VERSATILITY

Versa’s Security Ecosystem: Integrations that Power Modern SASE

Anusha Vaidyanathan

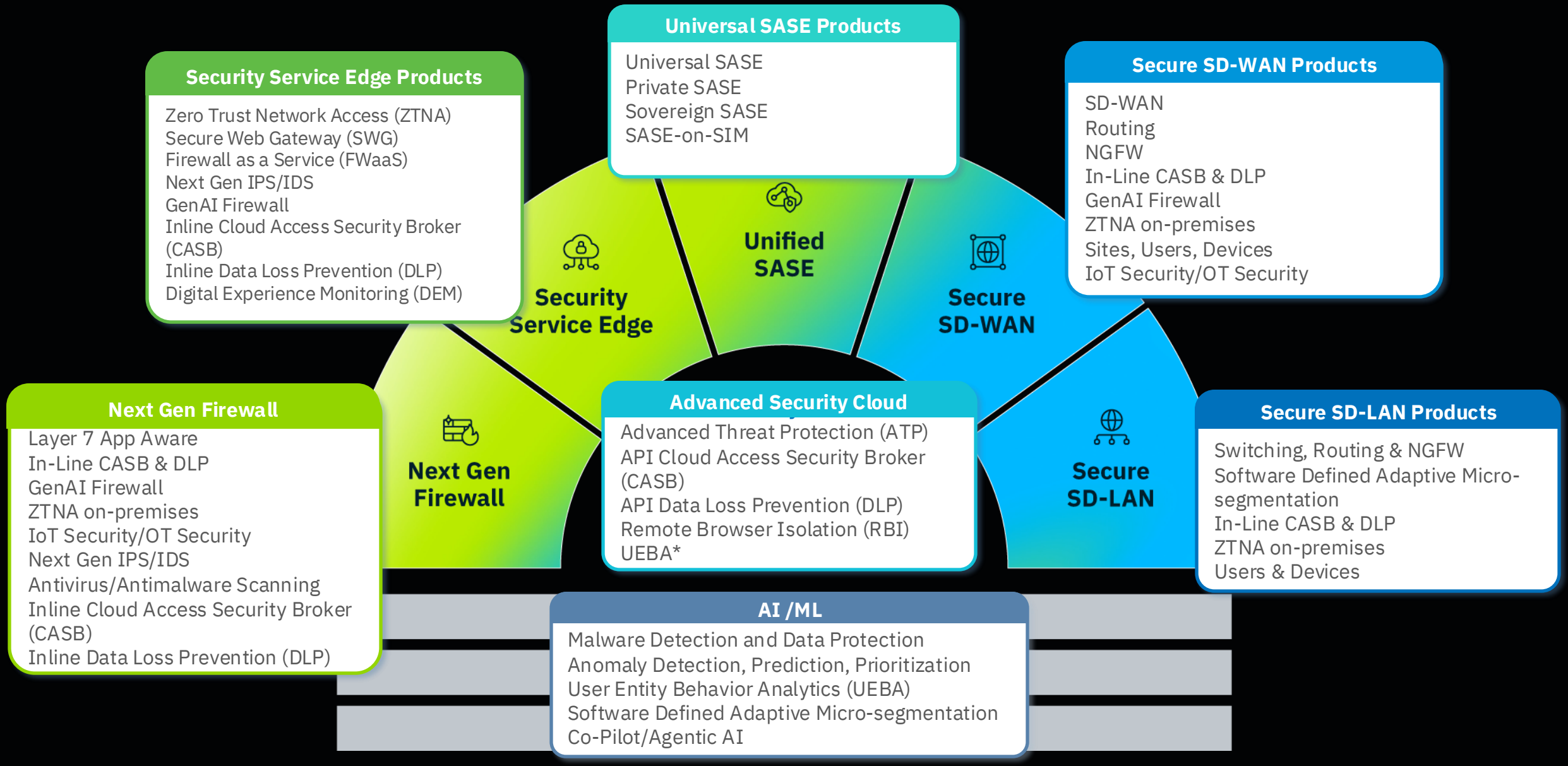
Sr Director, Product Management

Jon Taylor

Director and Principal of Security

Agenda

- VersaONE
- EDR integrations – SentinelOne, Crowdstrike, Defender
- UEM/MDM integrations – Intune, Ivanti



VERSATILITY

Integrates with modern enterprise ecosystem

END POINT PROTECTION
Versa can validate endpoint protection is installed, up to date and enabled.

Avast, ESET, Carbon Black, CrowdStrike, Bitdefender, McAfee, SentinelOne, Panda, Symantec, F-Secure, Trend Micro, Windows Defender

MULTI-CLOUD
Versa can be deployed in all Major public clouds in an automated manner.

Equinix, AWS, Google Cloud, Azure, Oracle Cloud, Megaport

IDENTITY PROVIDERS
Versa can authenticate users via leading identity providers and protocols.

