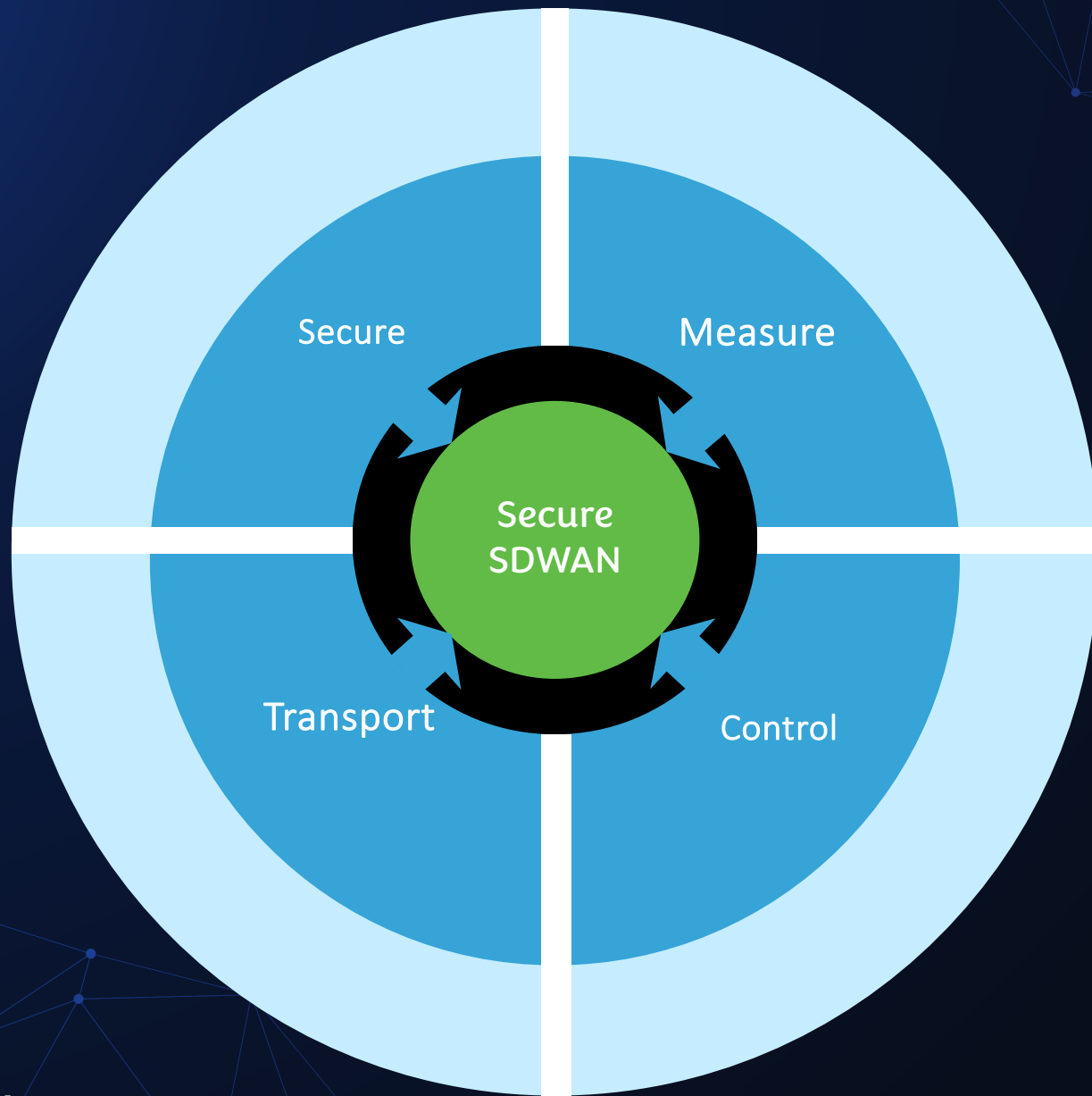


# Versatility 2024

## Transforming Connectivity

*Showcasing Our Latest Secure SD-WAN Enhancements*



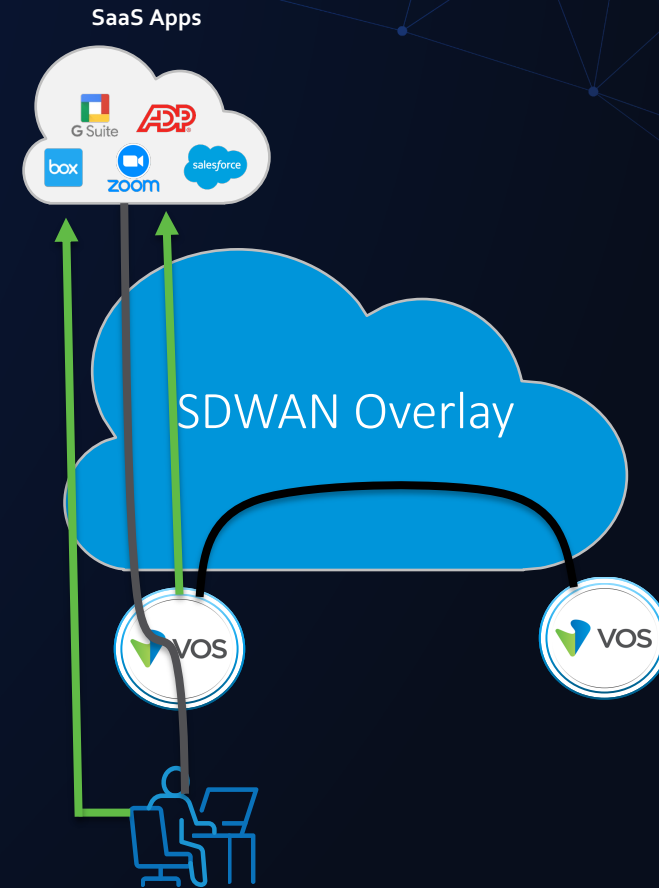
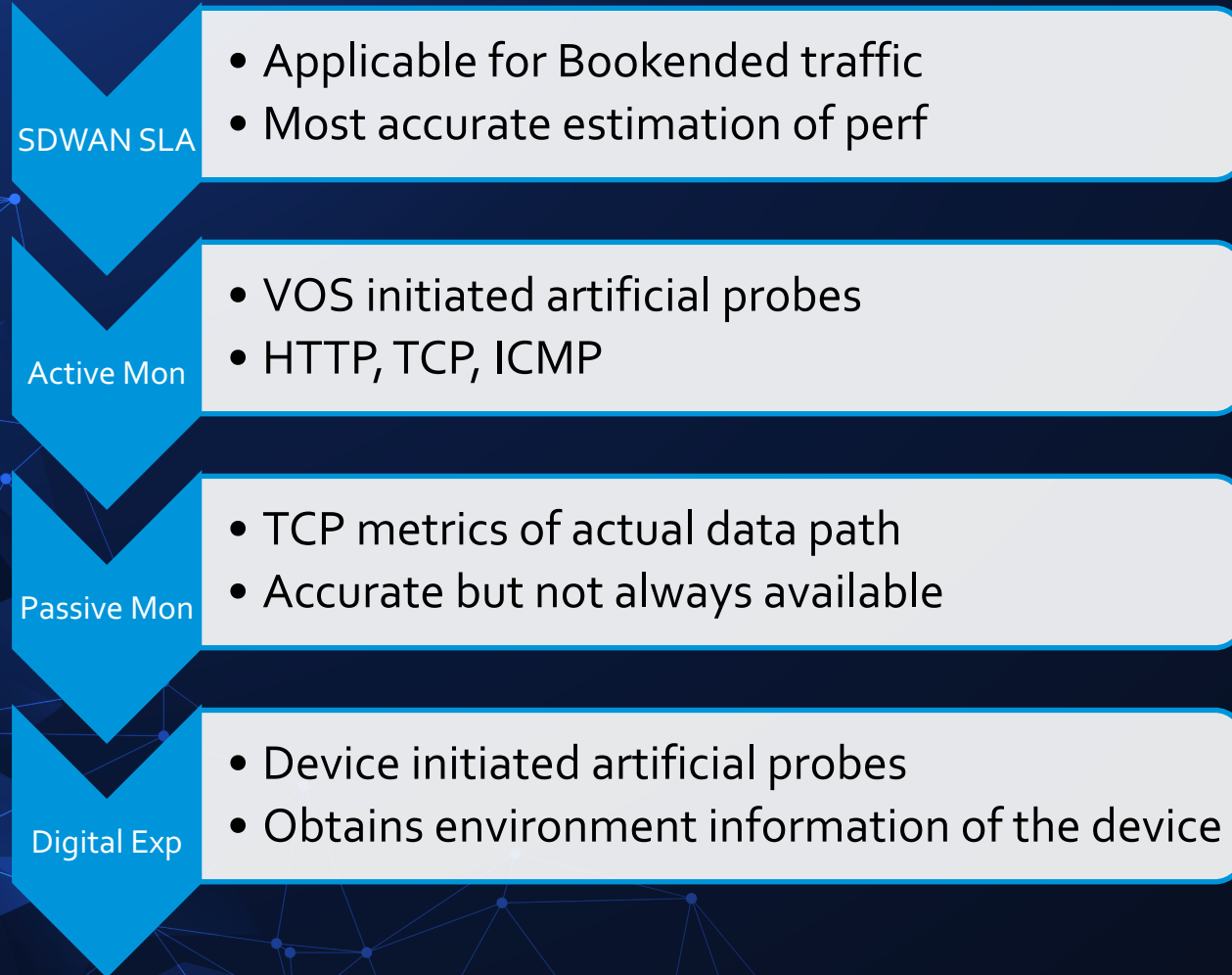


