real-time data analysis, early detection of data breaches, data collection, secure data storage and accurate data reporting to improve threat detection and response times.

Reduced staff requirements

Today's IT teams are increasingly resource and time constrained, so enhanced automation frees security analysts from time-consuming manual tasks and enables them to better orchestrate responses to threats. The best next-gen SIEM solutions utilize machine learning and user and entity behavior analytics (UEBA) to help ease the burden of overworked security analysts by automating threat detection, providing enhanced context and situational awareness, and utilizing user behavior to gain better insights.

Predictable IT and security spend

A next-gen SIEM solution that has a simple and predictable licensing model enables businesses to spend less to keep their data secure, regardless of the amount of data they have and the number of sources from which data is logged.

Enhanced compliance

Meeting compliance can be costly and complicated, though fines, legal fees and damaged reputations can be even more costly. SIEM solutions can automate data collection, store event logs, improve threat identification and reporting, restrict data access, and flag policy and compliance violations to ensure businesses meet their compliance requirements.

Four symptoms that your existing SIEM solution is up for replacement

Organizations spend considerable time and effort to establish and maintain SIEM. Businesses must train their teams, while operationalizing and optimizing workflow around the SIEM – efforts that can take years to establish. But the truth is, many times, it still doesn't feel right; there are a number of reasons why this unease persists among SIEM customers.

If your business can recognize one or more of the following symptoms, it's probably time to change:

1. Your SIEM is cumbersome to deploy and manage

It took months to deploy your SIEM. After a slow and difficult deployment, many organizations are still embattled with a large amount of their efforts directed towards ingesting new types of data feeds or simply setting up analytics. Changes to the configuration require extensive time and security resources to complete.

2. Your SIEM is inflexible

Your SIEM solution is limited to security data types, ultimately limiting your team's analytic capabilities within detection, investigation and response.

3. Your SIEM is antiquated

Your SIEM's main feature is log collection and provides little value without experienced analysts. It lacks the ability to leverage multiple sources of threat intelligence and provide advanced analytics such as machine learning, UEBA and orchestration.

4. Capital and operational costs are unpredictable

The complicated pricing scheme of your current SIEM makes it impossible to get the transparency and the detection/response capability you require. In reality, what you have purchased turns out to be a platform, not a security solution. You require experienced staff, and lots of it, just to keep your current system operational.

LogPoint compared to the competition

	LogPoint	Legacy SIEM	Open Source	Comparable industry leaders
UEBA applicable to all data sources	Yes	No	No	No
Common and flexible event taxonomy enables faster analytics	Yes	No	No	No
Turnkey security product vs. DIY security platform	Yes	Yes	No	No
Predictable pricing enables analytics of entire IT infrastructure	Yes	No	No	No
Full visibility across infrastructure without needing major changes	Yes	No	No	No
Ingestion of contextual data for enhanced correlation and analytics	Yes	Limited	Yes	Yes
Real-time and long-term application of correlation rules, advanced analytics and machine learning	Yes	Limited	DIY	Yes
Address non-security use cases (IT Operations)	Yes	No	DIY	Yes

See Gartner Peer insights

The Critical capabilities of a next-gen SIEM

According to Gartner, there are three main areas where a next-gen SIEM solution should excel – advanced threat detection, security monitoring and investigation and incident response. LogPoint delivers world-class results in each of these areas.

Advanced threat detection

With a next-gen SIEM tool, advanced threat detection can be executed in real time, allowing organizations to analyze and report on trends as well as user and entity behavior. With advanced analytics, organizations are empowered to monitor data access, application activity and can proactively detect and control advanced persistent threats (APT).

Threat detection capabilities include enrichment with internal or external contextual information, such as threat intelligence, user names or temporal knowledge. This enables security analysts to operate faster and more efficiently. Organizations should invest in SIEM solutions that provide access to effective ad-hoc queries, machine learning and UEBA capabilities, which will result in more effective and efficient threat hunting.

Security Monitoring

SIEM is an effective log management tool, allowing for basic security monitoring and is often used for compliance reporting and real-time monitoring of security controls. SIEM solutions should meet basic threat detection, compliance auditing and reporting requirements. With flexible and convenient collection and storage of logs, auditors' needs can be accommodated, making compliance much easier.