Microsoft Entra ID, Ping Identity, CyberArk, LDAP, Okta, ADFS, SAML, Duo, Google Cloud IAM, auth0

SECURTIY ANALYTICS
Versa can log all security events to all leading SIEM & SOAR platforms.

solarwinds, Datadog, Radar, CrowdStrike, McAfee, logpoint, splunk> a cisco company, SentinelOne

NETWORK MONITORING
Versa has integrations with leading network (NetFlow) monitoring tools.

Cisco Secure Network Analytics, SevOne, Net profiler

AUTOMATION
100% of Versa Capabilities are available via open API's. We have an established Versa automation community.

HashiCorp, Ansible, python, Postman, GitLab, Terraform

UNIFIED ENDPOINT MANAGEMENT
Versa works with the leading MDM solutions, including Microsoft Intune.

Microsoft Intune, ivanti

SERVICE DESK INTEGRATION
Versa can be integrated into ServiceNow And other popular ticketing systems. (Versa Integration fee for ServiceNow)

servicenow

NETWORK MANAGEMENT
Monitor Versa devices using industry standard SNMP Management tools such as Solarwinds.

solarwinds

VERSATILITY

Unified Risk Score - Endpoint Detection

VERSATILITY

Overview

Problem to Solve: Taking adaptive access to the next level with Versa Unified Risk Scoring

Static → Responsive → Adaptive

Challenge

Static Security Policies

- Sources could be –
- from X IP address/subnet
- on Y ports
- or Z location
- Users/groups

Application Risk

Browsing risky URL, malicious domains or IPs	Detect shadow IT or risky Gen AI applications	Block malicious file or sensitive data in transit

Endpoint Information profile (EIP)-

Is disk encrypted, domain-joined	Match users on a Windows XP laptop	Using an outdated Chrome browser	Expired device certificates

Solution

AI-enabled, Dynamic Policies with Versa Unified Risk Scoring

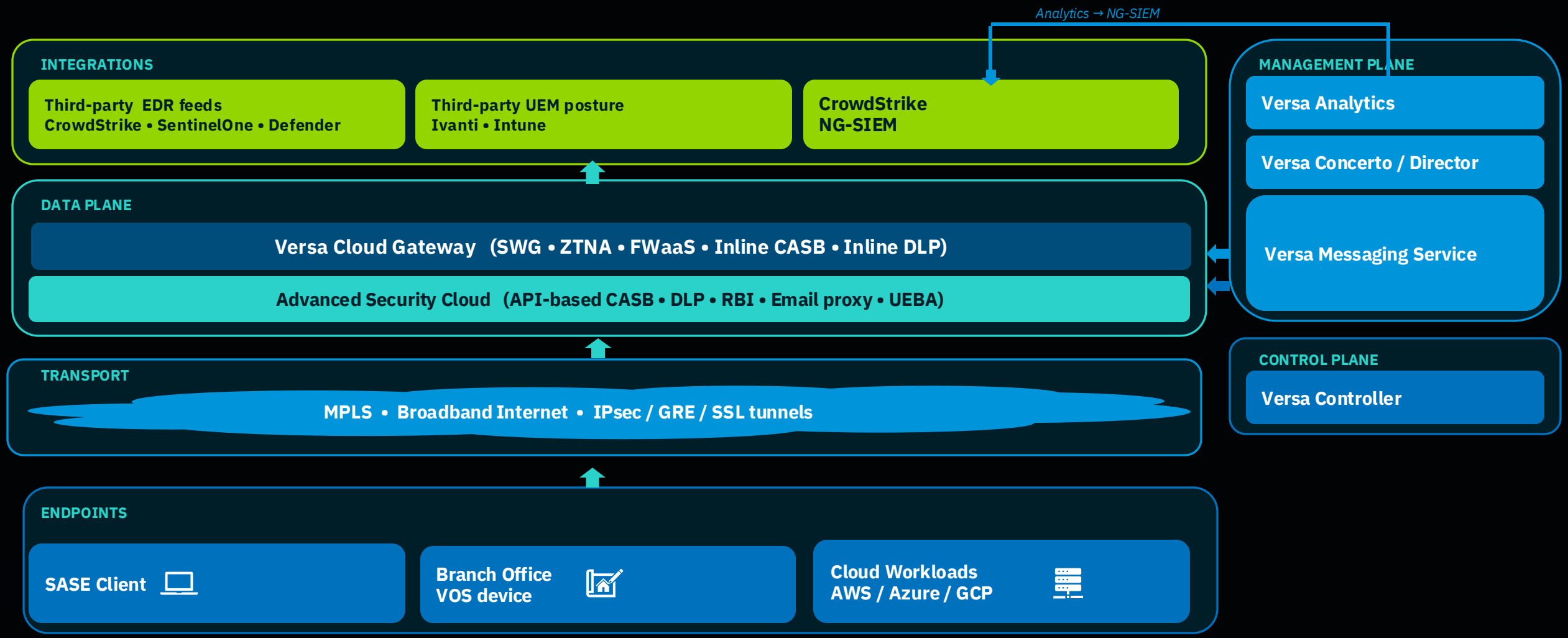
- Dynamic security policy enforcement by improving policy match criteria
- Driven by risky user actions, compromised or out-of-compliance devices

