SASE Operational Excellence

Matthew Yakhov
Sr. SE Manager

Naveen Kumar
Director Engineering

VERSA NETWORKS

Agenda

- Operational Excellence for SASE
- Zero Trust Network
- Connectivity
- Secure Web Gateway
- Anomalies in the Network
- SASE Monitoring
- Q & A

Versa·ti·li·ty 2023

VERSA NETWORKS

Achieving Operational Excellence for SASE at Scale

Versa·ti·li·ty 2023

VERSA NETWORKS

Running Networks Efficiently & Securely

Zero Trust Network Access(ZTNA)

Connecting SASE Fabric to Customer Network

Configuration of Security Policies

Connecting Users to Apps Securely

Find anomalies

Monitor Network Performance

Monitor Application Performance

Monitor End to End

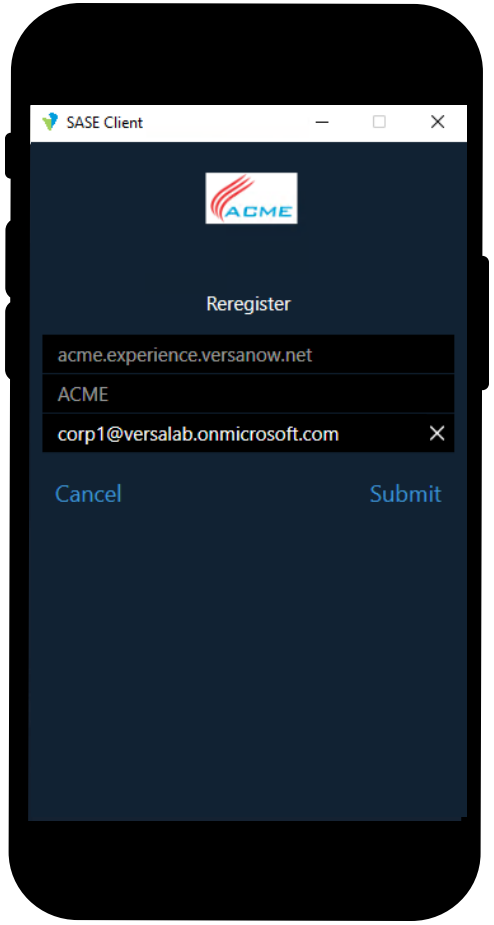
Zero Trust Network

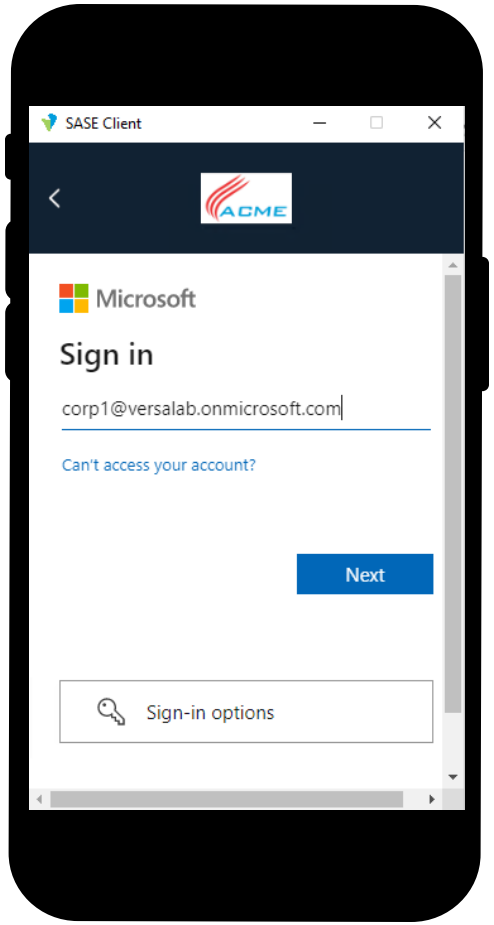
Versa·ti·li·ty 2023

VERSA NETWORKS

Zero Trust Network Access

Portal Policies





Authenticate before connecting to portal

- Use standard authentication like LDAP, SAML
- Enable MFA
- Enable email-based OTP
- Enable TOTP

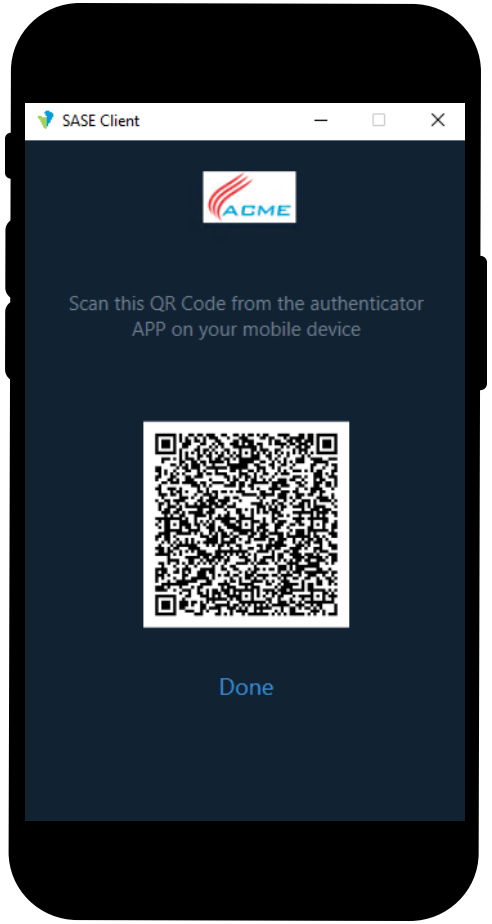
Check device status

- Check device is complaint
- Check device is upgraded to latest OS software pack
- Check firewall service is enabled
- Check device is running antimalware software
- Check device is running anti-phishing software
- Check device is running correct browser software version
- Integrate with Microsoft intune

VERSA NETWORKS

Zero Trust Network Access

Gateway Policies



Authenticate before connecting to gateway

- Use authentication like LDAP, SAML
- Enable MFA
- Enable email-based OTP
- Enable TOTP

Check device status

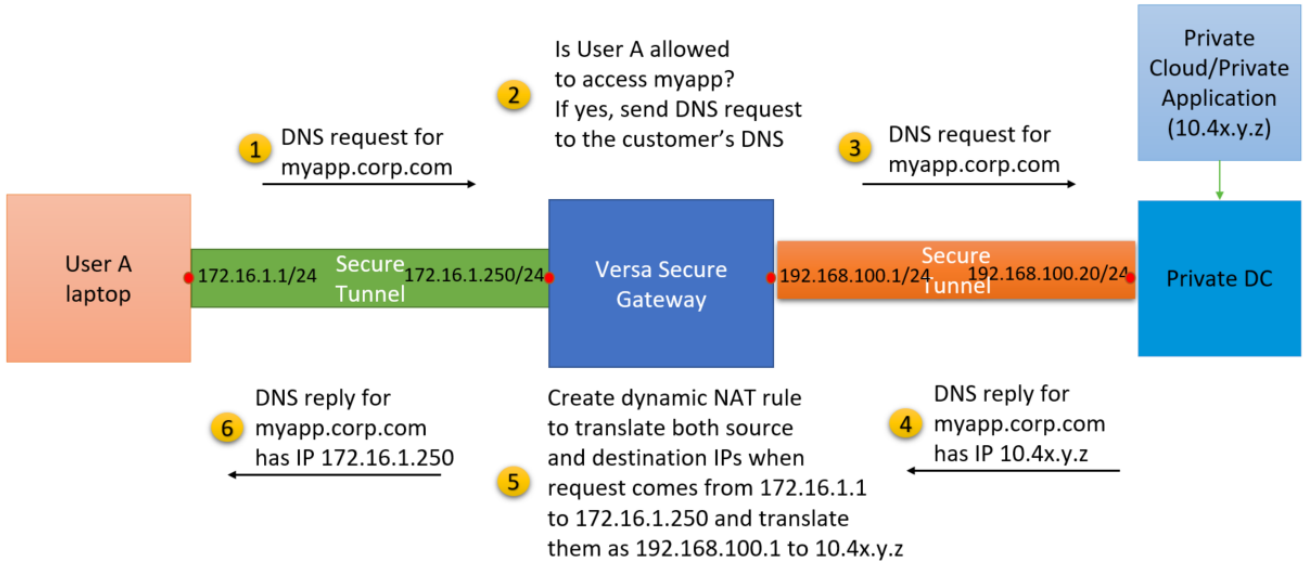
- Check device is complaint
- Check device is upgraded to latest OS software pack
- Check firewall service is enabled
- Check device is running anti-malware software
- Check device is running anti-phishing software
- Check device is running correct browser software version
- Integrate with Microsoft intune

VERSA NETWORKS

Zero Trust Network Access

Segmentation of Users

Versa SASE- Network Obfuscation Sequence



Assign different network for complaint and non compliant users

- Complaint users and non-complaint users does not share same network
- non-complaint user gets lesser privilege access compared to complaint user

Assign access to apps based on user roles

- Engineering users only get access to Engineering apps
- HR users only get access to HR apps