Popular use cases among customers for basic security monitoring cover a broad range of security sources, including:

- Perimeter and network devices
- Endpoint agents
- Critical applications
- Other infrastructure components

Investigation and incident response

Visualization is very important for making sense of your data. A next-gen SIEM can give you the clarity you need. We're constantly implementing new ways to visualize data and provide a level of visualization that makes it easy to interpret and respond to what your data is telling you. This is true for all our dashboards, reports and alerts, as well as ad-hoc queries.

Incident response and management should be easy, fast and actionable, making it convenient to manage incidents within your team and enabling effective forensic investigations. If not within the tool itself, it is important to have world-class integration options to dedicated tools both within and outside of SOAR. With business context, security intelligence, user monitoring, data monitoring and application monitoring – all within a single interface – analysts will be more effective and informed.

Implementing a next-gen SIEM solution or upgrading an existing SIEM to one that offers analytics and machine learning capabilities will allow organizations to keep up with today's expanding threat landscape – without the growing costs associated with highly-skilled security analysts and having to deal with outdated log volume and pricing models. Replacing a SIEM doesn't necessarily mean that your current investment is lost – some SIEM vendors will help you with a seamless transition to make sure full value is captured and transferred.

A next-gen SIEM should have the following capabilities and offerings:

1. Collects and analyze data from all sources in real time

Organizations today are generating and consuming more data than ever before. to keep up with this rapid increase of information, SIEM tools must be able to ingest data from all sources – including cloud and on-premise log data – to effectively monitor, detect and respond to potential threats. Next-generation SIEM solutions don't just have the ability to ingest and analyze more data, they thrive on it. The more data an organization can provide its SIEM, the more visibility analysts will have into the activities and the more effective they will be in detecting and responding to threats.

2. Utilizes machine learning to add context and situational awareness to increase efficacy

Today's attacks are becoming more sophisticated, meaning organizations need tools that are equally sophisticated. Attackers often rely on compromised credentials or coercing users into performing actions that damage their own organization's activity. To identify these types of attacks more quickly and accurately, SIEM tools should be equipped with machine learning capabilities in the form of UEBA to monitor both suspicious user behavior and activities stemming from the cloud, mobile, on-premises applications, endpoints and networks, as well as external threats.

With UEBA, organizations will see a dramatic increase in their SIEM's ability to track and identify threats. In addition, UEBA eliminates false positives so analysts have greater situational awareness before, during and after a threat occurs – meaning they are more effective and can spend their limited time on threats that will actually have an impact on operations.

3. Flexible and scalable architecture improves time to value

Legacy SIEM solutions don't compare to those offered today. Since the amount of data both produced and collected by organizations has skyrocketed over the past few years, organizations need big data architectures that are flexible and scalable, so they can adapt and grow as the business changes over time. With the ability to handle large and complex implementations, today's next-gen SIEM solutions can be deployed in either physical or virtual environments and on premise or in the cloud. Some SIEMs provide a very short implementation time and low maintenance resource requirements, resulting in the SIEM providing value within a matter of days.

4. Enhanced investigation and incident response

Next-gen SIEM solutions go beyond basic security monitoring and reporting, they provide analysts with the clarity they need to improve decision-making and response times. With new ways of visualizing data to help analysts better interpret and respond to what that data is telling them, incident response and management becomes more sophisticated. Better analytics means teams can more accurately manage incidents and improve their forensic investigations – all within a single interface.

5. Equipped with a unique pricing & licensing model

SIEM pricing models that are based on data usage are outdated. Data volumes are constantly increasing, and organizations shouldn't be punished for that. Next-gen SIEM pricing models should instead be based on the number of devices sending logs or entities, meaning organizations won't have to worry that their data usage is affecting the cost, but can instead focus on scaling for future business needs. Make sure you analyze the total cost of ownership, also for when the SIEM needs to scale – some vendors have added cost when increasing hardware capabilities or the number of employees that needs access to the SIEM.

LOGPOINT

Building your business case

Keep in mind that there are key differences between business use cases and technical use cases. While a business use case is often high level, strategic and provides rationale that can help to secure executive approval and funding for SIEM deployment, a technical use case, on the other hand, is often highly detailed and helps operationalize the SIEM in order to achieve its business goals.

Key elements for building a business use case for SIEM include:

1. Stabilization of IT Operations

SIEM helps businesses solve problems faster and more efficiently. By identifying problems before they have an impact on critical systems, businesses will be able to reduce downtime, which can have a positive impact on revenue and productivity. SIEM solutions enable businesses to investigate incidents more quickly. With logs that are more accessible, businesses can free up the time needed for investigations and reduce the manpower needed to complete them, ultimately reducing the cost for running IT operations. Lastly, by identifying the root cause of issues within IT operations, organizations can decrease the number of security incidents that occur, resolve issues faster, enable greater productivity by optimizing IT infrastructure and increase both performance and reliability.

