VERSA

DATA SHEET

Versa Secure Internet Access

Organizations continue to struggle with an expanded attack surface. This is a natural consequence of having applications, workloads, and networking functions running in a mix of SaaS services, public clouds, private clouds, and on-premises hardware, in addition to the "traditional" points of external internet exposure, all accessed by a hybrid workforce and growing numbers of IoT devices while chasing a fast-changing threat landscape.

Versa Secure Internet Access (VSIA) is a cloud-delivered service that ensures uncompromised protection and a one-stop management experience for all internet and SaaS-bound traffic while delivering an optimized user experience. It consolidates SWG, NGFWaaS, CASB, and DLP capabilities on the VersaONE Universal SASE Platform to secure your headquarters, branches, remote locations, home offices, traveling users, and even "client-less" devices accessing distributed applications. Designed specifically for security and infrastructure teams navigating the challenges of digital transformation, VSIA can be managed by Versa or the customer.

Benefits

Secure SaaS access

- Versa CASB inline and out-of-band inspection with true first-packet auto-recognition automatically secures access to thousands of SaaS applications from a globally distributed network of enforcement points, addressing potential security gaps for cloud services in a broad set of scenarios.
- Zero Trust least privilege access for users, applications, and devices from both inside and outside corporate networks is continuously verified throughout a session based on dynamic user behavior and device security posture.

Full-stack threat protection

- Layered security with deep scanning for threats consolidating NG-FWaaS, SWG, URL filtering, IPS, anti-malware, CASB, and DLP, including for SSL-encrypted traffic.
- AI-powered Advanced Threat Protection (ATP) with multi-sandboxing and User and Entity Behavior Analytics (UEBA) stop sophisticated ransomware, advanced persistent threats (ATPs), zero-days, and insider threats. Both include detailed insights into adversary behavior aligned to the MITRE ATT&CK framework including intel on threat actors, associated campaigns, and targeted industries among others.
- Leverages shared threat intelligence across customer and cloud-hosted applications to proactively establish appropriate protection mechanisms.

Comprehensive data protection

- Versa DLP monitors for pre-defined and custom data patterns across a range of protocols and file types while supporting flexible actions to protect sensitive data on-premises and in the cloud and ensure regulatory compliance.
- Advanced features ensure precise data identification while integration with Microsoft Information Protection (MIP) labels allows for seamless data classification.
- Endpoint DLP features enhance protection by restricting actions such as copy/paste, screenshots, and USB data removal.

Simplified management

- A unified management portal lets you configure once and enforce a set of web security, DLP, SaaS app, ransomware and malware protection policies for both on-premises and remote users and devices.
- Seamlessly deploy VSIA security into your existing environment with pre-built API integrations that make it easy to integrate with third party IAM, SIEMs, DLP engines, automation tools, and encryption engines.

Visibility that clarifies

- Versa's unified data lake and AIOps intelligence identify anomalous behaviors in real time, replacing noisy alerts with actionable insights and automated remediation.
- Combine real-time monitoring and reporting with deep dives into historical telemetry aided by VersaAI to quickly and easily diagnose, troubleshoot and resolve issues.

Uncompromised user experience

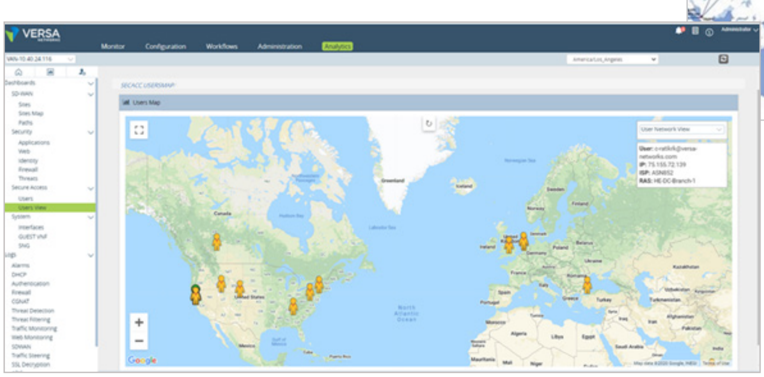
- VSIA was built on a cloud-first foundation designed to improve the user experience when they are accessing internet applications.
- Versa's single-pass architecture for all security, networking, and SD-WAN transport is done without creating complex network function service chains and ensures that the data packets spend the least amount of time in the cloud gateways, reducing negative impacts on the application experience.