Network obfuscation

- Hide user from application
- Hide application from user

VERSA NETWORKS

Connectivity

Versa·ti·li·ty 2023

VERSA NETWORKS

Connecting SASE Fabric & Customer Private Networks

Connection Methods

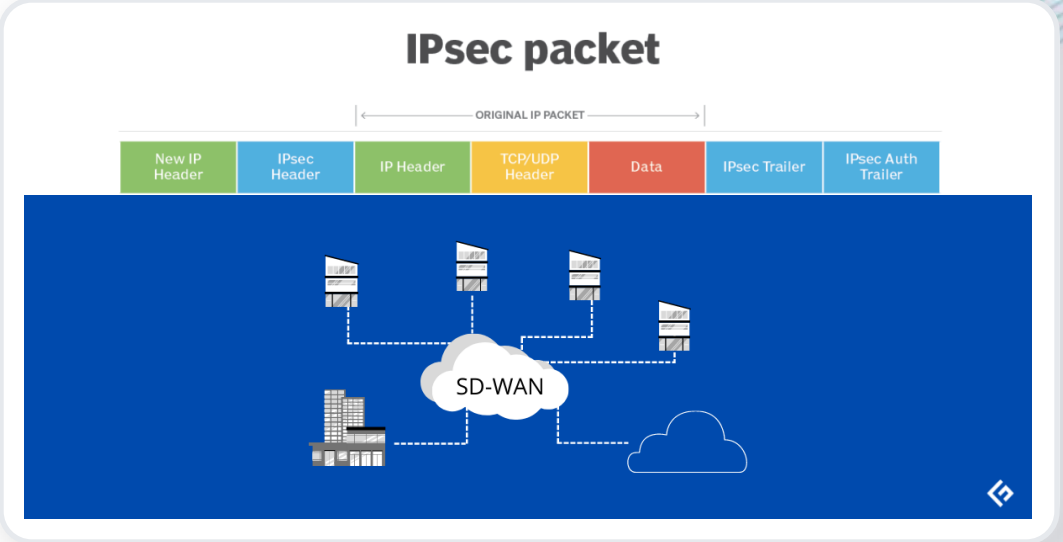
- Select the best option for your client
  - IPSEC
  - GRE
  - SD-WAN
- Routing between network segments
  - Static routing
  - BGP
  - BFD

Best Connectivity Options

- Site-to-site IPSec/Concentrator
  - Use strong encryption such as AES128/AES256
  - Use strong hashing – SHA256/SHA512
  - Avoid using MD5/3DES
- Open necessary ports:
  - UDP 500 for IKE Phase 1 (ISAKMP)
  - UDP 4500 for IKE phase 2

Use SD-WAN for best of all

- Benefits of SD-WAN:
  - Constant link monitoring
  - Traffic steering
  - Traffic conditioning (FEC/Replication)
  - Multiple paths
  - End-to-end monitoring



VERSA NETWORKS

Secure Web Gateway

Versa·ti·li·ty 2023

VERSA NETWORKS

Connecting Users to Applications in Secure Ways

Secure Web Gateway for SASE Clients and Office Protection

- Use protection methods based on customer requirements
  - Application Control
  - URL Filtering
  - IP Filtering
  - DNS Filtering
  - File Filtering
- Network Obfuscation
  - Antivirus
  - IPS/IDS
- TLS Security
  - SSL Inspection
  - SSL Decryption

Application Control

- Ability to recognize & control traffic for over 2800+ applications
- Policy Triggers
  - Applications
  - Application Groups
  - Application Filters (Family/Subfamily)
- Triggers can be combined with other match conditions
- Actions
  - Allow, Deny, Reject, QoS, Log
  - Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability, Anti-Virus)
- Available for all policy types

User /Group Control

- Authentication Support
  - Active Directory
  - LDAP
  - SAML
  - Local Database
- Policy Triggers
  - User
  - Group
- Triggers can be combined with other match conditions (and, or) actions
  - Allow, Deny, Reject, Log
  - Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability, Anti-Virus)
- Available for all policy types

IP Reputation & Filtering

- Geo Location
  - IP Address database spanning multiple countries
  - Enforce actions based on Geo Location
  - Match based on Source IP, Destination IP or combination of both
- IP Reputation
  - Protection against 12 million + malicious IP Addresses
  - Both IPv4 and IPv6 Addresses
  - Supports user-defined black & white lists
  - Updates in near real time
  - Match based on Source IP, Destination IP or combination of both
  - Threat types include:
    - Windows Exploits, Web Attacks, Phishing, Botnets, DoS, Scanners, Anonymizers, Spam Sources & Mobile Threats
- Automatic Geo & IP Reputation Updates via Versa Security Package

URL Reputation &Filtering

- URL Classification
  - 460+ million domains and 13+ billion URLs scored & classified
- 83 predefined categories, custom & Cloud app category support
- Supports user-defined black & white lists
- Web reputation
- Real-time Cloud lookups of URL categories & URL reputation
- Policy triggers
  - URL, URL category
- Triggers can be combined with other match conditions (and, or)
- Actions
  - Allow, Deny, Reject, Log, QoS
  - Block, Inform, Ask, Justify, Override
  - Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability, Anti-Virus)
- Available for all policy types
  - Access, QoS, PBF, Monitoring, Authentication, Decryption, SD-WAN
- Automatic URL category updates via Versa Security Package
- Works better with SSL/TLS Decryption

DNS Reputation & Filtering

- DNS-based protection & access control
  - Policy triggers from DNS query data
  - Combined with Zones, IP Addresses, Geo-Location, User/Group, Category, Reputation
  - Supports user-defined allow & deny lists
  - Actions include Allow, Deny, Reject, Log, QoS
- Global DNS Intelligence for zero-day threats
  - Passive DNS database
  - Block resolution of new domains until reputation is updated
  - Internal names, brand spoofing
    - Recognizes potentially suspect sites
    - DNS configuration errors
    - Provides enhanced phishing protection
- Integration with URL Category and IP Reputation Feeds

File Reputation & Filtering

- Signature-based file type identification
- Application, file type, direction & size-based filtering
- Reputation based filtering support
- Supports user-defined black & white lists
- File transfer detection on HTTP, FTP, SMTP, POP3, IMAP, MAPI
- Automatic file type updates via Versa Security Package

Anti-Virus

- Multi-layered detection
  - Heuristics
  - Emulation
  - Signatures
- Detection on HTTP, FTP, SMTP, POP3, IMAP, MAPI
- Cloud detection integration
- Automatic engine & signature updates via Versa Security Package

IDS/IPS

- Signature-based & anomaly-based detection/prevention
- Extensive coverage over the last 10 years
- Vulnerability signatures & anomaly detection engine
  - Provides real-time protection
- Additional coverage for vulnerabilities disclosed
  - Part of Microsoft Tuesday
- Support for PCN/SCADA signatures (modbus, dnp3)
- Support for Snort rule format
- Support for custom/user-defined vulnerability signatures
- Automatic signatures updates via Versa Security Package

SSL Inspection

- Security Checks
  - Expired certificates
  - Untrusted issuers
  - Unsupported
    - Ciphers
    - Key Lengths
    - Versions
  - Restrict certificate extensions
- Actions
  - Allow, Deny, Reject, Alert (allow & log)

SSL Decryption

- End-to-end SSL security
  - Decrypt
  - Inspect
  - Encrypt
- Traffic Visibility
  - Decrypt outbound & inbound SSL traffic transparently
  - Inspect the decrypted traffic for threats
  - Re-encrypt to both client & server
- Decrypt policy based on IP/Zone, User/Group, URL host, or URL host category

CLOUD ACCESS SECURITY BROKER (CASB)

1. Restrict Unauthorized Access
2. Identify Account Takeovers
3. Uncover Shadow IT
4. Cloud Data Loss Prevention
5. Internal and External Data Access Controls
6. Record Audit Trail of Risky Behavior
7. Cloud Phishing and Malware Threats
8. Continuous Monitoring for New Cloud Risks

VERSA NETWORKS

WHAT IS DATA LOSS PREVENTION?

Data loss prevention is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data

Types of DLP

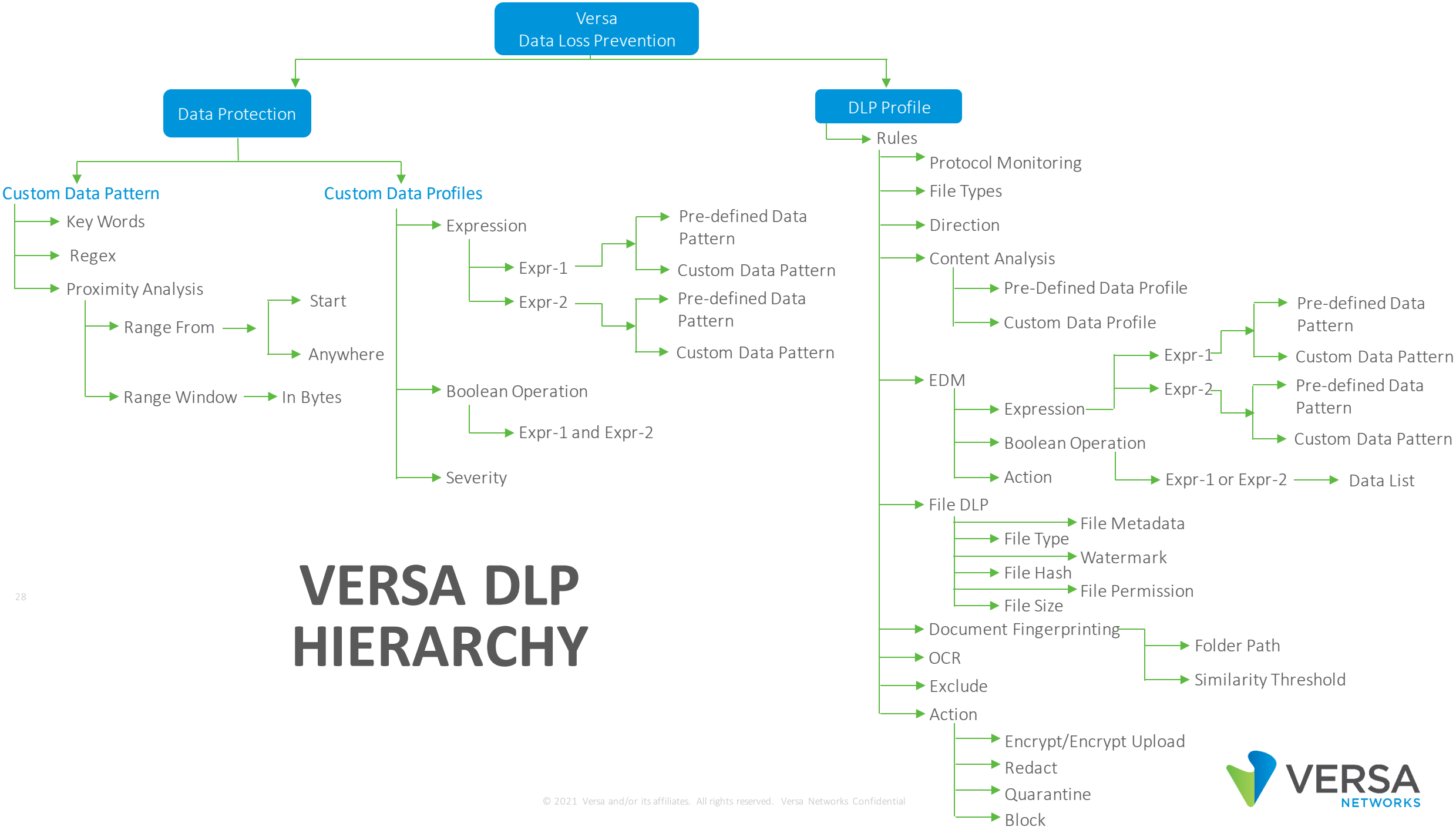
Network DLP Storage DLP Endpoint DLP Cloud DLP

