



SIEM Buyer's Guide 2023

The SIEM Buyer's Guide discusses the pros and cons of standalone SIEM platforms versus converged SIEM solutions and how to make the best security investment for your organization. You will discover the advantages of modern SIEM platforms and why you should include SOAR and UEBA in your security operations. Learn how converged SIEM platforms make it easier to strengthen their security posture.

GETTING STARTED

First-Time SIEM Buyer?

As a first-time SIEM buyer, you need to know which features and functionalities are essential for today's cybersecurity operations and what will be required to futureproof it along with the growth of your business.

Moving From A Log Management Solution?

Many organizations that don't have a SIEM tool place count with a log management tool. However, if you need to use logs to manage security, you will soon find that only collecting log data is not enough as you lack automation and real-time threat analysis, something that a log management tool is not able to provide.

Replacing A Legacy SIEM?

While legacy SIEMs identify security events from many devices, they have minimal capability to correlate the data and turn it into actionable intelligence. Legacy SIEMs collect limited log data and have static search queries that constrain the security team and result in a high percentage of false positives. Today, much better solutions are available.

Thinking About SOAR And UEBA?

SIEM, SOAR and UEBA play critical roles in facilitating cybersecurity operations to be highly efficient and manageable, adding competence and capability without placing a further burden on overstretched security teams. If you think SOAR and UEBA platforms are too sophisticated and complex and beyond your reach in terms of price and practicality, think again.

What Others Are Doing

Security teams are overwhelmed by alerts and understaffed in terms of headcount and skills. Even with numerous security tools deployed, they constantly struggle to improve efficiency or reduce risk.

Winning strategies to improve and advance cybersecurity posture now revolve around technologies that offer a more innovative and straightforward approach — Such as solutions that will be more effective and sustainable in the long run. While security vendors continue to build best-in-class automation platforms to optimize a 30, 50, or-100-person SOC, these solutions have many additional features that only big, and well-funded, security teams can integrate and exploit.

The market also offers a consolidated and holistic approach that unifies SIEM, SOAR and UEBA capabilities in a converged platform. The pre-integration and simplicity provided by a converged SIEM platform allows enterprises of all sizes to leverage cutting-edge AI and automation to enable their security operations to be more highly efficient and effective than they ever thought possible.

CONVERGED SIEM PLATFORM SOLUTIONS

Converged SIEM Platforms Combine These Essential Cybersecurity Tools Into A Unified Solution:



SIEM

Security Information
and Event Management



SOAR

Security Orchestration
Automation and Response



UEBA

User and Entity
Behavior Analytics



BCS

Business-critical
security



EDR

Endpoint Detection and
Response

Top Use Cases

Detecting compromised
user credentials

Endpoint malware
mitigation

Phishing investigation
and response

Threat Intelligence
management

Ransomware mitigation

Account misuse

Monitoring loads
and uptimes

Internal
reconnaissance

Threat Hunting

Tracking system changes

Converged SIEM Platform

SIEM

Central visibility and
control of cyber events

- Central collection and analysis of all security telemetry
- Early detection of cyber breaches
- Central storage of current and historic data
- End-to-end event reporting

SOAR

Faster investigation and
remediation of alerts

- Aggregate alerts and prioritize their severity
- Automate workflows and playbooks to accelerate threat investigation and remediation
- Guide analysts to consistent and optimal threat responses

UEBA

Identifying suspicious
patterns in user behavior

- Continuous monitoring and analysis of user and entity behavior
- AI-driven profiling of behavior norms, patterns
- Automated alerts when behavior baselines are breached
- Internal threat detection

BCS

Detecting threats to
critical applications

- Bring critical application (e.g., SAP) activity under the central security monitoring of SIEM
- Automate compliance monitoring of critical applications
- Save time with ready-to-use controls, checks, dashboards and reports

EDR

Detect and remediate
incidents in endpoints

- Full observability with log and telemetry collection
- Policy checks to notify you when an endpoint enters a non-compliant state
- MITRE ATT&CK enrichment for more context of TTPs used by actors
- Out-of-the-box playbooks to automate tasks and save time

Integrations

Asset & IAM platforms

SaaS solutions

Cloud security tools

Endpoint devices

Threat Intel Vulnerability
Management

Cloud workloads

EPP, EDR

On-premise workloads

APIs

Converged SIEM platform seamlessly integrates and automates the collection, correlation, analysis, investigation, and remediation of security events across IT infrastructure, users, and business applications.

ESSENTIAL SECURITY CAPABILITIES IN A CONVERGED SIEM PLATFORM

SIEM

Gartner defines [Security Information and Event Management](#) as “technology that supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.”