VERSATILITY

ARCHITECTURE

Versa SASE integrations — simplified view

Endpoints connect through transport to the Versa cloud, which integrates with third-party security platforms



VERSATILITY

CONNECTOR REGISTRATION

From registration to enforcement in 60 seconds

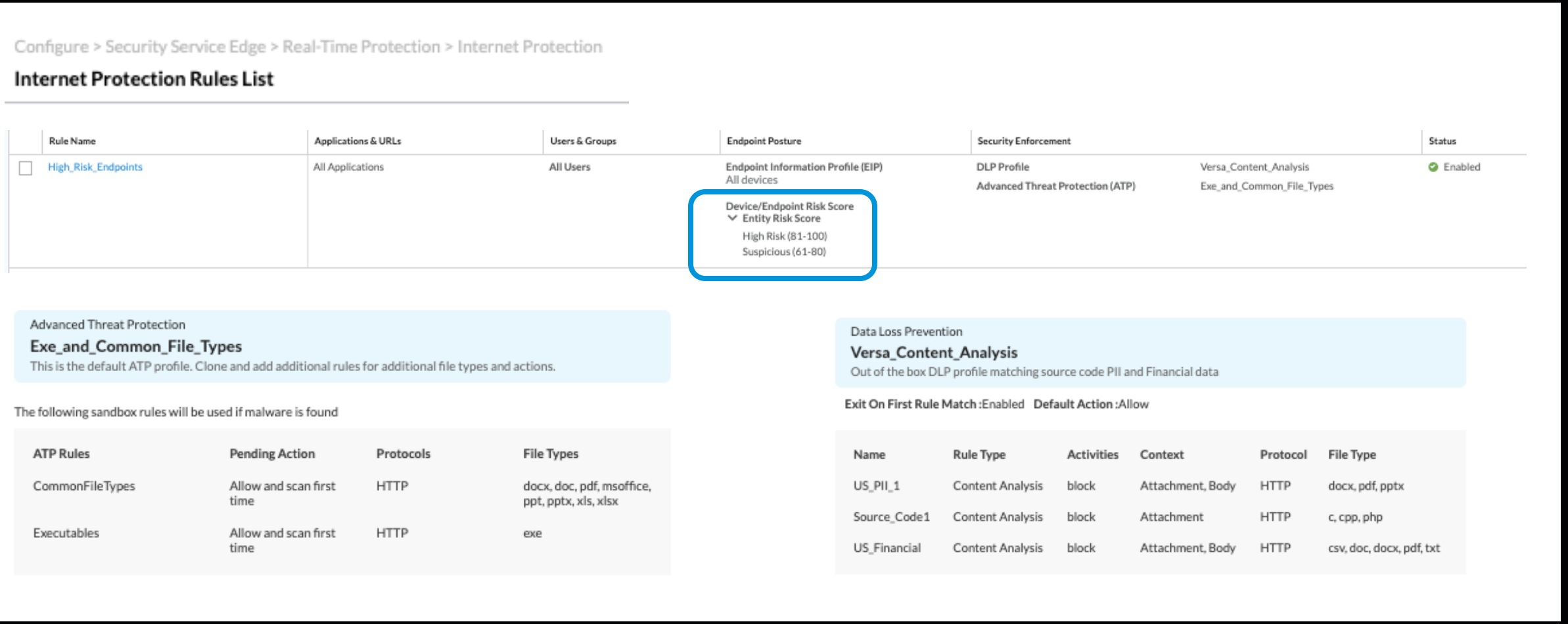
Concerto runs the full registration → first poll → publish cycle in about a minute

0 – 5 sec	1	**Register**	Connector registered, OAuth2 token obtained, polling thread started, risk profiles loaded into memory.
5 sec	2	**Pull**	First device list pull from the Microsoft Security Center/SentinelOne Security /CrowdStrike falcon API begins.
5 sec + collect	3	**Score**	Per-device vulnerability data fetched (up to 10 concurrent calls); ZTA / risk scores calculated and stored per device.
~1 min later	4	**Publish**	Aggregated scores published to VMS via Kafka; adaptive network policies take effect.
Every interval (10m – 24h)	5	**Repeat**	Full cycle repeats automatically; token refreshed transparently by the OAuth2 library.

