DATA SHEET

# Versa SASE-on-SIM for Mobile Operators

Most industrial and enterprise IoT and OT devices that rely on cell coverage for connectivity run low-power, application-specific operating systems that are therefore limited in their ability to support traditional client software, which is essential in traditional security architectures. Versa's cloud-managed, cloud-delivered SASE-on-SIM solution helps secure SIM-enabled IoT and user devices connected over 3G, 4G or 5G networks by leveraging the unique IMSI, device IMEI, or the MSISDN for identification, authentication and authorization to extend the full converged network security and software-defined WAN and LAN capabilities and benefits of the Versa unified SASE platform to these endpoints.

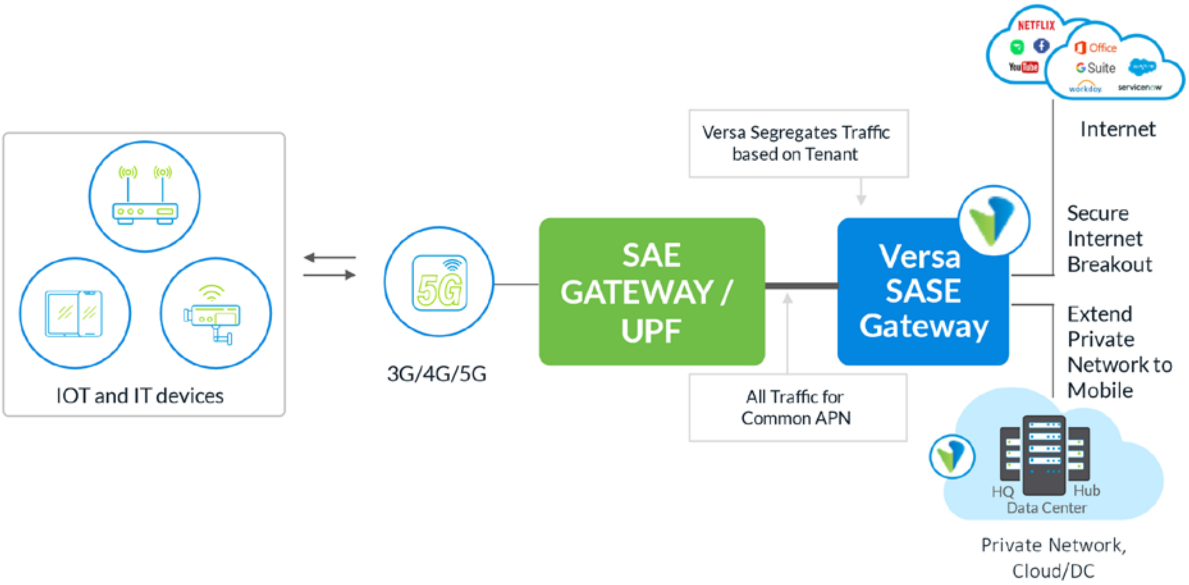


*Figure 1 – SASE-on-SIM Architecture*

The use of the IMSI or IMEI prevents movement of SIM cards to another device, ensuring that the intended service is deliv-ered for the specific target device, and enables the granular application of advanced security policies at the mobile network edge at the level of the subscriber. Just like client devices, traffic from SIM-enabled devices is scrubbed through a SASE point of enforcement where it undergoes security checks and tenant-specific policy enforcement before reaching enterprise re-sources. This model enables a decentralized, scalable, and secure approach to network access and data protection, aligning with the distributed nature of modern enterprise operations.

## Securing SASE-on-SIM devices

### Zero trust access to private applications

Versa SASE-on-SIM delivers clientless zero trust connectivity to applications hosted by the enterprise in the data center, private cloud and/or virtual private cloud instances of public cloud providers. The solution offers password-less authentication for identifying the user and for enforcing zero-trust policies. Inline with Zero Trust Framework, Versa SASE-on-SIM authorizes the user for each application access, provides a microsegment for each application access and obfuscates both application and user IP addresses. Versa SASE-on-SIM uses granular policy-based application traffic management to control and limit application access and visibility with every access event.

