Versatility 2025

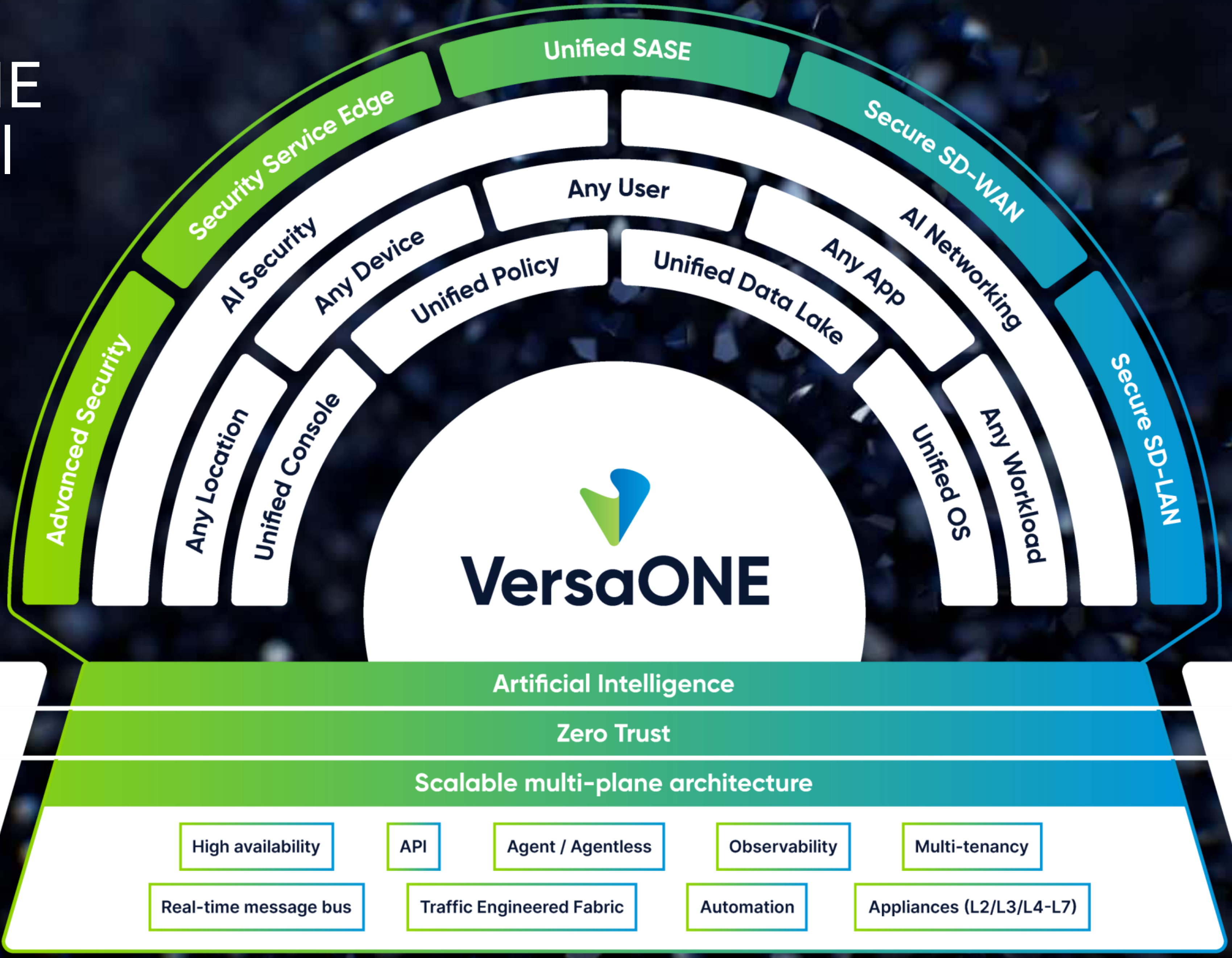
SSE Today - Best of breed cloud-delivered security

VERSA

SSE State of the Art

Versatility 2025

VersaONE Universal SASE Platform



Unified SASE

Security Service Edge

Secure SD-WAN

Advanced Security

Secure SD-LAN

AI Security

AI Networking

Any User

Any Device

Any App

Any Location

Any Workload

Unified Policy

Unified Data Lake

Unified Console

Unified OS

VersaONE

Artificial Intelligence

Zero Trust

Scalable multi-plane architecture

High availability

API

Agent / Agentless

Observability

Multi-tenancy

Real-time message bus

Traffic Engineered Fabric

Automation

Appliances (L2/L3/L4-L7)

INTEGRATIONS

- Identity Providers
- EPP / EDR
- MDM
- Threat Intelligence

INTEGRATIONS

- SSE / SD-WAN
- Multi-Cloud
- Security Analytics
- Network Monitoring/Mgmt
- Automation
- Service Desk

Versa SASE – Available Today

Secure Access

NGFW

ZTNA

Versa SASE client access

Endpoint Information Profile/ Device Posture

Threat Prevention

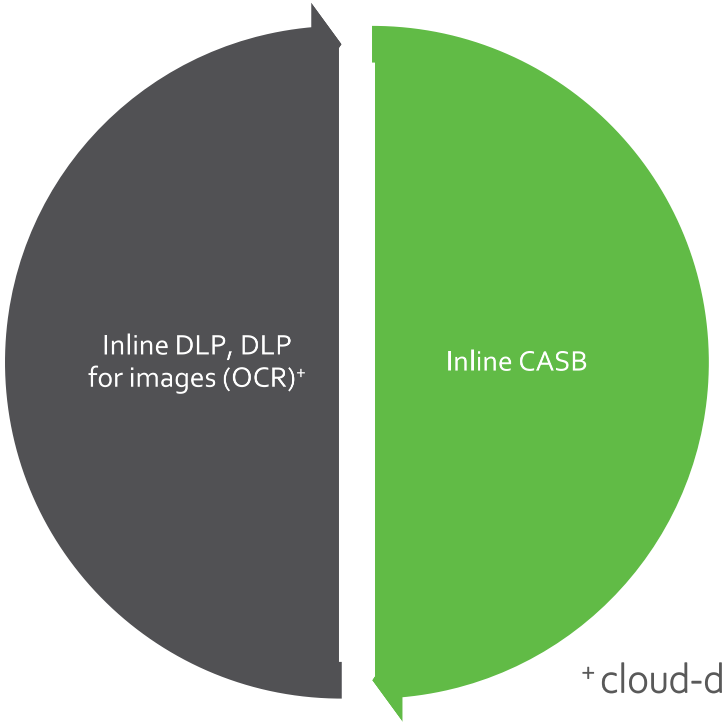
URL, IP, DNS Filtering, Malware Analysis,

File Filtering

IPS/IDS

ATP+

Data Protection



Inline DLP, DLP for images (OCR)+

Inline CASB

+ cloud-delivered

Versa Concerto Unified Management Portal

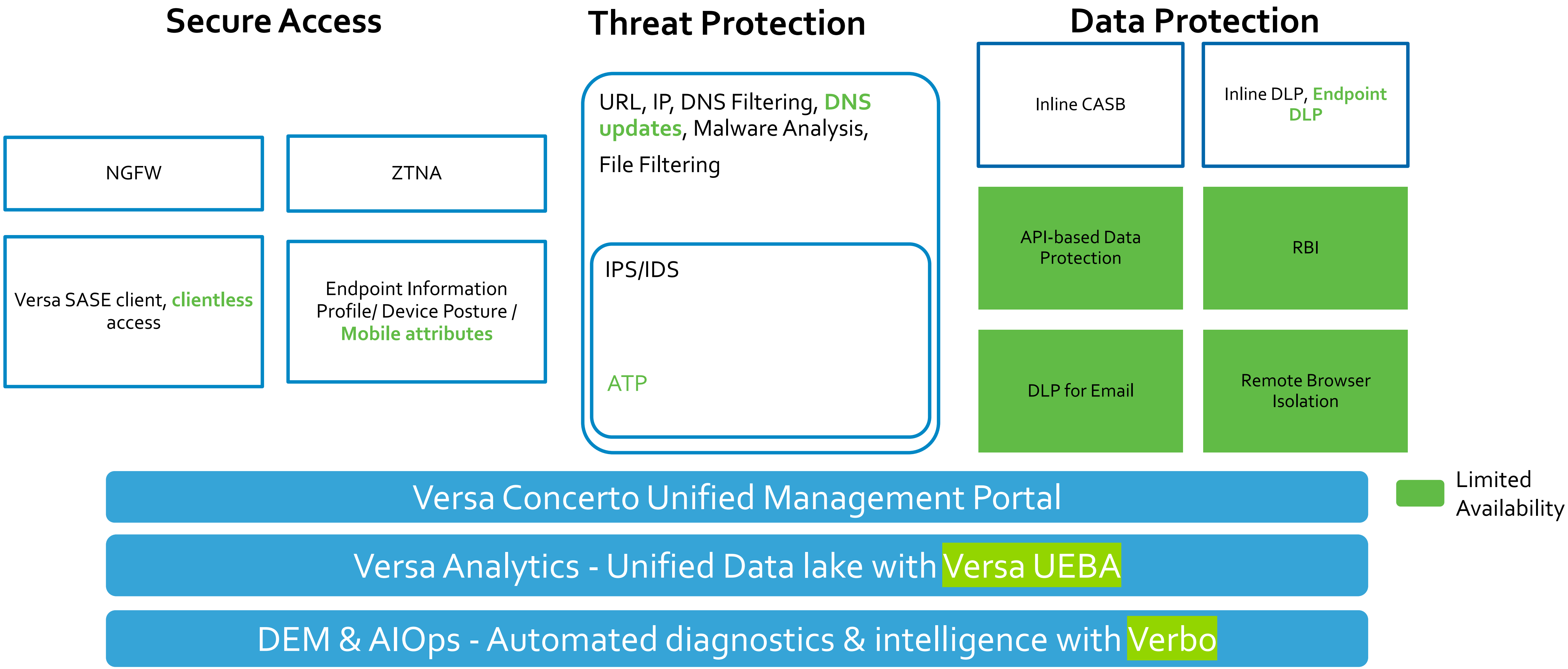
Versa Analytics - Predictive data analytics, Unified Data lake with Versa UEBA*+