Gartner also distinguishes between legacy and “modern” SIEMs. According to Gartner, a modern SIEM “works with more than just log data and applies more than just simple correlation rules for data analysis.” In short, modern SIEMs are more flexible and have more capabilities to detect and analyze threats to ensure fast remediation. Now that modern, analytics-driven SIEM solutions are readily available, there is no real incentive to buy a legacy SIEM, but every incentive to replace a legacy SIEM system.

SOAR

[Security Orchestration, Automation, and Response](#) tools automate the collection, analysis, and prioritization of alerts and security data from many sources and systems, so security teams have all the contextual information and intelligence they need for rapid detection and response. SOAR utilizes workflows and playbooks to automate repetitive tasks, ensure consistent threat analysis, and guide security analysts in decision making.

UEBA

[User and Entity Behavior Analytics](#) tools monitor and analyze the behavior of users and other entities such as applications, endpoints, and servers. Machine-learning (ML) is used to build and maintain a baseline behavior profile for every user and entity in the network. All actions are evaluated against these baselines to determine normal versus abnormal behavior.

Continuous tracking of user and entity behaviors provides valuable situational awareness before, during, and after responding to breaches, and assists threat hunters in knowing what to look for. While UEBA is a security technology on its own, it's not intended to replace a SIEM system but to work in conjunction.

BCS

Cyberattack targets have evolved beyond IT assets and infrastructure. Malicious actors increasingly target the datarich, critical applications that you use to operate your business and service your customers. Only advanced Converged SIEM Platforms bring business-critical applications such as SAP under SIEM surveillance and within the central security monitoring of the enterprise. Events from applications like SAP can reveal sophisticated, multi-vector attacks involving or originating in business-critical applications that would have been difficult to detect otherwise.

EDR

Attackers will always look for the path of least resistance, and in many cases, this leads to your endpoints. So, the ability to detect and respond to threats in endpoints is crucial. Logpoint's native endpoint agent, called AgentX, adds EDR capabilities to your Converged SIEM platform to help you secure your entire organization. In combination with SIEM and SOAR, it automates the detection, investigation and response of incidents in endpoints, performs compliance reporting and achieve log collection on all devices. By enriching events with contextual and operational data, SOC teams get more detailed analysis to easily resolve incidents.

CONVERGED SIEM PLATFORM SOLUTIONS






SIEM, SOAR and UEBA systems bring different capabilities to cybersecurity operations and contribute to a company's cybersecurity posture in multiple ways. . Most companies start with a SIEM platform. Many buy SIEM and UEBA to gain more granular threat intelligence. Some companies also add SOAR to automate threat prioritization, investigation and response.






Best-in-class standalone SIEM, SOAR, and UEBA products often require integration before they can start working together. The alternative to integration is inefficient manual methods and multiple user interfaces to learn. The additional time and money needed for integration often delays buying or results in partial integration.

Typically, BCS cannot be integrated with standalone SIEM, SOAR, and UEBA solutions. The complexity and costs are restrictive.

In a converged SIEM platform, SIEM, SOAR, UEBA, BCS tools and EDR capabilities are already integrated and ready to work in harmony behind a common interface, ensuring that you get the maximum value from each of them. Moreover, you still have the flexibility to implement the tools all at once or in stages.

The following table lists some critical use cases for SIEM, SOAR, UEBA, BCS and EDR tools and highlights the value of convergence.

Use case	 SIEM	 SOAR	 UEBA	 BCS	 EDR
Insider Threat Detection	Advanced analytics help you find malicious insiders that are difficult to uncover with traditional detection methods. Prevent security incidents before they cause irrevocable damage.				
Fraud and Risk Monitoring	Continuously monitor the behaviors of users, computers, and IoT devices and link events across your environment to uncover anomalies. Automated playbooks trigger the necessary action plan.				
Anomalous File Sharing and Data Exfiltration	Detect anomalous user activity based on historical and expected work patterns. Correlate data from users and other sources to identify lateral movement and prevent data from leaving the system.				
Malware Detection and Mitigation	Reconstruct the events that led to malware infection using the data at your disposal. Document the full scope of the breach, prevent additional systems from becoming infected and initiate playbooks to remediate incidents.				
Internal Reconnaissance	Gather evidence from network infrastructure to uncover anomalous behavior. When you investigate an alert, contextual information from related incidents and threat intel is automatically added to help detect and prevent attackers from gaining information.				
Regulatory Compliance Monitoring	Automated risk assessment monitoring centralizes and analyzes data across the organization to meet compliance standards. Comprehensive reporting proves adherence to compliance and regulatory frameworks.				

