Versa Terminal Server Agent

Per-user Zero Trust solution for virtual hosts delivered natively by VersaONE Universal SASE Platform

Introduction

A Zero Trust architecture assumes that the enforcement points know the identity of the user behind every connection. For an endpoint running the Versa SASE Client that assumption is true. There is one device, one user, and one tunnel. However, that assumption fails when shared hosts are used. With any type of shared terminal services solution each user's network traffic is sent with the same source IP address. Subsequently controls which build ZTNA security posture, including user-attributed logging, are ineffective and protection is limited to simple host-based firewall rules.

Today most organizations, that operate Microsoft Remote Desktop Services (RDS), work around this gap using a dedicated terminal-server policy which is bound to the host's IP address. It requires building a dedicated server farm for each department to achieve some sort of segmentation and subsequently authoring IP-based Next Generation Firewall (NGFW) rules for each segment. This significantly increases infrastructure, licensing and maintenance costs. Additionally, every connection is logged based on the server's IP address, so during an audit or security incident operations teams are unable to identify user activity. This means that terminal servers could operate in a place where identity-based security doesn't work.

The Versa Terminal Server Agent (TSA) closes this gap at the source. It runs on the Windows Server, gives each user a dedicated source-port range and sends the user with an IP:port mapping to the Versa Operating System (VOS) where security enforcement happens. By enforcing all ZTNA policies in a single pass, VOS applies unified user mappings across every security control and automatically associates each log entry with the user's identity.

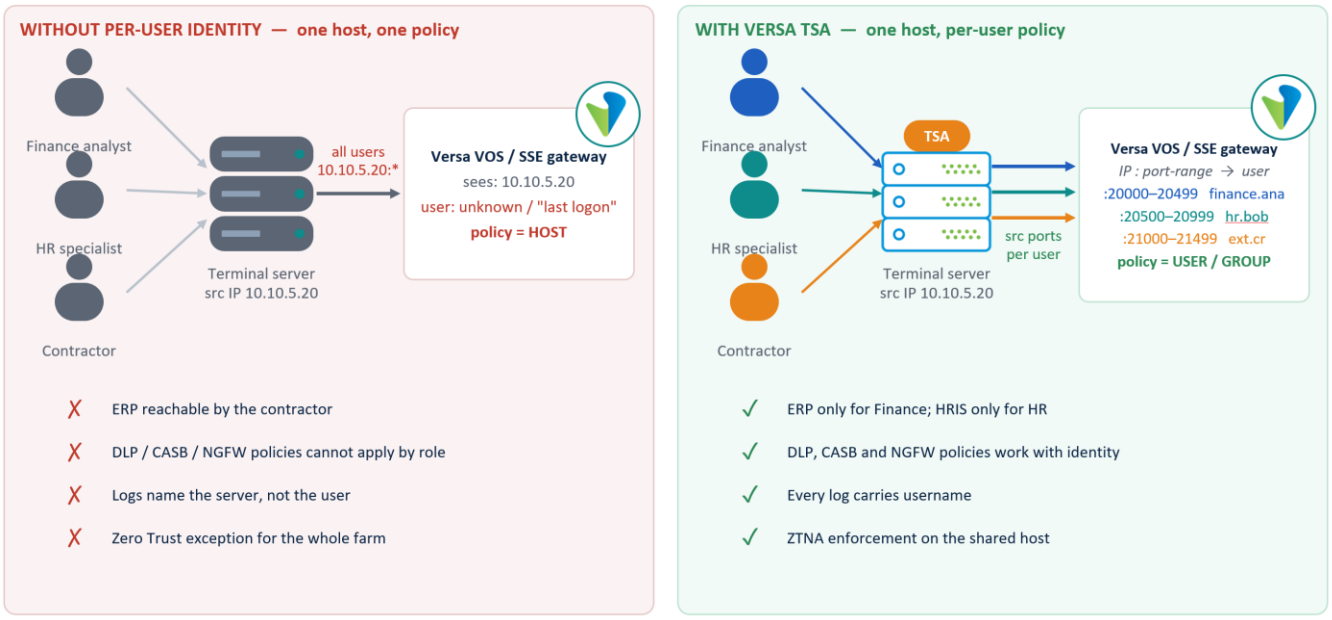
What businesses gain:

- **Zero Trust without dedicated zones and server farms -** Individual users on shared hosts are uniquely identified, enabling granular enforcement of user and group-based security policies. The host-based rules may be retired.
- **Microsegmentation is available on a shared infrastructure -** Finance, HR, engineering and any other departments can connect to the same server farm. Users can access only the applications authorized for their assigned groups.
- **Role-based data protection** - DLP, CASB, URL filtering and other policies, including GenAI Firewall may be applied per user and group.
- **Audit-ready analytics** - Every traffic flow is logged and associated with a unique user identity, while analytics provides an exportable event audit trail.
- **Lower cost of ownership** - Eliminates the need for dedicated server maintenance while maintaining consistent, per-user security posture standards.
- **Transparent to users** – Requires no additional tunnels, logins, or re-authentication prompts.

Blind spot in identity-based security

Every policy decision across the SSE stack is driven by flow-specific attributes. For user identity-based security policies the key attribute is a user or group bound to the data flow. On a single-user endpoint the source IP is a reliable attribute for the user. On a shared host it is not. The IP address identifies only the server, not individual users, as it is shared across all active user sessions. The only per-session attribute left for a data flow in IP header 5-tuple is the source port.

By default, operating systems assign source ports from one shared pool, with no relationship to the identity of who initiated session.



The table below summarizes blind spots and their impact:

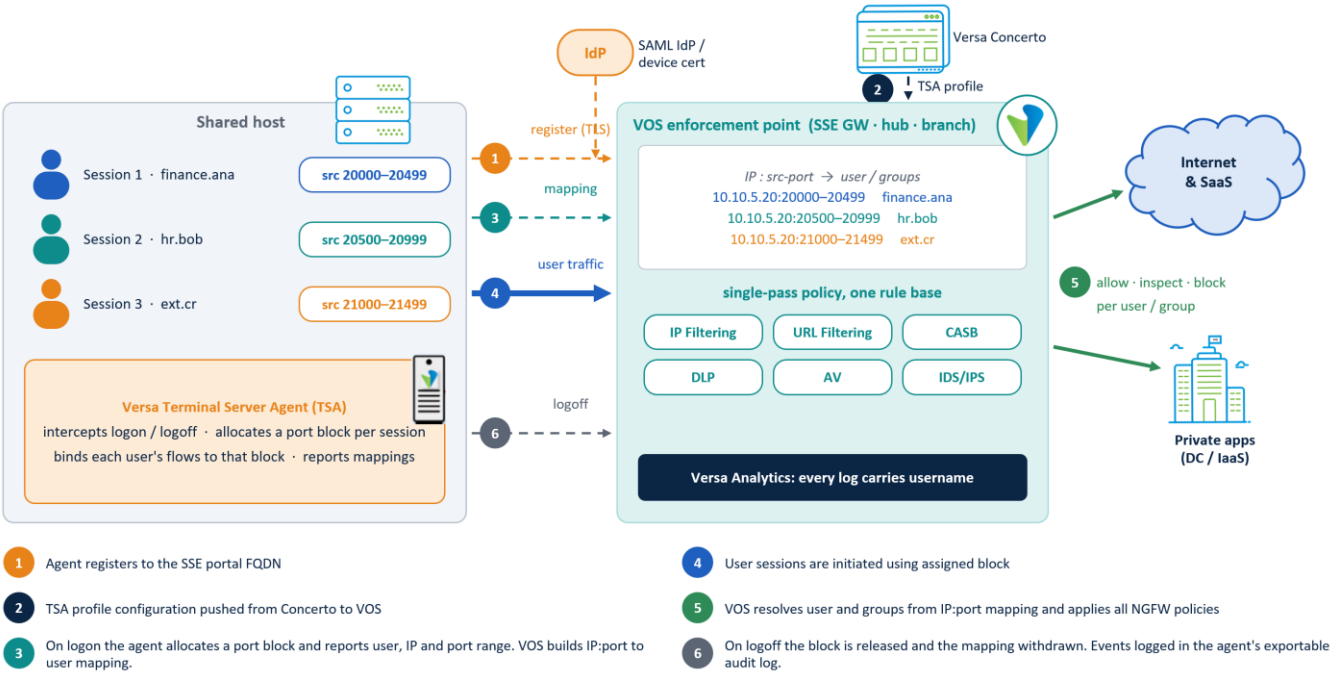
Technical symptom	Security blind spot
Host-wide entitlement. Any session initiated from the server farm inherits the broadest application access configured for that host.	Microsegmentation and security posture is broken for privileged access to business-critical systems. That increases the potential blast radius of a compromised account.
DLP, CASB and other NGFW security policies cannot evaluate the user's role.	Sensitive uploads, SaaS misuse, and generative AI prompts are governed by a single policy on the shared host, creating a trade-off between overly permissive security and overly restrictive access.
Logs and alerts are attributed to the host or to the last authenticated user.	Security incidents are bound to a host. Attributing an action to a user requires manual correlation of session logs that may not be retained.
Virtual-desktop environments operate outside of Zero Trust architecture principles.	100% Zero Trust milestones become difficult to achieve. Workarounds (per-department server farms, per-role subnets, single-session VDI) add cost and operational challenges.