## URL and IP Reputation, Categorization and Filtering

Versa SASE for SIM 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, inap-propriate sites like gambling or pornography to avoid legal liability, bandwidth management including voice and vid-eo 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

A majority of the web traffic is encrypted over HTTPS protocol. An effective security solution requires scrubbing of unen-crypted traffic for malicious behavior and mal-intent. Versa SASE on SIM includes TLS/SSL proxy which can decrypt the user traffic, and re-encrypt the traffic post scrubbing before forwarding it to the destination. Versa SASE for SIM solution. It in-cludes a TLS/SSL proxy which:

- 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 preven-tion, detects and prevents data leakage to enforce company compliance.
- Supports 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.

## Next Generation Intrusion Prevention (NG-IPS)

Versa SASE on SIM includes a Next Generation IPS solution. The solution provides:

- 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 tech-niques 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 frequently updated frequently (configurable for real time updates) by Versa's Threat Research labs 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.

## Seamless integration with mobile networks

Versa SASE-on-SIM is offered in partnership with Mobile Network Operators. The solution is built on standard interfaces supported by the MNO, integrating seamlessly into the existing mobile core network, and is natively multi-tenant. Each en-terprise customer of an MNO is provided with a private segment for data processing, policy enforcement, management and visibility, and devices are automatically assigned to an appropriate segment belonging to the customer.