2. Secure your data

SIEM enables greater visibility into what is occurring within your network, which is critical for helping businesses avoid loss of data or disruption to their services. High-level dashboards decrease the risk of breaches by offering simple overviews of suspicious activities across a business, and provide insight into potential brute force attacks, data loss prevention, data theft, compromised accounts and change monitoring. Optimizing compliance is important for any business. With SIEM, businesses can better monitor important processes and set up automated reports, which make processes related to General Data Protection Regulation (GDPR), the International Organization for Standardization (ISO) and Payment Card Industry Data Security Standard (PCI DSS) and other regulations and standards bodies quicker and easier. Lastly, SIEM improves detection and response capabilities by enabling businesses to quickly react to incidents. In addition, SIEM offers increased visibility and anomaly detection, helping businesses avoid or limit the losses occurred during and after breaches.

3. Gain new business insights

By having all your systems' log data available within the LogPoint solution, businesses can index all data and analyze what is happening across an organization at any time. Any activity can be benchmarked against what a business determines is normal and can be compared to any historical time period. By doing this, businesses increase visualization, making it easier to pinpoint what activity is deemed normal and what is not, which can help IT teams make better business decisions. When analyzing logs with LogPoint, businesses can also improve non-security areas such as:

- Service desk performance and enablement by decreasing the time to resolution
- IT spend by analyzing logs from storage or printers, which provides insight into where usage can be optimized
- Downtime predictions by pinpointing when a piece of equipment needs to be repaired to avoid potential downtime
- Business processes by simplifying with data-driven insights that provide data on trends within an organization so costs can be saved, and tasks can be automated.

4. Optimize business processes

SIEM drives increased revenue by providing better visibility into what is occurring within businesses on many levels, both internally and externally. For example, calling a customer just before a product needs maintenance or identifying unmet needs can both save costs and lead to upsell or service revenue opportunities.

SIEM improves business optimization and innovation by offering teams the ability to determine what changes need to be made to optimize specific business processes. In addition, you'll be able to gain contextual awareness by enriching your data with the right information, giving your organization a better understanding of what is tying up resources. This leads to increased user and customer experience and can give your organization the insights needed to create new initiatives that improve value both internally and externally.

To determine your technical use cases, consider the following:

1. Define the scope of your deployment

When choosing a SIEM solution, businesses should consider organizing a workshop, either internally or alongside a SIEM partner, to define and agree on the project scope and timeline. To define the deployment's scope and timeline, businesses need to identify, and more importantly prioritize, an initial list of use cases to dictate what the necessary log sources may be. In addition, it is important to agree upon a timeline for deployment to ensure the SIEM is aligning with the business' overarching goals.

2. Determine your priority data sources

Once the team has a handle of the ideal project scope, teams can then identify log sources within the scope to determine how they can obtain the relevant information needed. For example, firewalls, intrusion protection systems and antivirus software, all serve as prime data sources for SIEM, but there are many more. It is important that businesses prioritize the sources that will be included to ensure the SIEM provides the most accurate security protection possible.

3. Identify the high priority events and alarms

When it comes to protecting an organization against both insider and outsider threats, IT and security teams are often presented with an ever-growing list of security events that need to be analyzed and acted on. To break through the noise, SIEM can be used to make events and alarm data more insightful than ever, but businesses must first determine what their high priority events are and how they are derived from applications and devices within the infrastructure. This way, teams can use the SIEM to spend more time on the events and alarms that may be more damaging to the business and its data.

4. Pinpoint your key success metrics

A successful SIEM implementation and deployment is directly correlated with what a business' goals are. It is important that key success metrics are determined prior to deployment to ensure maximum ROI. For example, reducing information theft or improving how businesses monitor for potential intrusions or infections may be metrics to establish, but there are many others. It's important that businesses determine what success means for them and how the SIEM can be used to achieve it.