This problem is growing as more organizations are moving to shared, multi-session virtual desktops. Hosted virtual desktops made up about 46% of 2025 desktop-virtualization revenue, and DaaS is growing roughly 11.5% a year, which packs more users behind each IP address. At the same time, Zero Trust principles and microsegmentation require trust decisions to be based on individual user sessions rather than network location. Stolen credentials remain a leading

cause of breaches and shared jump servers used by admins, contractors and other departments to reach business critical applications, production system and OT systems are exactly where misuse is hardest to spot.

Solution overview using Versa Terminal Server Agent

Versa Terminal Server Agent (TSA) eliminates identity-based security blind spots in shared server environments by correlating the source IP address and port with individual user sessions, enabling precise user identification and policy enforcement. It is a lightweight agent installed on the Windows Server that controls how sessions are originated. For every interactive logon it allocates a dedicated block of TCP/UDP source ports, then binds ports from that block to user's outbound connections, and reports the username, host IP and port range to the VOS appliance or SASE gateway. VOS then maintains IP:port to user mapping and resolves each flow to a user and their groups for security policy evaluation. From that moment the shared host behaves like a set of individually identified endpoints.



The above diagram illustrates how it works in more detail. In this case 3 users from different departments are connected to the same shared host with the TSA agent installed on it. From the network point of view, all sessions look identical, because every packet leaves the server with the same source IP address. However, VOS will have IP:port to user mappings which will allow it to identify every user and enforce identity-based security policies accordingly.

Before users login, the TSA agent registers with the VOS instance using a configured Portal FQDN and credentials. Once registered, the agent receives its configuration from the TSA profile, which administrators manage centrally using Versa Concerto. The profile has information about which port range it can use, how many ports each user can receive and how often to sync with the platform. These settings are view-only on the host, so the policy always remains under central control.

For example, when user Ana logs in, the agent assigns her a unique source port range of 20000 to 20499 and reports to the VOS that this is a range on 10.10.5.20 that belongs to username finance.ana. Similarly, Bob gets 20500 to 20999 and contractor gets 21000 to 21499. VOS creates each entry in its IP:port to user mapping and looks up each user's groups from the configured identity source, so it knows not just who each person is, but which department or group they belong to.

From a user point of view everything works as usual. Their applications open connections normally while agents on the backend ensure that each new connection uses a source port from assigned port ranges. Traffic follows the host's existing route to the VOS. The agent doesn't change routing, doesn't build any dedicated tunnels, doesn't proxy anything, and each new session originates in the usual way.