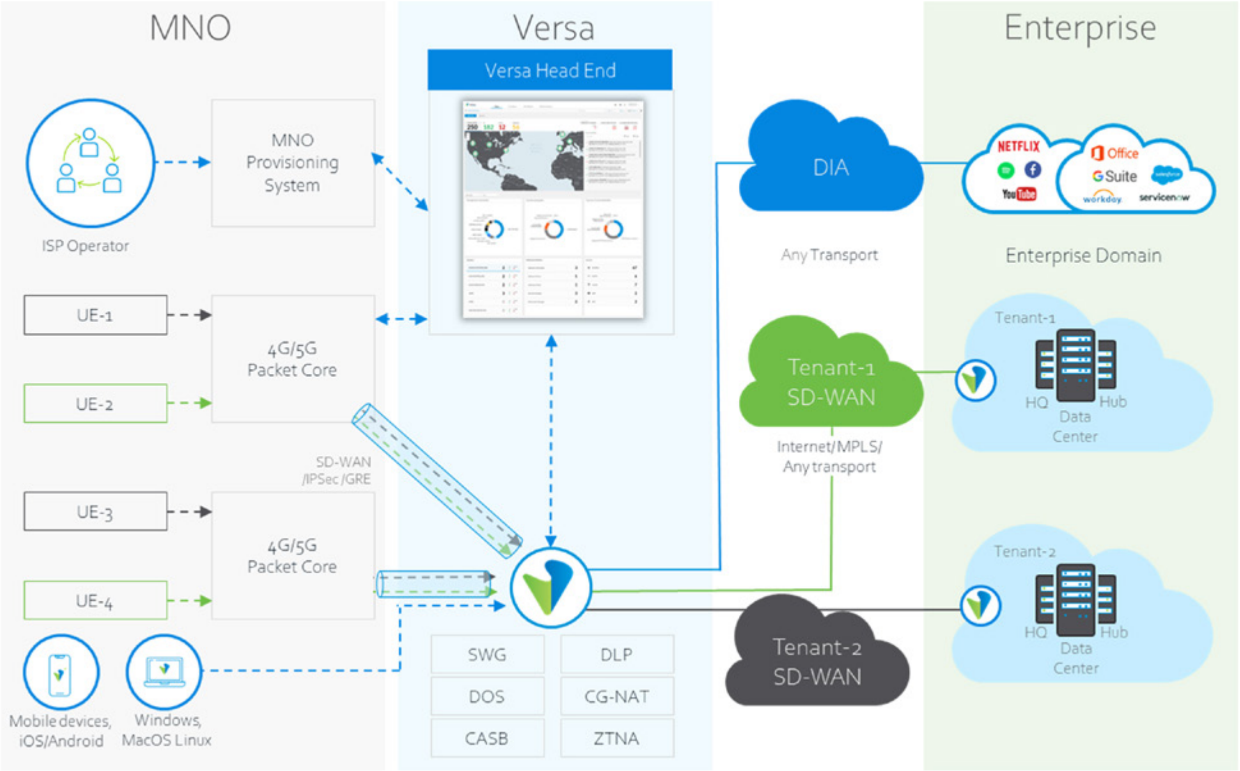


*Figure 2 – SASE-on-SIM seamless integration in MNO network*

Versa SASE-on-SIM enables MNOs to deliver a client-less SASE service for IoT and OT devices connected over their WAN network as a value-added-service. The solution also helps to consolidate private APNs implemented in the network, reducing the complexity and improving the scalability of the Mobile Network.

Versa SASE-on-SIM for Mobile Operators gives enterprise customers visibility into every user and device on the network, enables zero trust enforcement within the mobile operator network, and provides security for any-to-any connectivity be-tween users, devices and apps regardless of location. From an integration and deployment perspective, key benefits of Versa SASE-on-SIM include:

- No tunnels are used or necessary, reducing the operational and management overhead of maintaining and monitor-ing client versions, tunnels and ensuring compliance.
- Seamless integration with mobile subscription plans without the need to provision private APNs within the mobile network. This reduces the complexity of deploying the service and allows the solution to scale to a far greater num-ber of tenants.
- Backend integration with the enterprise's SD-WAN network to provide zero trust connectivity to customer applica-tions.
- Versa Cloud Gateways are deployed in partnership with MNOs to provide reliable and secure on-ramps for traffic from SIM-enabled devices. Gateways authenticate users in conjunction with the MNO network, authorize applica-tion access, and secure enterprise networks from external threats.

The overriding benefit is that a trade-off between IoT application efficiency and IoT security is no longer required, as Versa SASE-on-SIM allows IoT endpoints to be incorporated into full-fledged SASE-based security and networking, including single-pane-of-glass management, a full security suite and a single data lake for visibility and reporting.