AIOps - Automated diagnostics & intelligence with Verbo*+

Versatility 2025

VERSA

Versa SASE – What's new



Secure Access

NGFW

ZTNA

Versa SASE client, **clientless** access

Endpoint Information Profile/ Device Posture / **Mobile attributes**

Threat Protection

URL, IP, DNS Filtering, **DNS updates**, Malware Analysis,

File Filtering

IPS/IDS

ATP

Data Protection

Inline CASB

Inline DLP, **Endpoint DLP**

API-based Data Protection

RBI

DLP for Email

Remote Browser Isolation

🟩 Limited Availability

Versa Concerto Unified Management Portal

Versa Analytics - Unified Data lake with Versa UEBA

DEM & AIOps - Automated diagnostics & intelligence with Verbo

Versatility 2025

VERSA

Works with SD-WAN+SASE

Elite Secure SD-WAN	VSPIA/VSAF Professional (SASE)
NGFW	NGFW
URL, IP DNS Filtering	URL, IP DNS Filtering
Antivirus	Antivirus
NG-IPS	NG-IPS
File filtering	File filtering
ALS	ALS
CASB	CASB
DLP	DLP
ATP	ATP
DEM	DEM

🟩 Included in tier

⬛ Available as an add-on feature

Other Advanced Security add-ons like API-DP, RBI are also available with both SD-WAN and SASE

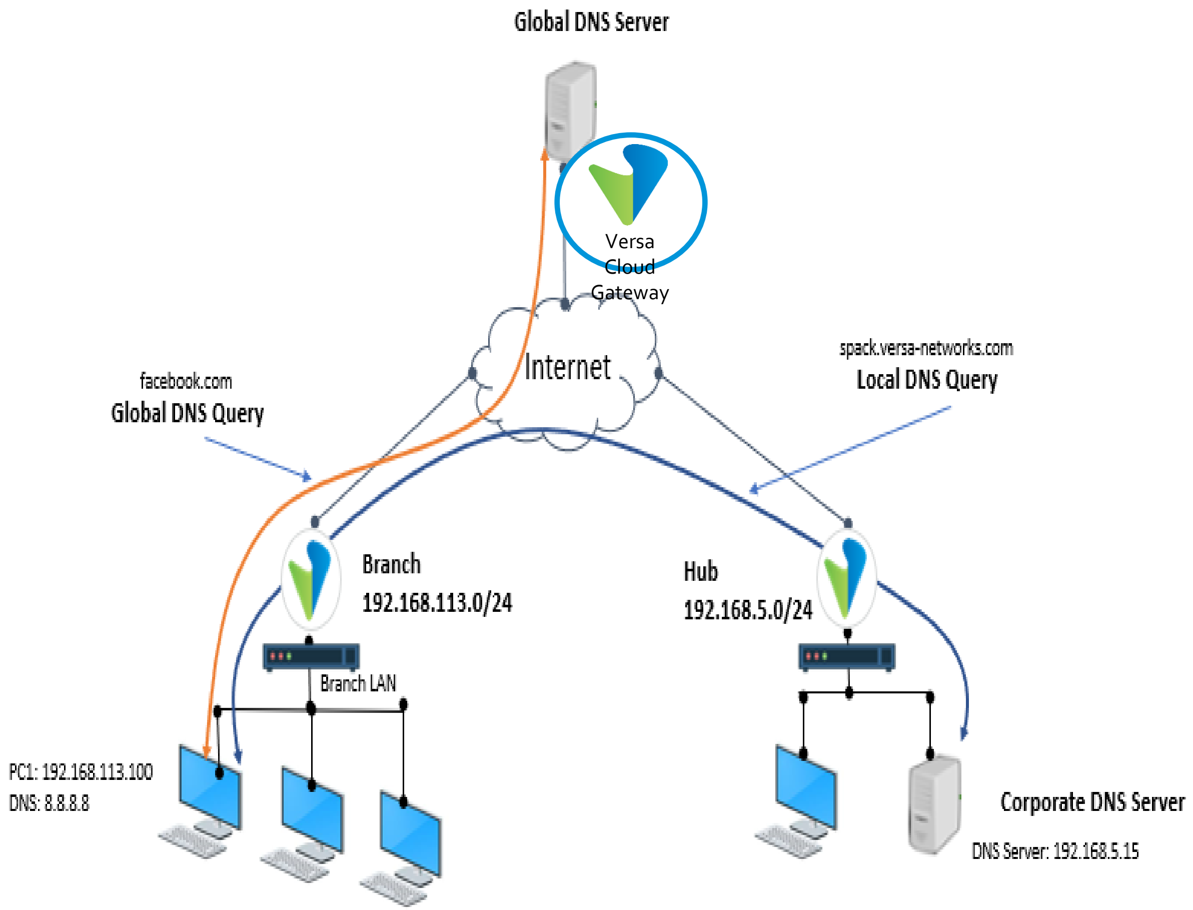
Why Versa for DNS Security

DNS security as part of unified SASE – no need for a standalone DNS vendor

Attractive built-in features with professional tier

DNS proxy (SD-WAN) in combination with DNS security provides efficiency, performance and security

DNS Security

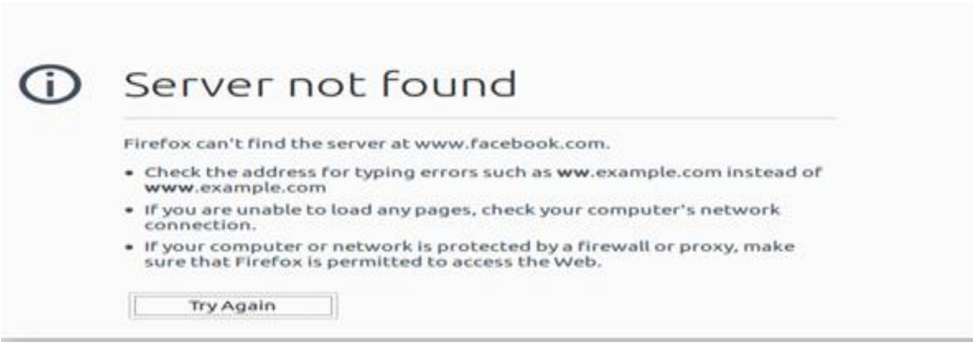


Use-cases

- Content security at the DNS level, prior to URLF
- Protection from DNS attacks (DNS Spoofing/cache poisoning, DNS Amplification/Reflection, DNS Tunneling, DNS Hijacking, DNS Rebinding)
- Policies to Blacklist/Whitelist domains with Allow/Block/Alert/Sinkhole actions
- DNS query-based actions for granular control
- Suspicious DNS tunnel detection
- Newly Observed Domains detection
- Reputation-based domain actions

DNS Filtering Use Cases

- Filter domains based on query type
- Allows granular control



Server not found

Firefox can't find the server at www.facebook.com.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Use Cases: DNS Query-based Policies

Use `AAAA` as query type to block IPV6 responses from `google.com`

Prevent DNS amplification/ reflection attacks

- Block unwanted DNS query types – Eg: AXFR, HINFO, ANY, IXFR
- Throttle Zone record information