VERSA NETWORKS

SUBSET OF VERSA DLP CAPABILITIES

1. Context Analysis
   - Protocol Monitoring
   - Endpoint Device ID Monitoring
   - AppID-based filtering
   - Endpoint location/IP address
   - Identity
2. File based DLP
   - File-type
   - File-size
   - File-name
   - File metadata
3. Content analysis (Header, body and payload)
   - Regex match
   - Keyword match
4. Predefined Data Identifiers:
   - Personal, Financial, Healthcare, and many more…
5. Predefined Data Profiles:
   - PCI-DSS, US HIPAA, US PII, US GLBA, US Financial, GDPR, and many more…
6. Custom Defined Identifiers and Data Profiles
7. Document Finger Printing
8. Microsoft Information Protection
9. Document checksum
10. Watermark validation
11. OCR
12. Document signature
13. Image classification
14. Document tagging

VERSA NETWORKS



VERSA DLP HIERARCHY

VERSA NETWORKS

Anomalies in the Network

Versa·ti·li·ty 2023

VERSA NETWORKS

Find Anomalies in the Network

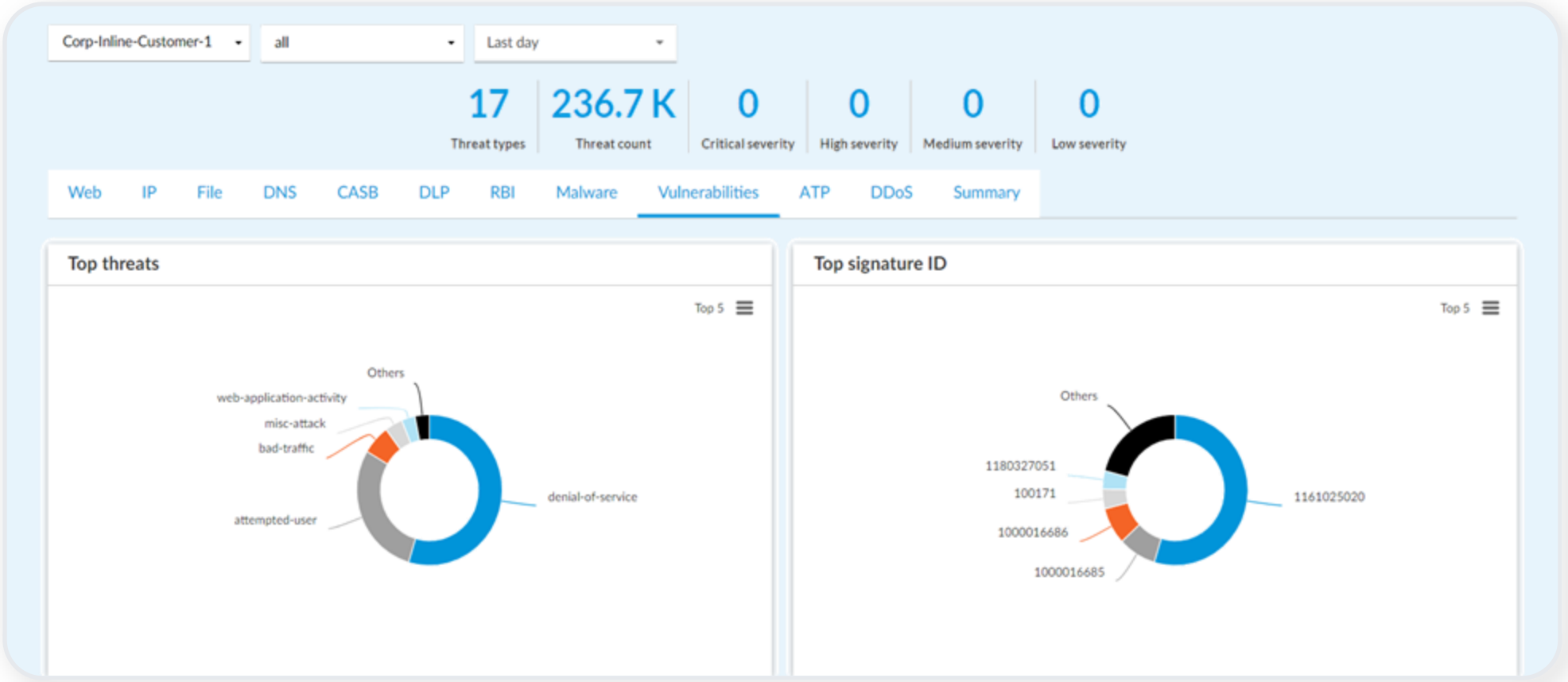
Find Bad Actors in the Network

- Find users accessing sites or resources with vulnerabilities
- Find users accessing sites or resources which has malware
- Find users accessing restricted sites or apps
- Find users leaking sensitive information
- Find users over utilizing network and app resources

Find Anomalies in the Whole Network

Vulnerabilities

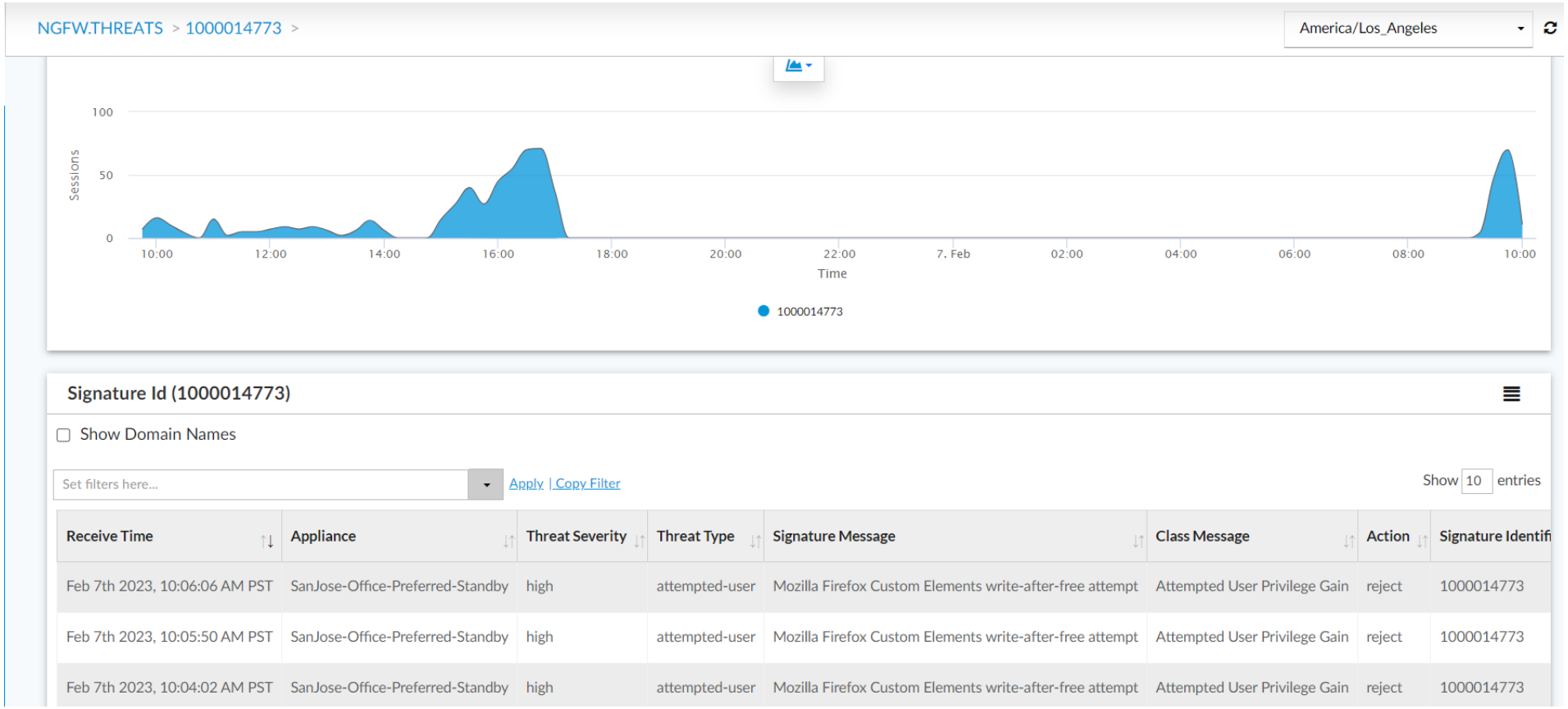
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Whole Network