## Unified SASE Architecture

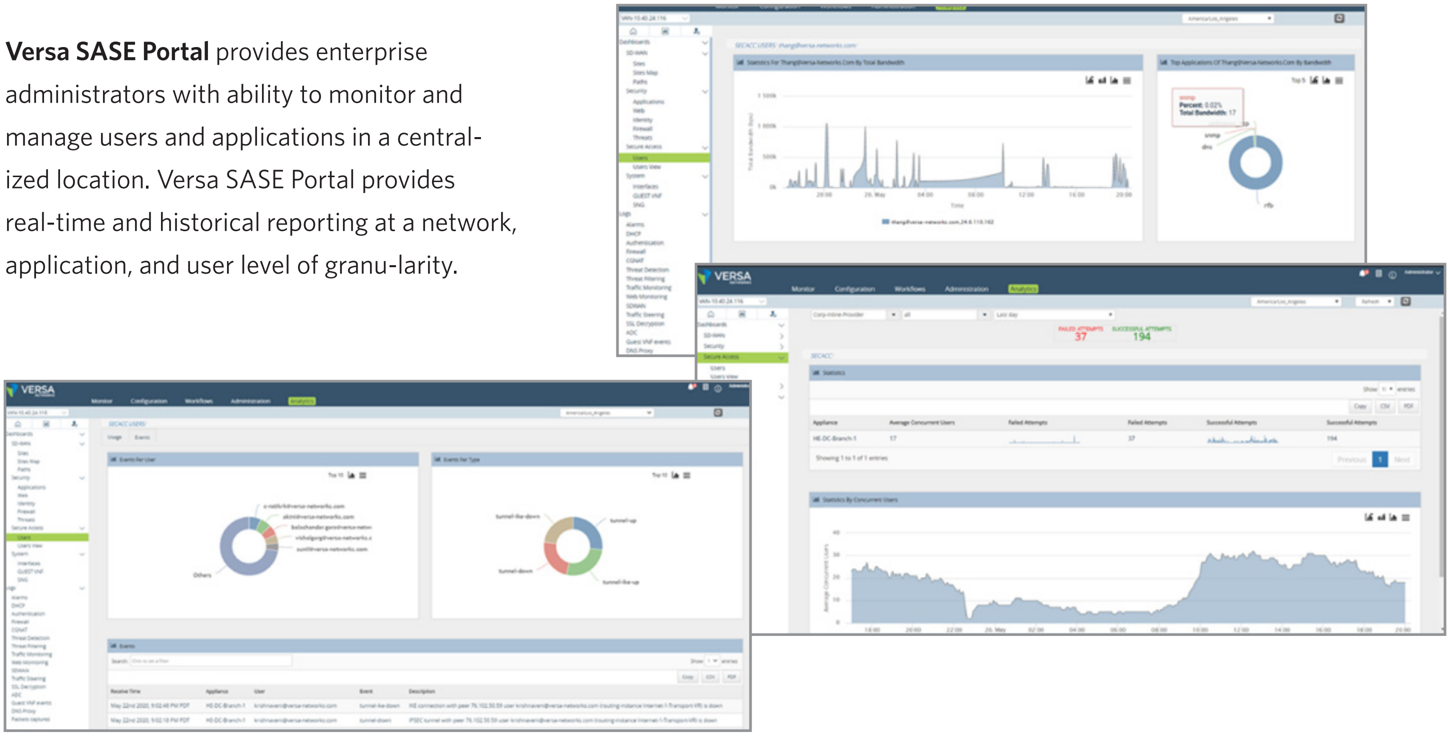
Versa SASE on SIM comes with an intuitive portal for provisioning, managing, and monitoring of security, routing, and SD-WAN services. Versa's SASE portal provides centralized visibility and control for internal, inbound and outbound traffic. The solution eliminates the need for organizations to deal with operational upkeep and other day-to-day tasks, reducing IT complexity and costs.

Versa SASE on SIM solution comes with a unified policy framework with single-touch deployment including sites that are leveraging Versa Secure SD-WAN. Versa policy framework covers devices and applications independent of deployment and access, providing a simpler policy deployment, configuration, and management through an automated and centralized policy engine.

### Versa Cloud Gateways

Versa Cloud Gateways are Points of Presence based on Versa's platform. They are deployed in partnership with MNOs to provide reliable secure on-ramps for traffic from SIM -enabled devices. Gateways authenticate users in conjunction with MNO network, authorize application access, and secure enterprise network from external threats. Versa Cloud Gateways integrate advanced routing, comprehensive security, and market-leading SD-WAN, with secure access. The Versa Cloud Gateways securely connect to and integrate with Enterprise's existing network and datacenter infrastructure.