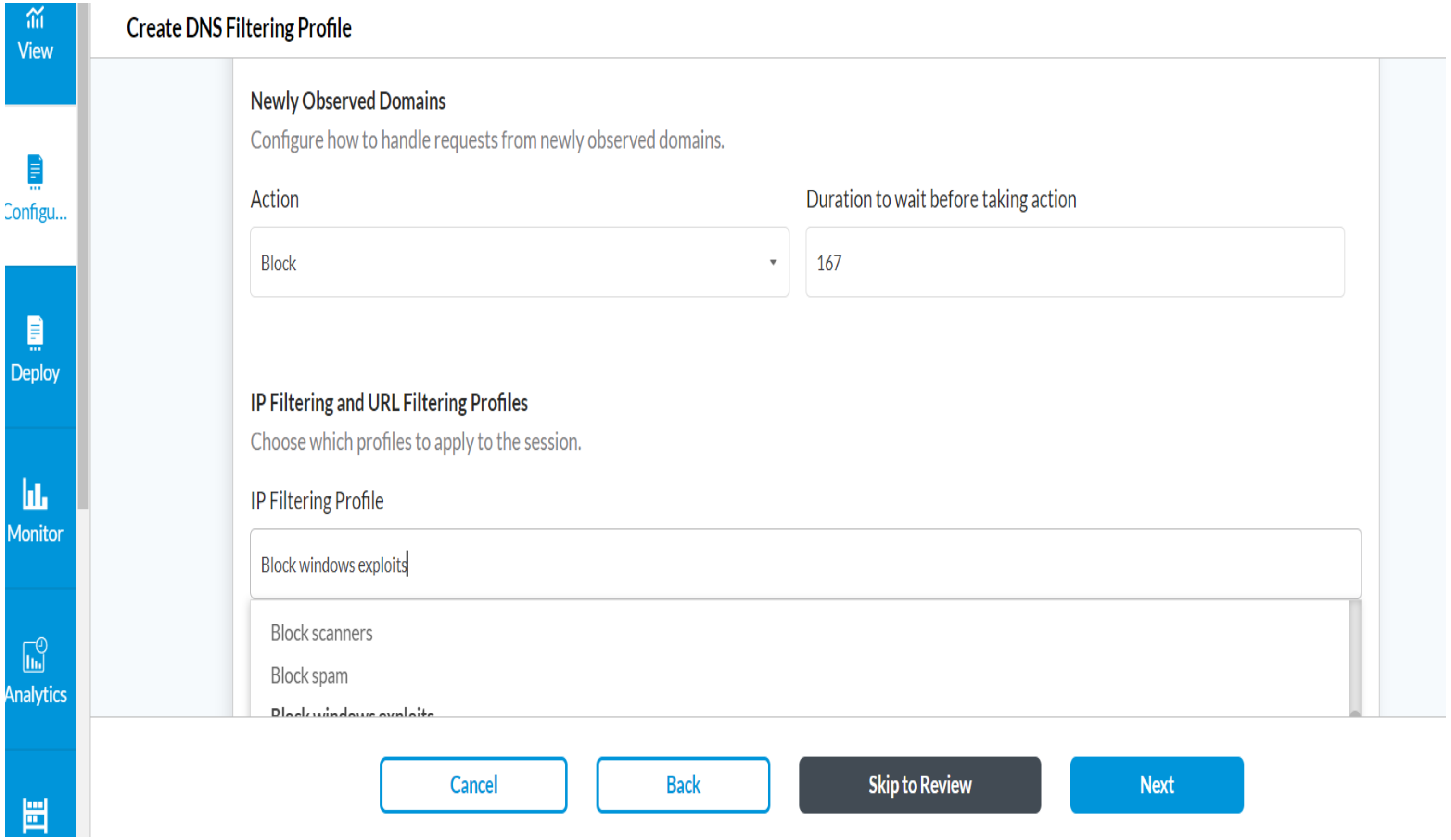
DNS Cache Poisoning

DNS Spoofing / Cache Poisoning

- Malicious actor corrupts the DNS server's cache, to return a “poisoned” IP address
- Users are redirected to a malicious domain

Versa's Solution

- Reputation-based filtering
- Block newly observed domains



Create DNS Filtering Profile

Newly Observed Domains

Configure how to handle requests from newly observed domains.

Action: Block

Duration to wait before taking action: 167

IP Filtering and URL Filtering Profiles

Choose which profiles to apply to the session.

IP Filtering Profile: Block windows exploits

Versatility 2025

VERSA

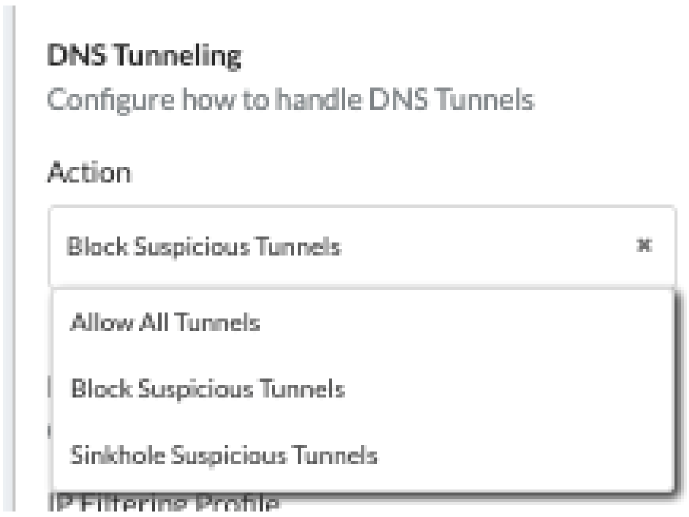
DNS Tunneling

DNS Tunneling

- DNS tunneling is a method of encoding data from other protocols into DNS queries and responses.
- This can be used to bypass network security measures, allowing for covert communication or data exfiltration by disguising it as normal DNS traffic.

Versa's Solution

- Versa DNS Tunnel detection can detect the malicious tunnels by using Invalid Character based detection, Frequency based detection and uncommon requests for the domains which have reputations as suspicious/malicious

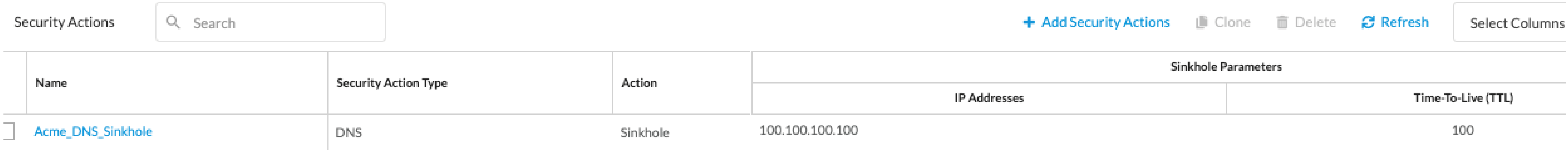


DNS Tunneling

Configure how to handle DNS Tunnels

Action: Block Suspicious Tunnels

DNS Sinkhole Action



Name	Security Action Type	Action	Sinkhole Parameters	
			IP Addresses	Time-To-Live (TTL)
□ Acme_DNS_Sinkhole	DNS	Sinkhole	100.100.100.100	100

- DNS Sinkhole is a mechanism/action to block access to malicious domains by “sinkholing” traffic to a non-routable address
  - Eg: Wannacry checked a domain before encrypting files, sinkhole the domain to prevent spread
- Primarily used to block access to malicious domains.