Versatility 2024

© 2024, Versa and/or its affiliates. All rights reserved. Versa Networks Confidential

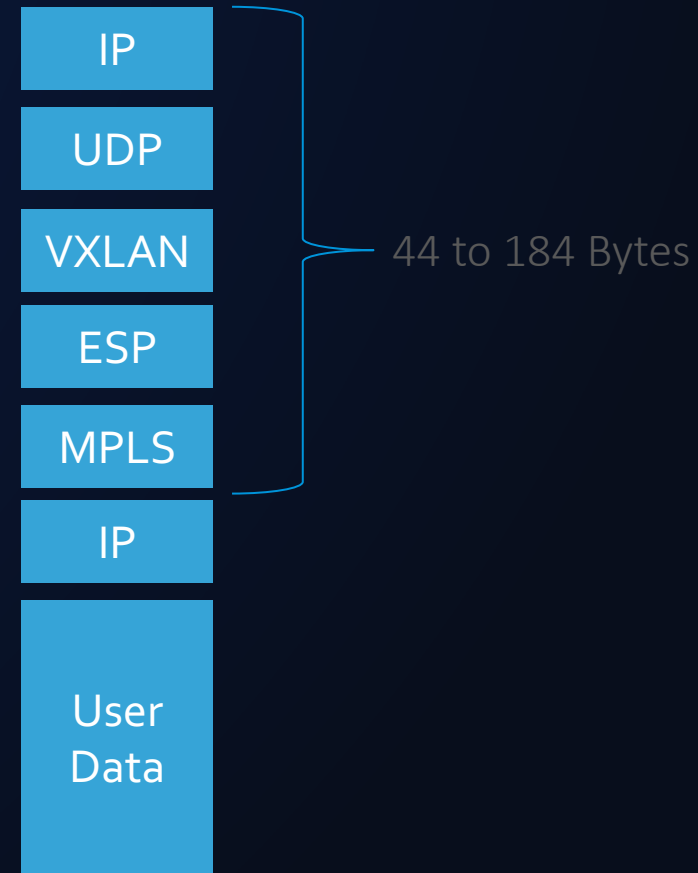


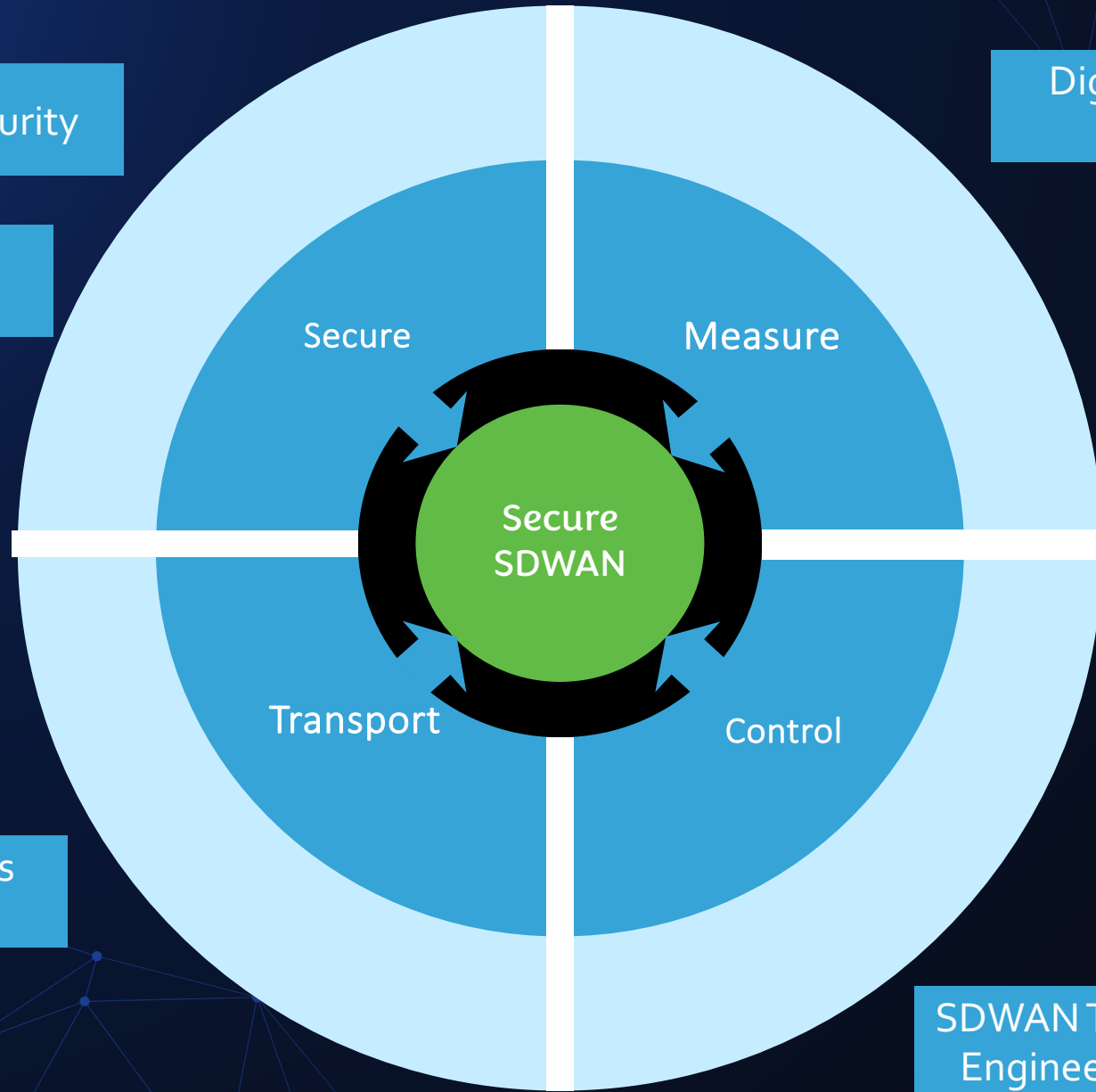
# Measure



# Transport

- SDWAN Header is used for creating a scalable overlay network
  - Secure Overlay using IPsec
  - Multiple Private Networks over single overlay
  - Link Diversity
  - Application and SLA based steering
  - Application Acceleration like FEC





