

SIEM Vendor Checklist 2026:

20 Questions to Ask When Evaluating a Next-Gen SIEM

Isn't it time you made the switch to NetWitness?

Many SIEMs are just specialized databases, collecting logs from various IT systems and applications, and providing tools to query the data. Originally architected for compliance use cases, over the years most have added security features to detect anomalies and alert security teams. The design center, however, remains the same.

In contrast, NetWitness Logs is purpose-built built for the threat detection, investigation, and response use case. While it has all the same SIEM compliance capabilities, NetWitness Logs is built for the SOC. It integrates seamlessly with all of your security tools and with other NetWitness products to create a true security foundation that serves the needs of all SOC personnel, from the newest L1 Analyst to the most skilled Threat Hunter.

Whether you're trying to simplify threat detection, reduce dwell time, or support your compliance, only NetWitness delivers the visibility and scalability that the most security-conscious SOCs require. By delivering pervasive log visibility, centralized monitoring and management, and dynamic parsing and enrichment at capture time, NetWitness dramatically speeds threat detection and response, from alerts to analysis to resolution.

If you want to empower your analysts with more time to look ahead and operate more strategically, then see for yourself how your SIEM stacks up to the comprehensive visibility and platform flexibility of NetWitness.

Can your SIEM ...

1. Accelerated, Targeted Threat Detection

- ☑ Provide useful actionable information for all levels of your security personnel - from L1 analysts to your most senior threat hunters?
- ☑ Quickly detect known bad and potentially damaging behavioral anomalies across your entire infrastructure?
- ☑ Detect threats utilizing up-to-date intelligence, from vendor-provided intelligence to commercial and open source feeds?
- ☑ Apply multiple threat detection techniques including simple and complex rules, advanced threat intelligence, identity-aware behavioral analysis, and cutting-edge AI?
- ☑ Dynamically parse, tag, index, normalize and enrich incoming logs at ingestion time and at enterprise scale?
- ☑ Automatically map events and investigations to the MITRE ATT&CK framework for standardized operations and increased compliance?
- ☑ Deliver high-quality compliance features, but is optimized for threat detection and true, actionable security?

2. Efficient, Flexible, User-Friendly Design

- ☑ Deliver complete deployment flexibility with modular options including on-premises, hybrid, or cloud environments, either self-managed or delivered as a service?
- ☑ Reduce operational costs with clear, value-based pricing, optimized usage of compute and storage resources, and streamlined administration?
- ☑ Expand to a fully integrated solution whenever you are ready, including network and endpoint data planes, UEBA, and asset prioritization?
- ☑ Enable point-and-click, visual threat hunting inside massive amounts of data with less effort, greater effectiveness, and the ability to make it easily repeatable?
- ☑ Provide integrated investigations and case management with options for robust security orchestration, time-saving automation, and highly effective response?
- ☑ Manage retention based on flexible organizational policies that can accommodate any range of geographies, regulations, and business goals?
- ☑ Transform terabytes of logs into easily understood and navigable information in a graphical interface, making it easy to visualize patterns?
- ☑ Provide a flexible interface that works for every role and skill level in your SOC and compliance group?

3. Unparalleled Visibility for Spotting Threats Anywhere

- ☑ Easily ingest logs from devices and applications on-premises, in private and public clouds, from SASE gateways, or SaaS applications?
- ☑ Connect your log-based threat detection with network traffic and endpoint telemetry so you can automatically detect and document the entirety of a security incident?
- ☑ Decrease your time to detect, investigate and respond to anomalies and threats?
- ☑ Connect to hundreds of devices and applications through pre-built parsers, or quickly build a custom parser with a point-and-click tool in minutes?
- ☑ Add both technical and business context to your log traffic as you receive it so you can more quickly investigate issues and better understand its impact everywhere in your organization?
- ☑ Offer comprehensive visibility into everything you need for both outstanding compliance and actionable security?

Want more out of your SIEM?

Find out how you can empower your security teams to rapidly detect, understand the full scope of a compromise and automatically respond to threats before business damage is done. NetWitness® Platform combines log, network traffic, user behavior and endpoint analysis with business context and threat intelligence to identify and respond to cyber threats, accelerating the speed and effectiveness of your team.

[Visit Our Website](#)