Versa SASE Client Highlights

Network connectivity checks

- User registration
- User and device authentication
- Location optimized connectivity to best gateway
- SLA monitored tunnels
- Encrypted tunnels

Posture and Compliance checks

- Enforced through Endpoint Information Profile (EIP) checks
- Hundreds of attributes – anti-malware, EDR, disk encryption, host firewall, file sharing
- Mobile, Process & registry checks, OS checks, cert expiry

New

Windows

MacOS, iOS, Android

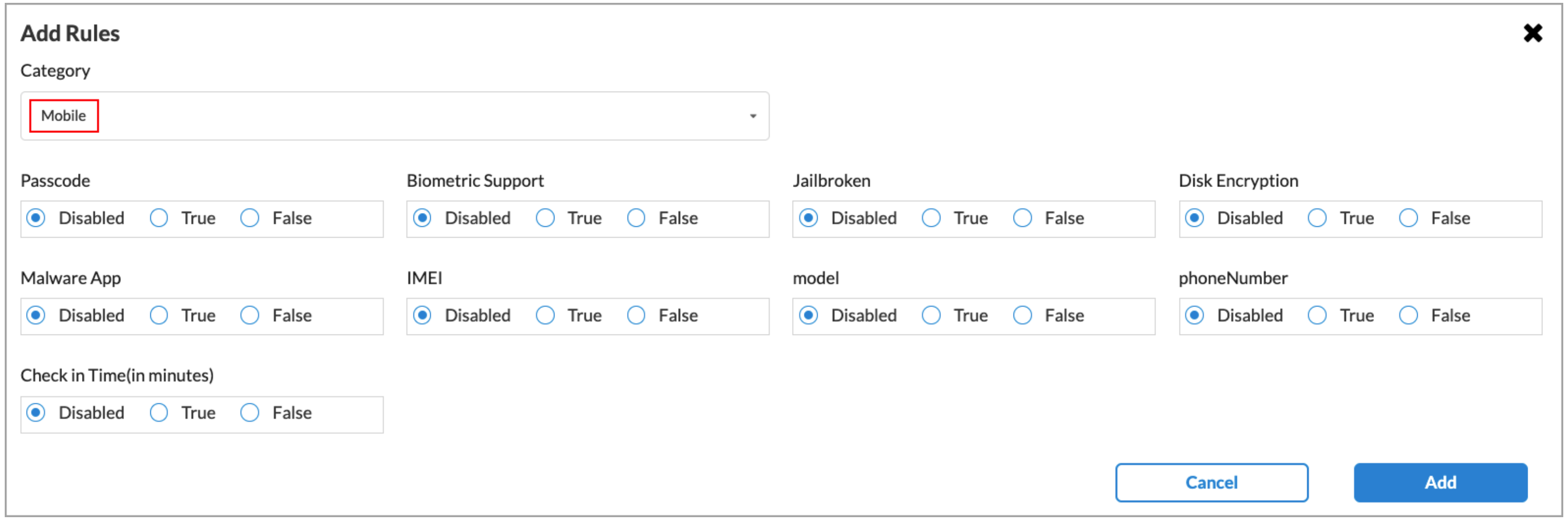
Linux

Endpoint Information Profile – Mobile attributes

ioS and Android

Mobile OS checks for-

- Jailbreak detection
- Passcode check
- Biometric support
- Specific model
- IMEI numbers
- Phone numbers etc.



Add Rules

Category: Mobile

Passcode: ● Disabled ○ True ○ False

Biometric Support: ● Disabled ○ True ○ False

Jailbroken: ● Disabled ○ True ○ False

Disk Encryption: ● Disabled ○ True ○ False

Malware App: ● Disabled ○ True ○ False

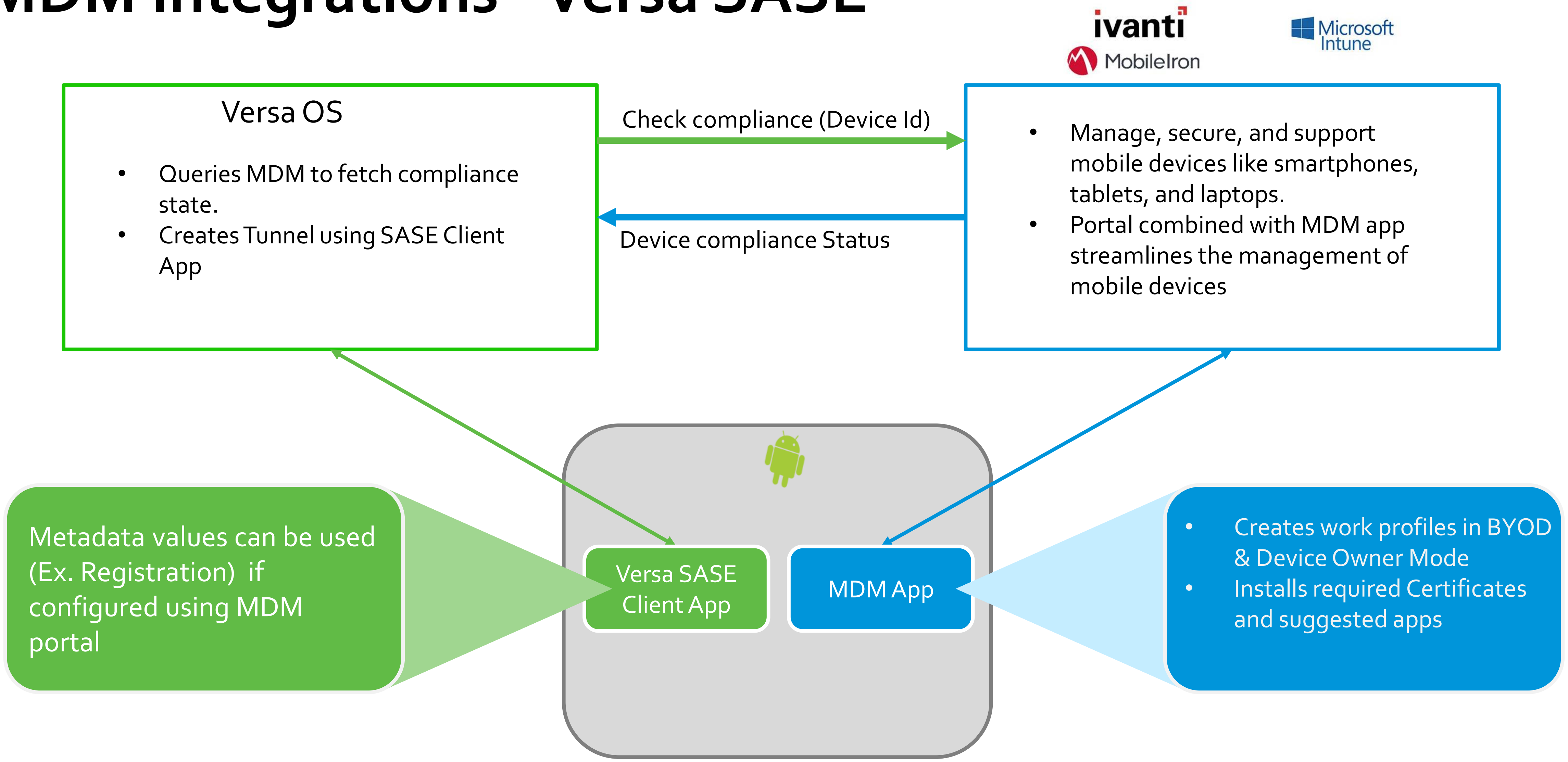
IMEI: ● Disabled ○ True ○ False

model: ● Disabled ○ True ○ False

phoneNumber: ● Disabled ○ True ○ False

Check in Time(in minutes): ● Disabled ○ True ○ False

MDM Integrations - Versa SASE



Versa OS

- Queries MDM to fetch compliance state.
- Creates Tunnel using SASE Client App

Check compliance (Device Id)

Device compliance Status

- Manage, secure, and support mobile devices like smartphones, tablets, and laptops.
- Portal combined with MDM app streamlines the management of mobile devices

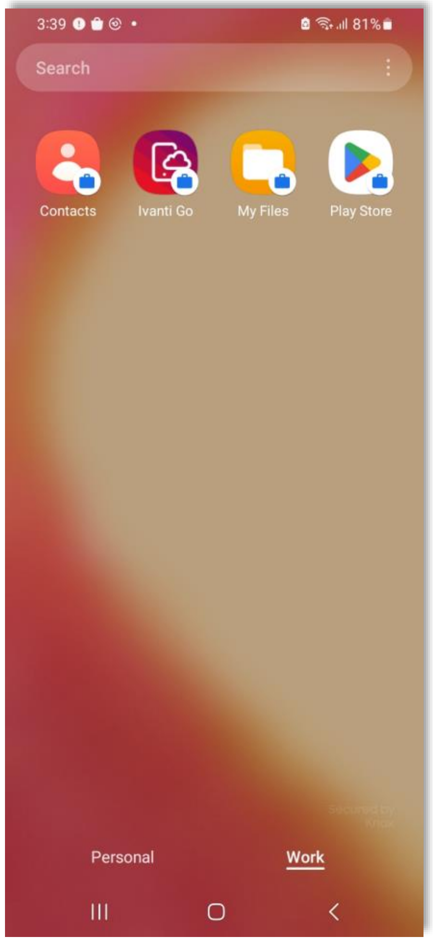
Metadata values can be used (Ex. Registration) if configured using MDM portal

Versa SASE Client App

MDM App

- Creates work profiles in BYOD & Device Owner Mode
- Installs required Certificates and suggested apps

