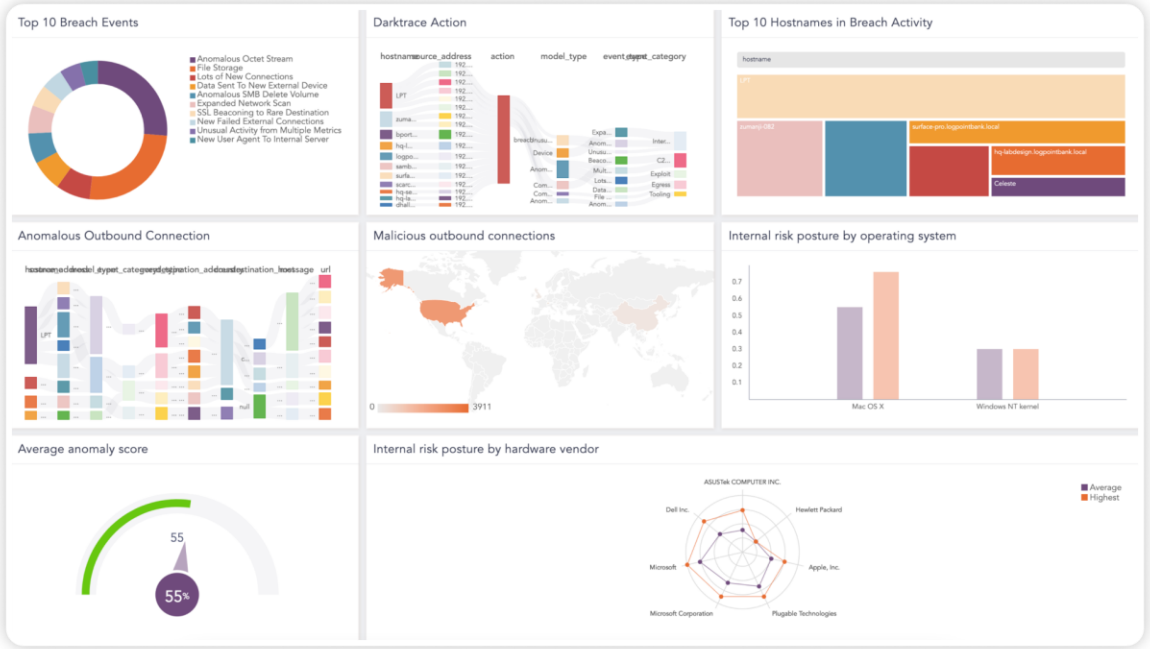
LOGPOINT

LOGPOINT SIEM

Security analysts can now turn their SIEM into a Cyber Defense Platform by unifying SIEM, SOAR, and UEBA capabilities. Logpoint SIEM is an end-to-end security event management platform for enterprises and MSSPs that accelerates threat detection, investigation, and response with easy add-ons. Instead of using various standalone products, SOC teams integrate data sets from disparate sources into a consolidated platform and get full visibility over the IT infrastructure.

MAKE FASTER, WELL-INFORMED DECISIONS WITH AN ALL-IN-ONE SAAS CYBER DEFENSE PLATFORM



In Logpoint SIEM, the alerts are mapped to the MITRE ATT&CK framework

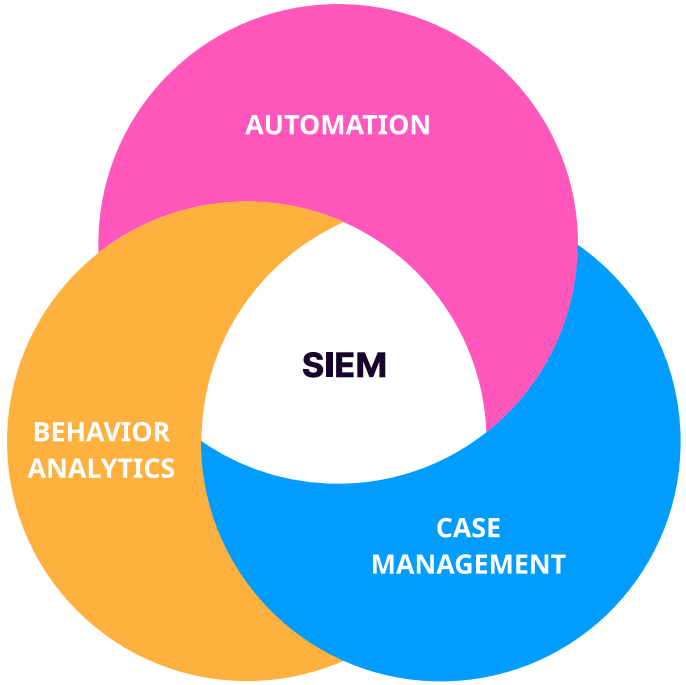
It comes with the same platform and functionalities that you love of Logpoint SIEM, but when deployed as SaaS, it brings extra benefits, such as easier deployment and hassle-free scaling.