IOT Security

On-prem ZTNA

Data Protection

Tunnel-less SDWAN

Digital Exp Mon

App Perf Monitoring

SDWAN Traffic Engineering

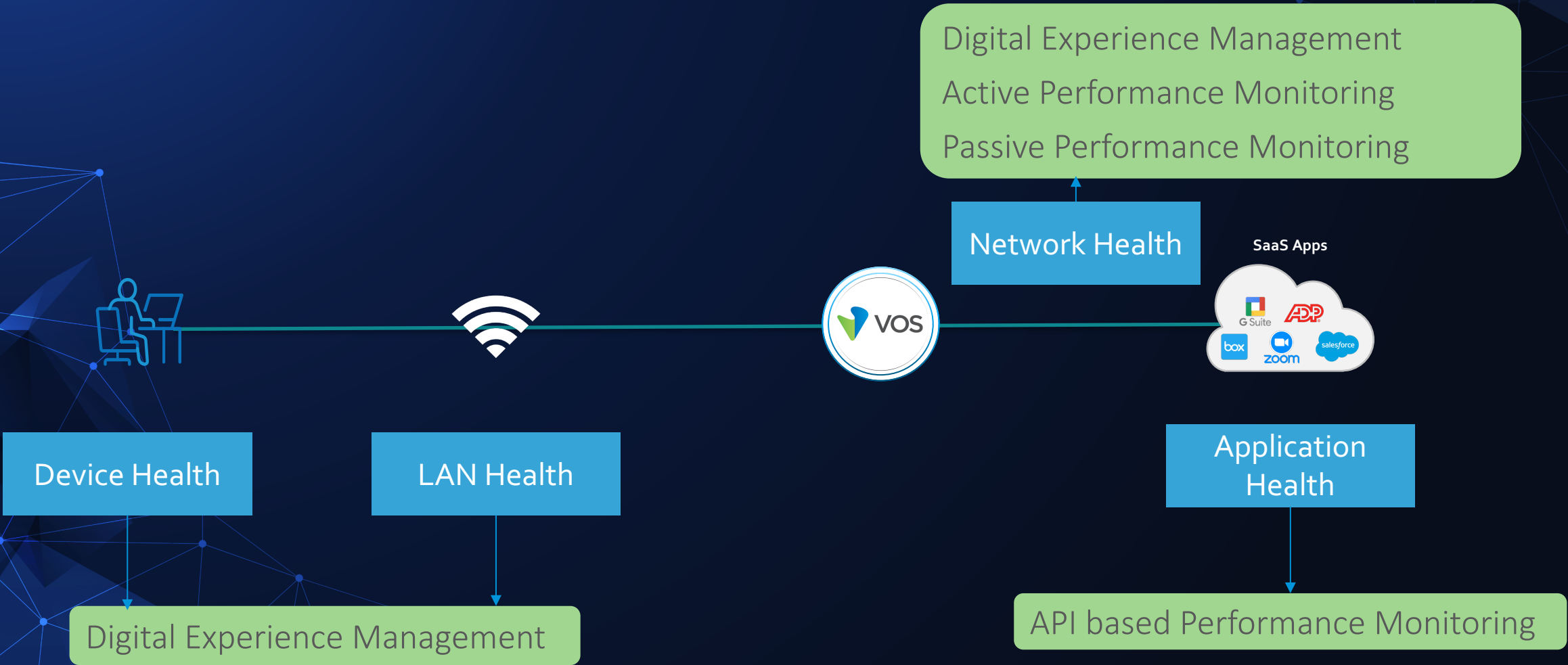
Versatility 2024



# Factors impacting User Experience



# Application Experience Monitoring Techniques



Versatility 2024

# Digital Experience Monitoring

## Measure

- Device Performance
- Network Performance
- SaaS App Performance

## Report

- Highlight actionable insights
- Provide granular and aggregate reports
- Historical reports for comparison

## Trace

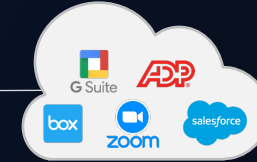
- Enable granular reporting for individual users
- Faster reporting for impacted users
- Proactively resolve issues

# DEM monitoring

- Loss/Jitter/RTT to Application
- Application Stats (Time to first byte etc)



SaaS Apps



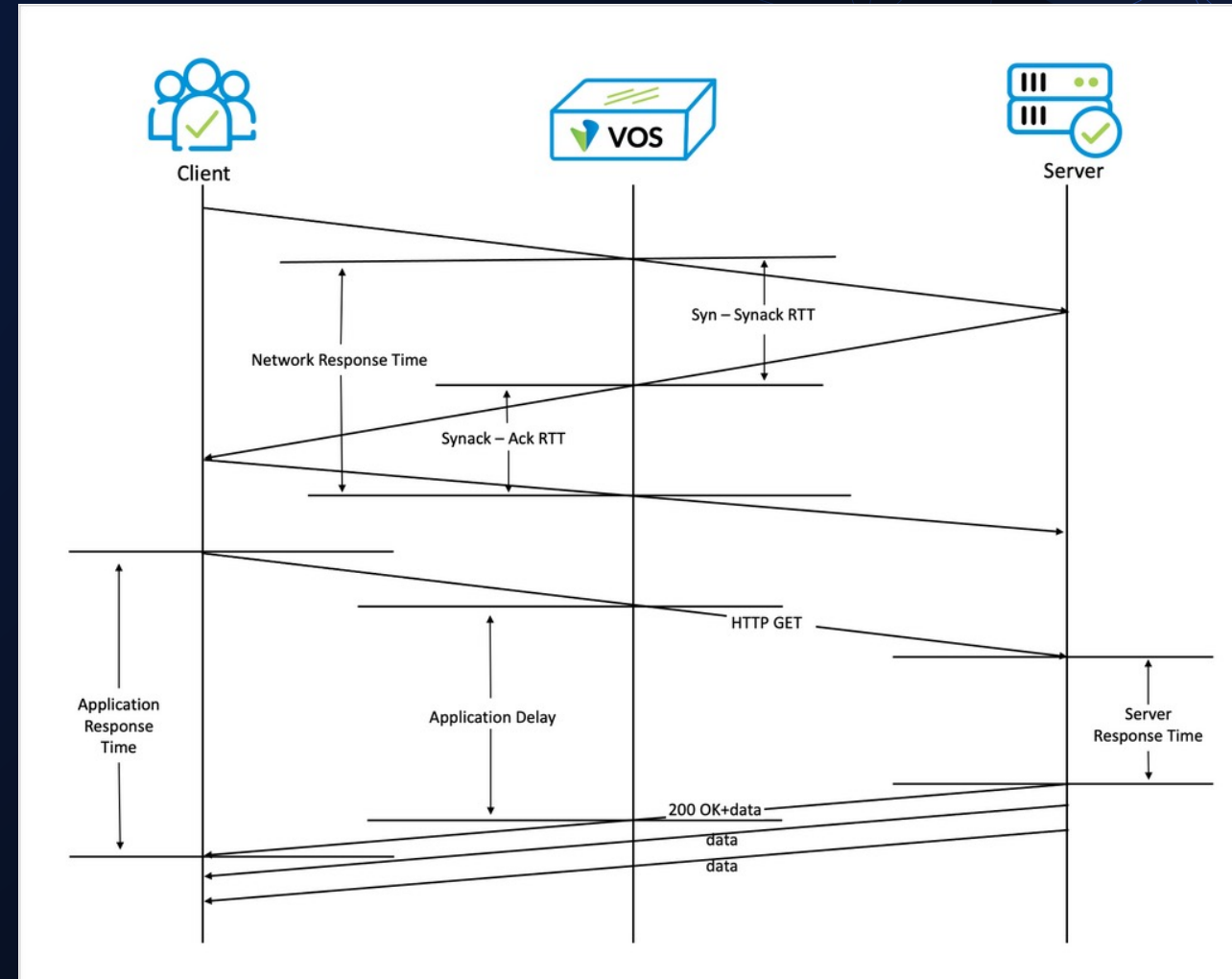
- CPU
- Memory
- Disk Queue

- SSID
- Signal Strength
- Loss/Jitter/RTT

Versatility 2024

# Active Application Performance Monitoring

- Passive measurement of TCP and HTTP traffic
- Close estimation of actual User Experience
- Important Metrics
  - Versa Link and Application Rank
  - Application and Server Response times
  - Network Response Times
  - TCP Retransmissions (Packet Loss)



## DEM

- **Benefits**
- Client Perspective of performance
- Faster troubleshooting due to device and local network information
- **Dis-advantages**
- Artificial Probes may distort performance
- Client resources are consumed

## Active APM

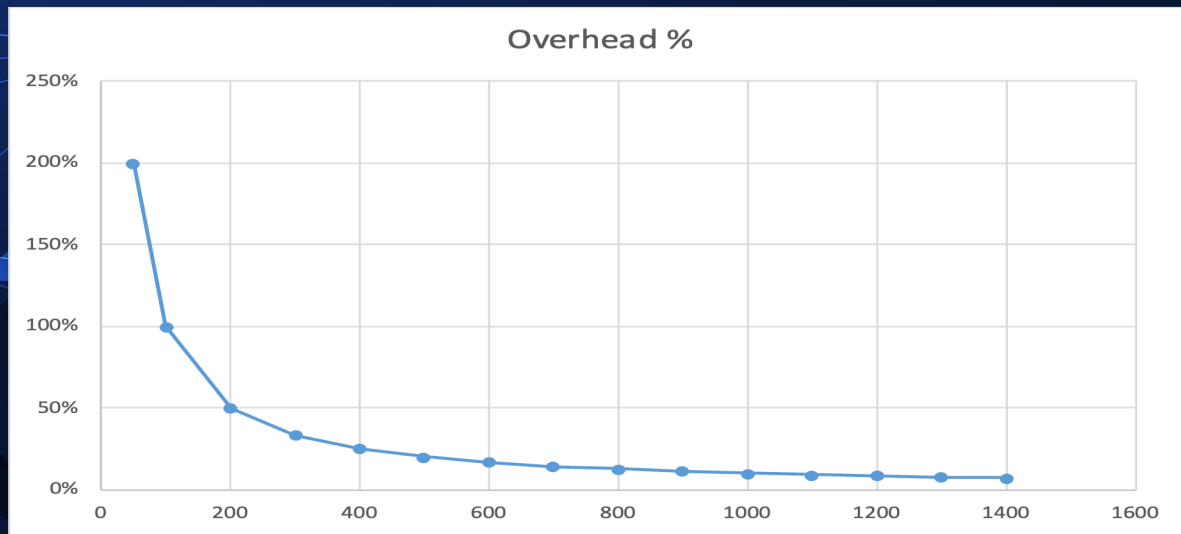
- **Benefits**
- Network Performance over individual links
- Always available
- **Dis-advantages**
- Slow detection of performance degradation

## Passive APM

- **Benefits**
- Performance as experienced by real traffic
- Fast response to degradation
- **Dis-advantages**
- Need active users

# When does SDWAN overhead matter?

Overhead as percentage of overall traffic

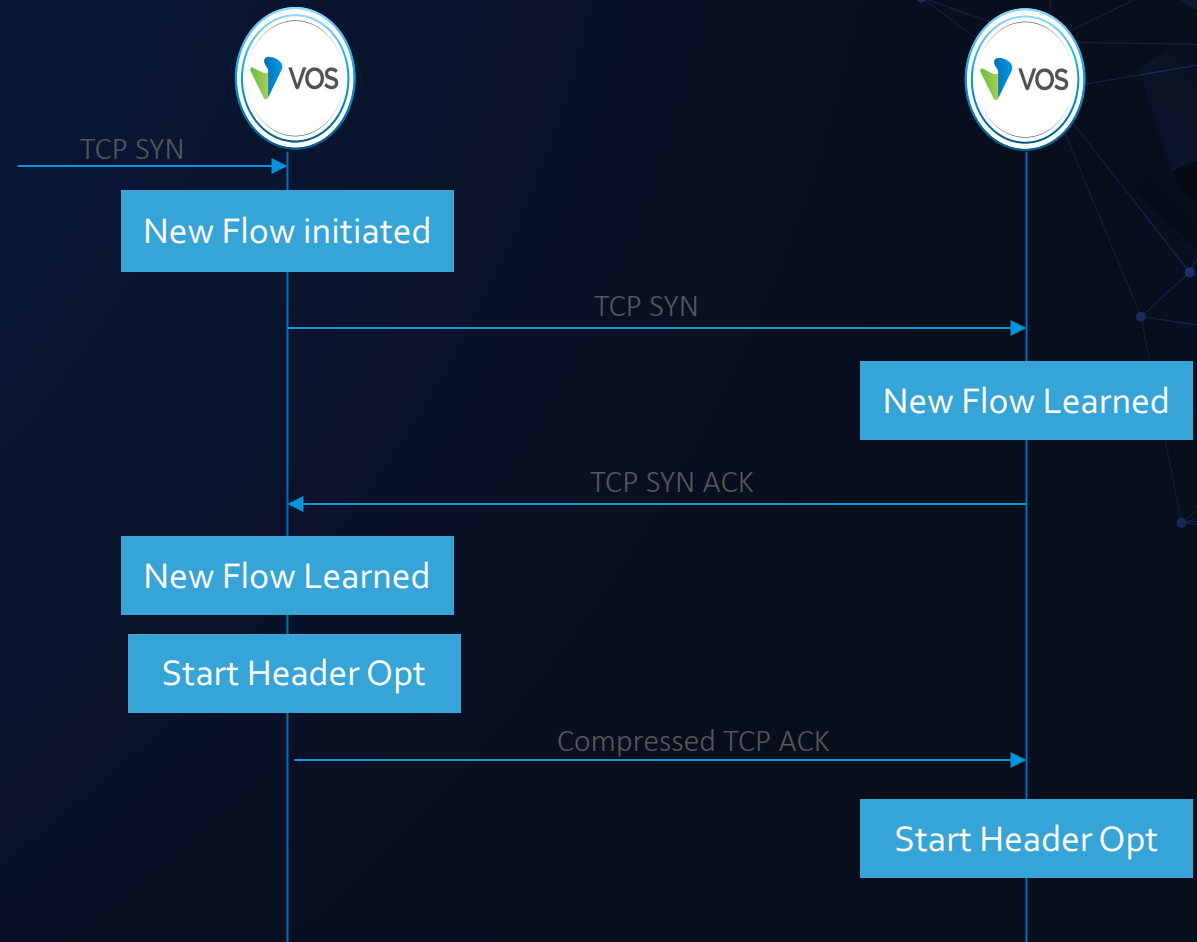


Price per Mbps



# Tunnel-less SDWAN

- Parts of SDWAN header is “constant” for a given flow
- For bookended traffic, source and destination learn “constant” headers
- Optimization is enabled once source and destination exchange capability



# Tunnel-less SDWAN

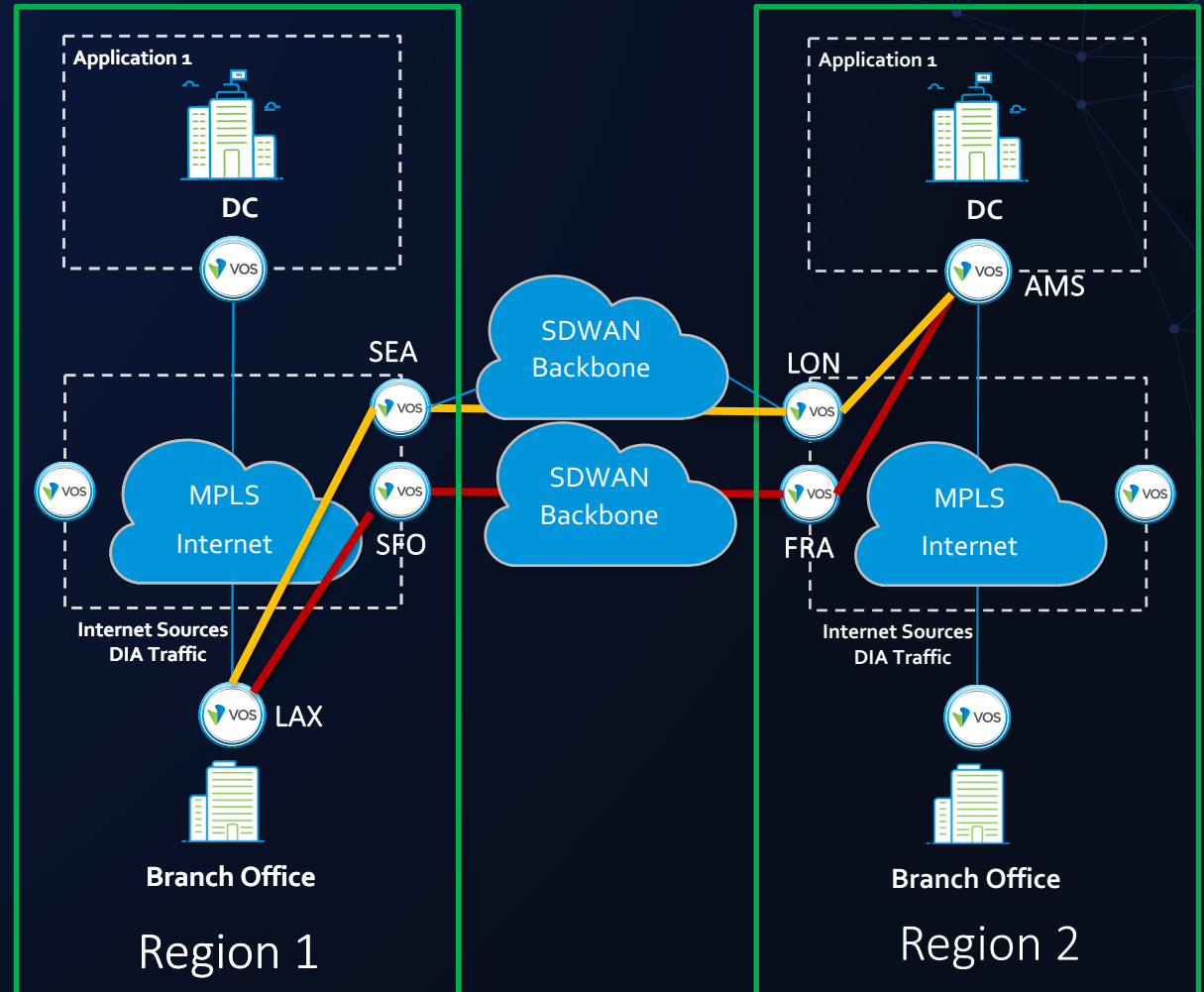
## Optimization Data

Payload	% Saving
50 Bytes	25% to 35%
80 Bytes	21% to 30%
200 Bytes	12% to 17%
500 Bytes	6% to 8%
1000 Bytes	3% to 5%
1400 Bytes	2% to 3%

- Benefits:
  - Improved goodput by reducing overhead
  - Improvement for high cost links and/or small packet size applications
- Versa Benefit
  - Transparently enable header optimization in your network
  - Enabled on unidirectional traffic, asymmetric flows
  - Enabled on per link, per application

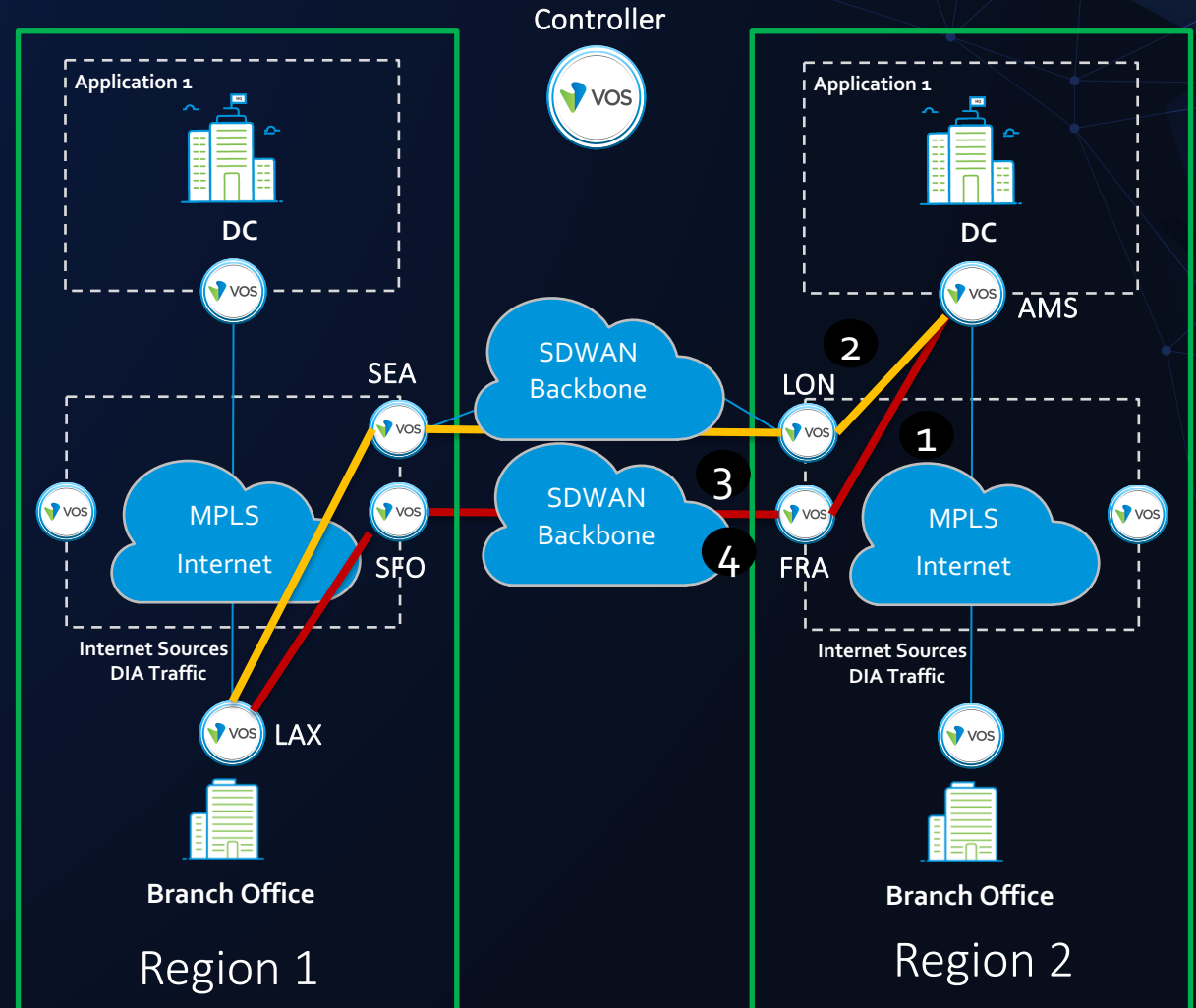
# Traffic Steering in Global WAN

- Customer has branch in LAX and Application in AMS. Customer intent is to choose the lowest latency path from LAX to AMS
- In Global WAN deployment, SLA based routing is challenging
- User experience is impacted by End to End QOS from User to Application
- SDWAN SLA is measured between VOS neighbors. Each hop makes decision based on next hop performance.

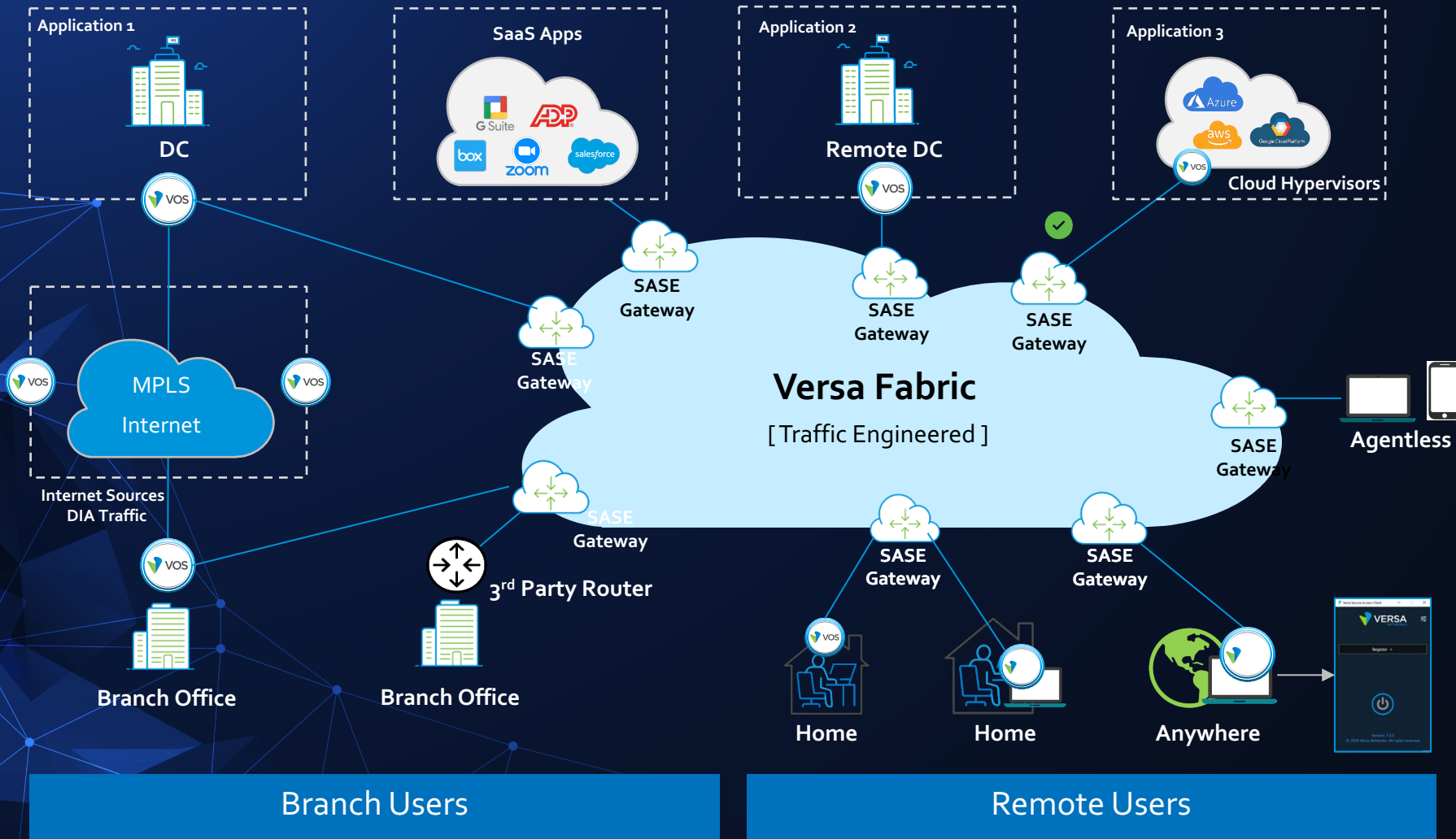


# Traffic Steering in SDWAN

- (1), (2), (3) and (4) are real time SLA measurements.
- These are distributed over MP-BGP to all nodes in the SDWAN overlay
- LAX calculates the best path towards DC in AMS based on the performance information.
- Say (4) gets degraded due to interruptions, LAX would be informed over MP-BGP.



# Leverage Versa Fabric



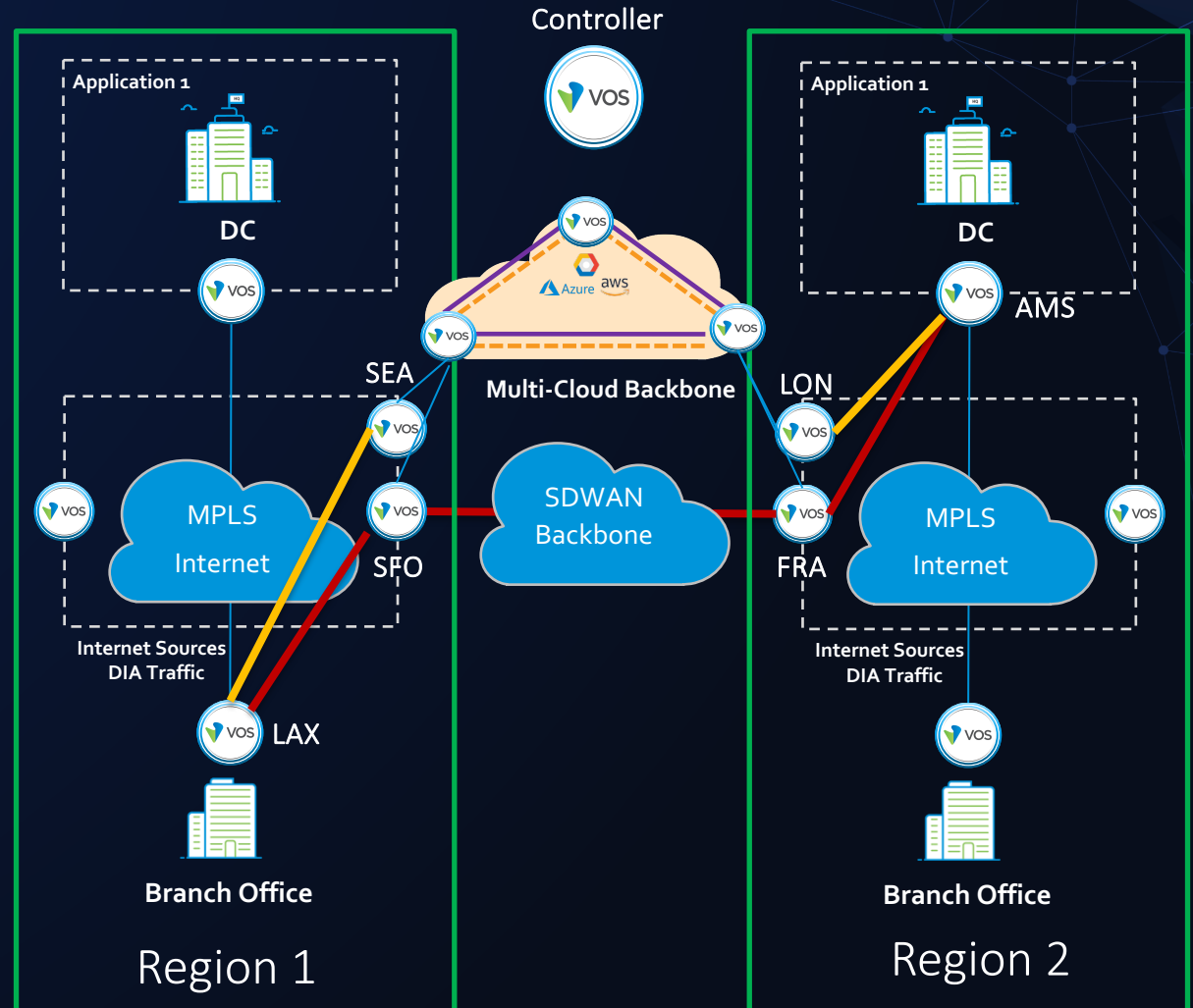
Single Pane of Management,  
Monitoring and Visibility

Versatility 2024



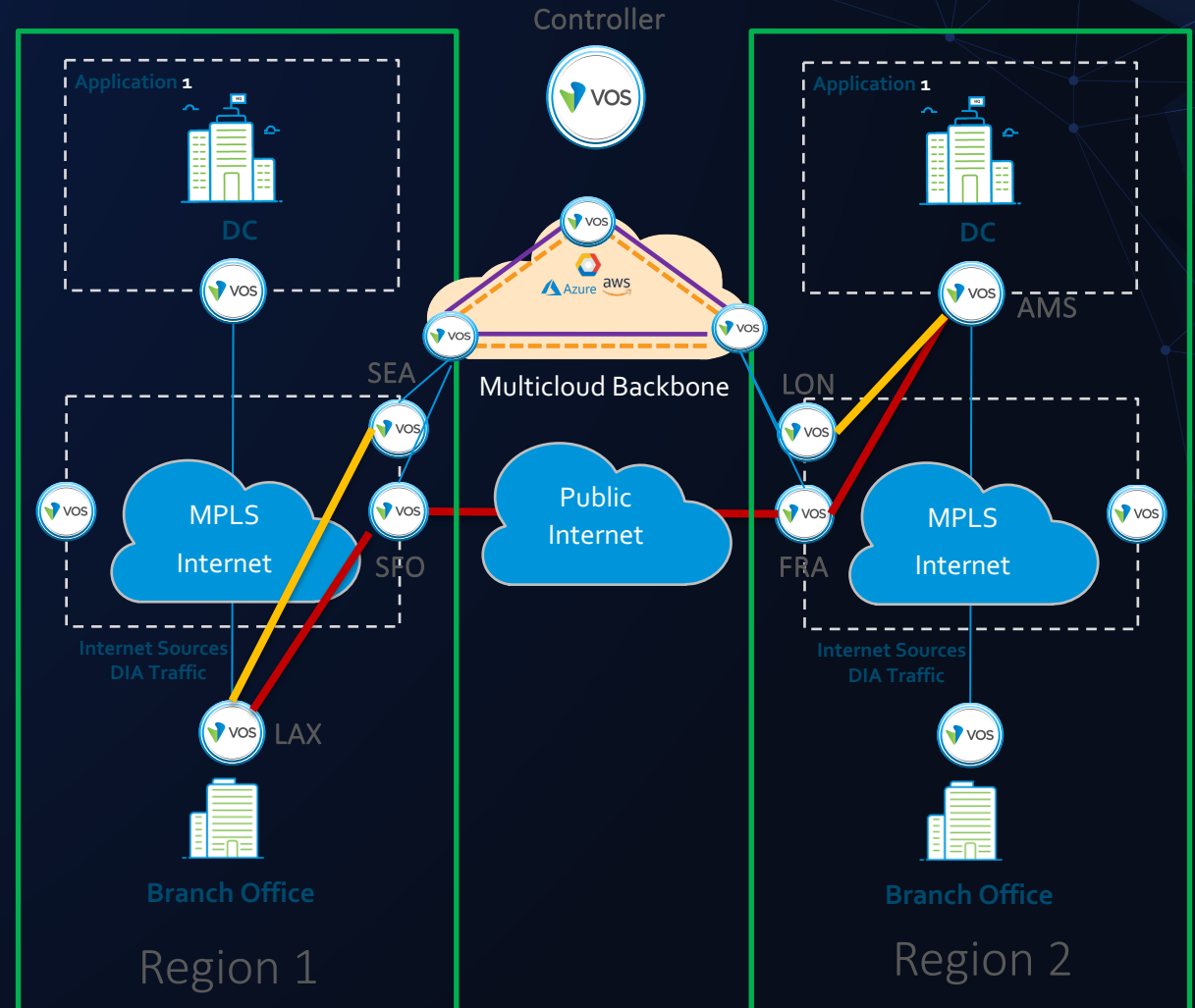
# Use Case 1: Leveraging CSP Fabric as Backup

- Leverage Multi-cloud backbone as “Backup” connectivity when primary backbone is degraded.
- Increases Network Resiliency



# Use Case 1: Leveraging CSP Fabric as Backup

- Leverage Multi-cloud backbone as “Backup” connectivity when primary backbone is degraded.
- Increases Network Resiliency
- Use “Public Internet” based SDWAN overlay for Global WAN connectivity
- Optimizes Cost



# Versa NGFW Capabilities

Network DLP	SAML, RADIUS	Single Sign-On	IP Reput. & Filtering	Anti-Malware / AV	File Reputation & Filtering	URL Reputation & Filtering	SSL, TLS Proxy
DNS Proxy	User, Group Policy/Traffic	Device Type Policy	Reverse Proxy	Dev ID & Device Policies	CASB	App Identification	DNS Reput. & Filtering
Forward Proxy	QoS, HQoS	NG-IPS	DOS Protection	Anti-Virus	Break and Inspect	IPv6 Native	ATP
Captive Portal	VRRP	Multi-tenancy	Carrier Class Routing	Template based Mgmt	VRF	BFD	Application Policy Based Control
Integrated Analytics	Route Reflector	Shaping, Marking	Multicast	Integrated SD-WAN	3 <sup>rd</sup> Party VNFs	Unified SASE	IKEv2 IPSEC
IP Geo Location	UEBA	Passive & Active Authentication	ZTNA	Lateral Movement Protection	IoT Security	Flow Mirroring	CGNAT

Versatility 2024

# Versa CASB

Ensure team members are in compliance with corporate policies for cloud application access.

## KEY CAPABILITIES

- Support for managed and unmanaged client devices
- Record audit trail of risky behavior
- Using machine learning to identify abnormal behavior
- Validate uploaded/downloaded content does not have malware.



## CATEGORY

## SAMPLE APPS SUPPORTED

## SAMPLE GRANULAR CONTROLS

### SOCIAL MEDIA

Facebook, LinkedIn, Instagram, WeChat, WhatsApp

posting, commenting, 'liking', file upload, file download, friend request, chat

### FILE SHARING

Box.com, dropbox, OneDrive, Google Drive

Upload file, download file, share file

### COLLABORATION

Google Suite, Microsoft Office, Slack, MS Team

Upload file, download file, share file, chat, create document, edit documents

### STREAMING MEDIA

YouTube, Twitch, Daily Motion, Vimeo., NetFlix, Prime Video

Post video, comment, like, Watch Stream, Search Stream, Download Video

### COMMUNICATION

WebEx, MS Teams, Zoom

Initiate Meeting, Share Screen, File sharing, Chat, Audio, Video, Record Meeting

# Shadow IT Discovery (CASB)

## Discover

- Discover the Shadow IT SaaS Apps utilized in the network
- SaaS App DB incorporated as part of the solution

## Report

- Filter the Apps based on Sanctioned/Unsanctioned App, App Rank
- Report the usage per application

## Control

- Admin can control based on Apps
- Admin can control the usage based on App Rank

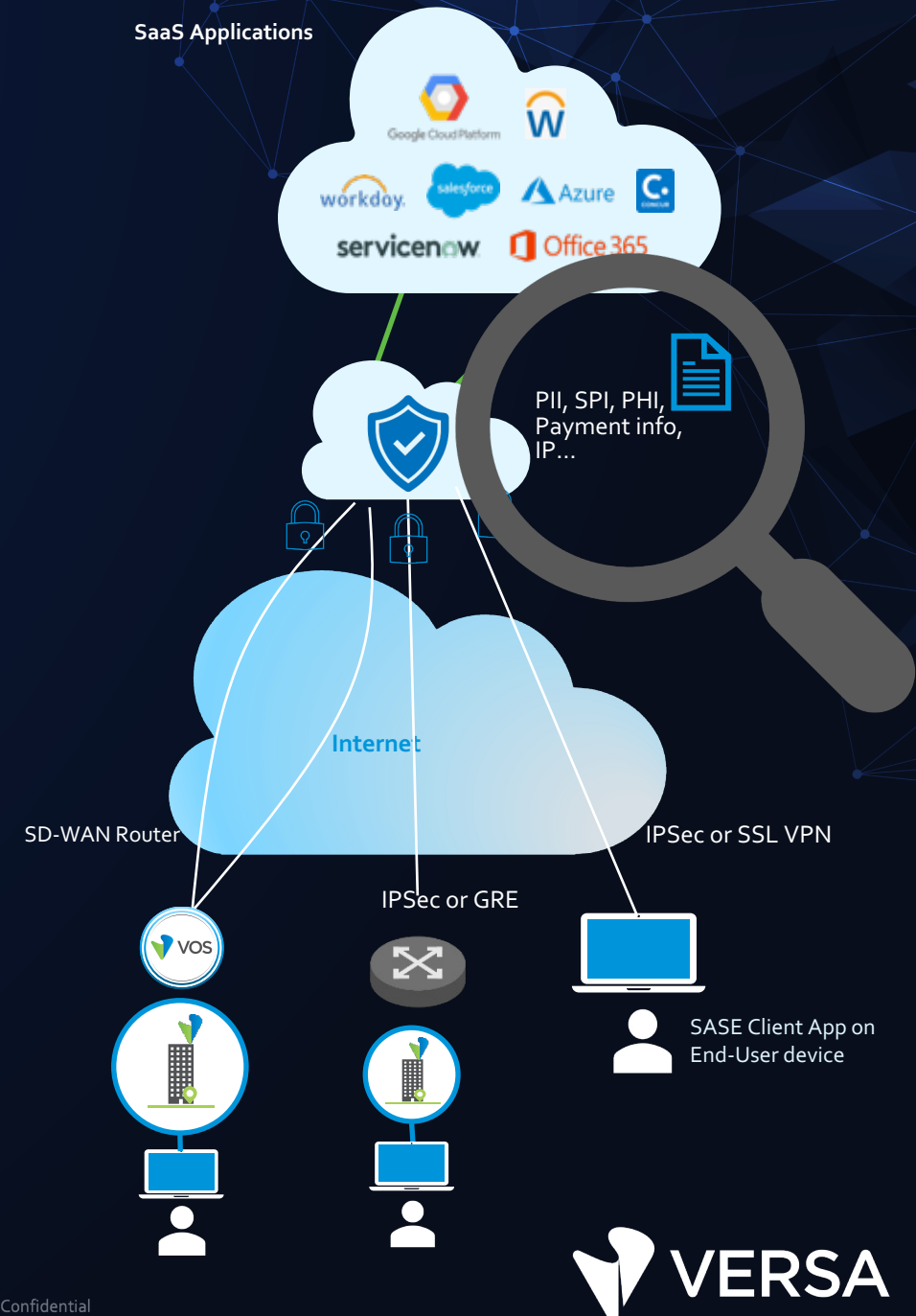
# Versa DLP

Protect data exfiltration and access controls for sensitive documents.

## KEY CAPABILITIES

- Pre-Canned Content Policies & Analysis (PCI, HIPAA, GDPR, etc.)
- Auto Recognize: Credit Card Numbers, Social Security Numbers, etc.
- Support for Microsoft/Azure Information protections
- Support for Exact Data Match (EDM) , OCR
  - Create custom definition of 'what is sensitive' based on Regex patterns and keywords)
  - Versa DLP can inspect header, body, payload and metadata.
- Actions Supported Upon Policy Violation
  - Alert, Block or Deny
  - Quarantine the Document
  - Redact Sensitive Information
  - Encrypt and upload
  - Set label in metadata

Versatility 2024

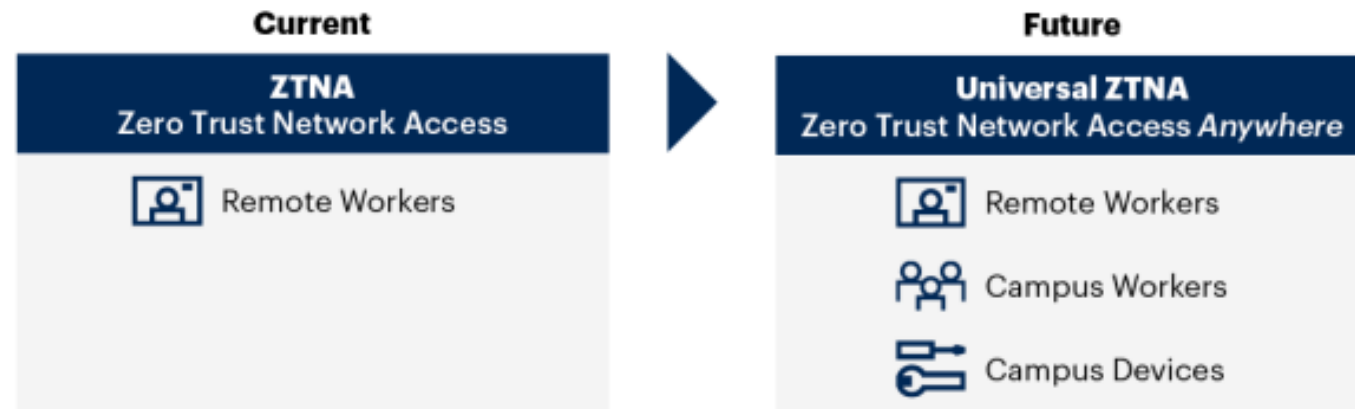


# Gartner Observing Adoption for ZTNA Anywhere

*"Gartner believes evolving existing ZTNA products to secure campus/branch environments better aligns with the future work pattern and zero trust principles and simplifies the operation and administrative burden to manage the solution"*

Campus Network Security and NAC are Ripe for Market Disruption, March 2022

## From Zero Trust Network Access to Universal Zero Trust Network Access



Source: Gartner  
764413\_C

Gartner.

Versatility 2024

© 2024, Versa and/or its affiliates. All rights reserved. Versa Networks Confidential



# Client based ZTNA

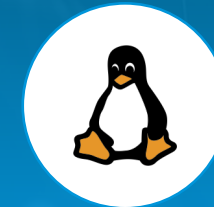
- ✓ **Facilitating connectivity and End-Device Profile Check**
  - User and device authentication
  - Connects to nearest VOS instances on-prem
- ✓ **End-Point (device) Information Profile (EIP) selection based on**
  - AV engine version, signature db version running on the End-Point
  - OS type & version, Security Patch versions
  - Corporate or personal device
  - Specific software installed or not
  - Disk encryption and other parameters
- ✓ **Policy application starting from client devices**
  - Compliance check
  - Traffic Steering via SASE Client
- ✓ **EIP based Policy Enforcement**
  - Implemented on the nearest VOS platform
  - Inline, high performance traffic processing
  - Managed via network and security policies
  - Reported on Versa Analytics



Windows 10



MacOS, iOS,  
Android



Linux

Versatility 2024

# Four Real Life Examples of IoT Security Hacks



## Unsecured IoT at University

Unnamed university's network was flooded with DNS requests for seafood restaurants.

Brute force attack took advantage of weak passwords on 5,000 IoT devices such as vending machines and lighting systems to bring the university's network to a standstill.

Source: Verizon Data Research Digest 2017

## IoT Cameras Hacked

IoT security camera range – NeoCoolCam – was found to contain a major security flaw that they can easily be hacked from outside the network.

Researchers at Bitdefender were able to access login screen to take control of 100,000+ cameras in use



## Hacking a Jeep

Security researchers were able to send instructions to a Jeep Cherokee through its entertainment system.

Not only were they able to remotely change the in-car temperature, they could also influence the vehicle's steering and braking systems. All it required was knowledge of the individual vehicle's IP address to take control.

## Mirai Downs Liberia Internet

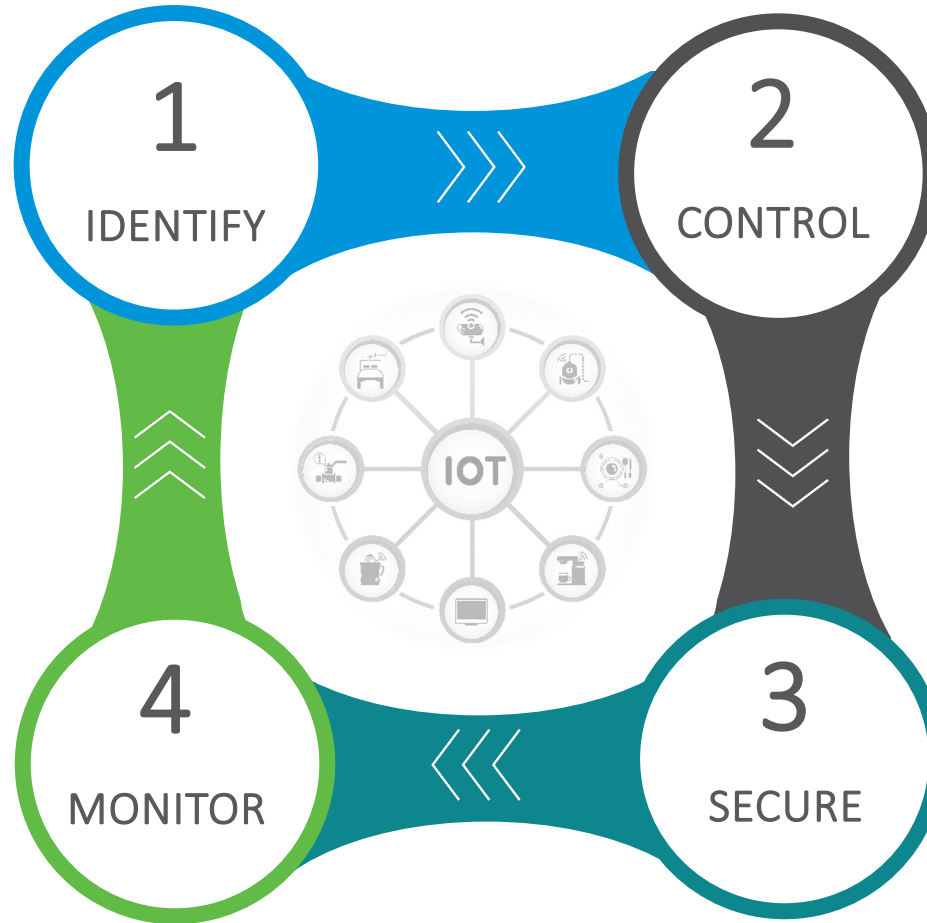
Mirai botnet was used in an attempt to take the entire country of Liberia offline in November 2016.

ZDNet reports that a Mirai-based botnet, was intermittently attacking IP addresses of the two telecom operators that co-own the only fiber cable coming into the West African nation of Liberia.



# Versa IoT Security Lifecycle Stages

- Device ID
- Device Categorization
- Network Access



- Traffic Analysis
- Traffic Segmentation
- Security Policy

- Traffic Patterns
- Event Logging
- Alerts

- Vulnerabilities
- Attacks
- Exploits

# Device Identification & Fingerprinting

- Device identification and fingerprinting
  - Analysis of flows generated by the Device
  - Browser data and other details to identify client device
  - Using MAC OUI, IP, network headers, DHCP field, Destination IP/HTTP/HTTPS info, protocols and more
  - Combination of data points used to give the best outcome
- Logging of client device connection activities
- Analytics support
  - Encrypted and signed archive files
  - Ability to process dated and signed files
- Comprehensive Device Library to help identify a large variety of devices, OS, browsers
  - Leverages device signatures developed in-house and licensed from 3<sup>rd</sup> party supplier
- Device Identification based traffic policies and management

# Thank you

Versatility 2024

