Versa Secure SD-LAN

Addressing LAN Challenges

For years, enterprises have grappled with the limitations of legacy LAN solutions and vendor lock-in. These rigid networks not only limit the ability to meet evolving business needs but also introduce painful operational challenges. These issues are driven by the need to stitch together fragmented point solutions into rigid architectures, decentralized management that requires manual configurations, and forced upgrades that are expensive, time-consuming and prone to errors.

And traditional LANs struggle to keep pace with today's Zero Trust tenets – which assume breach. With perimeter-oriented security approaches that implicitly trusts authenticated users, compromised devices have an unfettered ability to move laterally. The rise of IoT devices inside the network further expands the unsecured internal attack surface area.

Versa Secure SD-LAN is software deployed on LAN switches that natively combines switching, routing, security, and network services to software define the LAN. The solution delivers line rate performance with centralized management for the agility that organizations require today. And with user, device, and application awareness combined with a centralized policy repository, enterprises now have full visibility and control across the network, including IoT devices. This approach enables every switch and access point to become a Zero Trust point of enforcement.

Versa Secure SD-LAN Highlights

Software Define the LAN

By consolidating various components, such as Enterprise LAN switching, identity engine, NACs, device fingerprinting together with L2-L3 as well as L4-7 features into a single software stack, the complexity of deployment, observability, and policy enforcement is significantly reduced while transforming every Enterprise LAN switch into a Zero Trust policy enforcement point. This software-defined approach allows for seamless integration of new capabilities, providing agility and adaptability as networking needs evolve.

Versa Secure SD-LAN provides agility in the deployment of switches in any topology, while allowing network operator to define connectivity and security functions once and deploying them across the infrastructure seamlessly and consistently.

Adaptive Software Defined Micro-Segmentation.

Software defined adaptive micro-segmentation reacts to changes in device posture, user risk score and other factors. By continuously assessing trust in devices and the network, segments will dynamically adjust in real-time to prevent an incident from becoming a breach.

Flexibly Deployed

Versa Secure SD-LAN can be deployed with CSX hardware platform families or the CSG300 which combines WAN Edge and SD-LAN capabilities.

IoT Security

With the proliferation of Internet of Things (IoT) devices, gaining visibility and securing endpoints has become a critical priority for organizations. Versa Secure SD-LAN provides comprehensive, integrated IoT visibility and security controls, enabling IT teams to identify and categorize IoT devices on the network. Through techniques such as device fingerprinting and micro-segmentation, automated Zero Trust controls can be implemented to mitigate risks associated with compromised IoT devices.

Unified Management

Versa's Secure SD-LAN is a cornerstone of its consistent innovation, ensuring uniform policy enforcement across varied networks, including wired, wireless, and IoT. This not only fortifies security but also enhances management efficiency across diverse branch infrastructures. And as part of the platform's unified management and reporting, it integrates management and deployment integrated management and deployment across the infrastructure – from WAN, LAN, Cloud to Data Center.

Unified Big Data based Analytics

Versa's built-in Analytics is now available to provide unmatched visibility into the LAN without any need for additional tools or products. Versa's inline traffic processing capabilities deliver traffic, user, application, security events, ZTNA and many more points of relevance to provide in-depth insights and analysis to our customerss.

Licensing

Versa Secure SD-LAN is a subscription-based product offering and licensed on a per platform basis. Versa Secure SD-LAN license comes in 3 tiers.

Essential	Professional	Elite
Carrer class routing, switching, Zero Touch Provisioning and SD-LAN overlay connectivity	Essential subscription plus user and group traffic management, App-ID, device fingerprinting, stateful firewall, IP reputation feeds and filtering, web security	Professional capabilities plus UTM

Features	Essential	Professional	Elite
Comprehensive Layer-2 features Including Bridge-domains, virtual switches for multi-tenancy, xSTP, VLANs, VLAN manipulations, VLAN access/trunk mode, LLDP, IRB for integrated routing and bridging	✓	✓	✓
Comprehensive Layer-3 features DHCP client/server/relay, VRFs, Static NAT, carrier class routing protocols: OSPFv2/3, RIP-v2, BGP/MP-BGP, IGMP v2/v3, PIM SM/SSM, Auto/Boot-strap RP, BFD, IPv6 extensions of routing protocols	✓	✓	✓
Rich set of platform features LAG, rich set of QoS features (priority queuing, WRR, WRED and more), Shapers, Policers, ACLs, ZTP options, auto-provisioning, VRRP, Flow mirroring, Flow reporting, uCPE to host 3rd party VMs	✓	✓	✓
Overlay based connectivity VXLAN, GRE, MP-BGP EVPN, MP-BGP L3VPN, IKEv2 IPSEC	✓	✓	✓
Network Access Control (NAC) 802.1X single/multiple supplicants, RADIUS back-end, Certificate based and MAC bypass list-based authentication	✓	✓	✓
User Authentication with Enterprise authentication server support Integration with LDAP/Active Directory, SAML based SSO, MFA support with Microsoft Authenticator, Google Authenticator, Duo, Captive Portal based		✓	✓
Stateful Firewall, CGNAT with ALS support, DOS Protection Providing L3-L4 security, stateful address translation with ALG support		✓	✓
DNS Proxy, DNS Feeds and Filtering		✓	✓
Device Fingerprinting Device Identification and Fingerprinting of rich set of devices, including IoT/OT/BYOD, Device Type Policies, device classifications, risk assessment		✓	✓
URL and IP Feeds, Classification, Filtering URL, and IP Feeds, Classification and Filtering to protect devices on LAN from talking to untrusted or suspicious destinations on the Internet		✓	✓
Application Identification Ability to identify market leading number of applications and map to different application classes to manage traffic of each application class		✓	✓
Application, User, Device policy-based traffic control Using rich set of policies provided by VOS's natively built-in VPEF function		✓	✓
IoT Security Recognition of IoT protocols and applications, filtering		✓	✓
Application Identification, Application Policy, Network and User visibility Big-data based detailed visibility and analysis capabilities		✓	✓
Micro-segmentation With tagging options including VLAN, VXLAN, SGT and more. Hardware acceleration included			✓
Unified Threat Management NG-IPS, Antivirus, Malware Protection, File Filtering within the context of lateral movement protection, detection and prevention of spread of malware/ransomware within LAN			✓
SSL-TLS Proxy Including TLS 1.0/1.1/1.2/1.3 support to break and inspect TLS encrypted sessions that may be needed for encrypted application analysis, UTM functions on encrypted flows within the context of lateral movement detection and prevention			✓

VERSA NETWORKS

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