Logpoint SIEM SaaS enables you to

- Accelerate TDIR processes with expanded visibility and automation
- Gain time and efficiency by integrating different security tools
- Meet the strictest regulations with pre-configured compliance use cases
- Prioritize alerts and automate the investigation and response workflow with out-of-the-box playbooks targeting common security use cases
- Identify threats that otherwise go unnoticed using machine learning

Logpoint SIEM collects log data from devices and applications across the entire IT infrastructure. Logs are then transformed into high-quality data through normalization and correlations. The platform automatically identifies and sends alerts about abnormalities in user behavior using machine learning algorithms. In addition, Logpoint SIEM maps the alerts to the MITRE ATT&CK framework and enriches them with threat intelligence and contextual information to define the severity of the threats. Based on the information gathered, it automatically runs playbooks to investigate and respond to attacks quickly and safely in no time.

STREAMLINE SECURITY WITH A COST-EFFECTIVE PLATFORM



Short-staffed and with too many tools to deal with and too many alerts to look into, security teams struggle to investigate incidents and effectively respond to threats in a quick and proper manner; and this is a risk for the organization. Logpoint SIEM automates those time-consuming and repetitive tasks. It gives time back to analysts and provides them with tools for easy collaboration and better incident management.

Key benefits

Easy to deploy: As a SaaS platform, onboarding and implementation is a simplified process, making Logpoint SIEM available with a minimal lead time.

Simple to operate: Cloud-based delivery removes the hassle of maintaining and updating systems, allowing you to focus on security.

End-to-end platform: By adding threat intel, business context, and entity risk, weak alerts turn into meaningful investigations and fast responses.

Continuous product improvements: A dedicated team of security researchers regularly updates the product's detection and response capabilities, increasing your agility to deal with the emerging threat landscape.

A single tool for all security aspects of your business: Logpoint SIEM unifies and automates incident detection, investigation, and response processes, drastically improving SOC efficiency and minimizing compliance risk.

ENABLE YOUR TEAM WITH END-TO-END CYBER DEFENSE

Key features

Cloud-based deployment: Cloud-delivered Logpoint SIEM makes deployment and scaling hassle-free without losing the features of on-prem platforms or the benefits of consolidating all cyber security tools.

Data privacy: Logpoint SIEM has completed the SOC 2 examination and meets its criteria for cloud security, ensuring total isolation and protection of customer data to comply with GDPR, Schrems-II and the strictest data security regulations.

Support for 1.000+ data sources: Logpoint SIEM collects data from endpoints, cloud platforms, and business-critical applications, enabling covering the whole infrastructure with a single tool

Data normalization: Logpoint SIEM normalizes log data into a single common language, making it easy to correlate data across applications and identify patterns.

80+ detectors using machine learning: Logpoint SIEM uses machine learning to analyze user behavior to identify the known unknowns, allowing you to react, investigate, and mitigate quickly

800+ integrations out of the box: With an extensive list of supported log sources, you can orchestrate disparate tools and automate anything in your tech stack to prevent, detect, and respond to threats.

80+ ready-to-use playbooks: Logpoint SIEM automates the investigation and response processes, guiding the analyst on the next step to take and accelerating response time from hours to seconds.

Endpoint security: Logpoint's native endpoint agent provides additional insights into user actions and processes running on your endpoints to then automate investigation and response.

UNLOCK MORE BENEFITS WITH LOGPOINT SIEM SAAS

Save time and resources: Logpoint takes care of the architecture, so your organization can save on resources used on installation, hardware, and deployment errors. And because updates are automatically rolled out, security analysts won't have to spend time updating the software to the latest version.

Never miss on compliance: Organizations that are unaware of new compliant requirements might fail to install new compliance updates, resulting in otherwise avoidable fines. With cloud-delivered software, you gain peace of mind knowing that your systems comply with the latest data and security regulations and that your data is always stored inside the EU.

With transparent costs comes predictable budget: Logpoint SIEM offers transparent and clear pricing. With a licensing based on data ingestion for the SIEM and the number of workstations for add-ons, your Finance team doesn't have to worry about unexpected costs, and it doesn't affect how your analysts work as the price is not usage-based.

SaaS grows with your organization: When your organization grows, your cybersecurity platform should grow with you – so you can upgrade or downsize depending on your needs. With nearly unlimited storage and scalability, Logpoint supports your security growth. We ensure that Logpoint SIEM performs at its best so the analysts can do it, too.