Versa Next-Generation Firewall (NGFW)

Introduction

Today's fast evolving threat landscape demands comprehensive, advanced threat protection that legacy firewalls with rigid and reactive architectures are simply not made for. Traditional edge firewalls are often anchored to physical sites, however users need the same level of robust protection regardless of where they connect from: a branch office, HQ, a home office, or on the road. In addition, today's modern IT networks support a wide range of Internet of Things (IoT) and Operational Technology (OT) devices that are vulnerable to cyber-attacks.

Versa Networks next generation firewall (NGFW) accelerates digital transformation by providing comprehensive security in a single, scalable platform to address the most demanding use cases. Versa NGFW delivers advanced application layer capabilities to protect against the most evasive known and unknown threats across your entire network, with a single platform for networking, security, threat prevention, and centralized management. Versa NGFW uniquely classifies and protects all traffic in your network regardless of user, type of device or location, from all manner of threats, to enhance security posture, improve application availability and boost user experience.

Versa NGFW Key Features

Versa NGFW is a comprehensive network security product offering with Zero Trust based secure access, IoT/OT security and device fingerprinting, URL filtering, next generation intrusion prevention, and advanced security capabilities for data loss prevention, advanced threat prevention, and cloud access control.

Flexible Deployment Options

- On-premises, on bare-metal appliances
- In private data centers in virtualized form factor or,
- In popular public cloud environments such as AWS, Azure, GCP

Versa NGFW solution is available with a single pane-of-glass management and visibility to securely connect users and devices in enterprise branches to applications in or near any of the above deployment options. High availability options with active/active and active/passive modes ensures business continuity.

Application Aware, Resilient Network Security

Versa NGFW application identification capability identifies all applications across all ports with features such as Layer 7 Deep Packet Inspection (DPI), URL, protocol and port numbers, destination IP addresses and more, combined with comprehensive policy-based control. Built-in support for DOS protection, CGNAT (Carrier Grade NAT) and ALG (Application Layer Gateway) ensures a high degree of scale and security.

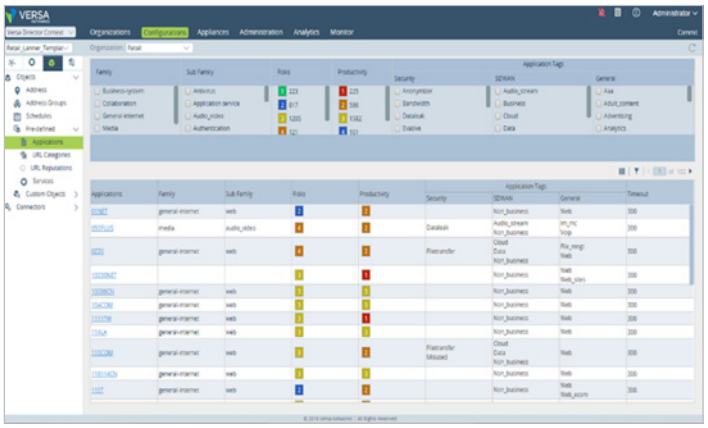
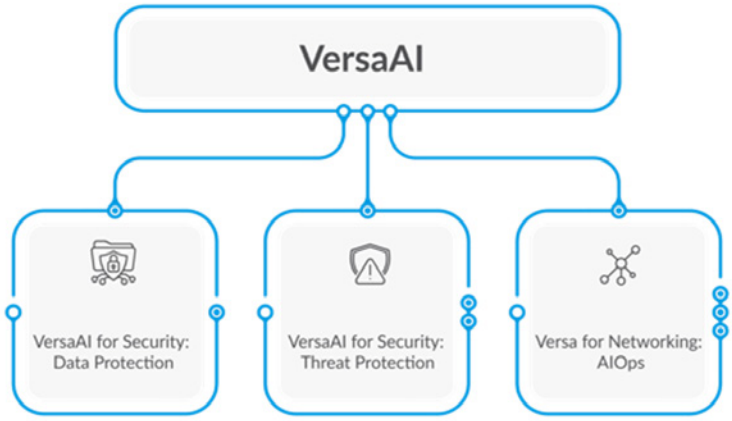


Figure 1. Versa NGFW applications dashboard

Versa AI

Embedded in Versa NGFW, Versa AI™ pioneers the future of Advanced Threat Prevention, Robust Data Protection, Intelligent AIOps and Network Insights. Versa AI™ enables the following AI/ML driven features that can be acted upon in real time:

- User Entity Behaviors Analytics – Detecting anomalous behavior across users, entities, and devices, such as impossible travel, bulk deletion, downloads etc.
- Malware Detection and Advanced threat Protection – Multi-stage AI/ML pipelines for pre-processing files, identifying malicious traffic early on in the sandbox before costly computations, and enhancing the security posture.
- Adaptive Software-Defined Microsegmentation – Zero trust conditional access continuously assessing user and device security posture.
- DLP and sensitive data detection – LLM (large language model) assisted models and protection, controls for Generative AI tools like ChatGPT, Gemini etc.,and cloud access controls to prevent sensitive data leakage.
- Versa Advanced Network Insights (VANI) - Predict network and appliance capacity, raise proactive alarms, provide (automated?) recommendations and Intelligent alerts.



User Authentication and User/Group Level Policies

Versa NGFW provides built-in user and group based access control capabilities. Versa Operating System (VOS™) can integrate with popular Identity Providers (IdPs) to authenticate users, perform MFA (multi-factor authentication) and obtain user and group information to apply security and access controls. Conditional access policies can be defined for different classes of users like executives, guests, employees, and contractors.

Versa provides the option to use the Versa Identity and Authentication Engine (IAE) as a centralized broker to help authenticate users in passive or in proactive forms and facilitate a seamless user experience by eliminating the need for repetitive authentication.

The Captive Portal authenticates users and manages access control based on user identity when inline user authentication capabilities are not deployed.

DNS Proxy and DNS Security

DNS Proxy - Using the information learned from authoritative DNS servers, as well as through DNS Reputation Feeds, the DNS Proxy secures DNS entries and prevents traffic from getting to untrusted, unknown or malicious sites known to work as Command & Control (C&C) centers for attackers.

DNS Security & Filtering - Secures the network and its clients from DNS hijacking, DNS based attacks, DNS reflection attacks, amplification attacks, phishing attacks, malware, ransomware, and botnets, along with protections to block access to compromised websites. This is provided at the DNS layer. Versa NGFW DNS Security uses global DNS threat intelligence gathered from hundreds of sensors across the globe to block resolution of new domains until reputation is updated. DNS Reputation Feeds are used to keep this database up to date.

URL and IP Reputation, Categorization and Filtering

Versa NGFW provides a rich set of URL and IP Categorization and Filtering capabilities in 80+ URL categories to enable safe browsing while blocking malicious sites. The URLs are categorized by reputation, risk and trustworthiness. In addition to predefined classes, Versa provides support for user-defined/custom classes that can be created and managed as needed. Hundreds of millions of domains and 13+ billion URLs are scored and classified for maximum threat coverage.

- 86 predefined URL categories including Generative AI, general Internet, to improve employee productivity, inappropriate sites like gambling or pornography to avoid legal liability, bandwidth management including voice and video sites.
- URL database is updated periodically via Security Package updates without the need for VOS or software upgrades.
- Real time Cloud Lookups of URL categories for those uncategorized in the VOS cache.
- Custom URL categories based on Regex and/or Fixed String Match.
- Customizable Captive Portal screens for policy enforcement and redirection.
- Support for Block, Inform, Ask, Justify, Override and Authenticate Pages.

TLS/SSL Proxy

- Protects against threats hidden in encrypted traffic by breaking open and inspecting TLS/SSL traffic and applying additional security policies for threat and data protection.
- Directs encrypted traffic based on application signatures, scans encrypted content for malware and exploit prevention, detects and prevents data leakage to enforce company compliance.
- Support for transparent or split-proxy modes.
- Supports TLS versions 1.0, 1.1, 1.2 and 1.3. Versa has been ahead of many security vendors in support for TLS v1.3.

Recommendation to use TLS 1.3 with TLS Proxy: Versa recommends use of TLS 1.3 for higher security as it incorporates improvements to ensure the confidentiality and integrity of communications.

- Perfect Forward Secrecy (PFS) employs the use of ephemeral keys to overcome confidentiality concern. PFS is mandatory with TLS 1.3. By generating a unique session key for every session that a user initiates, even the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key. Knowing the private key of the server no longer allows decrypting of the session.
- Parts of the handshake (server certificate values such as CName, SAN) are encrypted. This prevents malicious third parties (that rely on examining server certificates) from eavesdropping on the connection.

Next Generation Intrusion Prevention (NG-IPS)

- Signature-based and anomaly-based detection and prevention of vulnerabilities.
- Extensive coverage for vulnerabilities found over the last 10 years.
- Vulnerability signatures and anomaly detection engine updated dynamically via Security Package updates to provide real-time protection without needing to upgrade VOS.
- Coverage for vulnerabilities disclosed as part of Microsoft Tuesday.
- Support for PCN/SCADA signatures.
- Support for custom/user-defined vulnerability signatures.
- Support for Snort rule format.
- Support for lateral movement detection and prevention.

Malware Protection

Versa NGFW provides a rich set of embedded antivirus (AV) and malware protection capabilities using multilayered techniques such as heuristics, signature matching, emulation and more. Versa's AV uses an optimum set of hardware resources to achieve optimized cost, performance and market leading efficacy. Versa's AV signatures are updated frequently (configurable for real time updates) from Versa Cloud and Security Package updates through Versa Director which updates field deployed VOS instances, allowing customers to always use the latest antivirus signatures.

Advanced Threat Protection (ATP)

Zero-day vulnerabilities discovered "in the wild" leave open traps for attacks and zero-day malware exploits. Zero-day exploits go undetected until they are discovered and their signatures are added to IPS, Malware protection, and AV systems. Existing URL filtering and access security solutions are not effective in dealing with Advanced Persistent Threats (APTs) as APTs use advanced techniques like polymorphic variations of file hashes which makes it harder to detect malicious activity.

Versa ATP sandbox solution is a cloud-delivered multi-stage advanced security solution that prevents zero-day attacks with speed and efficacy.

- Performs static analysis and file examination without detonating or "executing" the file.
- Uses AI/ML based behavior analysis to classify a file with zero-day malware as malicious.
- Performs dynamic analysis or "detonation" of a file in the sandbox as the last stage in the pipeline to prevent malware downloads.
- Supports major operating systems and flavors of Windows, Android, OS X and Linux.
- Supports dozens of file types such as EXE, OLE, Word, PPTx, PDF, JavaScript.
- Maps the cyber kill chain using the MITRE ATT&CK framework.

File Filtering

Various types of viruses, malware and other malicious code travel using files. Versa NGFW's built-in File Filtering capability provides signature-based file type identification of various file types.

- Scans protocols HTTP, FTP, SMTP, POP3, IMAP, MAPI
- Computes a file hash signature and compares that against its database of file signatures to conduct an assessment.

Versa File Filtering function relies on file hashes and fingerprints and not just files names. This method decreases the load on more detailed analysis engines, such as NG-IPS, AV and ATP engines by taking action before such content inspection scanning functions kick-in.

Cloud Access Security Broker (CASB)

Versa CASB enforces consistent security policies across multiple clouds, and safeguards both users and corporate data. Versa CASB provides granular access control and administration of cloud-based data and applications, enabling security teams to identify and manage the use of cloud applications, for both sanctioned and unsanctioned (aka shadow IT) applications.

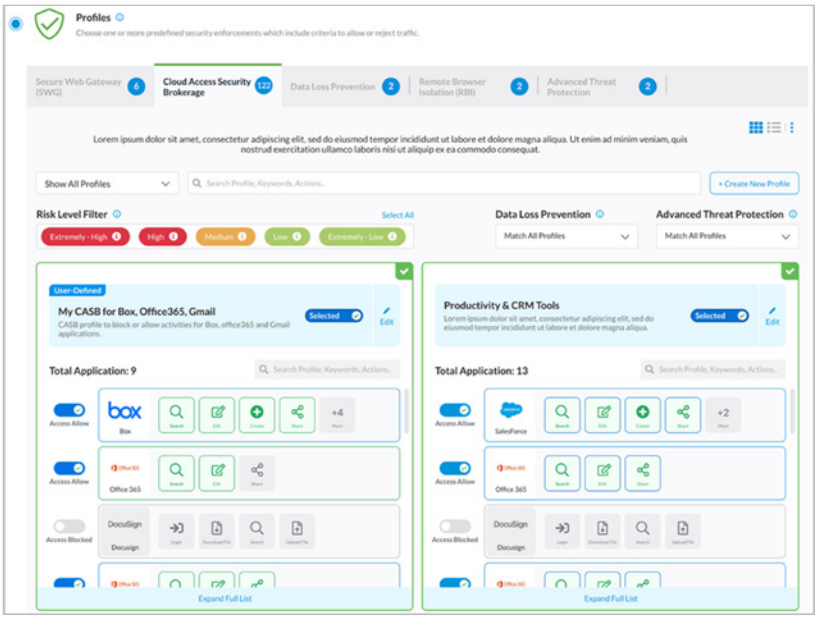


Figure 2. Versa CASB.

Shadow IT Discovery & Protection: IT systems and SaaS applications deployed by departments and users without the full visibility or control of the IT department are called Shadow IT. Shadow IT results in a fragmented application landscape where consistency, security, and governability could be compromised. This puts the enterprise at risk of data loss, sensitive leaks, unauthorized access, attacks, and non-compliance with initiatives such as SOX, GLBA, COBIT, FISMA, GDPR, CCPA, NYDFS, and HIPAA.

- Discovers and Protects against Shadow IT applications.
- Support for hundreds of SaaS applications.

- SaaS tenant restrictions with popular Google, Microsoft SaaS applications through HTTP header insertion and modification.
- Prevents sensitive data from being exfiltrated by unauthorized users or cybercriminals.
- Secures cloud applications, whether they are hosted in public clouds (IaaS), private clouds, or SaaS
- Provides granular visibility and control over cloud applications usage and data.
- Deploys inline on-premises or through API based functions available as a cloud service.

Data Loss Prevention (DLP)

Enterprises possess important data such as customer lists, intellectual property, employee data, financial data etc. and leakage of this data puts them at risk of cyber breaches, along with violating regulatory and compliance requirements. Market research indicates 18% of all files include sensitive data. Data leakage happens for various reasons, such as employee negligence (the most common reason), third party mistakes, system error, hacker attacks, or malicious insiders. Versa DLP detects and prevents potential data breaches or unauthorized data exfiltration with advanced techniques for scanning, detecting, and blocking sensitive or confidential data while in motion across the network.

- Implements blocking and reporting actions as configured by the network operator.
- Supports Exact Data Match - Data leakage on structured data using predefined or custom data patterns against a user-provided data set, Boolean operations with EDM.
- Document fingerprinting for e.g. fingerprinting documents in a given folder path.
- Microsoft Information Protection (MIP) and file based DLP.
- Protocol support for HTTP/HTTPS and more.
- Analyzes protocol headers, body, payload to DLP policies on respective fields.
- Support for popular file types.
- Deployment inline real-time and as a cloud service through API-based CASB.
- Integrated with URL filtering and CASB policies.

IoT Security, IoT/OT Device Fingerprinting and Classification

VOS's Device Identification / Fingerprinting and Classification capabilities enable network and security operators to identify network attached devices by hardware vendor, OS and application they are using.

- Recognizes over 1 million different types of IoT/OT/BYOD devices.
- Maps them to different device classes for ease of management, segmentation and policy-based management purposes.
- Enforces policies based on device categorization, posture and compliance.

Figure 3. IoT Security.

Hardened Security Stack and Operating System (VOS)

Versa Operating System is a hardened OS. This includes installation of the required minimal set of packages, use of signed binaries, rules for administrator password, privileged access management, password safe storage, and boot loader protection. The hardened security stack and operating system are verified and audited periodically with release updates.

Security Integrations & Certifications

- Threat intelligence feeds from industry standard and open source
- NAC: 802.1X and RADIUS Server integrations
- Cisco SGT integration
- APM/SIEM integrations for e.g. Splunk, SevOne, Thousand Eyes
- EDR/EPP, MDM integrations for e.g. Microsoft Intune
- DLP – Microsoft Information Protection (MIP) tags
- Highest Rated Enterprise Firewall for Lowest TCO, HTTPS Capacity and Rated Throughput ("Recommended" Rating, CyberRatings.org, 2023 Enterprise Firewall Test)

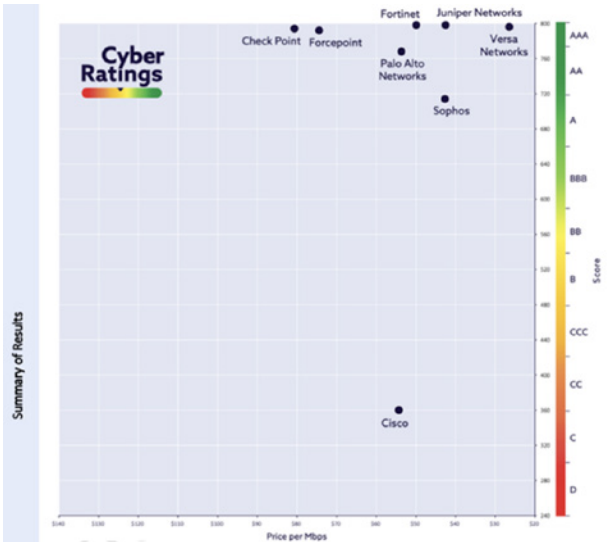


Figure 4. CyberRatings Security Value Map for Enterprise Firewalls, 2023.

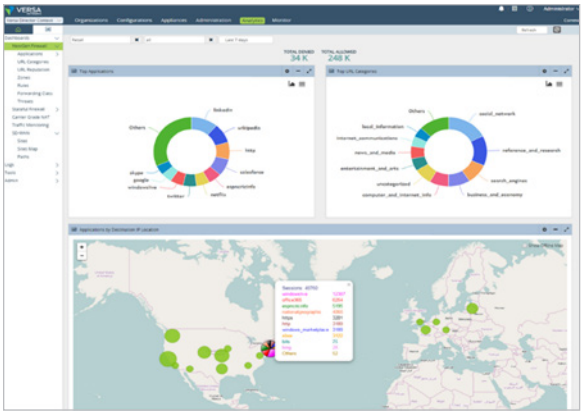


Figure 5 Versa Analytics.

Genuine Multi-Tenancy

Versa NGFW provides genuine multi-tenancy across Versa orchestration platforms, control plane, and data plane. This level of multi-tenancy isolates the policies, configuration, logs and statistics of every tenant, and keeps them segregated from that of the other tenants. This ensures enhanced security and high performance for each tenant.

Scalable Single-Pass Architecture

Versa Operating System is based on a single pass, scalable architecture that makes it simple and fast to deploy Versa NGFW from tens to thousands of locations, providing consistent policies across all locations. Say goodbye to limited visibility, manual configuration, troubleshooting and unmanageable alerts as Versa delivers unprecedented visibility, transforming your management experience and reducing your incident response time.

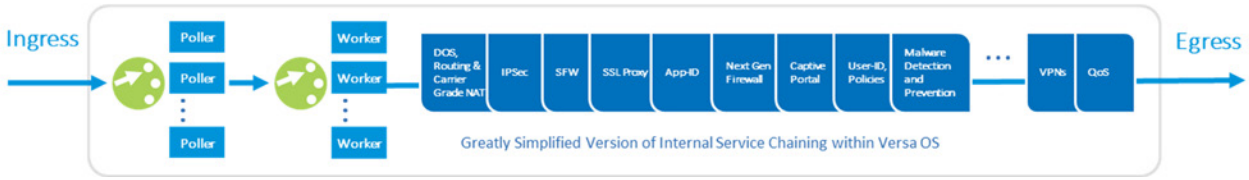


Figure 6. Versa Single Pass Architecture.

Natively Integrated SD-WAN

Versa delivers security and networking on the same software stack – seamlessly integrated as part of the Versa OS. Versa's fully integrated NGFW and SD-WAN solution will allow you to securely enable local breakout of Internet bound traffic from each of the branches, reducing the need to backhaul all traffic to a central data center.

Seamless Integration into Brownfield Deployments

Versa uses standards-based technologies as building blocks for Secure SD-WAN deployments. This allows the Versa solution to be seamlessly integrated into existing networks. Versa supports a rich set of routing protocols such as OSPF v2/3, RIPv2, MP-BGP, MPLS L3VPN, MPLS EVPN, VXLAN, BFD, VRRP, VRFs, VLANs and more to seamlessly tie into an existing enterprise network and make intelligent routing decisions.

For instance, MP-BGP route reflector can be used to create advanced topologies like partial mesh, Spoke-Hub-Hub-Spoke. Versa Secure SD-WAN solution supports templates and automation to create the needed topologies and seamlessly integrate into existing environments.

Ease of Deployment via Zero Touch Provisioning

Versa NGFW comes with fully automated, centralized configuration and management capabilities to reduce or eliminate the need for certified branch technicians and expensive mobile technical resources to be present on site. The collective set of capabilities make up Versa's Zero-Touch Provisioning (ZTP). Several different ZTP options are provided for Versa customers to address the needs of different deployment scenarios and business processes.

