

Zero Trust with Versa Security Service Edge

Dramatically simplify security between any app, device, user, location and workload, without compromising performance.

Secure Every Edge

Versa enables you to consolidate your security products into a unified platform that applies Zero Trust across your enterprise edge, everywhere it exists – whether your users are remote, in the office or on the road. With best-of-breed security built into our platform from the ground up, it provides superior protection without compromising user experience. Zero Trust principles allow you to identify users and devices, control access to resources, and quickly detect, respond and recover from threats. And the unified platform provides unparalleled observability that simplifies the design, deployment and lifecycle management.

Versa Secure Private Access

Go beyond other Zero Trust Network Access (ZTNA) services with Versa's unified security and network stack to protect users and workloads while delivering unparalleled user-app experience.

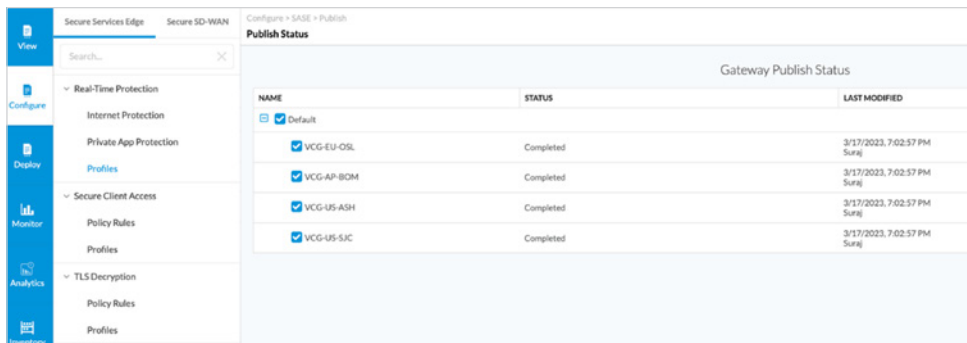
Versa Secure Internet Access

Cloud-managed and cloud-delivered, VSIA applies Zero Trust policies across enterprise sites, home offices, and traveling users accessing distributed applications without compromising security or user experience.

Enforce consistent Zero Trust security policies at every edge

Legacy security approaches are mired in the complexity of point products, with islands of isolated policies for every user, device, location and resource. To make matters worse, additional tools and resources are needed for configuration and lifecycle management of this fragmented infrastructure.

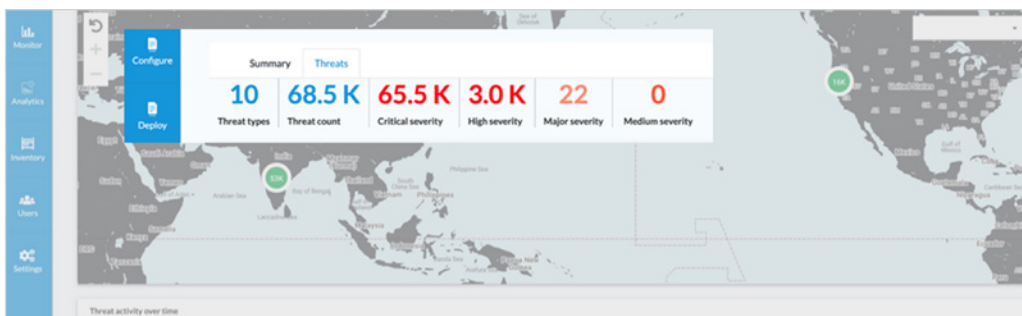
Versa's Zero Trust architecture enables you to deploy a least privilege policy that is dynamically distributed and enforced at every network edge, whether in Versa's cloud, your partner's cloud or on your premises. Versa's AI continually monitors user and device security posture, and enforces security policy at the closest edge. With Versa, a single security policy stays with the user – no matter where the user connects from, the device they use, or the application to which they connect.



Gateway Publish Status		
NAME	STATUS	LAST MODIFIED
<input checked="" type="checkbox"/> Default	Completed	3/17/2023, 7:02:57 PM Surtaj
<input checked="" type="checkbox"/> VCG-EU-OSL	Completed	3/17/2023, 7:02:57 PM Surtaj
<input checked="" type="checkbox"/> VCG-AP-BOM	Completed	3/17/2023, 7:02:57 PM Surtaj
<input checked="" type="checkbox"/> VCG-US-ASH	Completed	3/17/2023, 7:02:57 PM Surtaj
<input checked="" type="checkbox"/> VCG-US-SJC	Completed	3/17/2023, 7:02:57 PM Surtaj

Automated threat detection and response powered by AI Ops

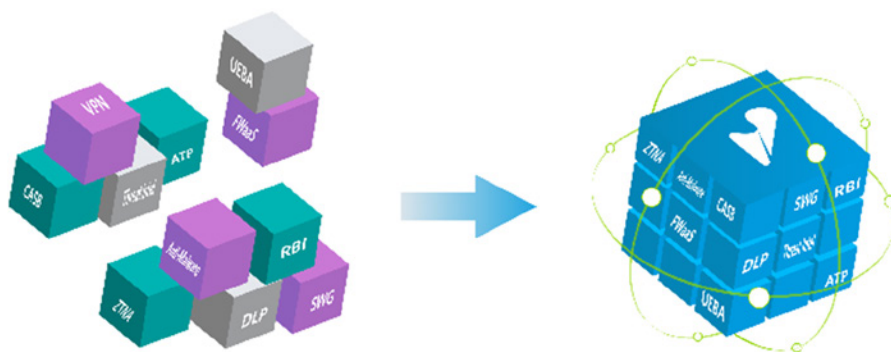
Enterprises have typically used adjunct tools outside of their security controls to try to identify anomalous behavior and security threats. But manually correlating unmanageable volumes of information characterized by fragmented context and limited identity data across disparate systems generates huge volumes of false positive incidents. On top of that, additional tools are needed to facilitate response and remediation.



With Versa's unified data lake and AI Ops, threats and anomalous behaviors are accurately identified in real time, replacing noisy alerts with actionable insights and automated remediation. Because security and network attributes are tightly integrated, Versa is uniquely able to correlate identity, device and network context across events, leading to improved threat identification accuracy.

Consolidate security point products into an integrated platform

Consolidate disconnected security products into a single, best-of-breed software platform that is centrally managed and controlled. With Versa, you can define once and consistently enforce a unified set of Zero Trust policies and functions to protect users, devices, sites, apps and workloads.



Unified Observability and Management

AIOps simplifies creation, automation, lifecycle management and delivery of all SASE services across tens of thousands of users and sites. Rich real-time, historical insights and AI/ML based anomaly detection reduce MTTD & MTTR for network & security events.

Don't let security ruin your user experience

Fragmented legacy security approaches chain point products together sequentially, delivering user experiences characterized by latency and reachability problems, and management complexity for the administrator.

Versa's AI-driven intelligence dynamically selects the best path to an application. Always-On connectivity ensures robust reachability to deliver a seamless experience even in the case of failures. The unified platform's single pass scanning architecture improves performance by applying multiple security services in parallel.