Use case	 SIEM  SOAR  UEBA  BCS  EDR
Intellectual Property Theft	Automatically investigate incidents to determine causation. Case management identifies relevant data to help you uncover where the attacker infiltrated the system and what was accessed.
Incident Prioritization and Triage	Quickly investigate incidents with root cause analysis, risk level priority, and automatic event context. Find and analyze relevant data to uncover threats or suspicious activity.
Compromised Account and Misuse Detection	Prevent unauthorized account use by anyone other than the account holder. Monitor how employees behave within the system and detect any unauthorized account use by account holders.
Threat Hunting	Threat hunting capabilities provide in-depth hunting and analysis through enrichment, correlation, machine learning and threat intelligence. Search proactively for cyberthreats that might otherwise evade detection.
Phishing Investigation and Response	Track who received phishing emails, clicked on any malicious links, or replied to them and take immediate action to minimize damage. Automatic playbooks and machine learning help minimize impact on your organization.
Vulnerability management	Risk-based prioritization based on anomalous user behavior, threat intel and machine learning, helps detect vulnerabilities in your organization. Automated playbooks help analyze and remediate each vulnerability.

EVALUATING STANDALONE SIEM VERSUS CONVERGED SIEM PLATFORM

Traditionally, security budgets are allocated to buy best-in-class products from leading vendors to shore up the vulnerabilities they perceive pose the most significant risk to the organization. However, many organizations, especially mid-tier businesses, are shifting away from best-in-class point solutions and adopting a more holistic and consolidated cyber hygiene and cybersecurity approach. Here are some things to consider before you buy.

Evaluation Criteria	Converged SIEM Platform	Standalone SIEM, SOAR, UEBA
Flexibility	<ul style="list-style-type: none"> • All capabilities from one vendor • All components are pre-integrated in the platform, ready to be activated when needed • Supports staged purchase and deployment from a single vendor • Rich and broad feature set 	<ul style="list-style-type: none"> • Ability to choose a best-in-class product from any vendor • Components are reliant on integrations and mapping between tools is often required • Might need to purchase different modules from different vendors • Sophisticated, but siloed feature sets
Integration	<ul style="list-style-type: none"> • SIEM, SOAR, UEBA, BCS capabilities are pre-integrated • Out-of-the-box normalization of data formats and alert taxonomy across all platforms • Cross-platform features usable out of the box • Pre-integrated with a broad set of IT, cloud infrastructure, and APIs 	<ul style="list-style-type: none"> • Extensive integration is required for platforms to work together • Additional integration is required to normalize data formats (even when platforms are purchased from the same vendor) • Cross-platform features require extensive setup and integration • Proprietary vendor protocols often require integration with IT and cloud infrastructure
Ease of Use	<ul style="list-style-type: none"> • One workplace for all functionality. Unified management interface and dashboards • Out-of-the-box, cross-platform playbooks, workflows, and remediation actions. Easy to customize if desired • With one UI and navigation to learn, onboarding is quicker 	<ul style="list-style-type: none"> • Multiple management interfaces and dashboards unless extensive integration is done • Significant expertise and time required to create cross-platform playbooks, workflows, and remediation actions • Complex. Significant SOC employee training required
Performance	<ul style="list-style-type: none"> • SaaS native means less operational overhead to strengthen cyber defenses • Eliminates the complexity of operating SIEM-SOAR-UEBA-BCS solutions without having to compromise on security performance and efficacy 	<ul style="list-style-type: none"> • Maintenance of 3 different tools to keep optimal performance • Excellent performance when SOC team has the expertise to exploit complex and highly sophisticated feature sets
ROI	<ul style="list-style-type: none"> • Best ROI for mid-tier enterprise, modest security budget 	<ul style="list-style-type: none"> • Best ROI for 30-100 person SOC, large security budget

WHAT TO LOOK FOR IN A CONVERGED SIEM PLATFORM

A converged SIEM platform should contribute significantly to making your cybersecurity operations simple, powerful, and affordable. To that end, there are a few key considerations to keep in mind when comparing converged solutions:

Coverage

The converged SIEM platform should provide threat detection and response across:

- Infrastructure
- Assets and endpoints
- Cloud platforms
- Business-critical applications

Architecture

The converged SIEM platform architecture should support:

- Big data infrastructure
- Unlimited data storage and long-term data retention
- Real-time collection and analysis of unlimited event logs in real-time
- Unified, real-time view of all event logs (IT and behavior)

Innovation

The converged SIEM platform should feature technologies that support:

- Cross-platform data analysis, correlation, and context
- Machine learning
- AI-driven automation of threat prioritization, investigation, remediation
- Support for full or partial automation

Tools

The converged SIEM platform should provide tools to assure fast incident response:

- Best-practice workflows to speed incident investigation
- Best-practice playbooks to ensure a consistent approach to remediation

- Fully automated or analyst-assisted remediation, with real-time guidance to the proper response

Flexible Deployment

The converged SIEM platform should support flexible deployment, including:

- On-premise: always an option to deploy hardware and software on-prem.
- Private Cloud: If much of your IT infrastructure is in the cloud, it makes sense to locate SIEM- SOAR- UEBA in the cloud as well.
- SaaS: Cloud-delivered services are attractive to enterprises that want to avoid the cost of installation, maintenance, and skilled personnel while retaining the ability to expand cybersecurity operations according to a predictable pricing scheme as their business grows.

Predictable Licensing

Beware of pricing schemes. Make sure you understand and can predict converged SIEM costs so you don't run into a data-versus-budget problem as your business grows.

Capacity-Based Pricing

Capacity-based pricing charges by volume - per message, gigabyte, event, second, etc. This pricing scheme can cause an organization to exceed its cyber budget as it grows and more users and cybersecurity systems generate more data. It's hard to know where your costs will end up.

User-Based Pricing

User-based pricing charges customers a certain amount per user (i.e., connected device) per year, no matter how much data each user generates. This is a more straightforward way to size a SIEM and control costs. Predictable costs bring SIEM, SOAR, UEBA, and BCS solutions within easy reach of numerous enterprises that previously could not afford them.

BUILDING THE BUSINESS CASE

With A SOC: The combined SIEM+SOAR+UEBA solution will make your SOC more efficient and more effective by providing more accurate and comprehensive threat intelligence, automating repetitive and time-consuming SOC processes, and enabling consistent and fast responses to potential threats and attacks in progress.

Without A SOC: Even enterprises with a small security team and no formal SOC should not rule out the unified SIEM+SOAR+UEBA solution. The cost, staffing, and resource savings that the unified solution provides could be the perfect solution for companies that don't have big budgets but still want to advance their cybersecurity posture.

A comprehensive solution will provide a blueprint and a roadmap to evolve your approach and results regarding cyber security.

How To Showcase The Value To Management

- Improved Communication Across the Board – get everyone on the same page
- Cost-effective
- Removing complexity and creating transparency – clear and measurable KPIs, methodology aiding collaboration
- Address the skills gap and lack of trained professionals – save of headcount, and keep moving forward

Pre-integrated with IT infrastructure across the enterprise

Converged SIEM platforms are pre-integrated with a broad spectrum of IT security systems, allowing enterprises to get up and running quickly. Likewise, native integration with on-premise workloads, cloud workloads, and cloud security tools support whatever deployment scenario (on-prem, private cloud, hybrid, SaaS) best suits each enterprise.

To achieve the same level of integration with best-in-class platforms requires expert resources and time.

WHY LOGPOINT

SIEM, SOAR, UEBA, BCS tools and EDR capabilities play an essential role in securing the enterprise from cyberattacks. Every organization can benefit from the capabilities they provide. However, many enterprises have resisted using SIEM, SOAR, and UEBA to improve their cybersecurity due to concerns about complexity, limited budgets, and lack of security skills. Moreover, companies that invested in SIEM technology could not include critical business applications in their central security monitoring operations.

Logpoint's Converged SIEM Platform overcomes these obstacles by providing a pre-integrated cybersecurity solution for threat detection and response that is:

- **Simple:** Easy to install, configure, integrate, and operate with a minimally staffed and skilled security team or SOC.
- **Powerful:** Flawless cybersecurity fundamentals that help companies build and maintain a solid cyber defense and advance the maturity of their security program.
- **Comprehensive:** Logpoint Converged SIEM Platform unifies threat detection and response across enterprise IT infra, assets, endpoints, cloud platforms, and business-critical applications and gives security teams all the tools they need for rapid investigation and remediation of internal and external threats.
- **Predictable licensing:** Cost effective both in terms of initial outlay and maintainability. There is no need to pay a premium for highly sophisticated features that you will never use. Logpoint pioneered the transparent per node license for SIEM solutions. We apply that same transparent and flexible licensing model to the Logpoint Converged SIEM platform to significantly reduce your total cost of ownership and provide predictability for your security investments.

Let us show you how to dramatically improve your cybersecurity posture right now by leveraging the Logpoint Converged SIEM Platform. [Contact Logpoint here.](#)