Supported Modes



BYOD modes

Android - Work profile

ios, iPadOS – User Enrollment

This device belongs to your organisation

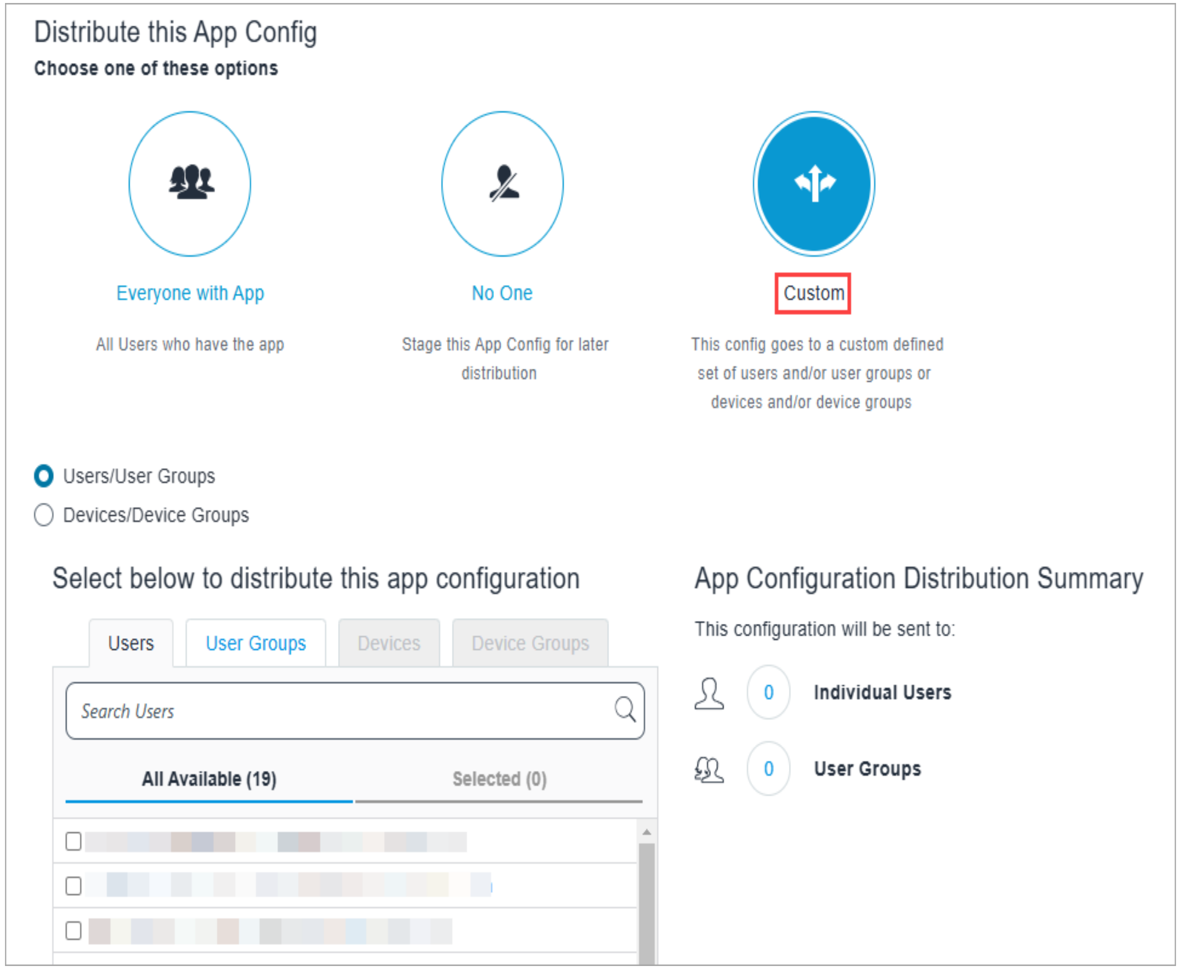
To learn more, contact your IT admin.

Fully Managed mode

Android - Device Owner Profile

iOS/ipadOS – Device Enrollment

Mass distribute Versa SASE client through Ivanti MDM



Distribute this App Config

Choose one of these options

Everyone with App

All Users who have the app

No One

Stage this App Config for later distribution

Custom

This config goes to a custom defined set of users and/or user groups or devices and/or device groups

● Users/User Groups

○ Devices/Device Groups

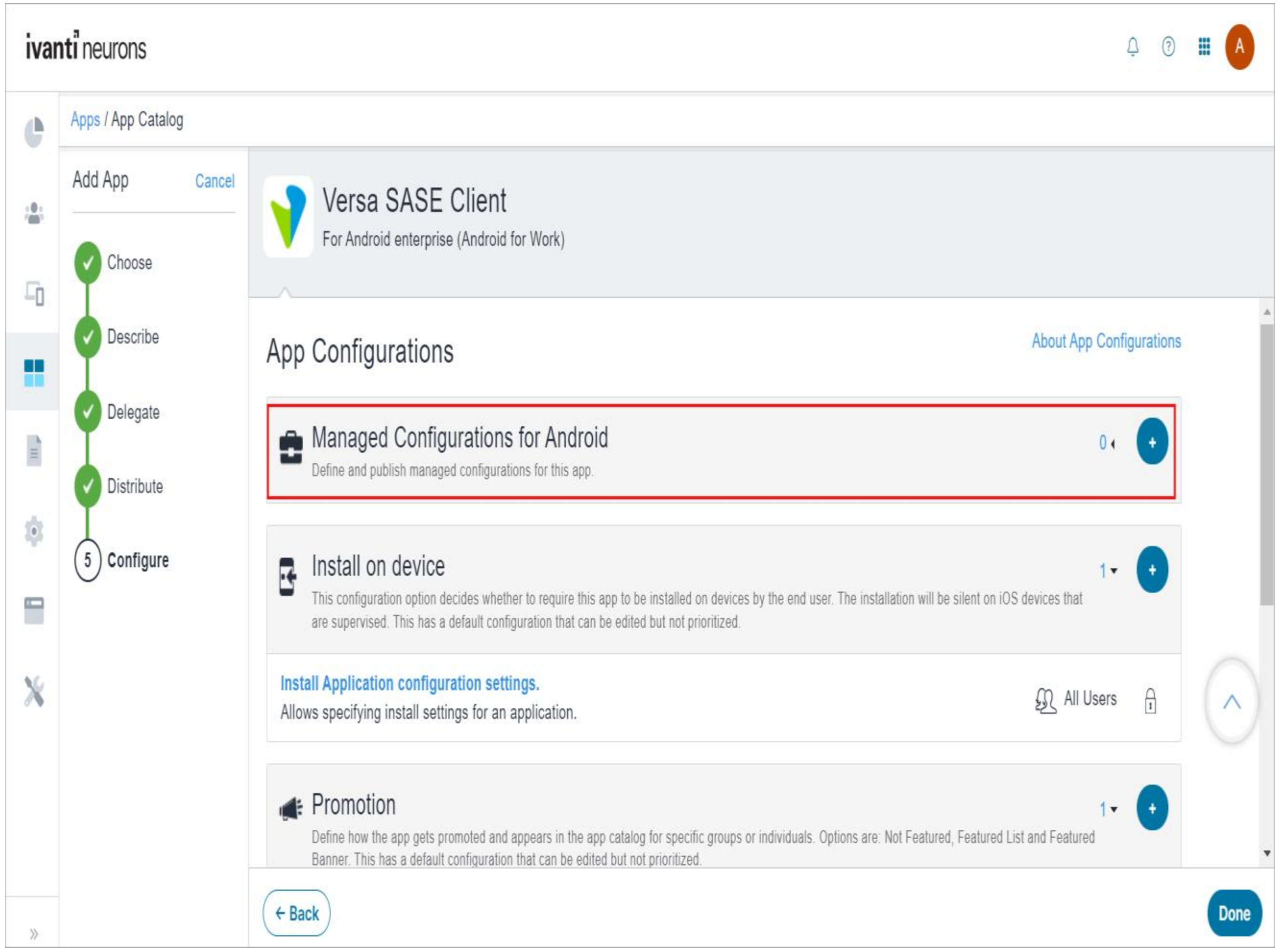
Select below to distribute this app configuration

App Configuration Distribution Summary

This configuration will be sent to:

0 **Individual Users**

0 **User Groups**



Versa SASE Client

For Android enterprise (Android for Work)

App Configurations

Managed Configurations for Android 0

Define and publish managed configurations for this app.

Install on device 1

This configuration option decides whether to require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritized.

Install Application configuration settings.