Vulnerabilities Continued

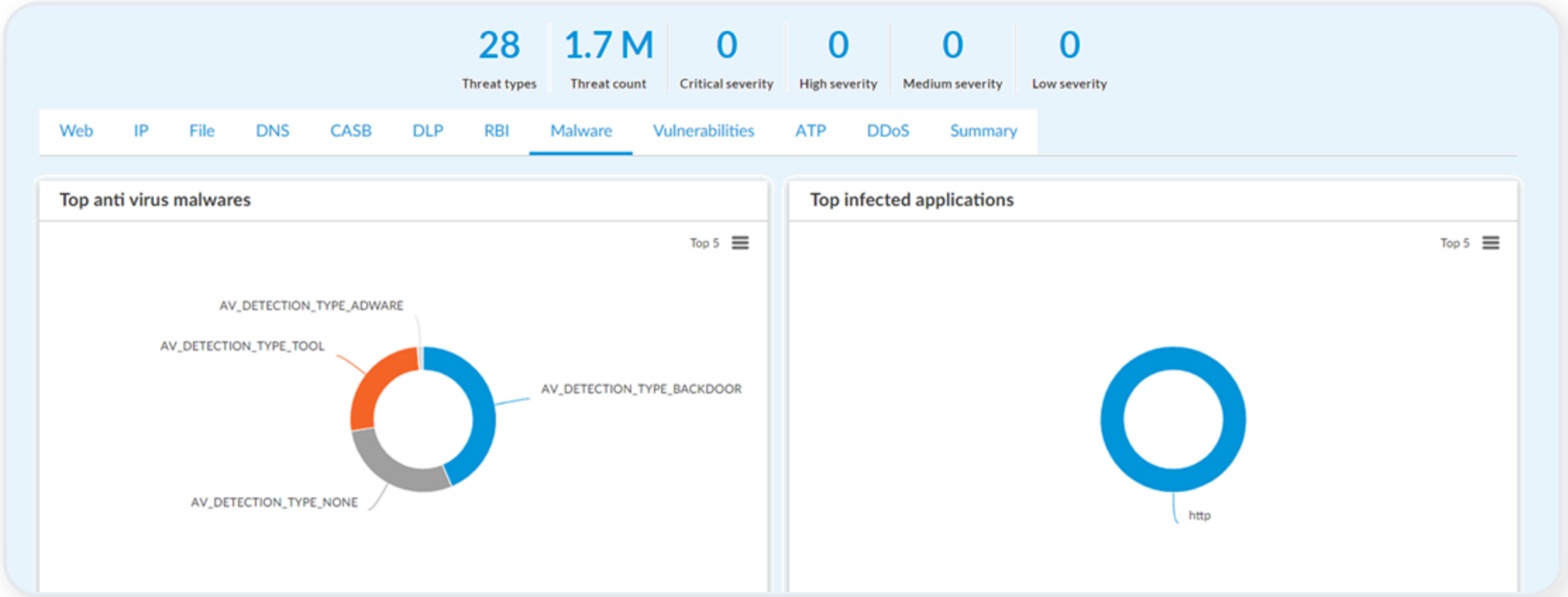
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Network

Malwares

- Find users accessing sites or resources which have malwares



Find Anomalies in the Network

Malwares Continued

- Find users accessing sites or resources which has malwares

Anti virus log (Bangalore-New-DC-Active)

Show Domain Names

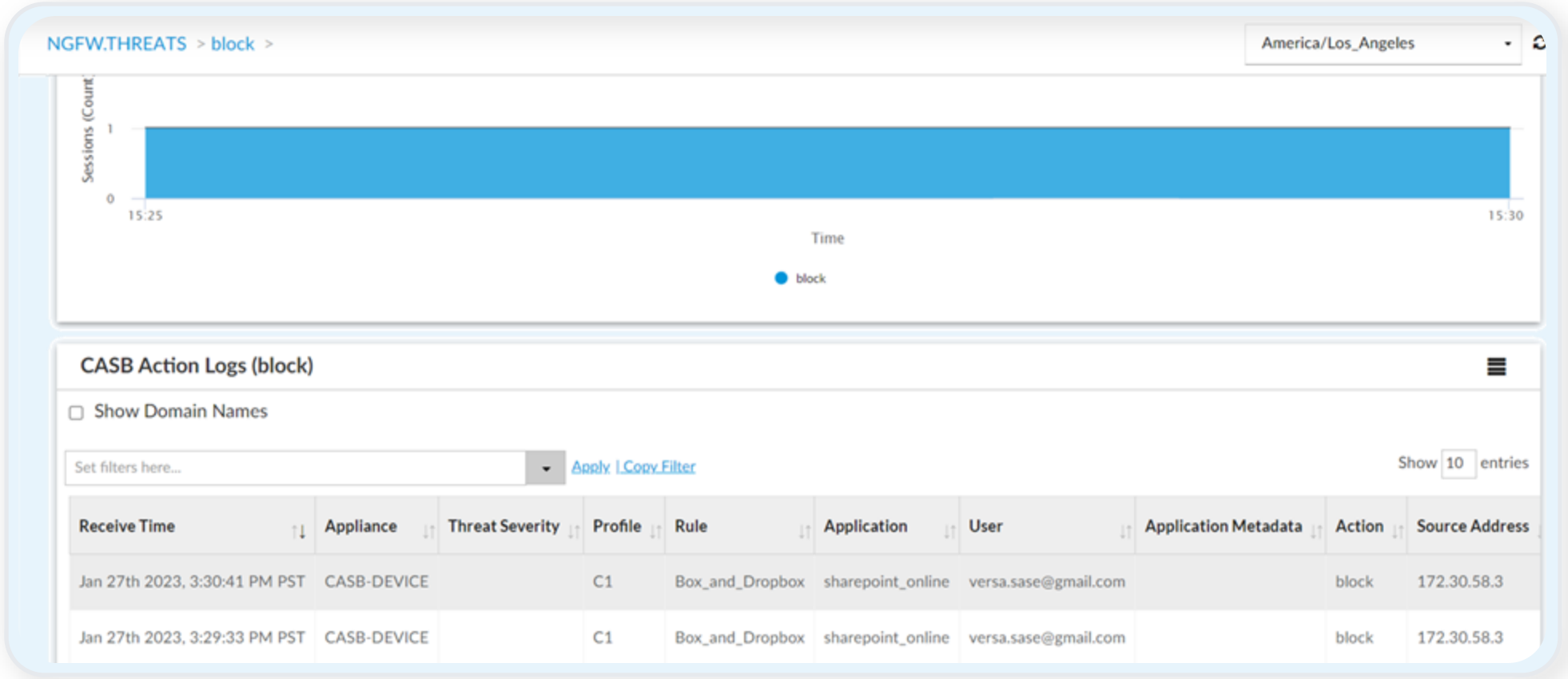
Set filters here... Apply | Copy Filter Show 10 entries

Receive Time	Appliance	Threat Severity	Malware Name	Malware Type	Application	User	Attacker	Victim	File Type	File Name
Jan 22nd 2023, 10:40:31 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:39:59 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:40:15 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:38:00 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 20th 2023, 6:08:52 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:8679e4648d480fa7fd5e
Jan 20th 2023, 6:01:40 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:8679e4648d480fa7fd5e
Jan 20th 2023, 6:01:34 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:582fb99abc61b81c30ff4
Jan 23rd 2023, 2:40:47 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.105.2	Unknown	sha256:582fb99abc61b81c30ff4
Jan 23rd 2023, 2:40:49 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.105.2	Unknown	sha256:8679e4648d480fa7fd5e