When a connection reaches VOS, it checks the source IP and port against the already created mapping and instantly knows whose traffic it is. VOS creates a session that is associated with the right user and group attributes and runs the

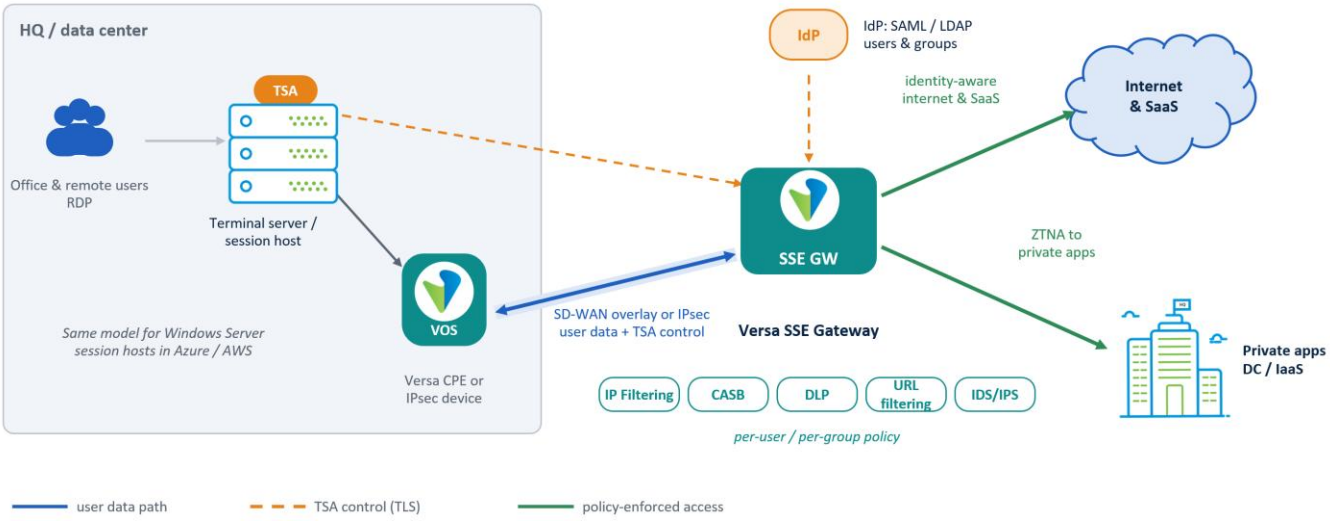
flow through a single-pass security policies enforcing it against all NGFW features like IP filtering, URL filtering, CASB, DLP, antivirus and IDS/IPS. As a result, Anna can have access to financial applications, while contractor who share the same server can be limited to a few resources or just allowed access to Internet.

Every decision and log entry carries the username which can be validated and a per flow/session report can be created in Versa Analytics. When a user logs off, the agent releases their port range and withdraws the mapping from VOS. Every logon, logoff and port allocation is recorded in the agent's event audit log, which can be exported for detailed analysis. The result is that each session is treated with its own identity, with its own policy and its own audit trail.

Reference architectures

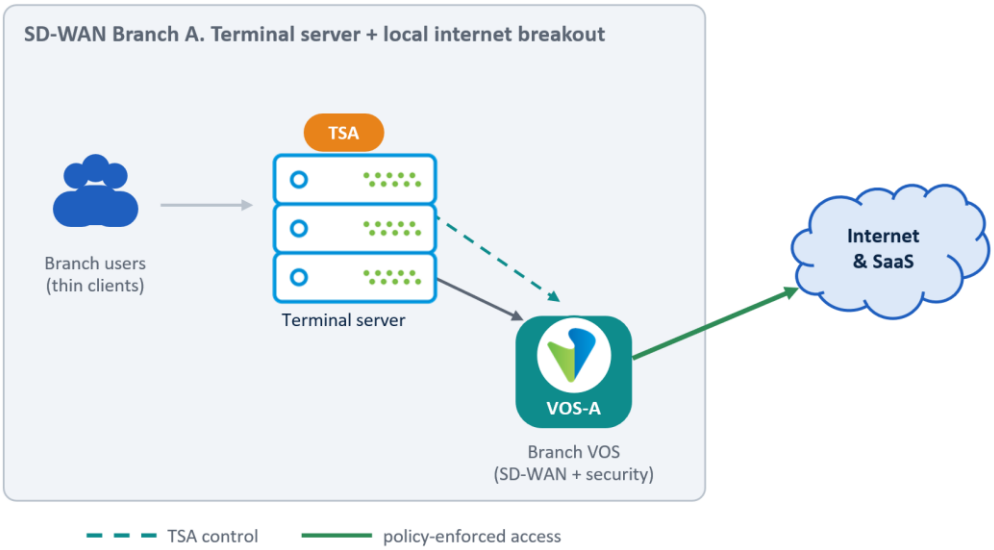
TSA operates independent of where enforcement happens. The key design consideration is identifying which VOS node processes the traffic requiring user attribution, as this determines where the agent should be registered. Below are three possible architectures.