VERSATILITY

Inspect risky users harder, not everyone

USE CASES: Unified Risk Score falls to high or suspicious, enforce Advanced Threat Protection, DLP for additional protection



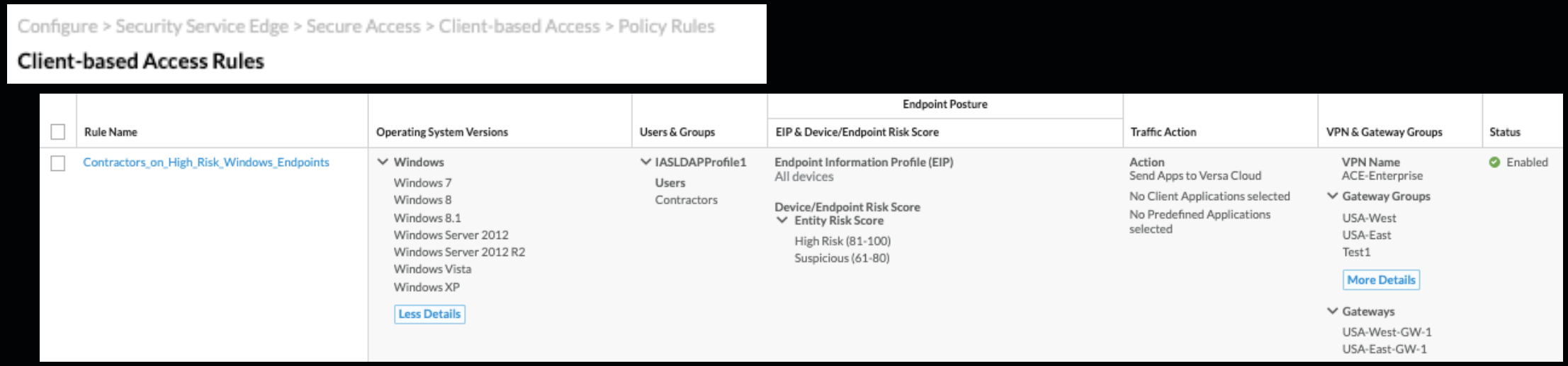
USE CASES

Tighten Secure Access for high-risk devices

High Risk Contractor user

Using Windows OS

When this user's Unified Risk Score falls to high or suspicious, send to the SASE gateway for additional inspection



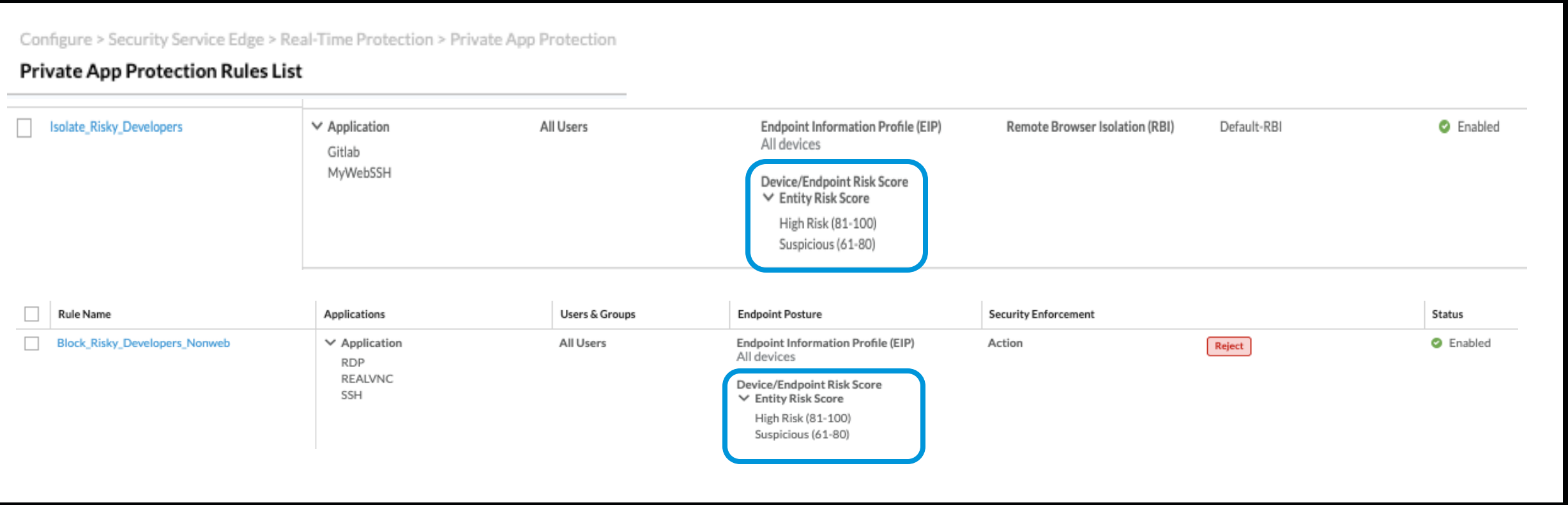
VERSATILITY

Quarantine compromised users on the private network

Isolate infected or Risky users accessing private/DC applications

Eg: Developers accessing WebSSH or their on-prem source code repo in gitlab – Isolate

