Dynamically Enforce Zero Trust Controls for Automated Threat Mitigation

Market Challenges

Modern security tools generate a wealth of valuable data across endpoints, networks, and cloud. One of the most consequential signals is a change in a device's risk level, yet this is also where many security architectures fall short. The signal exists, but the resulting security gaps are rarely closed in time.

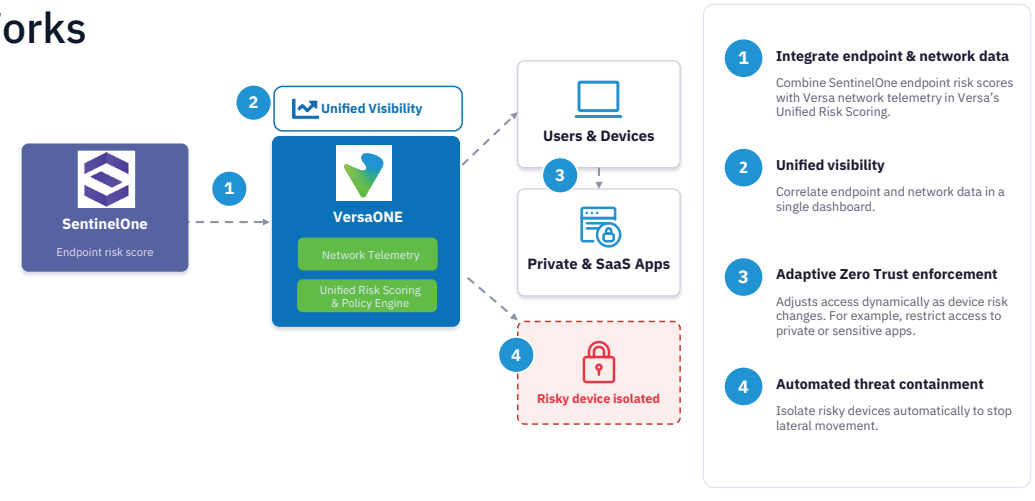
When a device's risk profile shifts, several gaps emerge. ZTNA access controls must reflect the change in real time rather than rely on a one-time static assessment that no longer reflects the current situation. Risky or compromised devices must be isolated before a threat can spread. Security teams need correlated visibility across endpoint, firewall, and network data to assess the full picture as it develops. Too much of this still depends on manual intervention, which delays response and widens the window of exposure. Organizations need continuous, risk-based enforcement that adapts in real time and automated response.

Joint Solution

SentinelOne and Versa have partnered to connect endpoint and network security, giving security teams end-to-end visibility and automated, risk-based policy enforcement. SentinelOne's Singularity Platform continuously detects and responds to threats across endpoints, identities, and cloud workloads. Versa's Universal SASE platform converges networking and security into a single cloud-managed service that enforces policy consistently across LAN, WAN, and cloud. Together, SentinelOne assesses and scores device risk while Versa translates that insight into real-time security policy and enforcement across the network.

Versa updates security policy dynamically based on a device's real-time risk, using SentinelOne's risk score among other factors. It applies inline controls that account for both a device's risk profile and the sensitivity of the application being accessed. As risk increases, Versa can microsegment suspicious devices to automatically isolate compromised endpoints and reduce lateral movement.

How it Works



SentinelOne and Versa integrate endpoint and network data to enforce Zero Trust dynamically as risk changes.

Versa integrates SentinelOne risk scores into its weighted Unified Risk Score to add context and enable adaptive, risk-based policy enforcement. Versa ingests these scores through an API from SentinelOne, at configurable polling intervals. Versa then updates security policy dynamically across its SASE platform. For example, Versa can reject an internet session when an entity's risk score is too high.

Key Use Cases

Versa applies network security policies based on each device's risk profile, matching the response to the level of risk.

Automatically Modify Access When Device Posture Changes

When a device's risk profile changes, Versa can modify the enterprise resources it can reach. High-risk devices can be restricted to limited internet access through context-aware policies and controls such as SSL inspection and advanced threat protection (ATP), while risky devices can be isolated or blocked from private applications and sensitive internal services.

Apply Additional Inspection to Risky Users and Devices

Versa can also route higher-risk users and devices through additional security inspection, applying deeper analysis to catch threats other controls might miss without fully blocking access.

Conclusion

By integrating endpoint telemetry with network policy, Versa and SentinelOne strengthen an organization's Zero Trust posture and closes the security gaps that arise when a device's risk profile changes. Access adapts continuously to real-time risk, and risky devices are isolated automatically, reducing lateral movement, accelerating response, and easing the burden on security teams.

Joint Solution Highlights

- **Adaptive Zero Trust Enforcement:** Dynamically adjust device access when risk profiles change.
- **Automated Threat Containment:** Automatically quarantine risky or infected devices to contain threats before they move laterally
- **Unified Visibility:** Correlate endpoint and network data to accelerate investigation and response

Integration Benefits

- Adaptive ZTNA
- Dynamic, risk-based assessment and enforcement
- Automated containment of risky devices
- Unified endpoint and network visibility
- Seamless integration and deployment

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, a global leader in SASE, 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 delivering 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.

Part# FAQ_VERSAONE-01.0