Versa's ZTP process works over the Internet, MPLS connections, in closed networks, as well as across LTE and 5G connections.

Integrated Big-Data Analytics and Visibility

Versa Secure SD-WAN solution comes with Versa Analytics which delivers near real-time big-data based visibility and control, baselining, correlation, prediction and feedback loop into Versa solutions. It provides near real-time and historical search, reports on usage metrics, performance metrics, trends, security events, and alerts.

Versa supports integration with 3rd party SIEM and monitoring platforms using standards-based log formats like syslog and IPFIX.

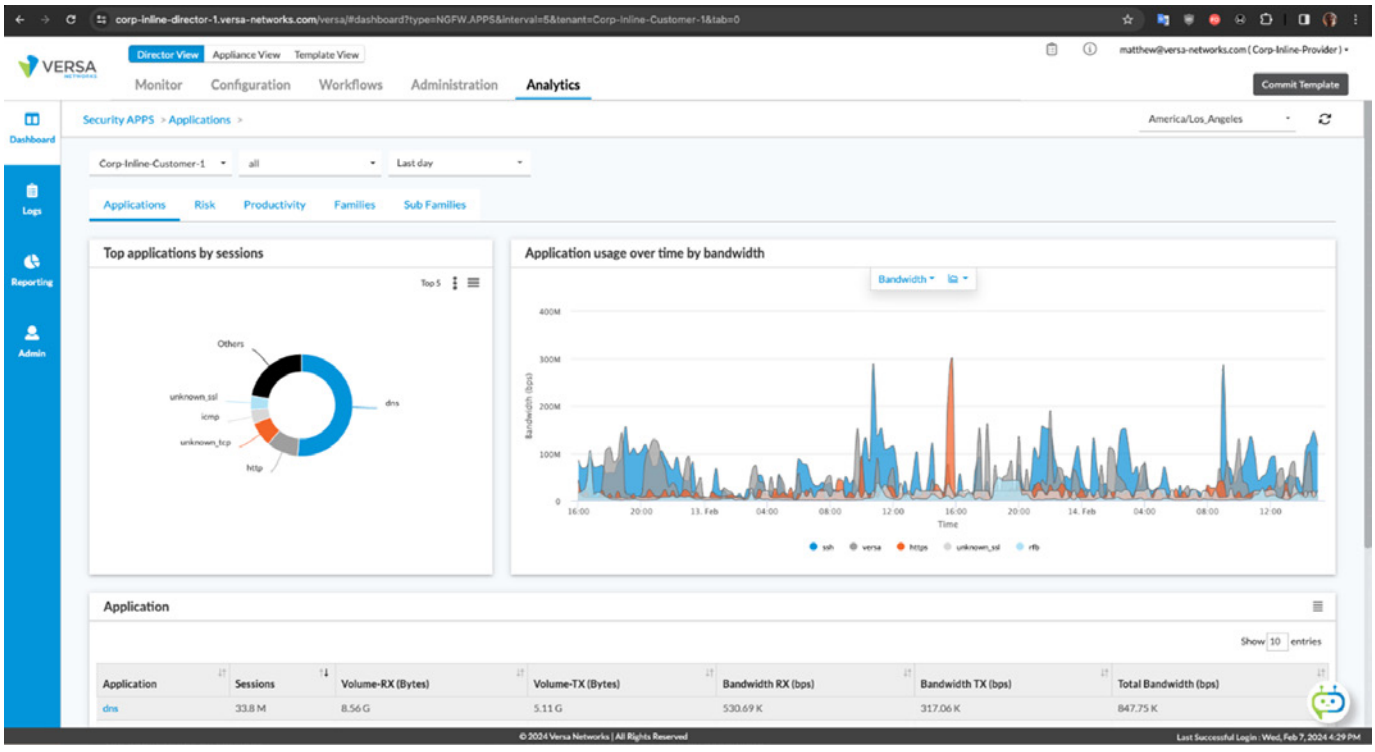


Figure 7. Versa Analytics – top applications and URL categories

Components of Versa Secure SD-WAN Solution

Versa Operating System (VOS)

VOS is a cloud-native, multi-tenant, multi-service software stack providing full set of L2, L3, L4-L7 routing and networking services and security services which powers Versa Secure SD-WAN, Secure SD-LAN, SSE solution. VOS can be deployed in branch offices, campus, hubs, data centers and public cloud environments. VOS capabilities are managed and monitored centrally using Versa Director and Concerto.