Reject non-web applications like RDP, VNC, SSH from infected users



Actions based on the EDR agent check

Detect that EDR agent is installed and is enabled in the endpoint, if not, reject user

New EIP objects to check for the presence of CrowdStrike Falcon/SentinelOne/Defender

Eip-object-endpoint-security-installed-any – Check for any EDR

FULL AUDIT TRAIL

Every risk change and policy decision is logged in Versa Analytics

Timestamp	User / Device	Signal	Score change	Policy decision
10:42:18 UTC	**j.chen / MBP-7841**	S1: activeThreats 0 → 3	**Trustworthy → High**	Block ERP, force redirect to
10:43:02 UTC	**k.patel / WIN-2210**	Defender: missing patch	**Low → Moderate**	Allow with inspection, alert SOC
10:44:55 UTC	**m.lopez / MBP-9120**	S1: mitigationMode =	**Trustworthy → Suspicious**	Block code repos and prod admin
10:46:11 UTC	**j.chen / MBP-7841**	CRWD: threats remediated	**High → Low**	Restore full access

SentinelOne Integration and Use cases

VERSATILITY

SentinelOne – Critical Risk Indicators

Critical Risk Indicators (Default weightage in risk score: 80%)
This table indicates the mapping of SentinelOne critical risk attributes to Versa Risk Score
Eg: If activeThreats=6 or detectionState=disabled, the device has a high risk, with a 80% weightage given to these

activeThreats

Ransomware drops on a finance laptop

S1 detects 6 active threats → score jumps to High Risk → Versa blocks ERP and file-share access until SOC clears the host.

detectionState

Agent stuck in learning mode after re-image

Detection state = learning_mode → device drops to Suspicious → Versa requires ATP inspection for SaaS until full_mode resumes.

mitigationMode

Contractor laptop set to detect-only

mitigationMode = detect → score caps at Suspicious → Versa allows browsing but blocks code repos and prod admin tools.

mitigationModeSuspicious

Pen-test workstation tuned to detect-only on suspicious

mitigationModeSuspicious = detect → score = Moderate → Versa permits internal apps but routes all egress through inspection.

SentinelOne – Operational Health Indicators

This table indicates the mapping of SentinelOne Security operational health attributes to Versa Risk Score
Eg: lastActiveDate > 7 days, risk score is high with a 20% weightage, rest are nice to have parameters

firewallEnabled

Engineer disables host firewall to debug

firewallEnabled = false → score moves to High Risk → Versa blocks production VPN until firewall is re-enabled.

lastActiveDate

Sales laptop offline for 8 days during PTO

lastActiveDate > 7d → device flagged High Risk → Versa requires re-authentication and posture re-check on first login.

userActionsNeeded

Pending OS update + quarantined file alert ignored

userActionsNeeded = 2 → score drops to Moderate → Versa shows remediation banner and limits access to sensitive apps.

missingPermissions

macOS upgrade strips Full Disk Access from agent

missingPermissions = 3 → device flagged High Risk → Versa restricts to remediation portal until permissions are restored.

VERSATILITY

CrowdStrike Integration Actions based on Zero trust assessment score

VERSATILITY

Use Case: Windows ZTA Score Drop

SCENARIO

A finance user's Windows 11 laptop misses a Microsoft patch cycle and a local admin disables BitLocker to troubleshoot a slow boot. The CrowdStrike Falcon sensor reports the change and the device's Zero Trust Assessment score falls from 92 to 64.

WINDOWS TRIGGERS LOWERING SCORE

- BitLocker disabled on the system volume
- Missing OS security update / out-of-date Defender signatures
- UAC weakened, Secure Boot off, or firewall profile disabled

VERSA SASE POLICY ACTION

- Versa pulls the new ZTA score via /zero-trust-assessment/entities/assessments/v1 and refreshes the device's Unified Risk Score
- Access to finance SaaS apps (ERP, payroll) is automatically downgraded to read-only and routed through full SSL inspection
- User receives a step-up MFA prompt; full access restores once the score returns above 80

Use Case: macOS ZTA Score Drop

SCENARIO

A developer running macOS Sonoma on a MacBook Pro disables FileVault and the built-in Application Firewall while debugging a kernel extension. CrowdStrike Falcon detects the posture change and the device's Zero Trust Assessment score drops from 88 to 59.