Seamless integration with Secure Private Access

- When combined with Versa Secure Private Access (VSPA), enterprise- hosted applications can also be accessed directly via Versa Cloud Gateways, delivering privacy, control, and enhanced performance.
- Through the combination of VSIA and VSPA services, applications avoid hair-pinning traffic to the enterprise data center, thus improving the overall application experience.

Service components

VSIA is a core offering of the Versa Unified SASE service running on the VersaONE platform with the following operational elements:



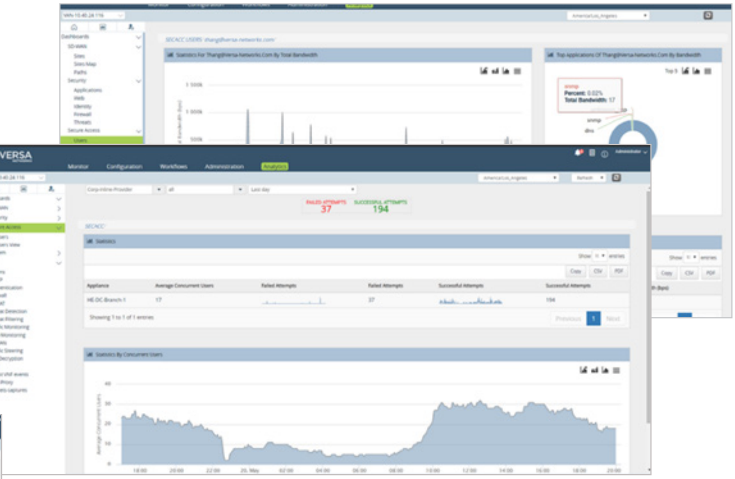
User: c-ratlikk@versa-networks.com
IP: 75.155.72.139
ISP: ASN852
RAS: HE-DC-Branch-1

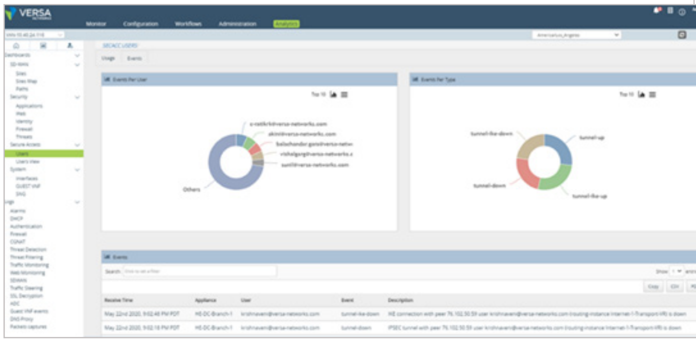
Versa Cloud Gateways

Versa's service points-of-presence are based on the industry-leading Versa Operating System and are globally distributed to provide reliable and secure on-ramps. The gateways authenticate users, authorize application access, and secure your enterprise network from external threats, while integrating advanced routing, comprehensive security, and market-leading SD-WAN. They securely connect to and integrate with your existing network and data center infrastructure, and intelligent gateway selection ensures that users and devices always connect to the closest and best- performing gateways based on real-time status and routing information.

Versa SASE Client

A software agent that runs on and extends the SD-WAN to client devices, Versa SASE Client creates a secure and encrypted connection to the Versa Cloud Gateway. Upon authentication and access authorization through the Versa Cloud Gateway, users can securely connect to enterprise applications in both the public and private cloud. The client supports application-aware policy to ensure that unnecessary traffic is offloaded at the device.





Versa Unified Portal

Versa's self-service portal gives enterprise administrators the ability to monitor and manage granular visibility of users and applications in a centralized location. The portal provides real-time and historical reporting at a network, application, and user level.

Service Tiers

Next Generation Firewall-as-a-Service	Essential	Professional	Elite
Application visibility and control w/DPI-enabled first packet auto-recognition	✓	✓	✓
Built-in stateful firewall with Denial-of-Service (DoS) protection	✓	✓	✓
QoS, traffic shaping, marking, classification	✓	✓	✓
Next Generation Intrusion Prevention System (NG-IPS)		✓	✓
File Reputation Feeds and Filtering		✓	✓
Malware protection – Single network antivirus engine		✓	✓
DNS Filtering & Security			
DNS forwarder, DNS proxy	✓	✓	✓
DNS Feeds and DNS Security		✓	✓
DNS tunnel detection – Block or sinkhole suspicious tunnels		✓	✓
Secure Web Gateway			
URL filtering, IP filtering, DNS filtering, GenAI dashboard	✓	✓	✓
Captive portal	✓	✓	✓
TLS inspection as forward proxy	✓	✓	✓
Management and Analytics			
Versa Concerto – Configuration, monitoring, license management, RBAC	✓	✓	✓
Logging – IPFIX, Syslog, Netflow, PCAPs with streaming to third-party SIEMs	✓	✓	✓
Dashboards and security reports for each service module	✓	✓	✓
AI observability – Verbo	✓	✓	✓
Digital Experience Management	**Essential**	**Professional**	**Elite**
Digital Experience Management – Essential	✓	✓	✓
Digital Experience Management – Professional	Add-on	Add-on	Add-on