Allows specifying install settings for an application. All Users

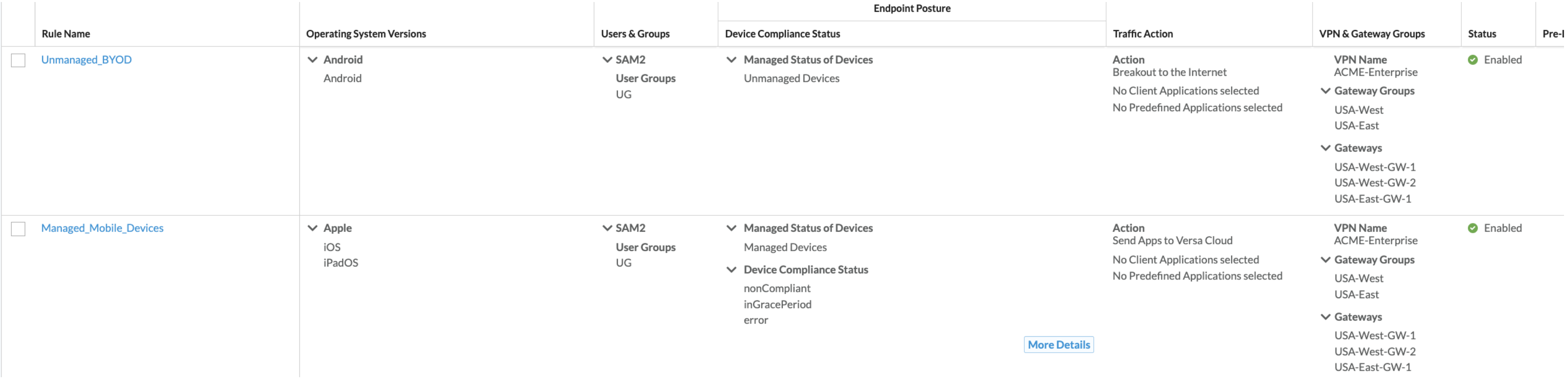
Promotion 1

Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritized.

Versatility 2025

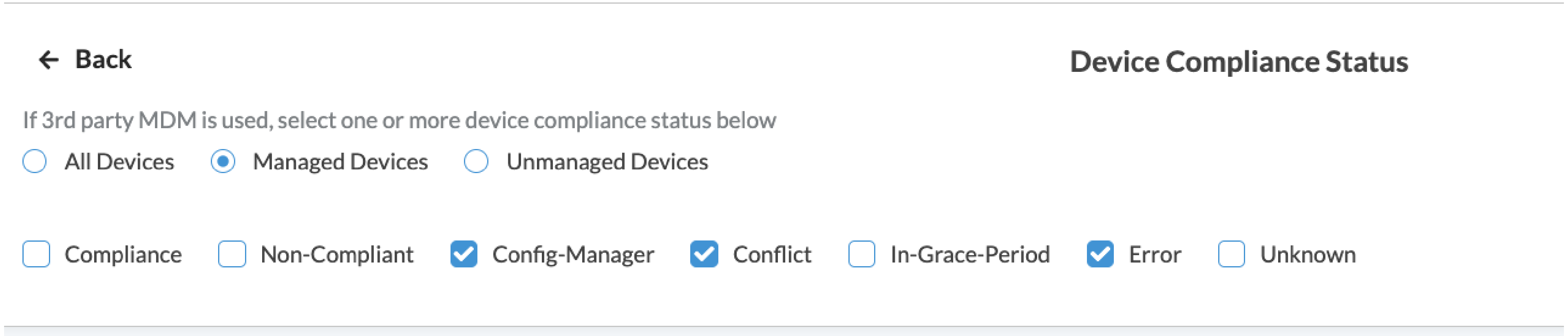
VERSA

Check Device Compliance and Enforce Security



				Endpoint Posture				
	Rule Name	Operating System Versions	Users & Groups	Device Compliance Status	Traffic Action	VPN & Gateway Groups	Status	Pre-I
□	Unmanaged_BYOD	Android Android	SAM2 User Groups UG	Managed Status of Devices Unmanaged Devices	Action Breakout to the Internet No Client Applications selected No Predefined Applications selected	VPN Name ACME-Enterprise Gateway Groups USA-West USA-East Gateways USA-West-GW-1 USA-West-GW-2 USA-East-GW-1	✓ Enabled	
□	Managed_Mobile_Devices	Apple iOS iPadOS	SAM2 User Groups UG	Managed Status of Devices Managed Devices Device Compliance Status nonCompliant inGracePeriod error More Details	Action Send Apps to Versa Cloud No Client Applications selected No Predefined Applications selected	VPN Name ACME-Enterprise Gateway Groups USA-West USA-East Gateways USA-West-GW-1 USA-West-GW-2 USA-East-GW-1	✓ Enabled	

Differential secure access policies



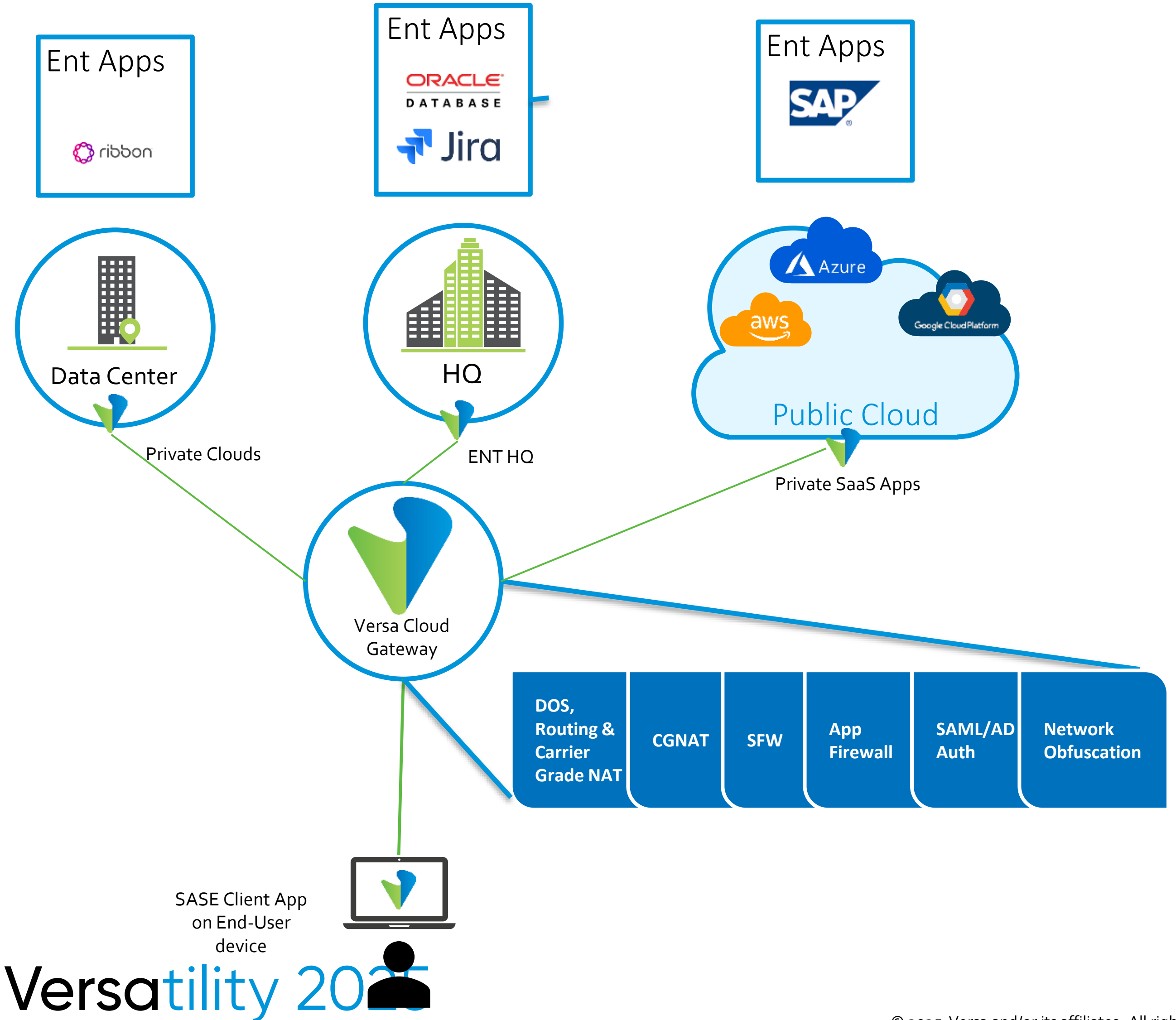
Device Compliance Status

If 3rd party MDM is used, select one or more device compliance status below

○ All Devices ● Managed Devices ○ Unmanaged Devices

□ Compliance □ Non-Compliant ☑ Config-Manager ☑ Conflict □ In-Grace-Period ☑ Error □ Unknown