MACOS TRIGGERS LOWERING SCORE

- FileVault disk encryption turned off
- Application Firewall or Gatekeeper disabled; SIP weakened
- OS minor version behind, XProtect / MRT definitions out-of-date

VERSA SASE POLICY ACTION

- Versa retrieves the updated ZTA via the CrowdStrike Falcon API and recalculates the Unified Risk Score in real time
- Access to source-code repos and CI/CD consoles is blocked; general SaaS traffic forced through SWG with DLP inspection
- Access auto-restores once FileVault & firewall are re-enabled and the score recovers

Microsoft Defender for Endpoint

VERSATILITY

MICROSOFT DEFENDER

Defender risk attributes in action

How Defender for Endpoint signals translate into Versa policy decisions

DEFENDER FOR ENDPOINT (20% WEIGHTAGE)

Versa pulls riskScore + machineHealthState; CVE data fetched from Defender Vulnerability Management

riskScore = High

Defender flags a developer laptop with multiple alerts

Live behavioral signals push riskScore to High → device classified High Risk → Versa blocks code repos and admin tooling, allows only remediation portal.

machineHealthState = inactive

Sales rep's laptop hasn't reported in 5 days

machineHealthState = inactive → device degrades to Suspicious → Versa enforces step-up MFA and disables direct internal-app routing.

exposureLevel = High

Critical CVE pending on a finance workstation

Defender VM flags exposureLevel = High → device drops to Moderate → Versa restricts ERP to read-only and forces all egress through SWG+DLP inspection.

onboardingStatus = unsupported

Contractor laptop never fully enrolled in Defender

onboardingStatus = unsupported → device flagged High Risk → Versa blocks SaaS access and routes user to remediation page until onboarding completes.

Unified Endpoint Management Integrations

Microsoft Intune
Ivanti Neurons

VERSATILITY

EDR vs UEM

Defender for Endpoint vs Unified Endpoint Management

They answer different questions. Versa fuses both into one risk decision.

DEFENDER FOR ENDPOINT

Threat & vulnerability signal

Answers: "Is this device under attack or exposed?"

- Active threats, alerts, and behavioral detections
- Device risk score (Low → High) from EDR telemetry
- Vulnerability exposure: CVEs, missing patches, weak config
- Machine health: agent active, signatures current

INTUNE / IVANTI UEM

Management & compliance signal

Answers: "Is this device managed and compliant with policy?"

- Enrollment state: corporate-owned, BYOD, or unmanaged
- Compliance verdict: encryption, OS version, passcode, jailbreak
- Configuration profiles: VPN, Wi-Fi, certificates, app allowlists
- App and OS lifecycle: installed apps, patch level, ownership

VERSA UNIFIED RISK SCORE

EDR threat posture × UEM compliance posture → one score that drives every access decision.

UEM Integration Problems to Solve

Bring Versa SASE and your UEM into one compliance loop

THE PROBLEM

Stand up UEM across Ivanti Neurons and Intune in one place

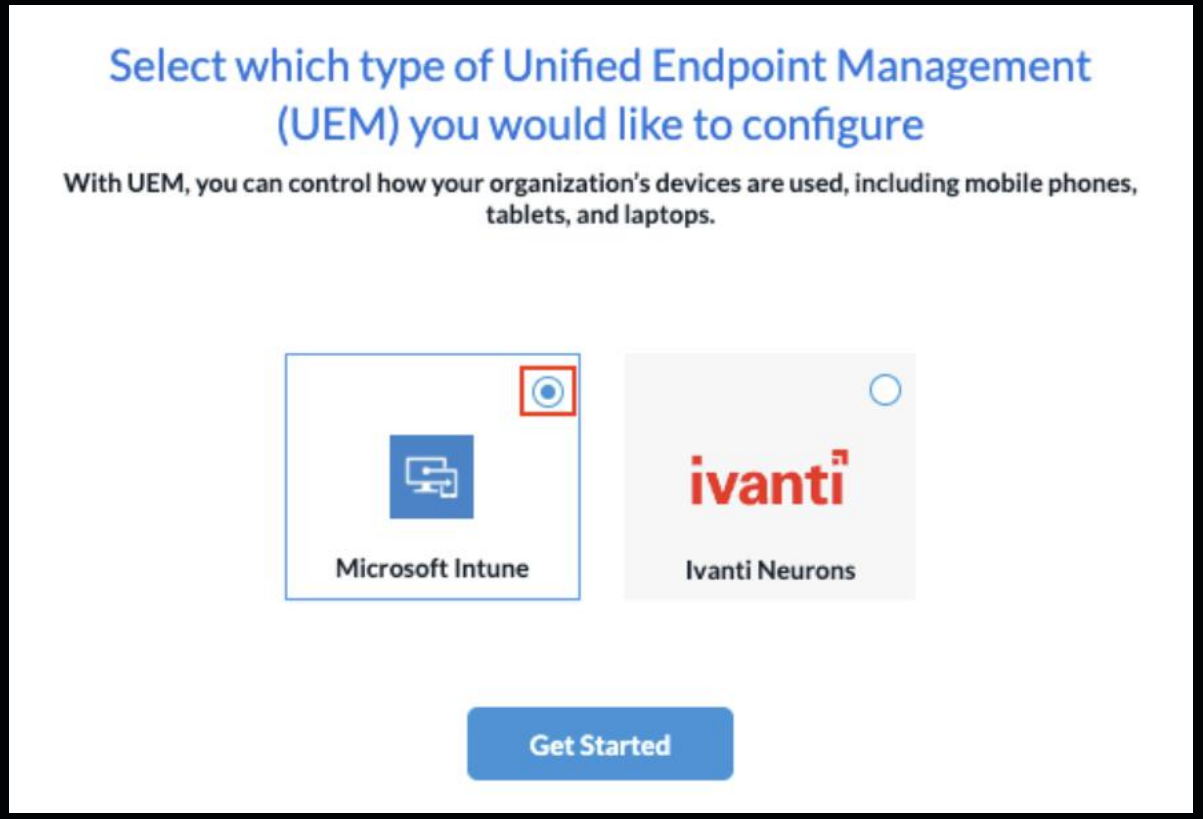
Use real-time device posture to gate Versa SSE access