5. Identify all environments you need to monitor

After you've identified your key use cases for a SIEM, you'll need to identify and monitor all the assets that are relevant for achieving your business goals. This includes all network devices that process security-relevant information such as routers, firewalls, web filters, domain controllers, application servers, databases, and other critical assets within your business' IT environment. Once you've identified the assets and environments that need monitoring, you'll also need to know the following to ensure your team is finding threats and addressing them correctly:

- WHO the bad actors are
- WHAT events to focus on
- HOW to respond when threats are detected
- WHERE these threats are in your environment
- WHY these are the biggest threats

Your SIEM use cases may relate to passing your next compliance audit or protecting the company's intellectual property. You should consider all of the critical applications and data your business relies on to support customers and keep business operations running. Consider which applications house data that might be the target of cyber criminals or which applications contain data that may impact your compliance status (e.g. credit cardholder data has implications for PCI DSS).

Time to Value

When you choose a SIEM solution that is already integrated with other essential security controls, you significantly reduce the time and effort required to procure, deploy, integrate and configure multiple point security tools. Instead, you can deploy quickly and realize a faster time to value. Security-focused SIEM solutions often include pre-built correlation rules to detect malware and more, so you can begin to detect threats on day one.

Cost Savings

A unified SIEM generates upfront and ongoing cost savings. Instead of having to deploy, monitor and maintain multiple point security and compliance tools, a unified solution can provide a single view for complete security monitoring and compliance management. This approach enables resource-constrained IT security teams to achieve a strong security posture with fewer resources.

Efficacy, Accuracy & Precision

Because detection is better coordinated among the built-in security controls, alerts are more accurate and correlation rules are more finely tuned than they would be for external or unknown data sources.

If you do already have some of these core technologies in place, then you'll want to clearly understand what it will take (how much time, money and effort) to integrate them with your SIEM and maintain that integration as things within your business change. Be sure to ask your SIEM vendor how they approach integration with other tools (including costs), and how long this part of the deployment is expected to take.

The successful evaluation and selection process

Important questions to ask during the purchasing process

1. What can I do if I don't have all of the external security technologies in place that can feed the SIEM (e.g. asset inventories, IDS, vulnerability scans, etc.)?
2. What is the anticipated mix of licensing costs to consulting and implementation fees?
3. How many staff members or outside consultants will I need for responding to SIEM alerts and managing the system overall?
4. How long will it take to go from software install to security insight?
5. How many staff members or outside consultants will I need for the integration work?
6. Do alerts and alarms provide step-by-step instructions for how to mitigate and respond to investigations?

SIEM Evaluation Process Stages

Phase 1 · Initial Review

- **Key Activities** – Determine the set of vendors you'll review and evaluate, based on the criteria we've included in this guide. Ensure those on your list provide the solutions and support needed to help your business achieve its goals.
- **Pro-Tip** – If possible, choose at least two or three vendors that your team will invest their time and effort with during the proof of concept phase. Know that not all vendors will qualify for an investment of your team's time and attention during an in-depth technical evaluation, so it is important to understand which providers will give your team the time and effort it needs to ensure a solution is worth investing in.

Phase 2 · Try it in your own environment

- **Key Activities** – Develop key evaluation criteria for each SIEM vendor you're exploring. Have your team run through test cases to ensure that the SIEM works as expected and addresses key technical requirements and satisfies your business goals.
- **Pro-Tip** – Look for vendors that offer a free trial, so you can go through the deployment process before making a final purchase. Design test cases that are as close to your business' real-world priority needs as possible. By testing and gathering feedback, you'll find out how easy (or difficult) the process is from installation to insight with the SIEM, which will ensure you choose the right solution for your unique business needs.

Phase 3 · Final Vendor Selection

- **Key Activities** – Gather and analyze all results from evaluation assessments and team feedback to determine which SIEM vendor is right for you. Be sure to evaluate subjective criteria such as rapport with the vendor team, as well as what their support hours and customer policies may be. While the technology backbone is of utmost important, ensuring you have the right team behind you can make the SIEM work even better for your business.
- **Pro-Tip** – Include all key stakeholders, in this process and document key reasons for selecting the chosen vendor. Feedback from both leadership teams and those who will be interacting with the solution on a regular basis will be important information to know, especially because it may come in handy at renewal time.

Choose LogPoint as your SIEM vendor

The digital era has ushered in greater possibilities for sharing and analyzing data across IT solutions and departments. This sharing brings vital contextual awareness to all levels of a business.

For most businesses, speed and capability matter more today than ever before. Completing an analysis quickly and accurately can have a direct effect on a business' operations and can open new opportunities for businesses to be more competitive in a competitive marketplace. In addition, cyber threats and data breaches are becoming even more frequent and impactful, meaning businesses must also be able to secure valuable enterprise and customer data.