Zero Trust Network Access



Use-cases

- Encrypted VPN based connectivity
- Securely access applications hosted in DC, Branch or Public Cloud
- Secure Private Access
- Zero Trust Network Access (ZTNA)

Security Services

- User/User Group based Policy
- Integration with Identity Providers
- Application Firewall
- Network, Application Obfuscation and Hiding

Versa Cloud Fabric

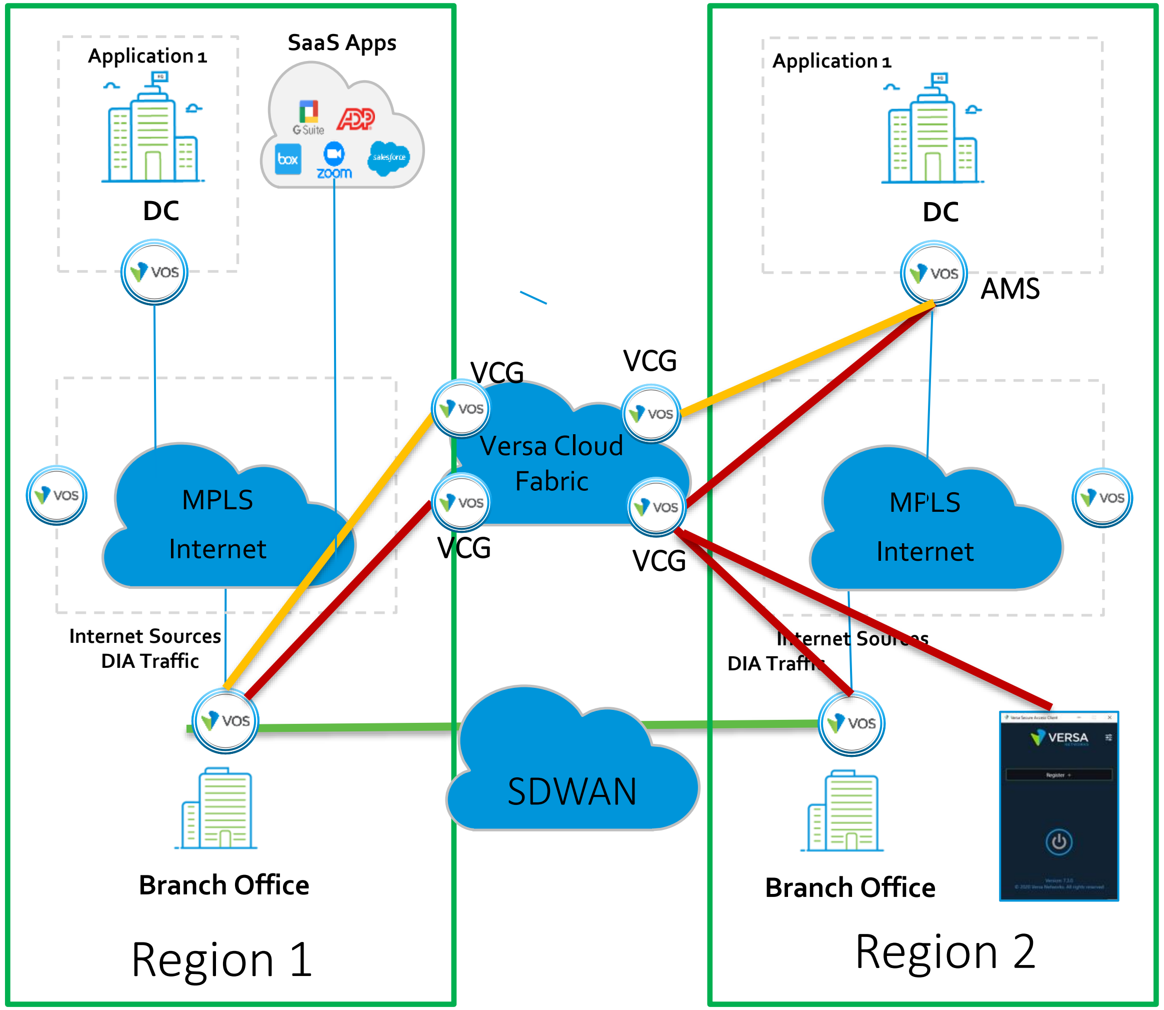
User Experience Challenge for a Global Enterprise

#1: Providing Reliable Connectivity Global Workforce is Expensive and/or Ineffective

#2: Extend Reliable Connectivity to Remote Users, Partner locations, SaaS/CSP locations

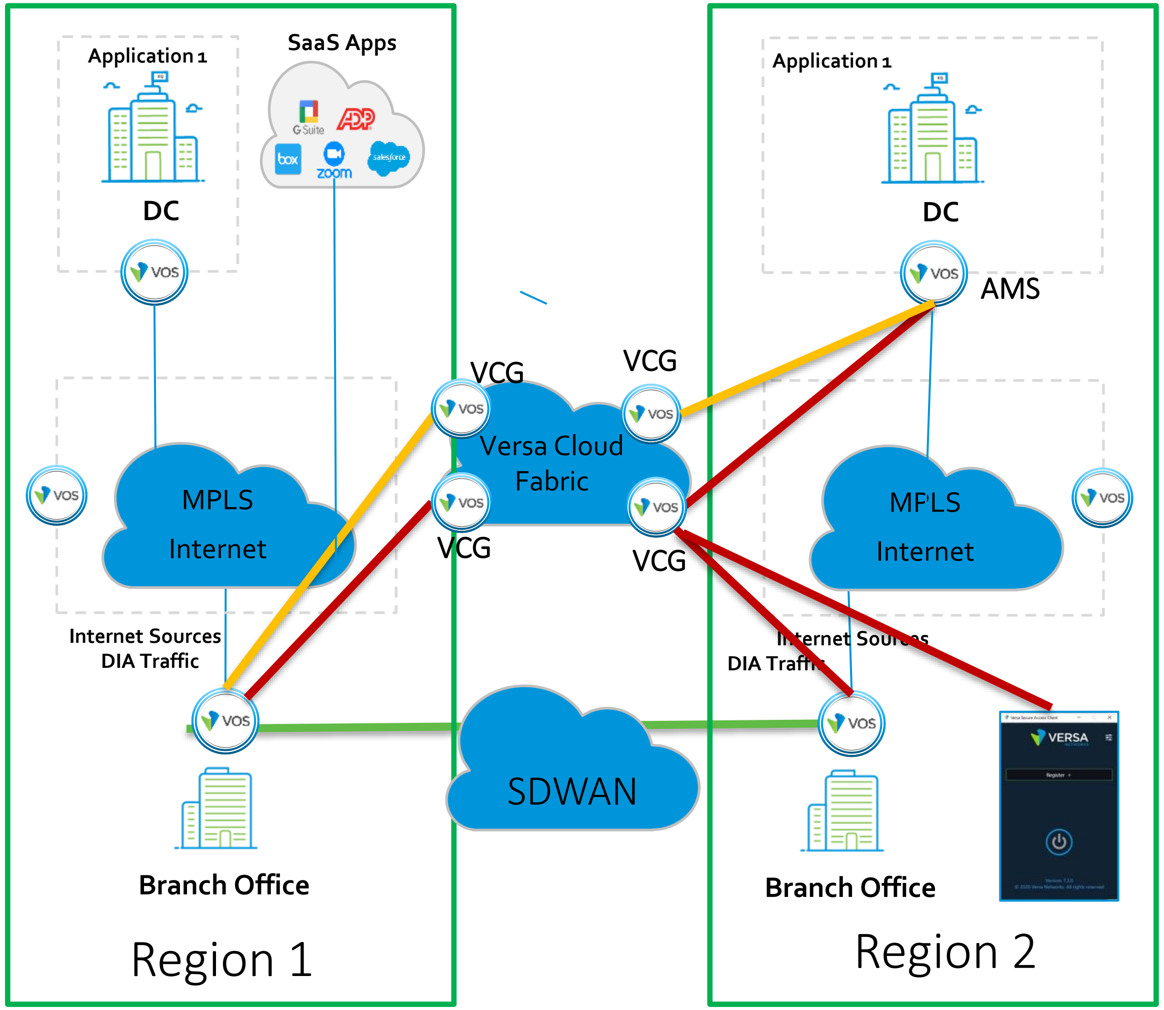
#3: Extend Advanced Security for traffic using global backbone

What is the Right Solution?