WHAT VERSA SOLVES

Posture flows from UEM into dynamic per-user policy

End-to-end security from endpoint to network to app

Push and update the Versa SASE client through UEM



VERSATILITY

INTUNE IN ACTION

Compliance becomes the access policy

One UEM profile, two outcomes — built directly into Secure Access policy rules

Configure › Security Service Edge › Secure Access › Client-based Access › Policy Rules › Endpoint Posture

COMPLIANT DEVICE

Sales laptop, fully patched, encrypted

Intune reports Managed + Compliant → policy rule with Endpoint Posture = Compliance matches → VPN session established, full access to internal apps.

NON-COMPLIANT DEVICE

Contractor laptop, missing patch

Intune reports Managed + Non-Compliant → policy rule with Endpoint Posture = Non-Compliant matches → restricted access; user redirected to remediation portal.

CRITICAL

Set the Certificate Issuer in Client Configuration — without it the client never sends the device ID, and policy never matches.

Versa + Ivanti MDM

Unified Endpoint Security & Policy Enforcement

HOW IT WORKS

Ivanti MDM Console API

↓

EIP Object Evaluation

↓

Risk Score Update

↓

Adaptive Policy Applied

Enforced via Endpoint Information Profile (EIP)

Mass Client Deployment

Push Versa SASE client to all endpoints via Ivanti MDM app catalog — silent enterprise deployment at scale

MDM Health Check

Verify Ivanti agent is installed, configured, and actively running on the endpoint

MDM Version Gate

Check agent version against minimum threshold — block or restrict access if below required version

Compliance-Based Policy

Map Ivanti compliance status per user/device to Versa risk score — apply differential ZTNA/SWG tiers