The first use case is when the terminal server is installed at the headquarters, a data center or IaaS and enforcement is at SSE gateway.



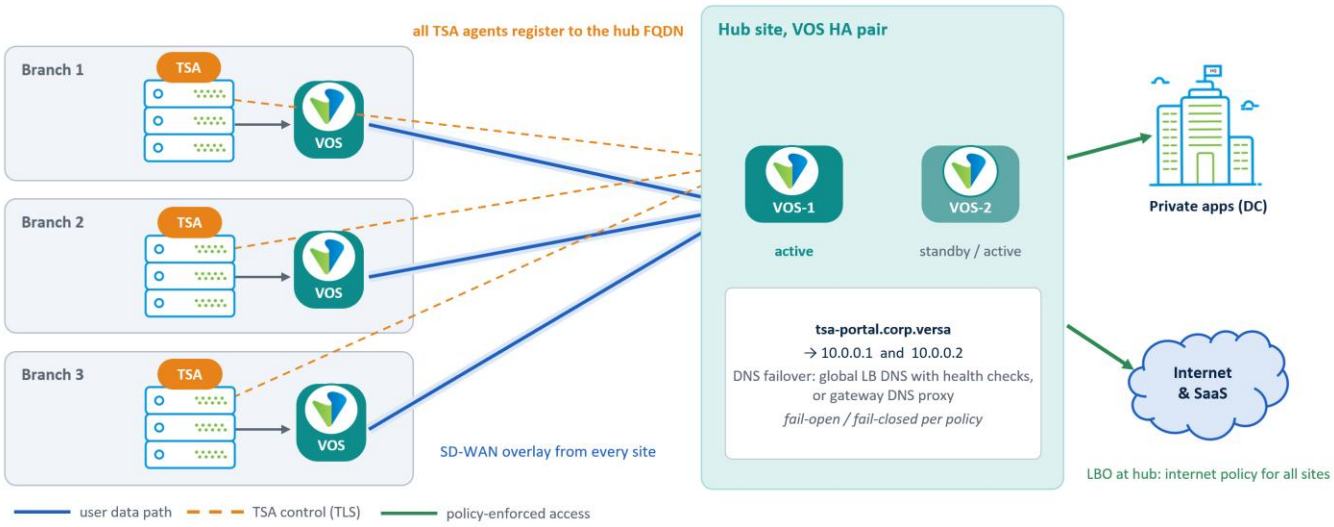
The host's outbound traffic is carried by the site's Versa CPE (or any IPsec-capable device) to the Versa SSE Gateway, where user and group policy is enforced for internet, SaaS and private application destinations. It is typically deployed with centralized server farms or when enforcement should happen on SSE Gateway.

The second use case is with the terminal servers hosted in a SD-WAN branch with local internet breakout.



Branch users work on a local terminal server behind a Versa SD-WAN appliance. Internet-bound traffic breaks out locally. Policy enforcement happens locally on a branch appliance (VOS). This architecture enables a local VOS node to inspect both public Internet and private application traffic, with connectivity to the data center established through an SD-WAN or IPsec tunnel.

The third use case includes many sites connected to a central Hub with high availability.

