Securing Digital Transformation Initiatives with Versa Secure Internet Access (VSIA)

Zero Trust Security against web-based threats, contorl over web access, regulatory compliance, single pane of glass for any device, location and user

BENEFITS

- **Continuous connectivity and protection** across all ports and protocols with optimal end user experience
- **Enhanced Web Security**
- **Advanced Threat Intelligence**
- **Secure SaaS Apps**
- **Secure Private Apps**
- **Global Scalability**
- **Single Pane of Glass** for SSE and SD-WAN with granular policy controls for ZTNA, VSIA, VSPA, DLP, CASB, NGFW, ATP for remote and on-prem users.
- **UEBA** (User Behavior Analysis)
- **Flexible Deployment Options**
- **Traffic Engineered Backbone** providing predictable, Low Latency, High Speed connectivity with 99.999% uptime

Digital transformation can deliver a host of business, productivity, and operational benefits, ranging from improved efficiency, enhanced customer experience, better decision making, increased agility and attractive business models.

However, legacy networks are based on hardware appliances and traditional static perimeter-based security, with traffic backhauled from branch offices and remote users to a centralized on-premises security stack for inspection. This architecture is not sufficient to protect cloud apps. Legacy networks are not designed to handle the distributed nature of cloud apps and lack visibility, which can leave them vulnerable to cyberattacks and data breaches.

This requires digital transformation to be paired with a Zero Trust construct to secure the new approaches to supporting users, data and apps. Namely:

- Shadow IT
- Securing Cloud Workloads
- Securing SaaS apps
- Securing Private Apps
- Expanded device profiles
- Expanded locations

Maintaining legacy networking equipment and disparate point solutions for such a large surface area creates complexity and inconsistent security enforcement across the infrastructure.

Modern Business Landscape

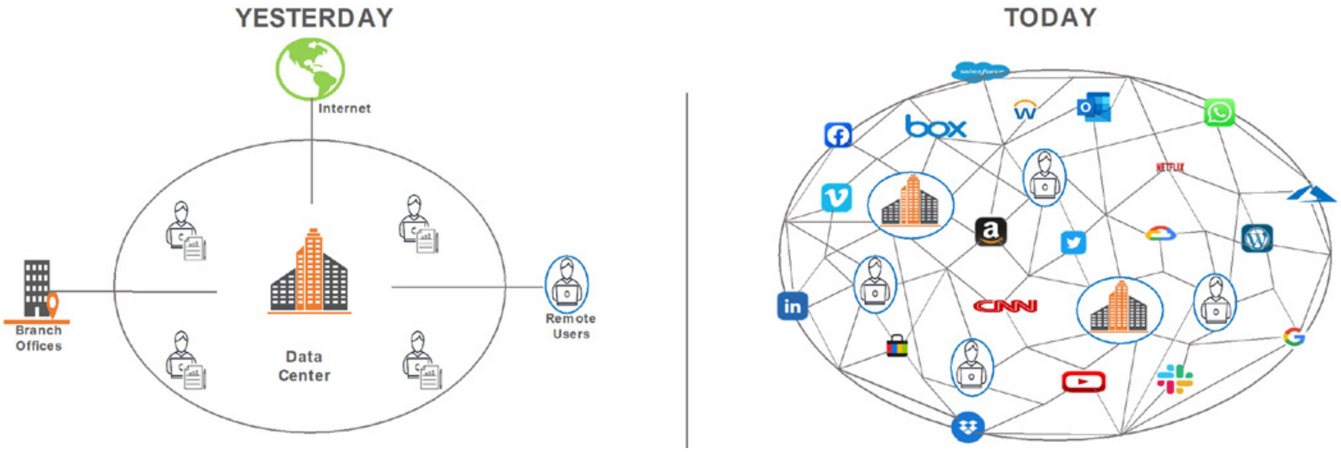
The hybrid work environment ensures users are no longer limited to specific physical locations to access apps and engage with digital services. They can access applications anywhere, anytime using smartphones, tablets through ubiquitous internet connectivity. The proliferation of users and their interactions with apps have resulted in the generation of vast amounts of data which leaves a digital footprint that, contributes to an expansive data landscape.

In a hybrid workforce setup, where employees work both remotely and in-office significant amounts of data are generated and require careful management. For example, Users in hybrid environments expect:

- The same SaaS app performance and connectivity experience whether a user is working remotely or onsite- using managed or unmanaged devices.
- Remote users accessing on-prem hosted applications such as SQL DB servers, would like to have same accessibility and performance when connecting as on-site user.