Versa NGFW

- Visibility and security of all users, devices and applications.
- Multi-tenancy for consolidating multiple networks while preserving separate, data, control, and management planes.
- Unified network management, deployment, and policy configuration.
- Templates and workflows for fast, error-free and consistent configuration & change management.
- Zero-touch provisioning for rapid and scalable deployment.
- AI/ML powered: a self-managing, self-healing, and predictive solution.

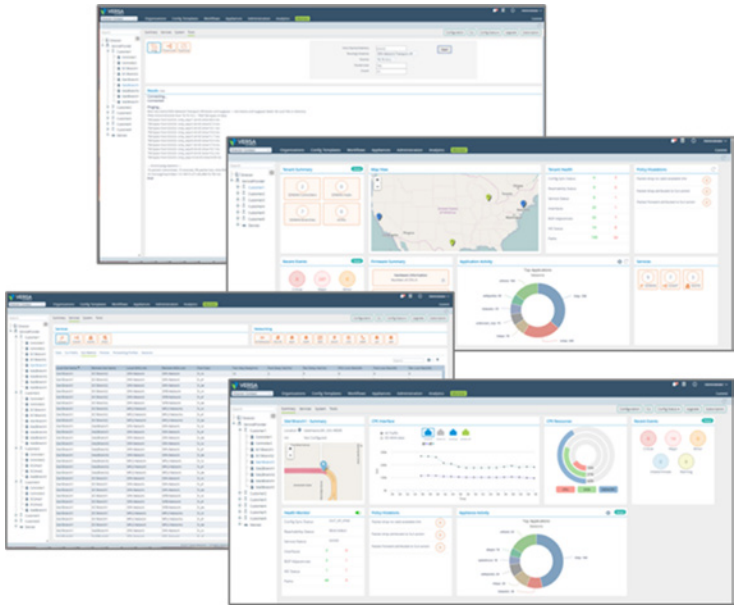


Figure 8. Versa NGFW management

Versa Director

- Scalable, multi-tenant network management and orchestration platform which provides essential management, monitoring, and orchestration capabilities for Secure SD-WAN network.
- Simplifies the network deployment with workflows, templates, and automation capabilities.

Versa Controller

- Provides scalable, resilient control plane for Versa Secure SD-WAN.
- Provides Route-reflector function to provide route-reachability for the VOS devices.

Versa Analytics

- Purpose-built for Versa Secure Cloud IP Platform for use-case focused analytics covering SASE, SD-WAN, SD-Routing, SD-Security, and SD- Branch.
- Rich, near real-time big data solution that provides visibility and control, baselining, correlation, prediction, and feedback loop into Versa solutions.
- Provides near real-time and historical search, reports on usage metrics, performance metrics, trends, security events, and alerts.

Figure 9. Versa NGFW Dashboard Trends and Alerts.

Versa Concerto

- Versa Concerto runs on top of Versa Director, Versa Analytics, and Versa Controller elements, providing an easy to use single-pane-of-glass management for Secure SD-WAN, Secure SD-LAN and SSE (Secure Service Edge) services.
- Versa Concerto is based on a microservices architecture and is designed to run in public or private clouds, making horizontal scaling both easy and flexible for customers.

Versa Messaging System (VMS)

- Versa Messaging System (VMS) provides a scalable information exchange solution which powers Identity Engine, Zero-Trust-Everywhere, IoT Security and other services.

Product Capabilities Summary		
Carrier class routing protocols	**SSL Inspection**	**Identity and Authentication Engine**
Stateful Firewall, DOS Protection, CGNAT, IPSEC	**TLS/SSL Proxy**	**ZTNA on-premises**
User Authentication, User/Group Policies	**NG-IPS**	**Data Protection on-premises** • **Inline CASB** • **Inline DLP**
DNS Proxy, DNS Feeds and Security	**Malware Protection**	**ATP sandboxing – cloud-based**
Application ID, App Policy-based Forwarding	**File Reputation Filtering**	**API based CASB, DLP – cloud-based**
URL & IP Feeds, Categorization, Filtering	**IoT/OTSecurity, Device Fingerprinting and Identification**	

Versa groups relevant features for each of the use-cases to make it easier for our customers to purchase and deploy. For details on licensing and feature tiers, please contact your Versa sales representative or Versa partner.

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