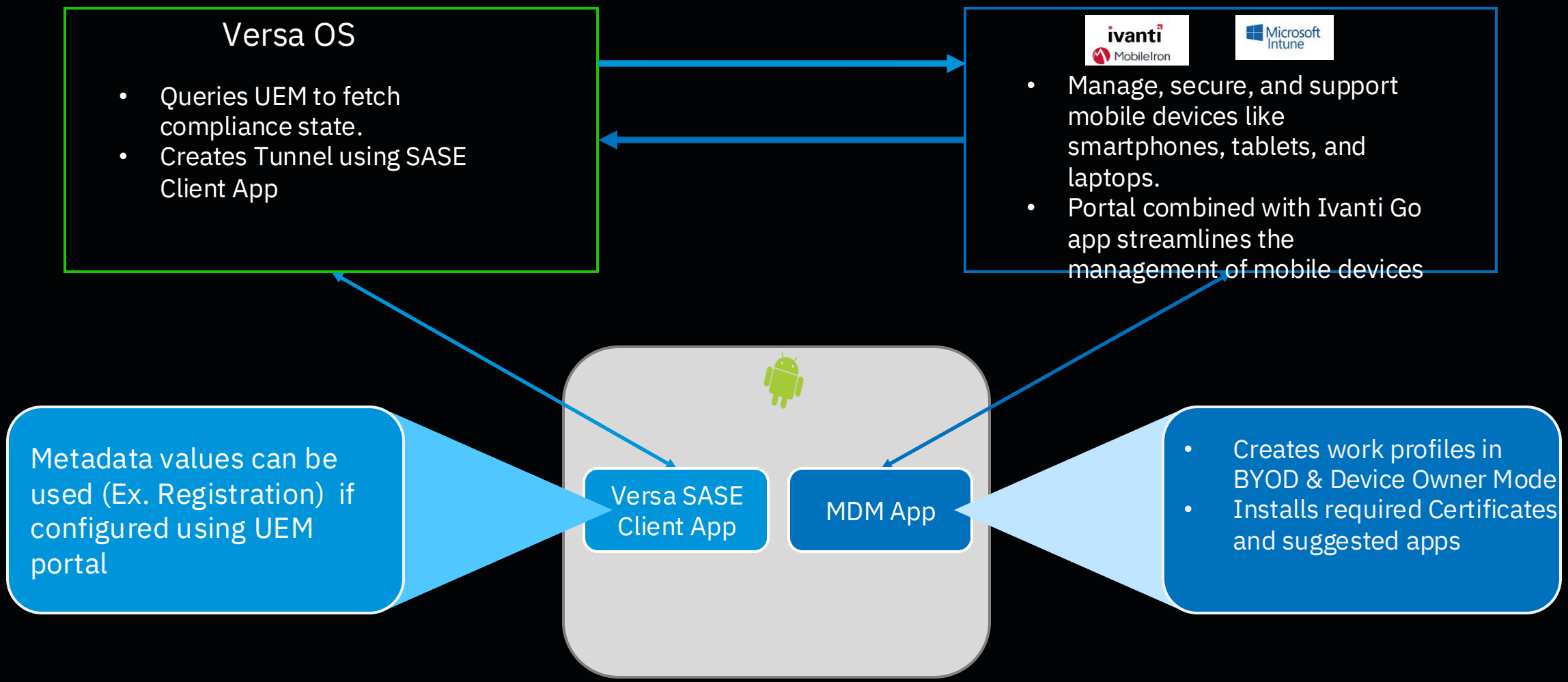
Privilege & Encryption

Detect lost admin privileges or decrypted disk — trigger step-up auth or quarantine policy

Out-of-Contact Detection

Device not checked in beyond threshold → treat as unmanaged, apply restrictive fallback policy

UEM Integrations - Versa SASE



ENROLLMENT MODES

Two modes, every modern device

Match the right enrollment posture to who owns the device

BYOD

Personal devices

Work data stays separate from personal data.

Android	**Work Profile**
iOS / iPadOS	**User Enrollment**

Privacy-preserving — IT manages the work container only.

Fully Managed

Corporate devices

Organization owns the device end to end.

Android	**Device Owner Profile**
iOS / iPadOS	**Device Enrollment**

Full control — apps, network, restrictions, remote wipe.

CLIENT ROLLOUT

Mass-distribute the SASE client

Push Versa to thousands of devices through Ivanti r Intune— zero touch, zero tickets

1

Package

Upload the Versa SASE client to the Ivanti app catalog with a signed config.

2

Target

Assign by group, OS, or device posture — corporate, BYOD, contractor.

3

Deploy

UEM silently installs and configures on every device in scope.

Net result

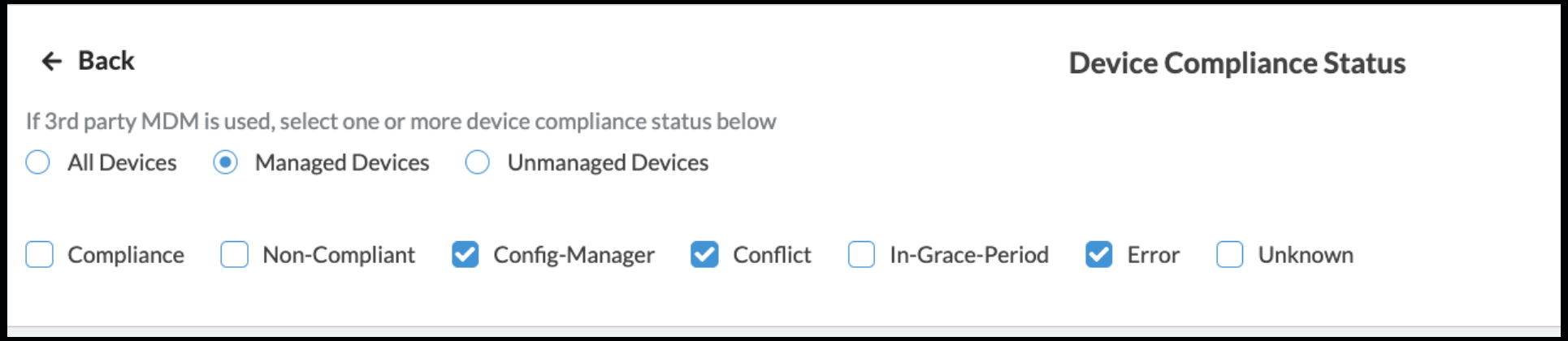
Thousands of devices secured in hours, not weeks — without touching a single endpoint.

VERSATILITY

Check device compliance and enforce security

Rule Name	Operating System Versions	Users & Groups	Endpoint Posture: Device Compliance Status	Traffic Action	VPN & Gateway Groups	Status
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



VERSATILITY

POSTURE-AWARE ACCESS

Compliance becomes the access policy

UEM checks device health. Versa decides what that device can reach.

COMPLIANT

Full access, frictionless

- OS patched, disk encrypted, MDM healthy
- Versa applies trusted-device policy
- Direct path to SaaS, internal apps, sensitive data
- User never sees a step-up prompt

NON-COMPLIANT

Reduced access, automatic

- Posture check fails — jailbreak, missing patch, etc.
- Versa downgrades to limited policy in real time
- Sensitive resources blocked; remediation page served
- Logs and alerts route to SOC instantly

VERSATILITY