Security Operations Capability Vendor Integration

Consolidate SASE telemetry, UEBA insights, and SIEM/SOAR/XDR workflows for faster detection, investigation, and response.

Key Benefits

- Unified SOC visibility across users, devices, branches, applications, network flows, and security events.
- Faster detection and response through SIEM, SOAR, XDR, and threat-intel integrations.
- Adaptive SASE enforcement using UEBA confidence scores, endpoint risk, and policy context.

Challenges

Security Operations Centers need a complete view of users, devices, applications, network paths, and threat events, but telemetry is often fragmented across endpoint, network, cloud, and SASE tools. When SIEM, SOAR, XDR, and access controls operate in silos, analysts spend more time correlating events manually and less time containing threats. As a result, risky users, compromised endpoints, lateral movement, and data exfiltration attempts may remain active longer than necessary.

Solution

VersaONE integrates with Security Operations vendors and turns SASE into a security operations sensor and enforcement layer. Versa collects network, firewall, access, application, threat, DLP, IPS, SD-WAN, and user activity telemetry, then exports it to SOC platforms such as Cisco Splunk, Microsoft Sentinel/Defender XDR, CrowdStrike Falcon NG-SIEM, Google SecOps/Chronicle, Elastic, Securonix, Exabeam, IBM QRadar, and Rapid7. Versa UEBA adds behavioral risk context, and Versa policy can use risk, user, device, and application context to dynamically deny, isolate, inspect, segment, log, or trigger response workflows.

Business Value

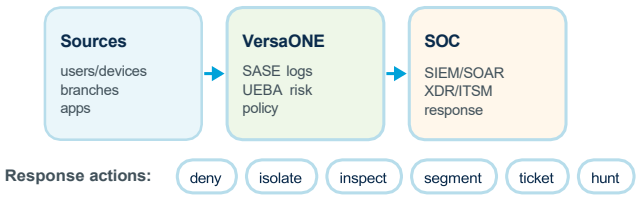
Use Case/ Challenge	1. SOC teams lack a single view across endpoint, network, cloud, user, and application activity. 2. Manual correlation across SIEM, SOAR, XDR, and SASE tools slows triage and response. 3. High-risk users and compromised devices can remain active when detection is disconnected from enforcement.
Solution	1. Export Versa SASE, SD-WAN, NGFW, SWG, CASB, ZTNA, DLP, IPS, and Analytics logs to security operations platforms. 2. Feed Versa telemetry into Cisco Splunk, Microsoft Sentinel/Defender XDR, CrowdStrike Falcon NG-SIEM, and other SIEM/ SOAR ecosystems. 3. Use UEBA, endpoint risk, and policy context to trigger inline actions such as deny, isolate, inspect, segment, or log.
Benefits	1. Faster detection, investigation, and threat hunting with correlated SASE and endpoint telemetry. 2. Reduced manual correlation and stronger SOC workflow automation. 3. Better compliance readiness with centralized, searchable, audit-ready logs. 4. Inline response that contains threats before lateral movement or data loss expands.

Technical Solution

Versa network operations capability combines telemetry collection, analytics, experience monitoring, and change workflow context. Versa Analytics Insights analyzes telemetry from endpoints and traffic to identify probable root causes

for site, link, traffic, and application issues. Client-based Digital Experience Monitoring periodically measures end-to-end network and application performance for user devices using the Versa SASE Client. NetOps teams can then export alerts, metrics, logs, and policy context to observability, alerting, automation, and ITSM tools.

SASE-to-SOC Telemetry and Response Loop



Vendor Integration Patterns

Cisco Splunk

SIEM and log analytics

Stream Versa Analytics machine, alarm, event, and threat logs to Splunk using syslog/IPFIX workflows and the Versa app for Splunk dashboards.

Microsoft Sentinel / Defender XDR

SIEM/SOAR plus endpoint and cloud context

Forward Versa SASE security events and logs into Microsoft security operations workflows and correlate network activity with Defender endpoint, identity, and cloud detections.

CrowdStrike Falcon NG-SIEM

Endpoint and network threat correlation

Ingest Versa firewall, SD-WAN, application, network threat, vulnerability, and access logs into Falcon NG-SIEM via Falcon LogScale for unified investigations.

Broader SecOps Ecosystem

SIEM, SOAR, XDR, threat intel, and ITSM

Integrate with Google SecOps/Chronicle, Elastic, Securonix, Exabeam, IBM QRadar, Rapid7, and additional SOC platforms through log forwarding and API workflows.

Key Capabilities

- Full SASE telemetry export: Send SD-WAN, NGFW, SWG, CASB, ZTNA, DLP, IPS/threat, app, access, and analytics logs.
- Flexible SIEM destinations: Configure primary/ secondary FQDN or IP, destination port, TCP/UDP transport, and VPN context.
- UEBA risk analytics: Detect abnormal behavior, calculate confidence scores, and classify users into risk bands.
- MITRE ATT&CK behavior coverage: Monitor bulk actions, failed logins, impossible travel, risky countries, and ATT&CK techniques.
- Closed-loop response: Deny, isolate, inspect, segment, open tickets, or trigger response workflows.
- Compliance-ready operations: Centralized logs support investigations, reporting, audits, and regulated environments.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa

Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.

Part# SB_SASE-SECOPS-01.0