Network Infrastructure Vendor Integration

Unify SD-WAN, SSE access, NAC, DDI, IPAM, DNS threat intelligence, and network detection context across hybrid enterprise infrastructure.

Key Benefits

- Unified infrastructure context across SD-WAN, SSE, NAC, DNS, DDI, IPAM, and cloud connectivity.
- Secure traffic steering from branches and campuses to SSE services using policy-based or route-based tunnels.
- Identity-aware access through NAC, RADIUS, TACACS+, Active Directory groups, and 802.1X controls.
- DNS-layer threat protection using high-risk domains, malicious IPs, lookalikes, DoH bypass indicators, and threat feeds.

Challenges

Enterprise infrastructure now spans branch offices, campus networks, remote users, cloud services, data centers, and multiple security enforcement points. Network teams often manage access control, DNS/IPAM, SD-WAN, SSE, and threat detection in separate systems, making it difficult to connect identity, device, IP, domain, application, and tunnel context. The result is slower onboarding, inconsistent policy enforcement, and blind spots when traffic shifts between local breakout, cloud security gateways, and private applications.

Solution

VersaONE integrates with Network Infrastructure vendors and combines their capabilities into a unified network and security solution. Versa Secure SD-WAN steers traffic to third-party SSE services using GRE, IPsec, proxy chaining, routing, and automated workflows; Versa gateways ingest risk and threat context such as bad IP addresses, bad FQDNs, user risk, device risk, and application risk. Network access integrations with Cisco ISE enable 802.1X, RADIUS, TACACS+, and Active Directory group-based control, while DNS/DDI and IPAM intelligence from Infoblox can enrich policy, investigation, and threat prevention workflows. The result is a unified enforcement model across LAN, WAN, cloud, SaaS, and internet traffic.

Business Value

Use Case/ Challenge	1. Branch, campus, remote-user, cloud, DNS, and security-service infrastructure are managed through separate tools and policies. 2. Network access, DNS intelligence, IP identity, and traffic-steering decisions are often siloed from SASE enforcement. 3. Manual onboarding of SSE tunnels, NAC controls, and network infrastructure changes increases deployment risk and slows response.
Solution	1. Integrate VersaONE with SSE access, NAC/802.1X, DDI/IPAM, DNS threat intelligence, NDR, and SD-WAN ecosystems through tunnels, APIs, telemetry, and policy context. 2. Use Versa SD-WAN and SASE gateways to steer traffic to cloud security services while maintaining local breakout, segmentation, and branch resilience. 3. Enrich security policy with user, device, site, application, DNS, IP, and risk context from infrastructure platforms.
Benefits	1. Consistent policy enforcement across LAN, WAN, cloud, SaaS, internet, and private applications. 2. Faster infrastructure onboarding with workflow-driven tunnel creation, connector configuration, and policy deployment. 3. Better threat prevention by combining DNS-layer intelligence, access identity, and SASE inspection. 4. Improved auditability through centralized visibility into access, routing, segmentation, and policy decisions.

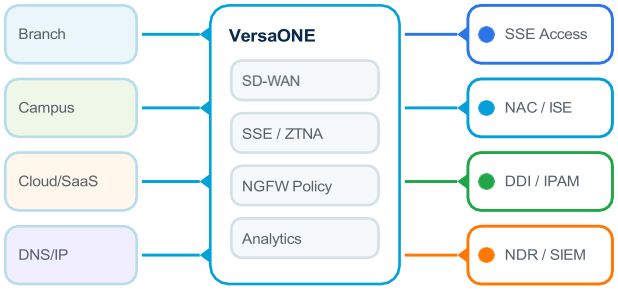
Technical Solution

Versa SASE network infrastructure capability combines traffic steering, access identity, DNS intelligence, segmentation, and telemetry. Versa Director and workflows simplify SSE onboarding by creating site-to-site tunnels and connector-based integrations. Versa SD-WAN supports policy-based and route-based IPsec VPNs, BGP, VRFs, and active monitoring, while infrastructure integrations enrich policy decisions with network, user, device, IP, domain, and application context.

Category Capabilities

- SSE Access: Steer branch and campus traffic to third-party SSE clouds using GRE, IPsec, proxy chaining, primary/secondary service nodes, and API/workflow automation.
- NAC / 802.1X: Integrate with Cisco ISE for RADIUS-based device authentication, NAS attributes, TACACS+ administration, and Active Directory group mapping.
- DDI and IPAM: Use DNS, DHCP, IP address, and domain intelligence to connect network identity with SASE policy, investigation, and compliance workflows.
- NDR and Threat Context: Enrich detection with traffic, DNS, user, device, site, IP, application, and risk context to identify anomalous flows and suspicious infrastructure.

Network Infrastructure Integration Loop



Outcomes: unified policy | secure access | threat intelligence | operational visibility

- SD-WAN Infrastructure: Apply BGP, VRFs, segmentation, local breakout, QoS, active-active branch design, and tunnel monitoring to keep access resilient and controlled.

Vendor Integrations

Zscaler SSE	Cisco ISE	Infoblox DDI/IPAM
Secure internet and SaaS access	NAC, 802.1X, and TACACS+	DNS threat intelligence
Integrate Versa Secure SD-WAN with Zscaler Internet Access using site-to-site IPsec tunnels, primary and secondary ZEN targets, CMS connectors, BGP/VRF topology, and workflow-based deployment.	Use Cisco ISE with Versa for RADIUS authentication, 802.1X device access, TACACS+ administration, Active Directory groups, and authentication/authorization/accounting workflows.	Apply DNS-centric threat intelligence for high-risk domains, lookalikes, malicious IPs, DoH bypass indicators, ransomware, malware C&C;, RPZ feeds, TIDE, Dossier, and SIEM enrichment.

Infrastructure Workflows Enabled by Versa

Connect	Automate secure tunnel and connector setup for SSE, cloud security, branch, data center, and partner infrastructure.
Authorize	Use NAC, 802.1X, RADIUS, TACACS+, certificates, and directory groups to control users, devices, and administrators.
Enrich	Combine IPAM, DNS, DDI, threat feeds, site, device, application, and user-risk context with Versa security policy.
Enforce	Apply consistent segmentation, NGFW, ZTNA, SWG, routing, and inspection policies across LAN, WAN, cloud, SaaS, and internet paths.

Additional ecosystem vendors include: Microsoft Entra Internet Access, Palo Alto SSE, Netskope Security Cloud, Akamai, BlueCat, EfficientIP, ExtraHop, Vectra AI, Darktrace, Corelight, Gigamon, and ServiceNow.

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-NETINFRA-01.0