- Solution should be consumable as a Service
  - Without the need to deploy or procure bandwidth and hardware
- Customer provides the “intent” of the networking, abstracting complex configurations
- Solution should provide connectivity for remote branches and remote users
- Solution is provided for optimized connectivity to
  - Private Applications
  - SaaS Applications
  - Cloud Workloads
- Integrated Security/Micro-segmentation

Introducing Versa Cloud Fabric



Technology

- Traffic Engineered SD-WAN over Versa Backbone
  - End to End QoS based traffic Steering. Always chooses best path from your branch to the destination.
- Cold-Potato routing between the Cloud Gateways

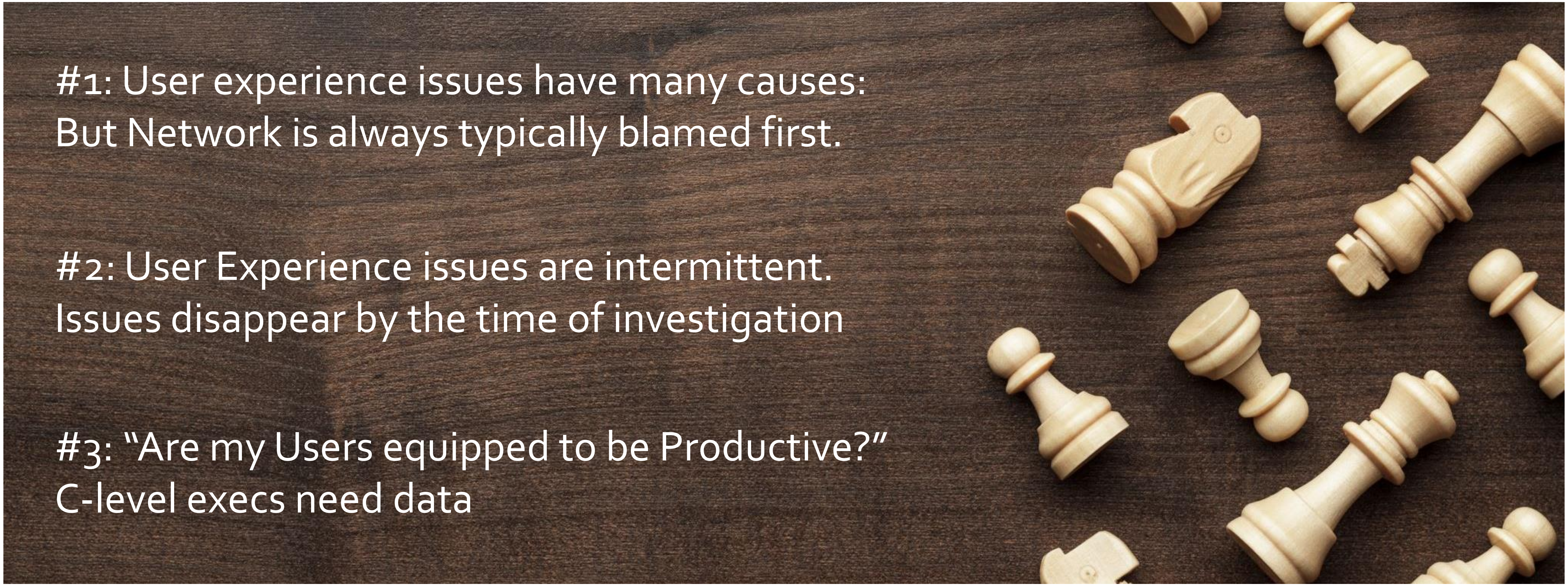
Use cases

- Branch to Branch connectivity
- Optimized SaaS App connectivity (For Branch users and Remote Users)
- Cost and Performance optimized Multi-Cloud connectivity

Digital Experience Monitoring

Versatility 2025

User Experience Challenge



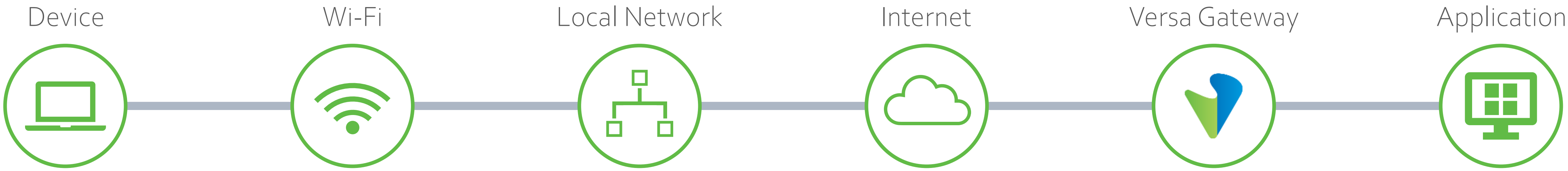
#1: User experience issues have many causes:
But Network is always typically blamed first.

#2: User Experience issues are intermittent.
Issues disappear by the time of investigation

#3: “Are my Users equipped to be Productive?”
C-level execs need data

Versa’s DEM Solution : End-to-End Monitoring

Measures performance metrics of various segments



Device

Wi-Fi

Local Network

Internet

Versa Gateway

Application

- Device Health: CPU/Memory/ Disk/Battery

- WiFi Signal Quality, Tx/Rx

- Local network performance metrics: Latency, Jitter, Loss to ISP

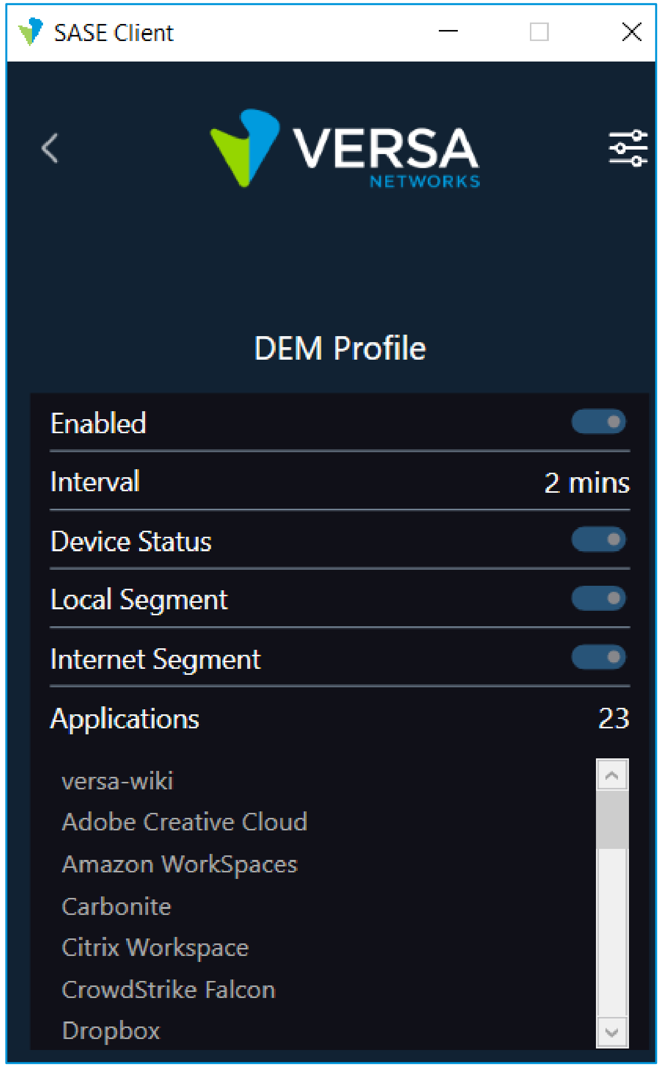
- Internet performance metrics: Latency, Jitter, Loss on internet to gateway

- Gateway performance metrics: Latency, Jitter, loss on SD-WAN and application network

- Application performance metrics: DNS lookup time, TCP connect time, SSL handshake time, HTTP latency, time to first and last byte etc

Versa’s DEM Components

- SASE Client:
  - DEM enabled SASE client performs end to end monitoring of user’s network and application performance
  - Sends synthetic probes periodically to determine the performance metrics
  - Exports of statistics and status for analytics to consume:
    - Device
    - Local segment
    - Internet segment
    - Application servers
- SASE Gateway:
  - Configures clients with DEM profiles
  - Exports DEM metrics received from SASE clients to analytics
- Analytics
  - Provides end to end visibility and actionable insights



SASE Client

VERSA NETWORKS

DEM Profile

Enabled	●
Interval	2 mins
Device Status	●
Local Segment	●
Internet Segment	●
Applications	23

versa-wiki
Adobe Creative Cloud
Amazon WorkSpaces
Carbonite
Citrix Workspace
CrowdStrike Falcon
Dropbox

Versatility 2025

VERSA

Benefits of Using DEM for SASE Observability

- Proactive, shorter latency, accurate, and customer centric decision making

Enriches visibility

Actionable insights

Improved user experience

Reduces time in troubleshooting issues

Optimizes business strategy

Thank you