Find Anomalies in the Network

Restricted Apps or Sites

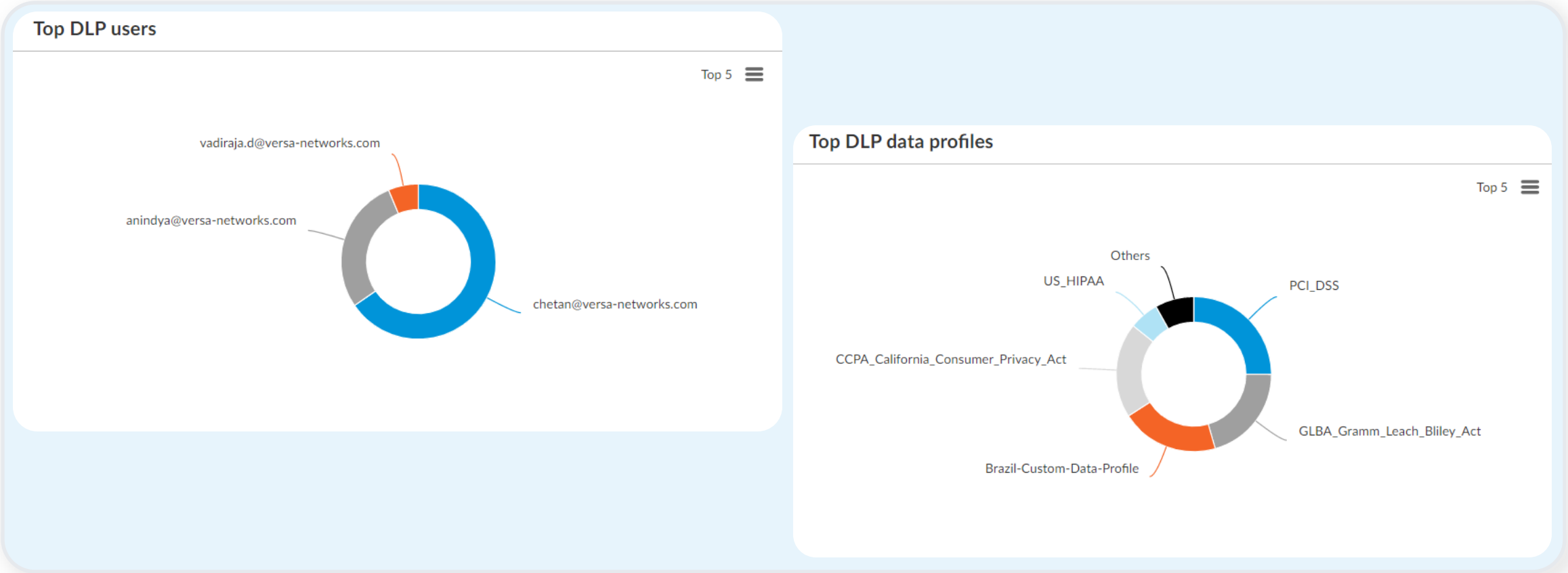
- Find users accessing restricted sites or apps



Find Anomalies in the Network

Leaking Sensitive Information

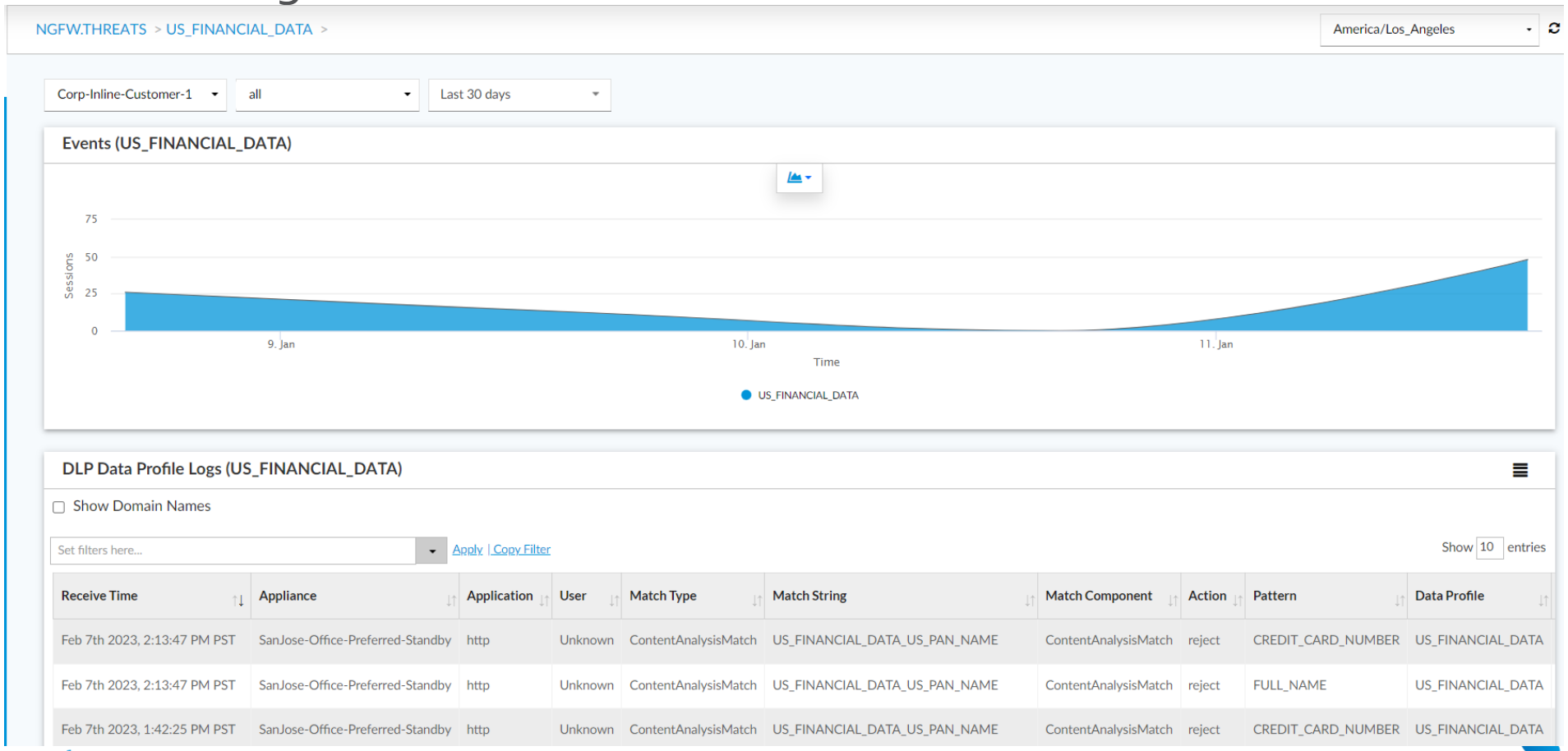
- Find users leaking sensitive information



Find Anomalies in the Network

Leaking Sensitive Information Continued

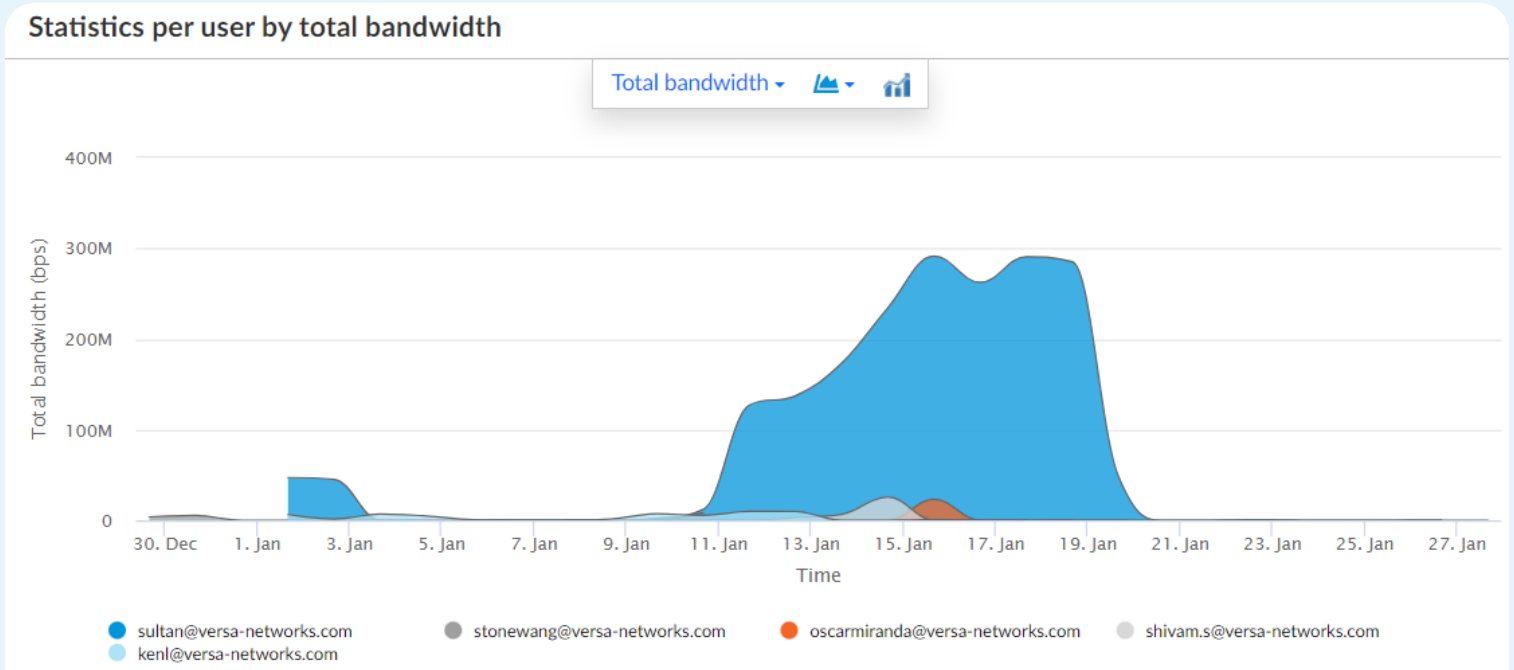
- Find users leaking sensitive information

