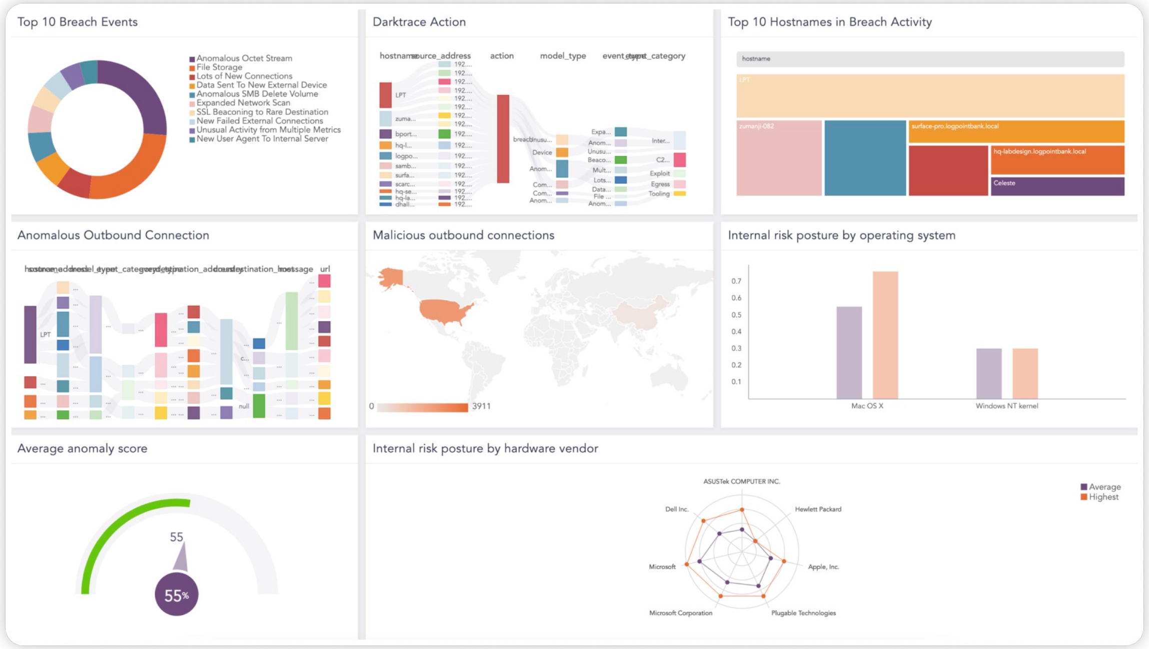
LOGPOINT

LOGPOINT CONVERGED SIEM

Logpoint Converged SIEM helps SOC teams combine data sets from multiple sources. Instead of using multiple standalone products, they now have one single source of truth. Converged SIEM is the only unified platform that delivers SIEM+SOAR, UEBA, Endpoint Security and BCS capabilities as a service directly to enterprises and MSSPs – all from a single plane of glass.

