Vulnerability & Threat Management Vendor Integration

Continuously identify, prioritize, and reduce exposure by connecting vulnerability intelligence to SASE enforcement.

Key Benefits

- Correlate exposure: Combine scanner, endpoint, user, app, and network signals in one risk-aware SASE control plane.
- Prioritize real risk: Weight VTM and EDR attributes so teams focus on high-risk entities and exploitable paths first.
- Enforce at the edge: Apply IDS/IPS, NGFW, SWG, ZTNA, quarantine, and block policies close to users and branches.
- Validate remediation: Use analytics, logs, packet capture, tickets, and reports to confirm risk reduction.

Challenges

Security teams often have more vulnerability findings than they can action. Scanners, endpoint tools, and threat feeds identify risk, but enforcement still depends on manual correlation across firewalls, SSE policy, SD-WAN branches, cloud apps, and tickets. Attackers exploit this gap when exposed assets remain reachable, high-risk devices keep accessing sensitive apps, and threat context is lost between tools.

Solution

VersaONE integrates with Vulnerability & Threat Management vendors and brings vulnerability, threat, and entity risk context into the SASE enforcement path. Concerto integrates Vulnerability Threat Manager sources such as Qualys, Tenable, and Microsoft Defender, combines findings with unified entity risk profiles, and distributes calculated risk to SSE gateways. Versa IDP/IPS, NGFW, SWG, ZTNA, ATP, CASB, and analytics can then enforce policy, generate evidence, and help teams reduce exposure without separate point-product workflows.

Business Value

Use Case/ Challenge	1. Scanner findings and asset risk are isolated from SASE policy. 2. Vulnerabilities need prioritization by exploitability, entity context, and business criticality. 3. Threat detection and remediation require coordinated enforcement across branch, cloud, remote access, and internet traffic.
Solution	1. Ingest VTM telemetry from Qualys, Tenable, and Microsoft Defender and unify risk scoring in Concerto. 2. Associate vulnerability profiles with access policies and apply predefined or custom IDP signatures, SPack updates, and ATP protections. 3. Stream events to Versa Analytics, SIEM, and ITSM for investigation, reporting, and remediation workflows.
Benefits	1. Faster reduction of attack surface across SD-WAN, SSE, ZTNA, NGFW, SWG, and cloud access. 2. Lower alert noise through risk-based prioritization and contextual policy enforcement. 3. Stronger compliance posture with analytics, logs, packet capture, and audit evidence.

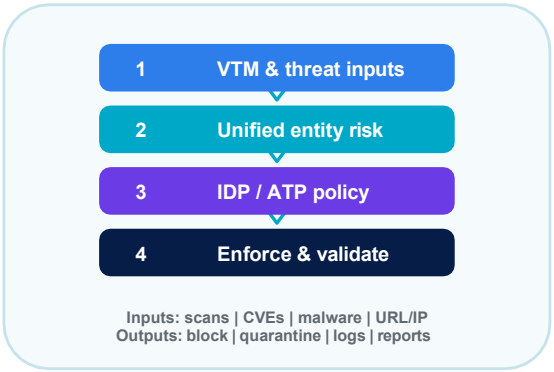
Technical Solution

Versa vulnerability and threat management connects exposure sources with policy enforcement. Scanner findings and threat telemetry are ingested by Concerto, normalized into unified entity risk profiles, and distributed to SSE gateways and security services. Policy determines whether to allow, log, block, quarantine, apply ZTNA restrictions, trigger packet capture, or open a response workflow.

Category Capabilities

- Threat Intel: URL, IP, malware, vulnerability, and DDoS analytics for detection, trend analysis, and reporting.
- IDP: IDS/IPS with predefined and custom vulnerability profiles, signature and anomaly detection, packet capture, and logs.
- ATP: Malware and threat analytics with policy actions to block known attack vectors, rogue traffic, and suspicious payloads.
- VTM: Scanner findings from Qualys, Tenable, and Microsoft Defender integrated into entity risk and SASE policy.

Vulnerability-to-Enforcement Loop



Vendor Integrations

Tenable	Qualys	Microsoft Defender
Exposure and vulnerability findings Use scanner context in entity risk scoring, prioritization, and policy decisions across Versa SASE.	Vulnerability scanner telemetry Ingest findings, poll updates, prioritize exposures, and drive enforcement from the SASE control plane.	Device and vulnerability signals Combine vulnerability, endpoint, and security risk context with VTM and EDR-driven enforcement.

Vulnerability & Threat Workflows Enabled by Versa

Ingest	Connect VTM sources and threat analytics, including scanner, CVE, URL, IP, malware, and DDoS data.
Normalize	Consolidate assets, users, devices, applications, accounts, and identities into unified risk profiles.
Prioritize	Weight EDR and VTM attributes and focus investigations on high-risk entities and exposures.
Enforce	Apply NGFW, IDP/IPS, ZTNA, SWG, ATP, quarantine, and block actions from policy.
Validate	Use Analytics, SIEM, ITSM tickets, packet captures, and reports to confirm risk reduction.

Additional ecosystem types of vendors include: cloud security, threat intelligence feeds, and vulnerability scanners.

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-VULTHREATMNGMNT-01.0