To counter these threats and remain competitive, most every company today is undergoing digital transformation in one form or another. At LogPoint, we recognize that many of our customers are going through change. With the exponential growth in data volume every year and resulting demand to implementing IT systems to increase efficiency, reduce costs and spark innovation, our purpose is to support customers as they undergo digital transformation. Our customers place their trust in us because they recognize that LogPoint is one of the most innovative cybersecurity companies in the world.

Enter our next-gen SIEM solution

With a large variety of SIEM solutions to choose from, you need to ensure you select one that best fits your business' needs. LogPoint leverages advanced analytics, accelerated by machine learning, to improve your cybersecurity posture and efficiently automate relevant responses to both internal and external threats. Here's what makes LogPoint unique:

Ease of use

Customers are passionate about receiving the best, most detailed analytics capabilities possible. Our unique taxonomy makes it easy to gather, analyze and act on data, and the solution is supported with lightning-fast analytics and rich reporting capabilities that don't require advanced skillsets.

Cost management

LogPoint offers unparalleled transparency into ROI and predictability for costs and outcomes. Our license is based on the number of nodes, meaning there's no extra cost related to the growth of your company's data volume or how many events per second you receive.

Unmatched certification

We have a reputation for offering superior security, which is why even the customers with the most stringent security requirements place their trust in us to handle their valuable data. We've earned EAL 3+ certification. It's required by NATO and in critical infrastructure organizations like the military, intelligence agencies, utility companies and telcos.

Customer-centric

Working closely with European clients has enmeshed data privacy into both our company culture and the product that we offer our customers. The LogPoint ecosystem is built on a customer-first culture, which means that we go the extra mile to solve problems and add value for our customers. See what our customers say via Gartner's Peer Insights.

UEBA

Our industry-leading UEBA module helps our customers prioritize their time, so they can focus on abnormal behavior that would otherwise be very time consuming to investigate. UEBA presents the required contextual information to the security team, enabling faster and more well-informed decision making. The advanced analytics makes cybersecurity teams smarter by accelerating detection and response to threats without increasing security analyst workloads.

Five reasons why leading brands choose LogPoint

1. People prefer LogPoint's intuitive analytics and advanced threat hunting capabilities

LogPoint's unique taxonomy harmonizes data from cloud applications, core infrastructure, security products and proprietary applications, among other sources. By leveraging this taxonomy, analytics is consistent across all data sources and use cases, enabling analysts to focus on the output of behavioral analytics, machine learning and correlations use cases. The taxonomy extends to the integration layer, allowing easy consumption of threat intelligence, adding business context to events and integration with the rest of your infrastructure.

2. A flexible security analytics platform to fit your business and technology strategy

LogPoint supports companies with security strategies that are on-premises, in the public cloud and through a managed security service provider. By supporting more than 400 of the most critical security data sources, customers can ingest data from virtually any source – from databases to cloud applications like Amazon Web Services, Microsoft Azure and ERP platforms such as SAP.

3. Unmatched time-to-value makes it resource efficient to implement and expand LogPoint

Our customers tell us that time-to-value is a huge factor for why they choose our solution. LogPoint gives you a full SIEM solution that provides valuable analytics within a matter of days. Adding UEBA capabilities to enhance the SIEM takes no more than 6 hours, which brings customers unmatched time-to-value.

4. Predictable and transparent total cost of ownership

LogPoint works with your infrastructure, and we believe that the licensing model should not be a limiting factor when planning how and which data sources you would like to ingest data from. Our node-based pricing for SIEM is straightforward, and unlike other SIEM vendors, it covers all servers and data ingested – giving you the control and predictability to know exactly what the total cost of ownership will be.

5. Large partner community enables maintenance-free security operations

LogPoint takes a 100 percent customer-centric approach. You can join an ecosystem of some of the best global integration and technology partners, as well as hundreds of customers. We provide 24/7 service and enjoy a consistent 97 percent satisfactions among customers for our support.

LOGPOINT

About LogPoint

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Our advanced next-gen SIEM, UEBA and Automation and Incident Response solutions, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses. We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions. Our offices are located throughout Europe and in North America. Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence. With more than 50 certified partners, we are committed to ensuring our deployments exceed expectations.

Contact Chess

If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution, do not hesitate to contact the Chess Team on **0344 770 6000** or email **marketing@chessICT.co.uk**