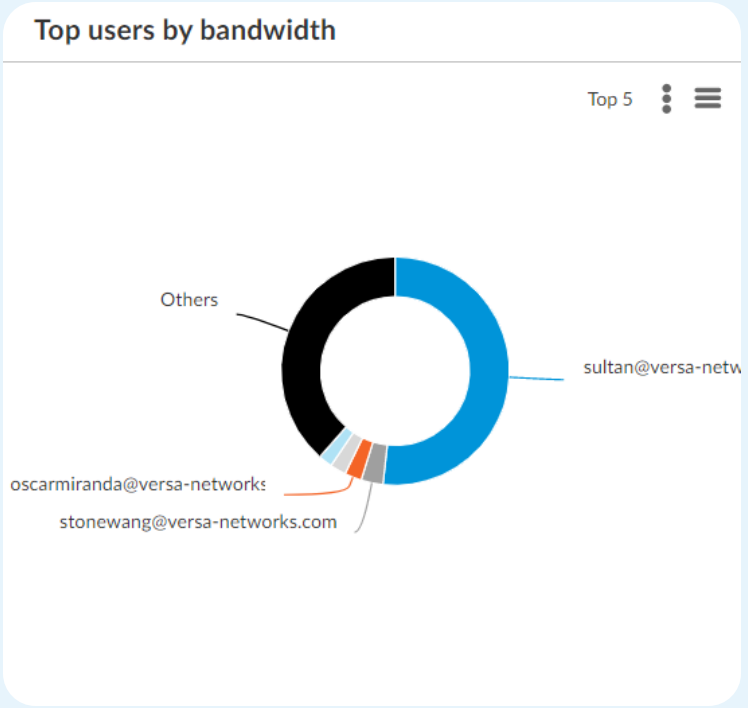


Find Anomalies in the Network

Over Utilizing Resources

- Find users over utilizing network bandwidth





Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

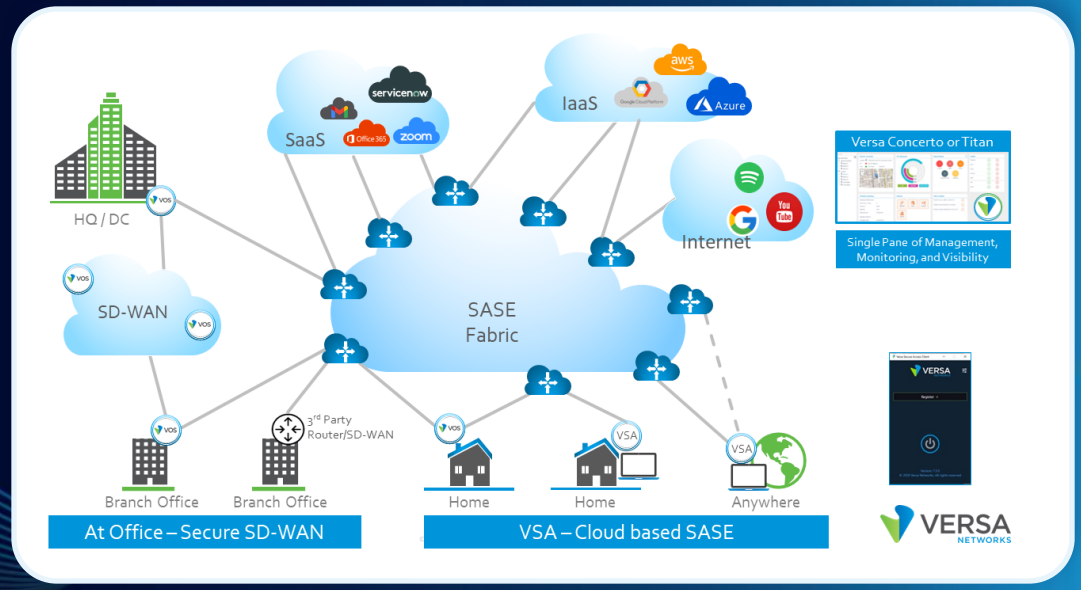
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

End-to-End Monitoring

- Monitor Customer End Device
- Monitor Customer LAN Network
- Monitor Transport Issues
- Monitor Application Performance
- Monitor Connectivity Between SASE & Customer Network
- Hop by Hop Monitoring



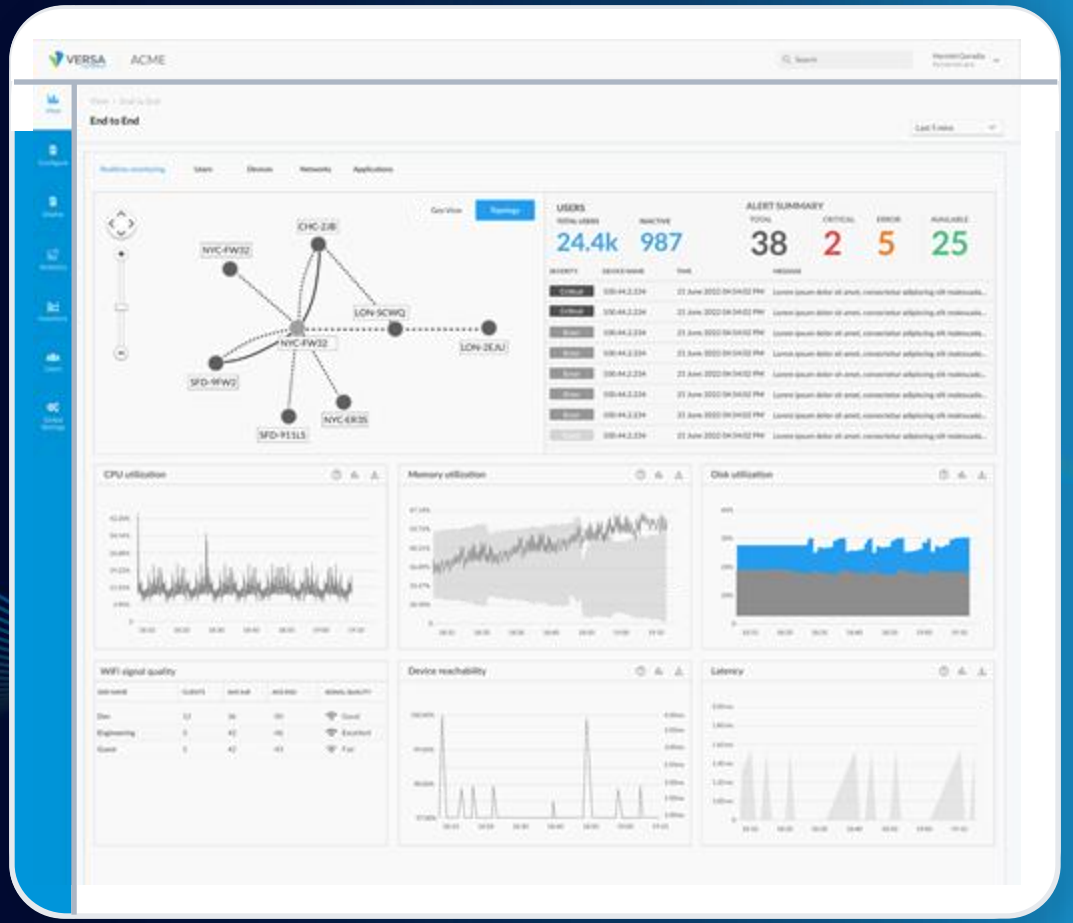
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

Monitor Customer End Device

- Monitor for High CPU
- Monitor for High Memory
- Monitor for High Disk I/O
- Monitor for Weak WiFi Signals
- Monitor for LTE Signal Strength
- Monitor for Unstable Nexthop Connectivity

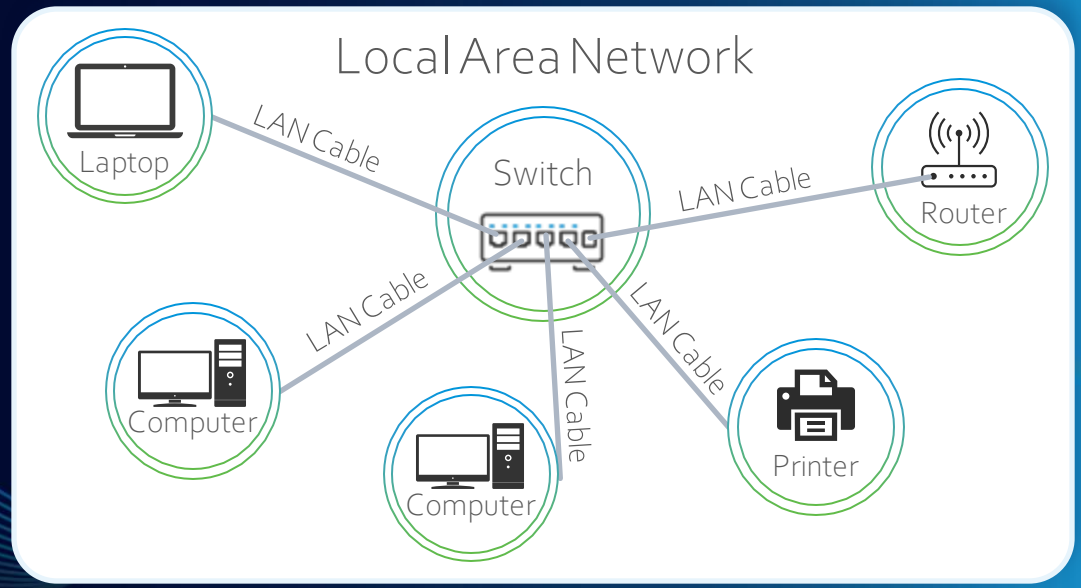


VERSA NETWORKS

SASE Monitoring

Monitor Customer LAN Network

- Monitor L2 Loops
- Monitor ARP Issues
  - ARP Flood, ARP Not Resolved, etc.
- Monitor for Routing Issues
  - Routing Missing, Route Loops
- Monitor for Duplicate IPS
- Monitor for Bandwidth Issues
- Monitor for Latency Issues
- Monitor for Duplicate DHCP Server Issues