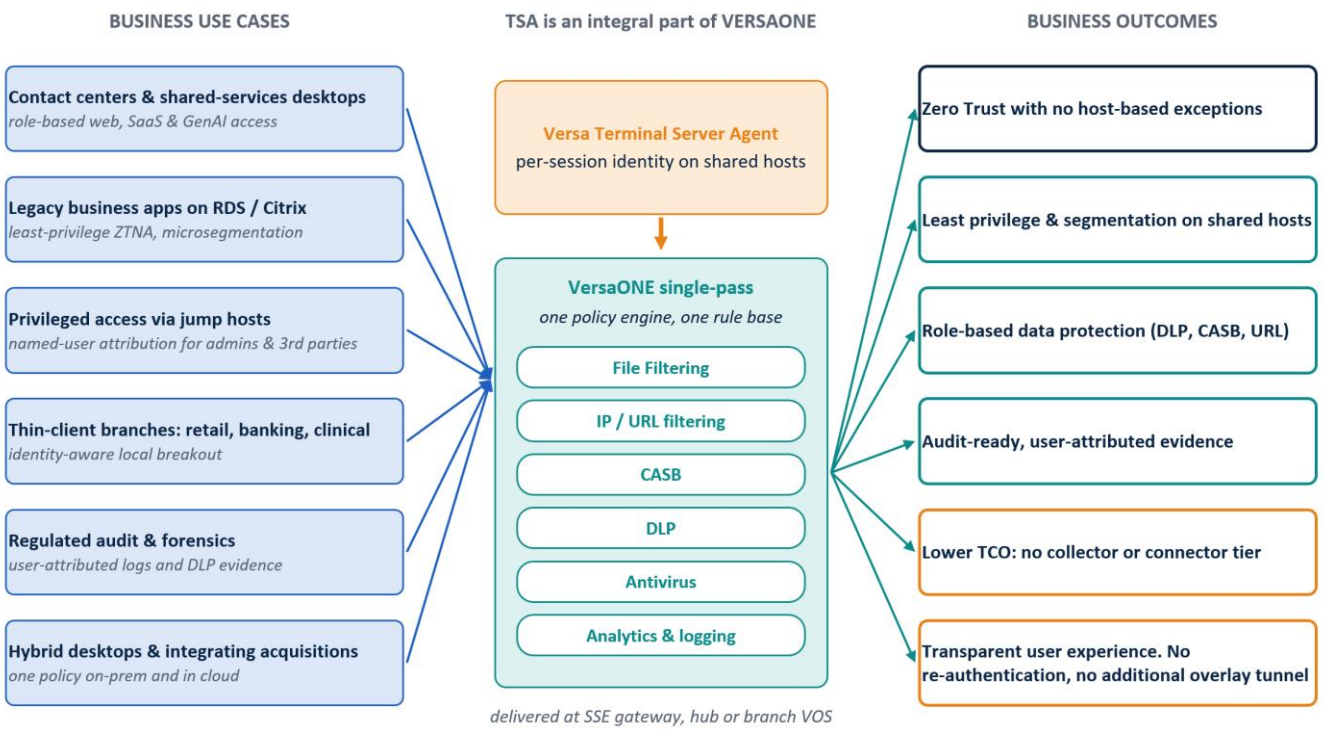


Each branch hosts a local terminal server for latency-sensitive applications, while private applications are hosted behind a Hub site. All TSA agents register to the Hub's portal FQDN, which resolves to both members of the Hub VOS pair. Local Internet breakout is also configured at the Hub. As a result, Internet policy and Private Application protection policies are enforced at the Hub location, providing a central location for security posture enforcement, preserving ZTNA architecture and microsegmentation requirements.

Resilience is achieved by configuring DNS to include both gateway IP addresses, enabling automatic failover. This is implemented either by a global load-balancing DNS service with health-checks to Hubs, or by the gateway's built-in DNS proxy, which answers the portal FQDN with its own address and follows routing failover.

Solution summary and Business outcomes

Shared infrastructure should never mean shared identity. Identity-based security is an integral part of a true ZTNA architecture. In the VersaONE platform, identity replaces the network location as the source for security posture enforcement. Access decisions are no longer based on where a user connects from. Instead, every request is verified against who the user is, which device they are using, and what they are authorized to reach.



The main business value is no security posture exception by using VersaONE platform. Shared hosts are an integral part of ZTNA architecture, as a result each connection is enforced by role-based data protection which significantly reduces the potential blast radius of compromised credentials. Additionally audit-ready reports and user-attributed evidence shortens investigations and reduces compensating controls.

For more information about how to implement Versa Terminal Server Agent see our Implementation Guide.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com

About Versa
Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.

©2026 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and FlexVNF are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners.