Versa Endpoint Client

Background

As businesses continue to embrace remote and hybrid work environments, the need for secure access to corporate resources from any location has become a critical concern. One of the driving forces behind this shift is the necessity for flexibility and scalability, as users demand the ability to access applications and data instantly, regardless of their location. The traditional network perimeter is disappearing and securing user access to both cloud and on-premises applications requires a modern approach that can adapt to this dynamic landscape.

While organizations have succeeded in providing remote access, traditional security solutions, designed for static, location-bound environments, fall short of meeting the agility required in today's fast-paced world. Slow deployment cycles, inflexible security models, and complex infrastructure lead to significant gaps in protecting remote users and sensitive data. In contrast, organizations now require security that is seamless, instantaneous, and adaptable—responding to the changing needs of the business, while maintaining robust protection across every connection.

Introducing Versa Endpoint Client

Versa Endpoint Client is a cross-platform software agent available for Windows and macOS endpoints, as well as mobile devices (iOS, Android). It provides users with seamless, reliable access to corporate networks, applications, and data—whether they are working remotely or on the go. Integrated within Versa's Secure Access Service Edge (SASE) framework, Versa Endpoint Client enables organizations to maintain secure connections to both on-premises and cloud-based resources, ensuring business continuity and productivity from any location.

With Zero Trust access capabilities, Versa Endpoint Client verifies user identity and device health at every connection, allowing only trusted users and devices to access specific resources. Additional security features like multi-factor authentication (MFA), device posture validation, and encrypted traffic inspection help protect sensitive information and support compliance with corporate security standards. This adaptive access control ensures that security measures align dynamically with real-time user conditions, reinforcing security for a flexible workforce. Versa Endpoint Client uniquely supports deployment on virtual machines within remote data canters, enabling organizations to extend secure access to applications hosted across diverse environments and ensuring seamless integration with existing infrastructure.

Versa Endpoint Client offers an intuitive experience that balances ease of use with robust security, empowering organizations to protect their networks while providing employees with dependable, secure access to essential resources anytime, anywhere.

Target Use Cases of Versa Endpoint Client

- Secure Access for Remote and Mobile Users: Ideal for remote and hybrid workforces, Versa Endpoint Client provides secure access to corporate resources within private networks, enabling employees to connect from any location. Always-On VPN ensures continuous protection in transient environments, while fail-close mechanisms block network access if secure connectivity is disrupted, maintaining a strict security perimeter. By supporting IPSEC, SSL and GRE tunnels, Versa Endpoint Client enables secure, flexible network access to corporate resources from anywhere, keeping both users and data protected.

Versa Endpoint Client is designed to work seamlessly across both IPv4 and IPv6 network protocols, ensuring compatibility with diverse network environments. Supporting IPv4 allows the client to operate on traditional and legacy network infrastructures, which remain common in many organizations. At the same time, IPv6 support ensures that the client can handle modern, expanded IP addressing and enhanced security and efficiency features that come with IPv6 networks. This dual support is especially valuable for enterprises transitioning from IPv4 to IPv6, as Versa Endpoint Client can operate across both protocols without disrupting connectivity or compromising security.

- Secure Internet Access: Versa Endpoint Client ensures that users access the internet safely by inspecting and filtering traffic to protect against online threats. Features such as SSL/TLS inspection and Proxy Configuration enable secure browsing by monitoring encrypted traffic and filtering out malicious content. Split Tunneling and Trusted Network Detection allow users to route only necessary traffic through secure channels, optimizing performance while maintaining strong protections for public internet access. Supported IPSEC, and SSL tunnels provide encrypted channels as needed for securing traffic in varied internet environments.
- On-Premises ZTNA: For organizations with user and device posture-based network access control, the Versa SASE Client provides a secure enterprise perimeter for LAN environments. Versa's on-premises Zero Trust Network Access (ZTNA) solution ensures only authenticated users and compliant devices have access to LAN resources. The level of access is regulated by policy-based access control. Multi-Factor Authentication (MFA) and Certificate-Based Authentication verify users and devices, while Role-Based Access Control (RBAC) and dynamically assessed security posture allows administrators to set role-specific policies for granular access control. This ZTNA model protects enterprise LAN resources by enforcing least-privilege access and reducing the risk of unauthorized access or lateral movement within the network.
- Endpoint DLP and Compliance Enforcement: To prevent data loss and ensure compliance with corporate policies, Versa Endpoint Client includes Endpoint Data Loss Prevention (DLP) and Host Information Profile (HIP) capabilities. These features monitor device compliance in real-time, while Endpoint Posture Assessments and Identity Services Engine (ISE) integration verify that devices meet security standards before accessing sensitive resources. This use case ensures that data remains secure and that only compliant devices can access critical resources.
- Centralized Logging, Reporting, and Monitoring: For organizations requiring in-depth visibility into user activity and network health, Versa Endpoint Client provides centralized logging and reporting. This capability offers IT teams detailed insights into connection status, user behavior, and potential security risks, supporting proactive threat detection and enabling compliance with auditing requirements.
- Virtualized Data Center VM-Based Endpoint Access: Traditional SASE solutions primarily focus on cloud-delivered services, leaving a critical gap in securing on-premises data centers. Existing approaches often lack visibility, particularly for dynamic posture assessment of workloads within multi-tenant data centers. Versa uniquely addresses this by extending its Versa Endpoint Client capabilities to on-premises data centers, enabling dynamic micro-segmentation and real-time security posture assessments directly on workload VMs. By leveraging Endpoint Information Profiles (EIPs) and policy-based enforcement, workloads are classified and secured based on tenant, device type, and risk factors. With integration into Versa's SD-LAN overlays and support for Security Group Tagging (SGTs), Versa ensures seamless traffic separation and compatibility with multi-vendor SDN solutions, making it the ideal choice for hybrid environments.
- Mobile Device Management (MDM) Integration for Enhanced Security: For organizations managing mobile workforces, Versa Endpoint Client integrates with Mobile Device Management (MDM) solutions, enabling administrators to enforce device-level security policies on mobile endpoints. This integration provides centralized policy management and compliance enforcement, securing data on both corporate and personal devices used within hybrid and mobile work models.

Versa Endpoint Client supported features Specifications

Network Access
Always-On VPN
Management VPN Tunnel
Split Tunnelling
Trusted Network Detection
Pre-Logon
Connect Failure policy
Captive Portal hotspot Detection
Captive Portal hotspot remediation
SSL/TLS Inspection Split DNS
Proxy Configuration
Auto-Connect and Seamless Reconnect
IPV4/IPV6 support
IPSEC/GRE/SSL Tunnels

Authentication and User Access
Single Sign-On
Multi-Factor Authentication
Certificate Based Authentication
Role-Based Access Control
ZTNA
Traditional Authentication
LDAP, RADIUS, SAML, OTP
Application-Specific-Access Control Policies

Partnerships
Endpoint Security Providers
MDM Integrations
Identity Provider Integration

Posture and Compliance
Host Information Profile
Endpoint Posture Assessments
Antimalware and Firewall integration
Device Compliance Enforcement
Vulnerability Assessment
ISE Posture and Compliance

Logging, Reporting, and Monitoring
Real-Time Monitoring
Detailed Activity Logs
Centralized Logging and Reporting
Issue Reporting & Diagnostic Logs

Licensing

The Versa Endpoint Client is a key component of Versa Secure Access Fabric (VSAF) and is included as part of Versa's comprehensive product suites including Versa Secure Private Access (VSPA) and Versa Secure Internet Access (VSIA). There is no independent licensing required for the Versa Endpoint client, as it is offered as part of broader offerings. This ensures that organizations can deploy secure access solutions with full feature integration, without the need for additional licensing or separate procurement processes.

Support

Support is provided via the Versa Networks support portal. There is a direct link to the Versa support ticketing system to resolve your issues. You can visit our the Versa Support page at https://support.versa-networks.com to open a support ticket and contact support personnel. Additionally, you can get more information in the portal by clicking the info icon for each configuration. For more details on any feature, you can also refer to Versa Documentation. Access to the document page is available in the dashboard in the top right corner.

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

© 2024 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# ENDPNTCLIENt-01 2024-1211