INCREASE EFFICIENCY WITH AN ALL-IN-ONE CYBERSECURITY SOLUTION

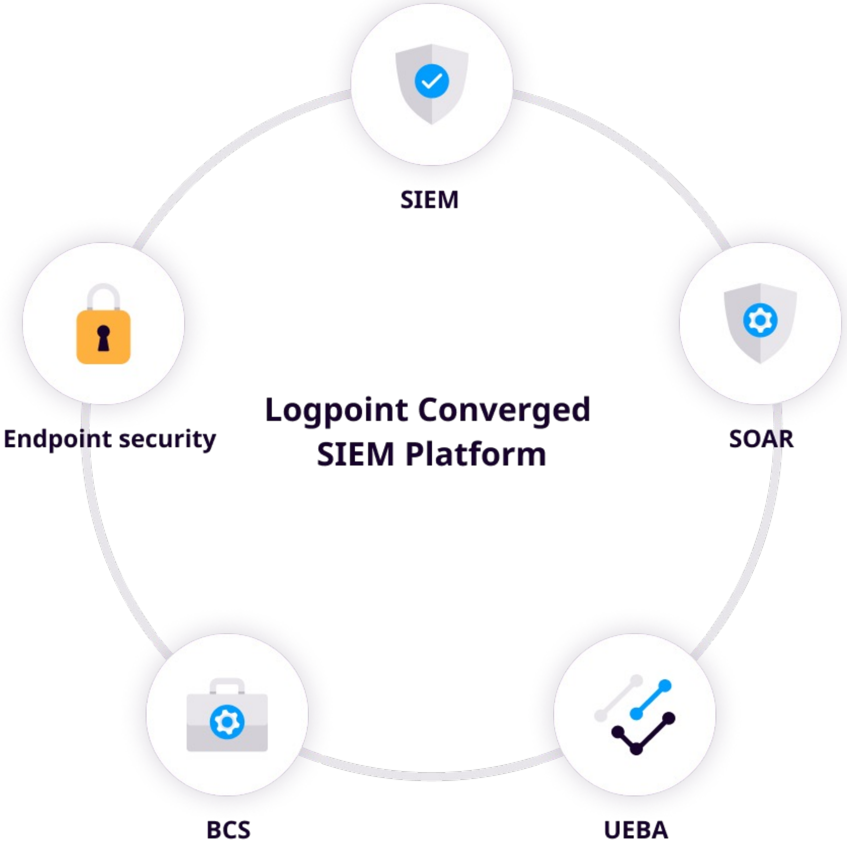

Top 10 Breach Events
Anomalous Octet Stream
File Storage
Lots of New Connections
Data Sent To New External Device
Anomalous SMB Delete Volume
Expanded Network Scan
SSL Beaconing to Rare Destination
New Failed External Connections
Unusual Activity from Multiple Metrics
New User Agent To Internal Server
Darktrace Action
hostname
source_address
action
model_type
event_type
event_category
Top 10 Hostnames in Breach Activity
hostname
LPT
zumanji-082
surface-pro.logpointbank.local
hq-labdesign.logpointbank.local
Celeste
Anomalous Outbound Connection
Malicious outbound connections
0
3911
Internal risk posture by operating system
0.7
0.6
0.5
0.4
0.3
0.2
0.1
Mac OS X
Windows NT kernel
Average anomaly score
55
55%
Internal risk posture by hardware vendor
ASUSTek COMPUTER INC.
Hewlett Packard
Apple, Inc.
Plugable Technologies
Microsoft Corporation
Microsoft
Dell Inc.
Average
Highest

Logpoint Converged SIEM enables you to

- Collect and centralize log data
- Meet the strictest compliance regulations with ease
- Detect the most advanced threats utilizing machine learnings
- Boost SOC productivity with automated alert triage
- Automate the whole detection, investigation, and response workflow with out-of-the-box playbooks targeting the most common security use cases

Converged 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 solution automatically identifies and sends alerts about incidents and abnormalities using machine learning algorithms. In addition, Converged SIEM maps the alerts to the MITRE ATT&CK framework, brings in threat intelligence, and gathers contextual information to define the severity of the threats. Based on the information gathered, necessary response playbooks are automatically run mitigating the attacks quickly and safely in a matter of seconds.

THE MOST EFFICIENT AND EFFECTIVE WAY TO PROTECT YOUR BUSINESS



Security teams are short-staffed. These staff shortages mean teams are struggling to investigate incidents and effectively respond to threats in a quick and effective manner. Logpoint Converged SIEM automates time-consuming and repetitive, yet critical, actions so your team can collaborate and manage incidents more effectively.

Key benefits

Efficiencies of scale: One platform providing full integration of data from endpoints, SIEM, UEBA and SAP into SOAR.

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

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: Converged SIEM unifies and automates incident detection, investigation, and response processes, drastically improving efficiency and minimizing risk.

ENABLE YOUR TEAM WITH AUTOMATION

Key features

Consolidate your tech stack: Thanks to our converged approach, SIEM, SOAR, UEBA are fully integrated in one platform to accelerate TDIR processes.

Data privacy: Converged SIEM assures total isolation and protection of customer data and is compliant with the strictest data privacy regulations, including Screms-II, General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

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

Data normalization: Converged 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: Converged 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: Converged SIEM orchestrates disparate tools and automates actions

75+ ready-to-use playbooks: Converged SIEM automates the investigation and response processes, accelerating response time from hours to a matter of seconds.

Endpoint security: Powered by SIEM, SOAR and UEBA, our native endpoint agent, AgentX, comes with endpoint detection and response capabilities.