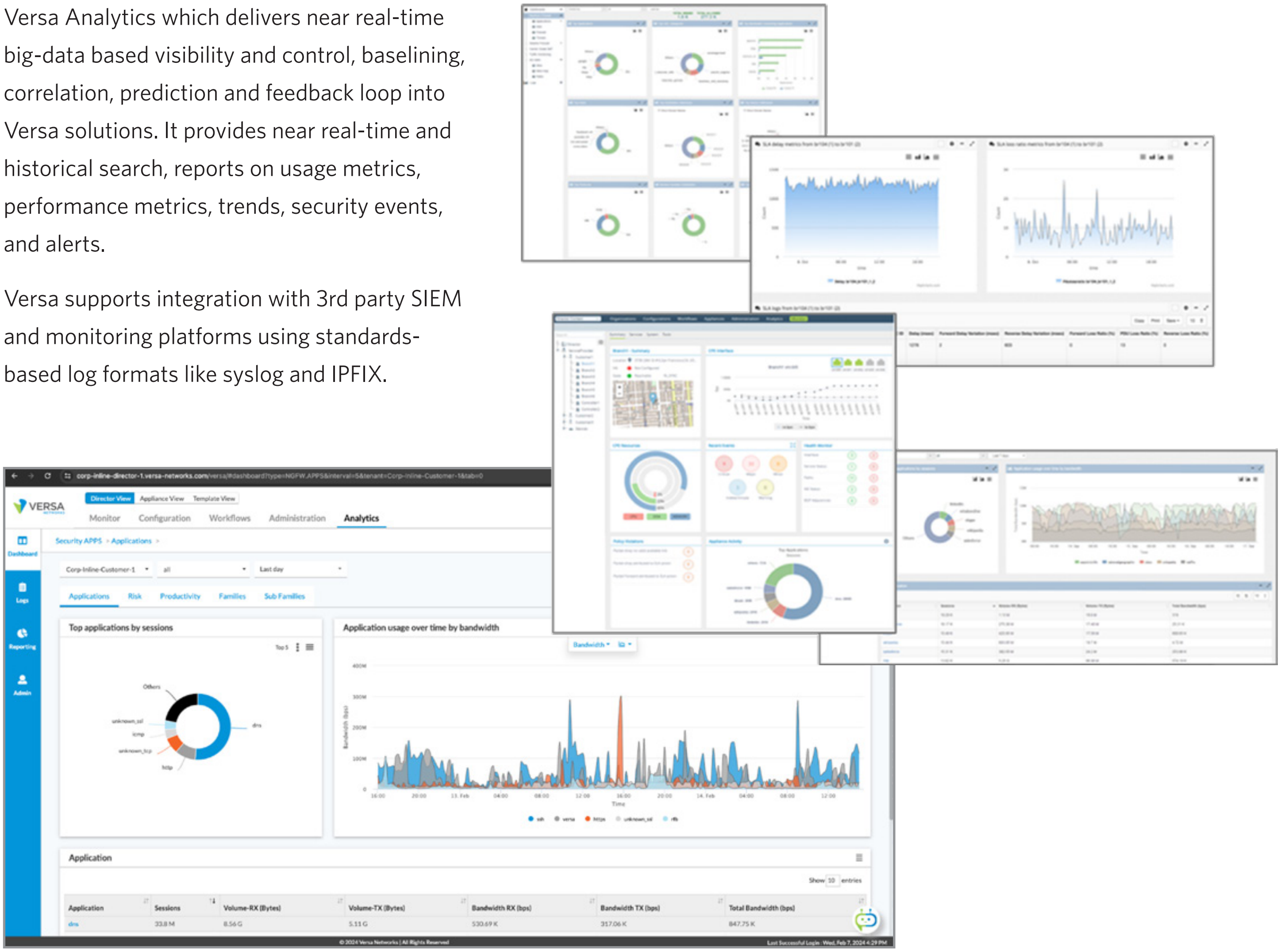
**Versa SASE Portal** provides enterprise administrators with ability to monitor and manage users and applications in a centralized location. Versa SASE Portal provides real-time and historical reporting at a network, application, and user level of granu-larity.



## Integrated Big-Data Analytics and Visibility

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.



| Application | Sessions | Volume-RX (Bytes) | Volume-TX (Bytes) | Bandwidth RX (bps) | Bandwidth TX (bps) | Total Bandwidth (bps) |
|---|---|---|---|---|---|---|
| dns | 33.8 M | 8.56 G | 5.11 G | 530.69 K | 317.06 K | 847.75 K |

© 2024 Versa Networks | All Rights Reserved
Last Successful Login : Wed, Feb 7, 2024 4:29 PM

## How to Order

Versa SASE-on-SIM is delivered in partnership with Mobile Network Operators. A Versa account manager can help you iden-tify MNOs who can offer SASE as a value-added service for your requirements.

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