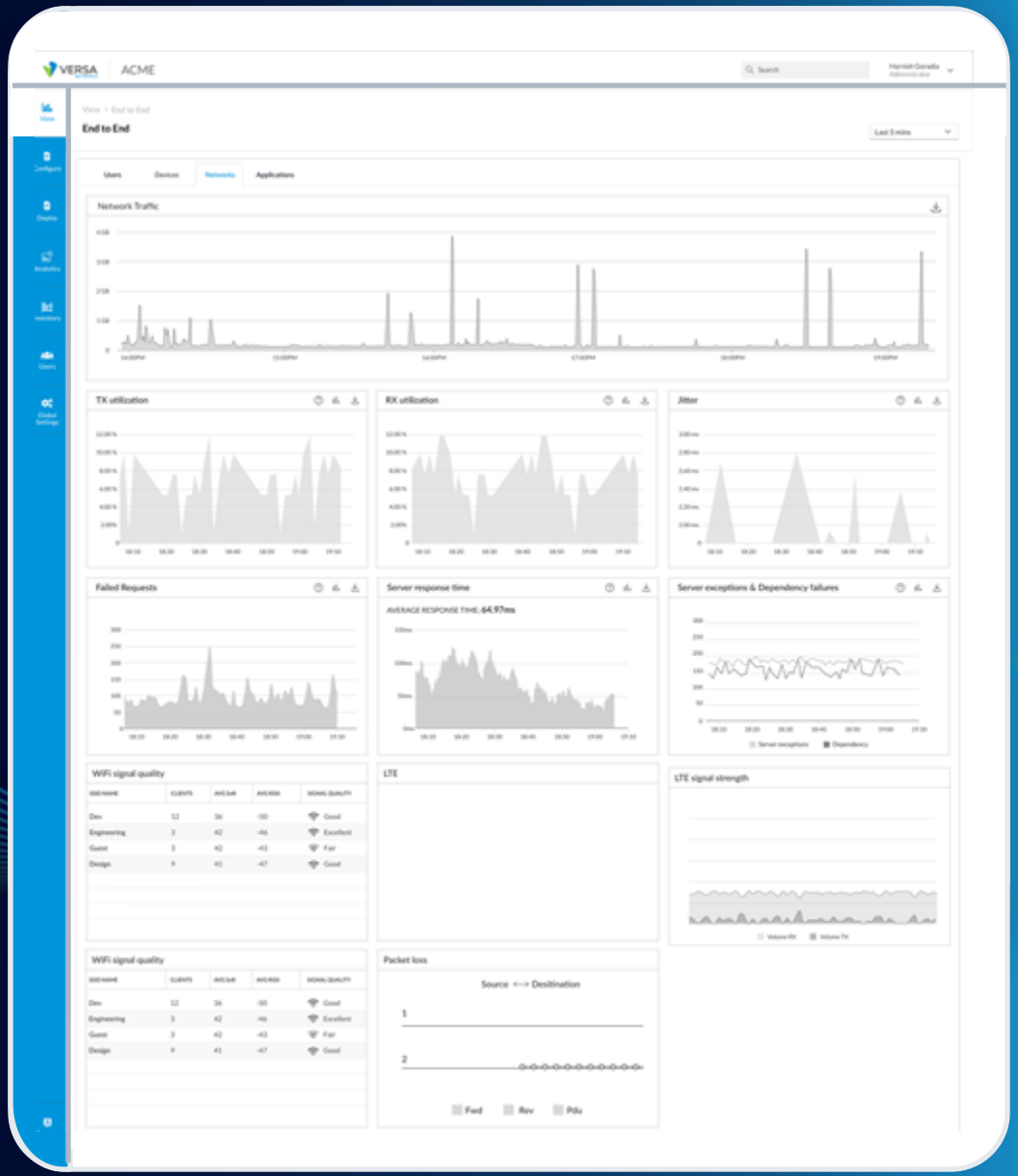
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

Monitor Transport Issues

- Monitor Packet Loss on Transport/WAN
- Monitor Latency and Jitter on Transport/WAN
- Monitor Bandwidth



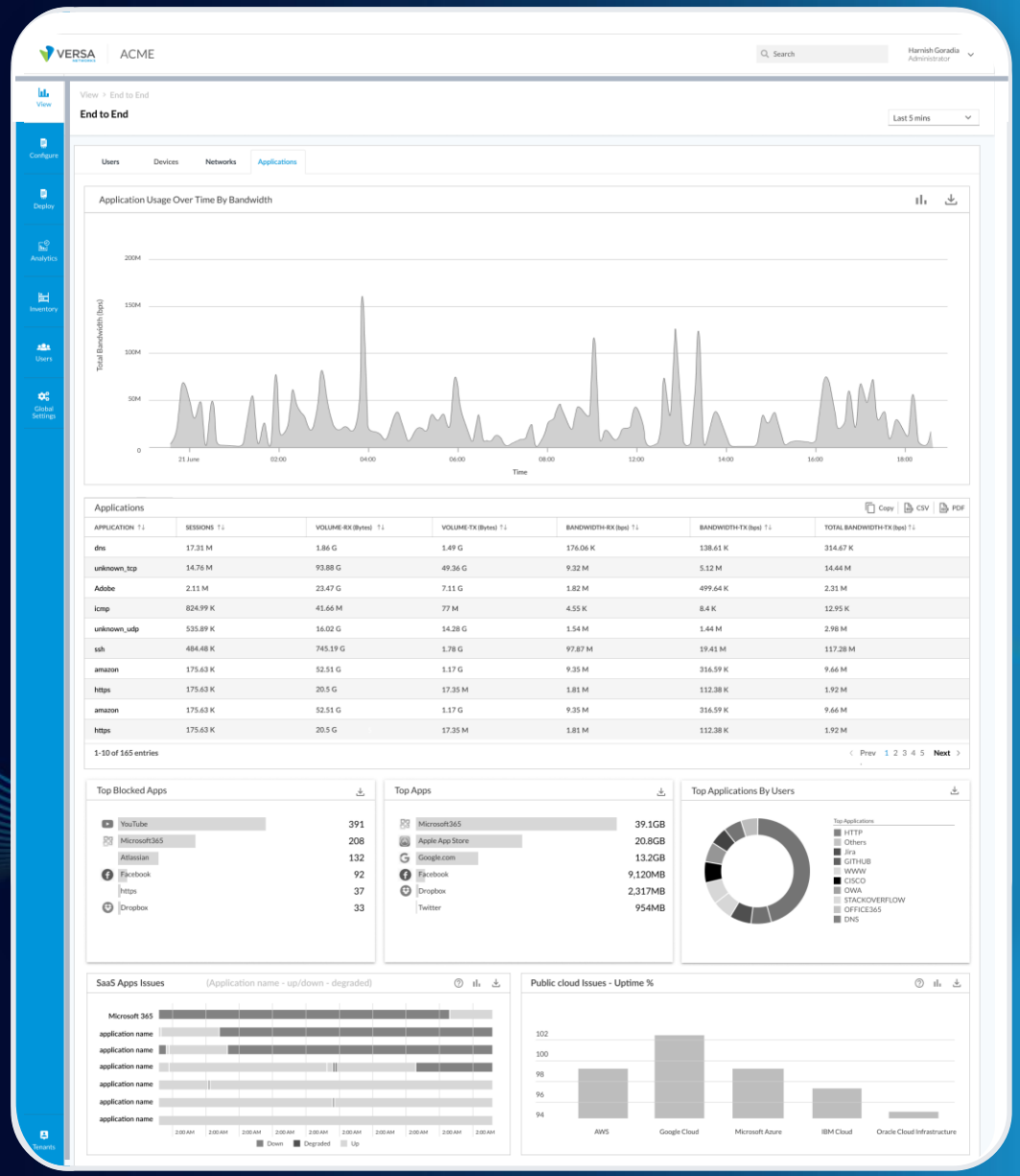
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

Monitor Application Performance

- Monitor Network Response Time
- Monitor Re-Transmissions
- Monitor Connections Aborted, Refused
- Monitor Passive Bandwidth Usage of Applications and Come Up With Score
- Monitor for Outages in SaaS Applications like Office365, Salesforce, etc.
- Monitor for Outages in Public Clouds like AWS, Azure, GCP, etc. based on where the user apps are located



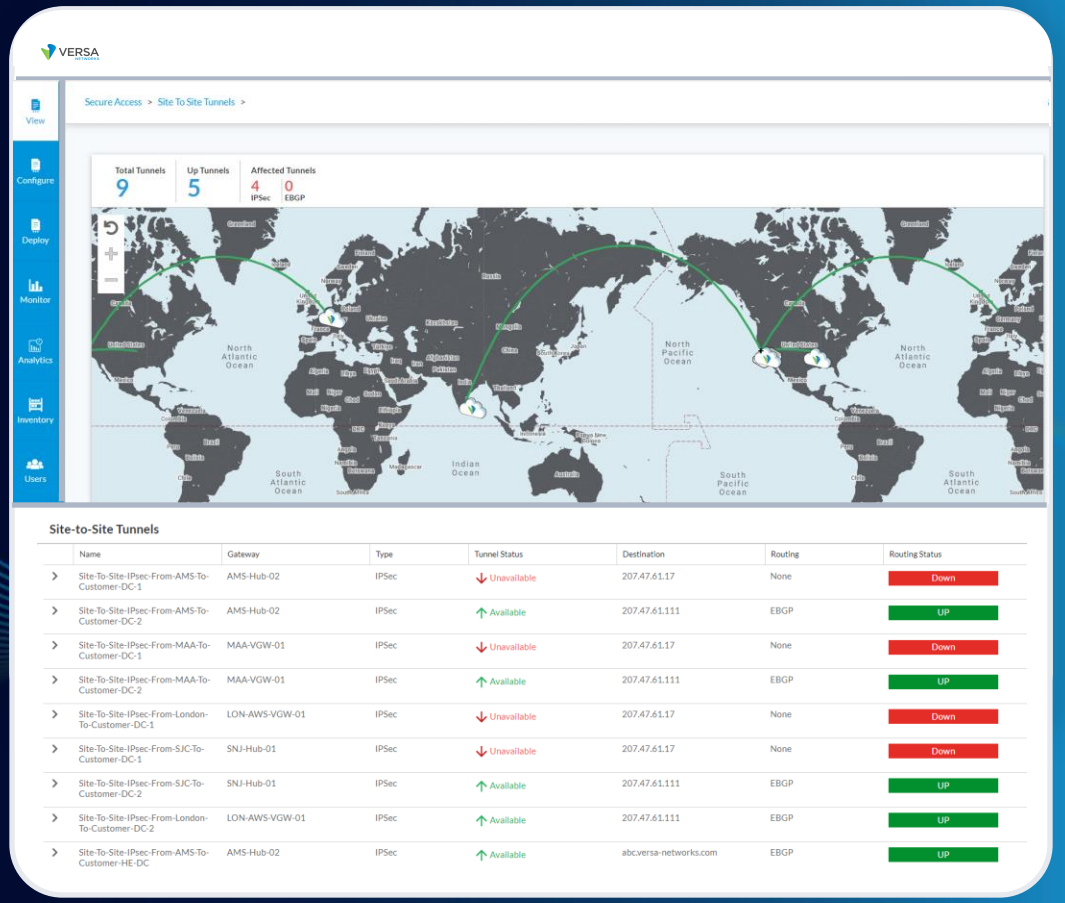
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

Monitor Connectivity between SASE & Customer Network

- Monitor IPsec/GRE/SD-WAN Tunnel
- Monitor Dynamic Routing Protocols within Tunnels



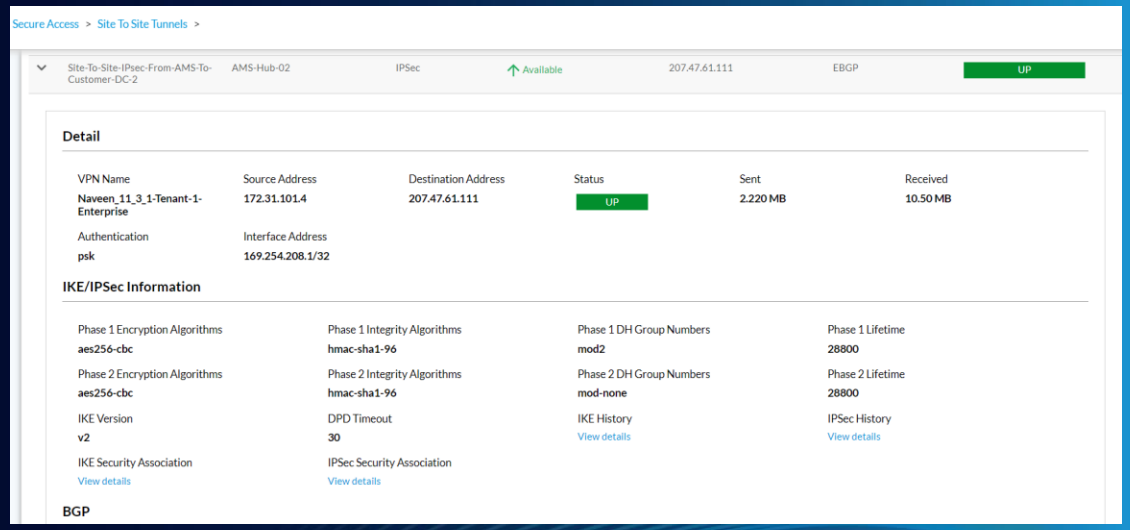
Versa·ti·li·ty 2023

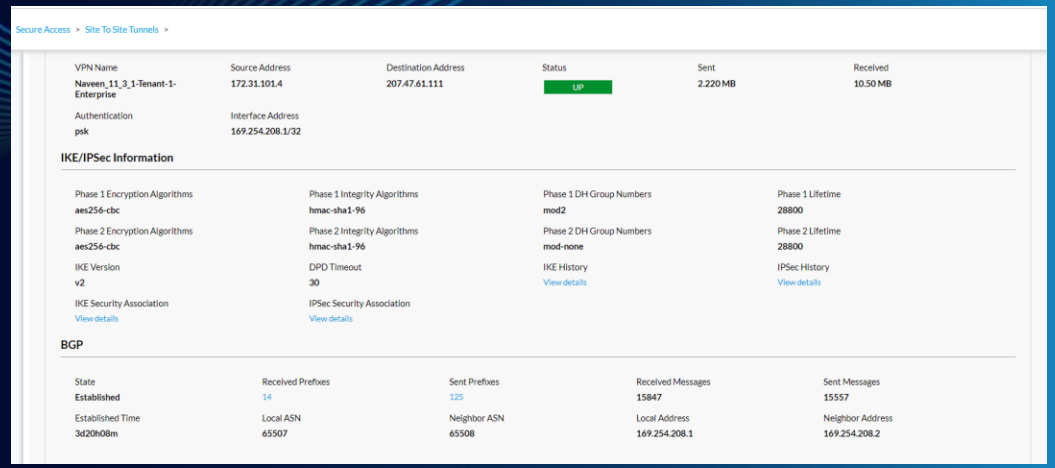
VERSA NETWORKS

SASE Monitoring

Monitor Connectivity between SASE & Customer Network Continued

- Monitor IPsec/GRE/SD-WAN Tunnel
- Monitor Dynamic Routing Protocols within Tunnels





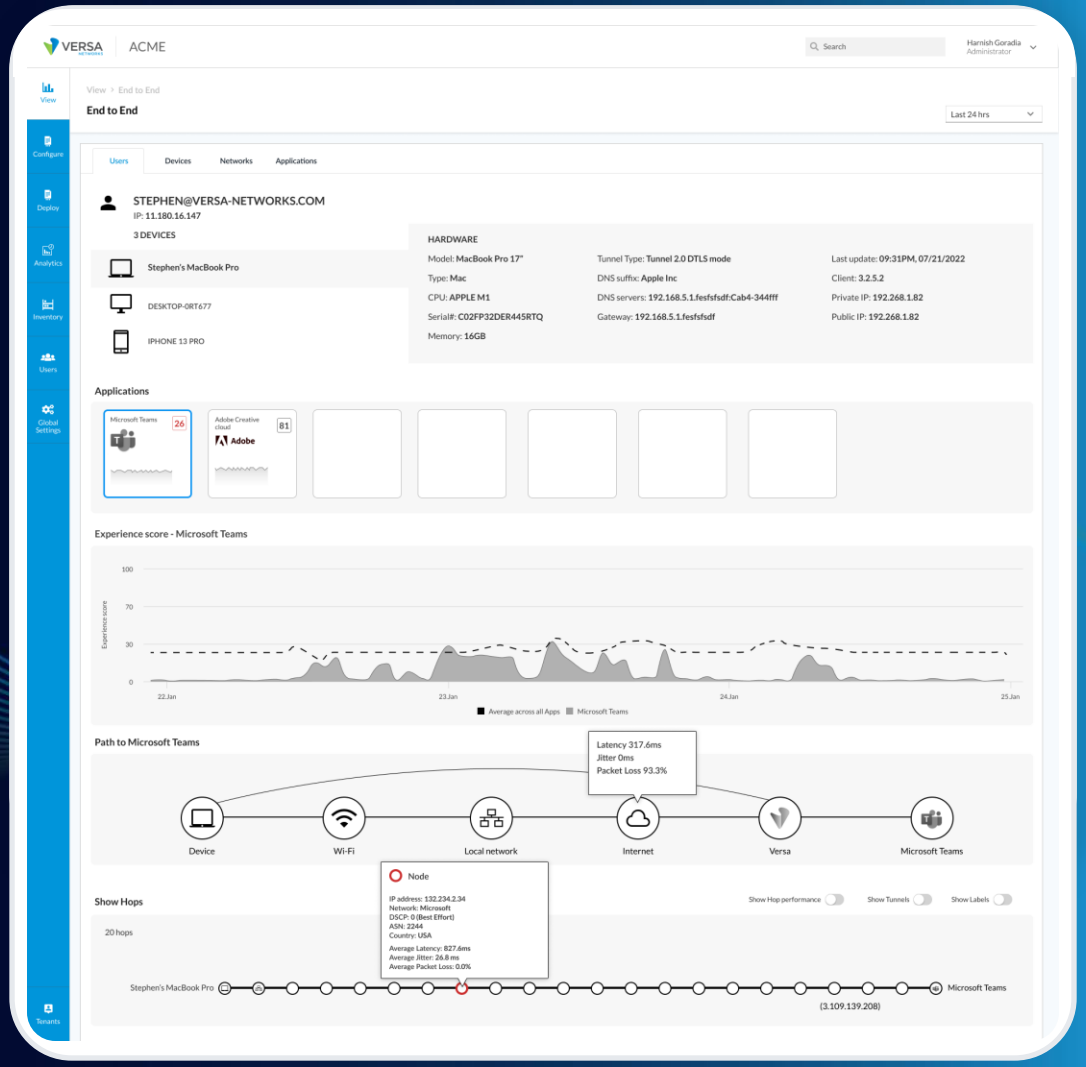
Versa·ti·li·ty 2023

VERSA NETWORKS

SASE Monitoring

Hop by Hop Monitoring

- Report latency for every network hop from user device to user app
- Report jitter for every network hop between user device to user app
- Monitor packet loss for every network hop between user device to user app



Versa·ti·li·ty 2023

VERSA NETWORKS

Questions

Versa·ti·li·ty 2023

VERSA NETWORKS

Thank you

Versa·ti·li·ty 2023

VERSA NETWORKS