Identity Management			
Integration with SAML, LDAP, AD, Identity proxy, Local	✓	✓	✓
Multi-Factor Authentication (MFA) - TOTP, SAML, email-based	✓	✓	✓
Access to VSIA Gateways			
User, group, and application access policies w/continuous security posture check	✓	✓	✓
Clientless application access – Application proxy (Reverse Proxy), PAC file based access		✓	✓
Versa Endpoint Client based access (Windows, macOS, iOS, Android, Linux, Chromebook) via IPsec VPN, TLS VPN, GRE	✓	✓	✓
Site to Site IKEv2 IPSEC or GRE based access	✓	✓	✓
SD-WAN based access to gateways	✓	✓	✓
Cloud Access Security Broker (inline)			
Cloud applications visibility & control for web, mobile apps		✓	✓
Shadow IT discovery		✓	✓
Cloud risk and policy enforcement for sanctioned & unsanctioned apps		✓	✓
SaaS tenant control restrictions		✓	✓
IT/IoT/OT Security			
Automated device discovery, fingerprinting, and identification		Add-on	✓
IoT and SCADA protocol identification and security		Add-on	✓
Data Loss Prevention (inline)			
Pre-defined & custom data patterns – ePHI, PII, PCI-DSS, HIPAA, GDPR, etc.		Add-on	✓
Rich set of protocols & file types – incl. HTTPS, email, PDF, Office, images (with OCR), etc.		Add-on	✓
Exact Data Match (EDM), Indexed Document Match, Document fingerprinting		Add-on	✓
Data classification through Microsoft Information Protection (MIP) labels		Add-on	✓
Supported actions: Allow/Block, Redact, Tokenize		Add-on	✓
Endpoint DLP – Prevent copy/paste, screenshots, and USB data removal		Add-on	✓
GenAI Firewall			
Web filtering of GenAI sites		Add-on	✓
Data Leakage Prevention to prevent sensitive data from leaking to GenAI sites / tools		Add-on	✓
Advanced Threat Protection			
Advanced Threat Protection (ATP) – Multi-AV, AI/ML, sandboxing, bare metal analysis, MITRE ATT&CK mapping – Limited profiles and file types			✓
Advanced Threat Protection (ATP) – Multi-AV, AI/ML, sandboxing, bare metal analysis, MITRE ATT&CK mapping – Unlimited profiles and file types		Add-on	Add-on
API-based Data Protection			
Retroscan and scheduled scans for scanning existing data at rest		Add-on	Add-on
Connectors for IaaS applications – AWS, Azure, GCP, OCI		Add-on	Add-on
Connectors for SaaS applications – Microsoft, Google, Confluence, Salesforce, ServiceNow, et al.		Add-on	Add-on
API CASB with activities control for supported SaaS/IaaS apps		Add-on	Add-on
Cloud DLP for SaaS/IaaS apps, Actions: Encrypt, Quarantine, Forensics, Legal hold (requires DLP)		Add-on	Add-on
Cloud ATP for SaaS/IaaS apps (requires ATP)		Add-on	Add-on
API-DP Essential – Includes retroscan, CASB for up to three IaaS or SaaS connectors			✓
User Entity Behavior Analytics (UEBA)			
AI-powered anomaly detection for risky users – multiple supported actions including MITRE ATT&CK mapping		Add-on	Add-on
Streaming logs from Versa Analytics through Versa Messaging Service (VMS)		Add-on	Add-on
Add-Ons			
Remote Browser Isolation		Add-on	Add-on
DLP for Email (through SMTP proxy)		Add-on	Add-on
ATP for Email (through SMTP proxy)		Add-on	Add-on

For more information on Versa Secure Internet Access and other Versa services, please reach out to a Versa account representative.

VERSA

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