These dynamics necessitate a focus on security to protect sensitive information and maintain operational resilience to address challenges that include unauthorized access, data security, need for responsible data governance, and the prevention of data breaches. As organizations embrace digital transformation and accommodate remote work, the surface area for potential security vulnerabilities expands. Ensuring robust security measures are vital by implementing protection mechanisms such as:

- Endpoint Security
- Network Security
- Data Protection
- Incident Response
- Access Management

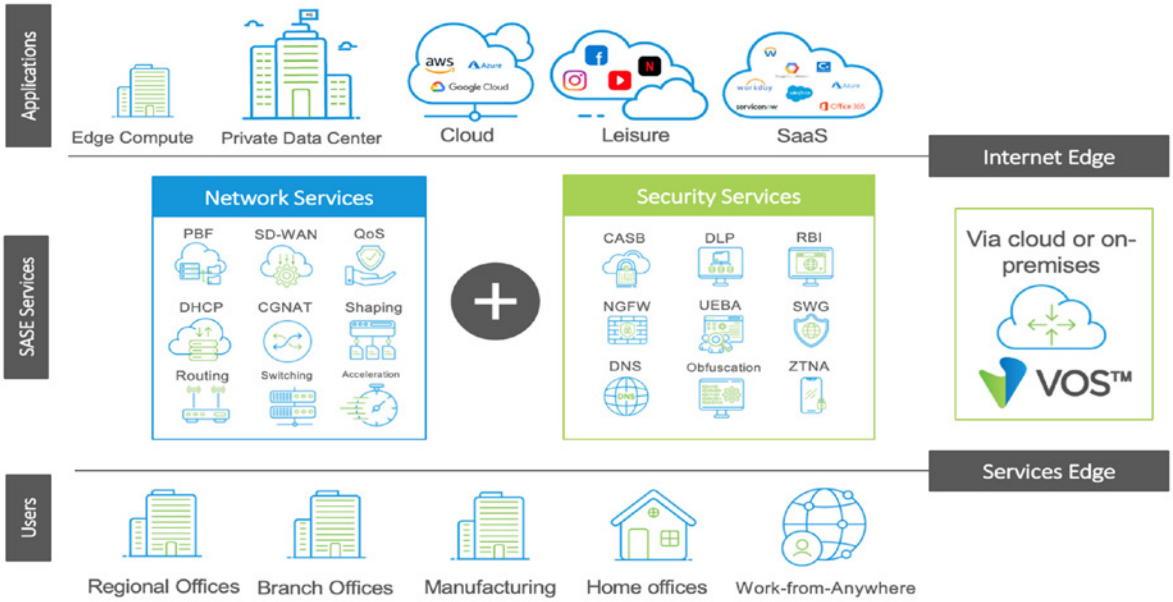


This requires digital transformation to be paired with a Zero Trust framework. It provides secure access to applications and resources regardless of their location or the user's device, enhancing security and enabling digital transformation initiatives.

Versa Networks: The Leader in SASE

Versa Networks has been delivering SASE capabilities several years before SASE became an industry term. Versa delivers a unique approach to networking and security challenges with a Single-Pass Parallel Processing architecture combining industry-leading SD-WAN, integrated full-stack security, advanced routing, and sophisticated analytics into a single software image. Moreover, Versa unites these benefits into a single, intuitive management interface, minimizing business friction, simplifying IT operations, and reducing appliance and management sprawl.

