Endpoint Security Vendor Integration

Integrate EDR, XDR, MDM, and UEBA telemetry with VersaONE Universal SASE to enforce risk-aware access in real time.

Key Benefits

- Adaptive access using endpoint posture, risk, identity, app, and location.
- Inline enforcement across ZTNA, SWG, CASB, NGFW, and SD-WAN.
- Automated containment: deny, isolate, quarantine, or inspect.
- Unified visibility across endpoint and network telemetry.

Challenges

Enterprises rely on endpoint tools to detect compromised devices, but endpoint telemetry is often siloed from network and application enforcement. Static Zero Trust policies cannot account for changing device posture, active threats, unmanaged endpoints, or unusual behavior. As a result, risky devices may continue accessing private applications, SaaS, cloud services, and the internet while SOC teams manually correlate endpoint and network events.

Solution

Versa integrates with Endpoint Security vendors and extends SASE policy decisions with endpoint context from leading EDR, XDR, MDM, and UEBA systems. Versa Endpoint Information Profiles assess device posture, such as anti-malware, firewall, disk encryption, OS, patch status, data-loss protection, and management status. When endpoint risk changes, Versa adapts access inline by permitting, denying, isolating, quarantining, or applying deeper inspection across SD-WAN, SSE, ZTNA, NGFW, and cloud security controls.

Business Value

Use Case/ Challenge	1. Static Zero Trust rules fail to reflect real-time endpoint risk. 2. Siloed endpoint and network telemetry slows detection and response. 3. Compromised or unmanaged devices may remain active without inline enforcement.
Solution	1. Integrate endpoint risk, posture, EDR/XDR alerts, MDM status, and UEBA signals into Versa policy. 2. Enforce adaptive access across private apps, SaaS, internet, LAN, WAN, and cloud resources. 3. Trigger dynamic containment actions such as deny, isolate, quarantine, or full inspection.
Benefits	1. Adaptive ZTNA that responds to changing device risk. 2. Reduced lateral movement from high-risk or compromised endpoints. 3. Unified endpoint and network visibility for faster investigations. 4. Streamlined compliance through auditable access and policy decisions.

Technical Solution

Endpoint platforms provide risk and posture signals such as threat detections, endpoint health, vulnerabilities, patch status, encryption and firewall posture, managed-device status, and active response actions. Versa consumes this

context through integrations and maps it to policy through the Versa SASE Gateway, Endpoint Information Profiles, and the VersaONE policy engine. The result is an adaptive enforcement loop that connects endpoint telemetry, inline SASE inspection, application access, and SOC workflows.

Vendor Integration Patterns

CrowdStrike Falcon

EDR, ZTA scoring, and NG-SIEM

Falcon endpoint risk and Zero Trust Assessment scores can drive Versa access policies; Versa telemetry can also enrich CrowdStrike NG-SIEM for correlated threat hunting.

Microsoft Defender for Endpoint

EDR plus device compliance workflows

Microsoft endpoint risk, threat, and compliance signals can be used with Versa posture-aware policies; MDM workflows can deploy and manage the Versa SASE Client.

SentinelOne

Endpoint threat and response telemetry

SentinelOne threat and risk context can trigger adaptive enforcement in Versa, including stronger inspection, session denial, or quarantine workflows for compromised devices.

Other Endpoint Ecosystem

Antimalware and posture vendors

Other endpoint security vendors include Avast, Bitdefender, ESET, F-Secure, Kaspersky, McAfee, Panda, Symantec, Trend Micro, Webroot, and Windows Defender.

Key Capabilities

- Dynamic Risk-Based Access Control: Adjust private app, internet, SaaS, LAN, and WAN access based on real-time endpoint posture and risk.
- Inline Policy Enforcement: Apply SWG, CASB, DLP, malware, URL filtering, IPS, ZTNA, and NGFW controls according to device context.
- Automated Containment: Deny, isolate, quarantine, or force enhanced inspection when a device becomes risky or compromised.
- Unified Visibility: Correlate endpoint events with user, device, path, application, firewall, and security telemetry in one policy and analytics model.
- Flexible Deployment: Support cloud, on-premises, hybrid, managed, and sovereign deployment models using a unified SASE platform.

VERSA

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-ENDPTSEC-01.0