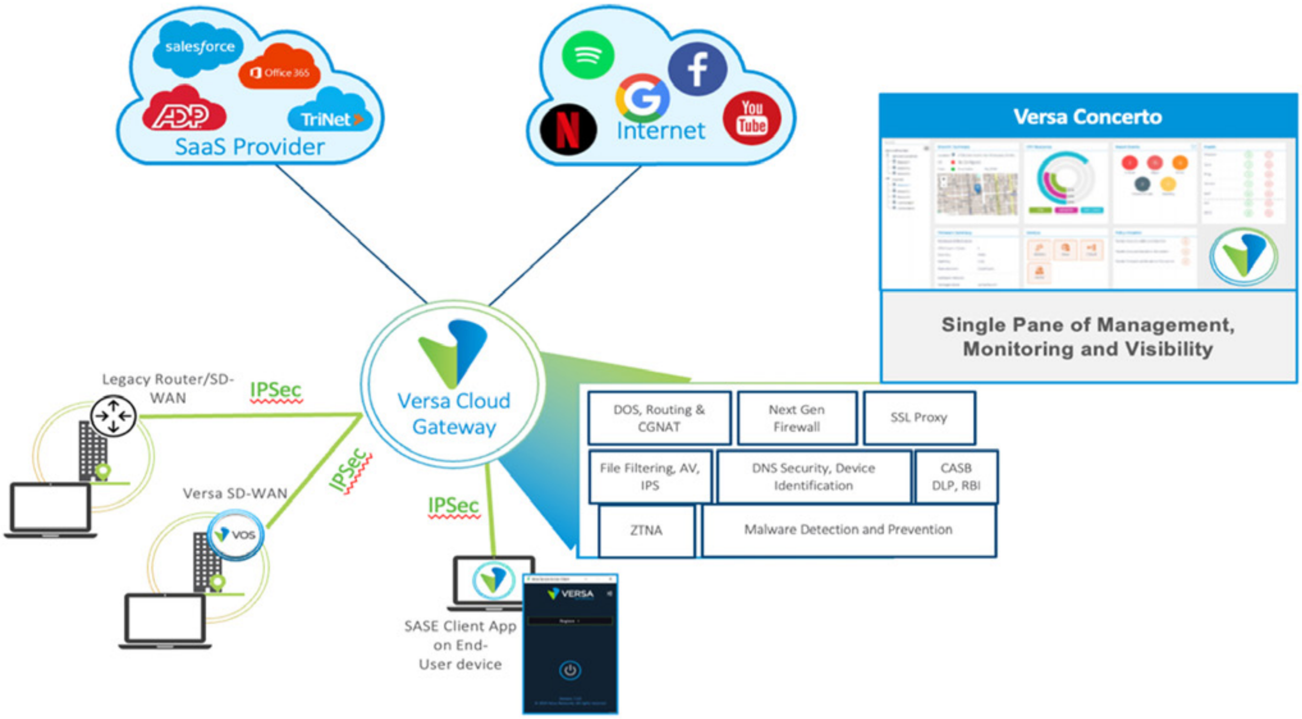
Versa's reimagination of network architecture enables services to not be chained together but built into a single pass software image with high levels of performance and security. Versa Secure Internet Access (VSIA) leverages this distinctive approach at the forefront of its architectural design to allow for optimal performance and security. It only decrypts a data packet once for both networking and security requirements, reducing the overall risk exposure.



Versa Secure Internet Access (VSIA)

Securing today's cloud and mobile-first enterprise requires a fundamentally different approach built on zero trust. Versa Secure Internet Access, is built on a Zero Trust security framework and architecture that focuses on providing secure access to resources regardless of the user's location or network environment. It is based on the concept of Zero Trust, which assumes that no user or device should be trusted by default, even if they are inside the network perimeter. VSIA eliminates legacy network security solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach offering.

Versa Secure Internet Access is part of the Versa Unified Secure Access Service Edge (SASE) platform, integrating full stack security, Identity & Access Management (IAM), Versa Secure Access and SD-WAN into a simple, hassle-free service that runs on cloud, on-premises or on a mix of these locations. The solution protects against web-based threats such as malware, ransomware, and phishing attacks.



Key Features include

- **Integration with SASE Architecture:** The VSIA solution is built on Versa Networks' Secure Access Service Edge (SASE) architecture, which integrates network and security functions to deliver a unified and consistent security posture across an organization's entire network. This integration enables the VSIA solution to provide advanced security capabilities that extend beyond traditional web gateway solutions, such as cloud application visibility and control and user and group-based policies.
- **Unified Management:** The VSIA solution is designed with a user-friendly interface that makes it easy for organizations to configure and deploy security and networking policies. The solution provides granular policy controls, which enables organizations to apply policies based on user, group, device, or location. This user-friendly interface also provides advanced reporting and analytics capabilities, enabling organizations to gain valuable insights into their network security posture.
- **User Behavior Analysis:** The VSIA solution provides user behavior analysis that enables organizations to detect anomalous behavior and prevent insider threats. The solution provides visibility into user activity, which enables organizations to identify and mitigate security incidents.
- **Comprehensive Security Capabilities:** The VSIA solution includes several key features, including CGNAT, URL filtering, DNS filtering, file filtering, IP filtering, anti-malware and threat protection, SSL/TLS decryption, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), RBI, and ZTNA-based policies. These advanced security capabilities provide comprehensive protection against a wide range of security threats.
- **Single Software Stack:** Versa offers cloud security, and networking functions delivering SASE framework on single software stack, Versa Operating System (VOS) built from ground up. The solution does not force a lock-in between software and hardware enabling NGFW, UTM and ZTNA capabilities through single software stack and better integration and convergence.

- **Improved Visibility:** By providing real-time visibility into web traffic, help organizations identify potential threats and respond quickly to security incidents.
- **Regulatory Compliance:** Meet regulatory compliance requirements, such as those related to data privacy and security
- **Industry Recognition:** Versa Networks' VSIA solution has been recognized by industry analysts such as Gartner, Dell'Oro, Cyber Org Rating, and CRN for its advanced security capabilities and integration with SASE architecture.

Versa Secure Internet Access can be an ideal solution for organizations looking for:

1. Simplified Cloud Delivered Security architecture.
2. Integrated Security Stack: Enhance comprehensive web security and protect networks from online threats.
3. Content Control: Enforce acceptable granular policies and maintain compliance, productivity, and security.
4. Advanced Threat Intelligence: Stay up to date with security incidents.
5. End-To-End Monitoring: End-to-end visibility and control Users, Devices and Apps.

Versa Secure Internet Access Solution

Versa Secure Internet Access solution includes following AI-powered security and data protection services to help you stop cyberattacks and data loss.

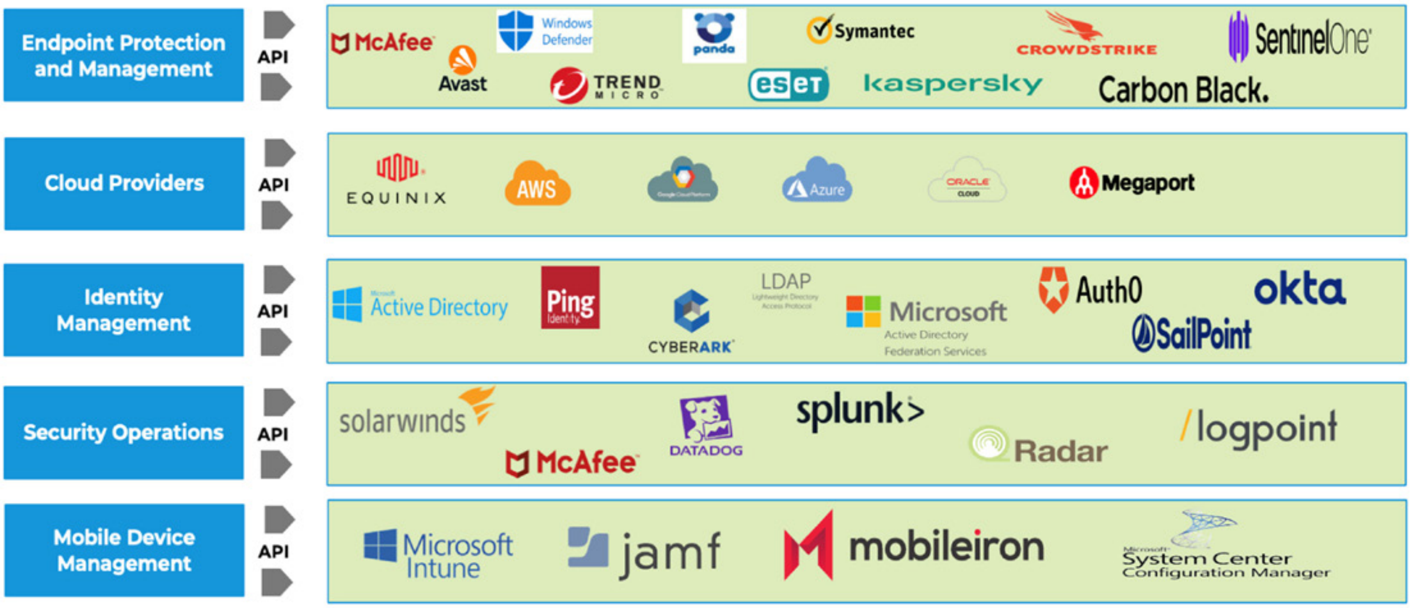
- Next Gen Firewall and IPS – Extend protection to all ports and protocols and replace edge firewalls with a cloud native architecture.
- Cloud Access Security Broker - Secure SaaS and IaaS destinations with integrated CASB to protect data, stop threats, and ensure compliance
- Data Loss Prevention – Protect data in motion and data at rest with full inspection using advanced capabilities such as EDM, OCR, AI/ML
- Remote Browser Isolation – Detect and make web-based attacks obsolete and prevent data loss
- Advanced Threat Protection- Detect and stop unknown elusive malware with AI-driven quarantine, sharing and protection across users in real time.
- Zero Trust Branch Connectivity – Reduce risk and complexity for users, servers, and IOT devices.
- End-To-End Monitoring – Help IT helpdesk reduce time-to-detect and time-to-resolve with end-to-end user and application performance visibility.

Versa Networks Zero Trust Integration Ecosystem

Versa VSIA's Zero Trust is a security framework and architecture that focuses on providing secure access to resources regardless of the user's location or network environment. It is based on the concept of Zero Trust, which assumes that no user or device should be trusted by default, even if they are inside the network perimeter.

In Versa's Zero Trust architecture, access to resources is based on multiple factors, including user identity, device health, location and behavior, continuous monitoring, and analytics. These factors are evaluated dynamically and continuously to ensure that only authorized users and devices can access the requested resources.

Versa Networks' solution is designed to provide integration capabilities with existing network infrastructure, cloud platforms, and third-party systems through APIs and SDKs. This allows enterprises to streamline their network operations and enhance overall network security and performance.



Versa Secure Internet Access Editions

Refer to Secure Internet Access Datasheet for more details on Licensing information.