VERSATILITY

Identity in Versa Solution

Connect. Secure. Simplify.

Rahul Vaidya

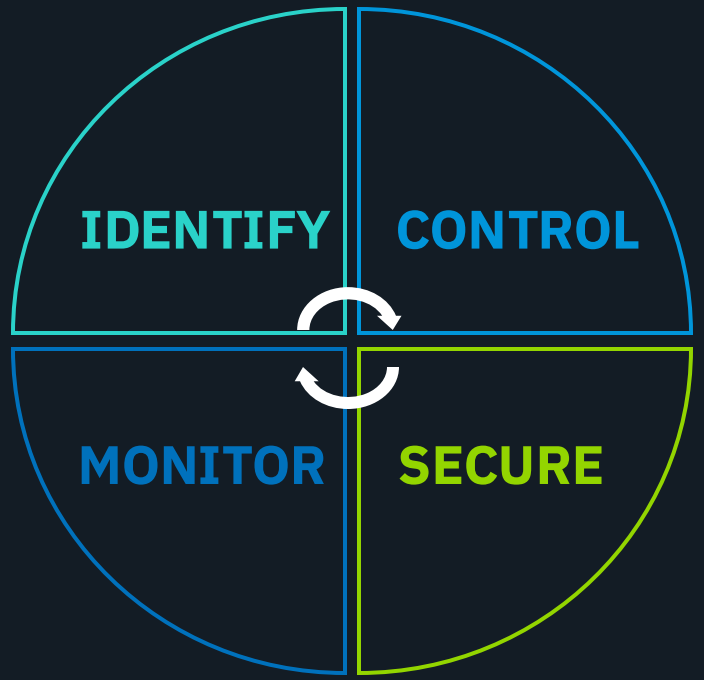
Director, Product Management

Agenda

How to leverage Identity for better security and better user experience

Secure SDWAN

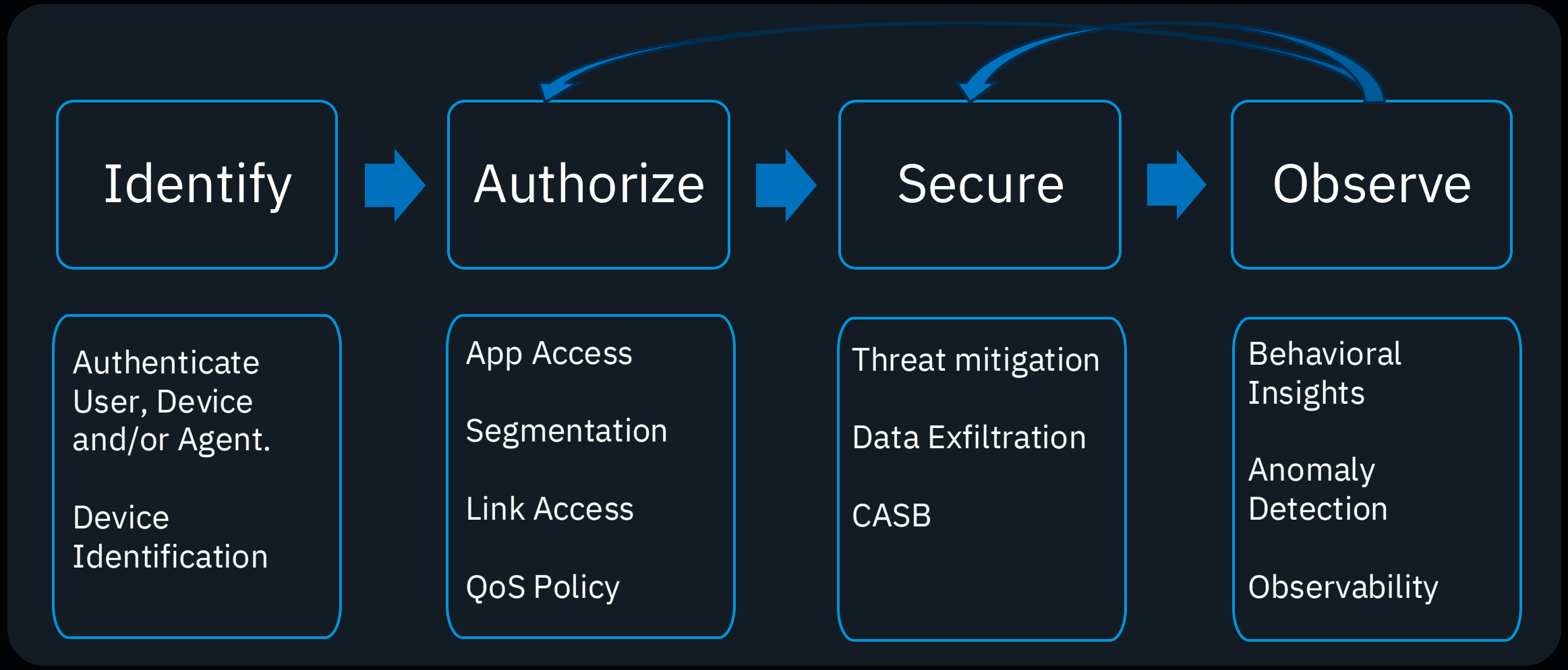
SSE



NGFW

SD-LAN

Identity is the anchor for Intelligent Secure Network

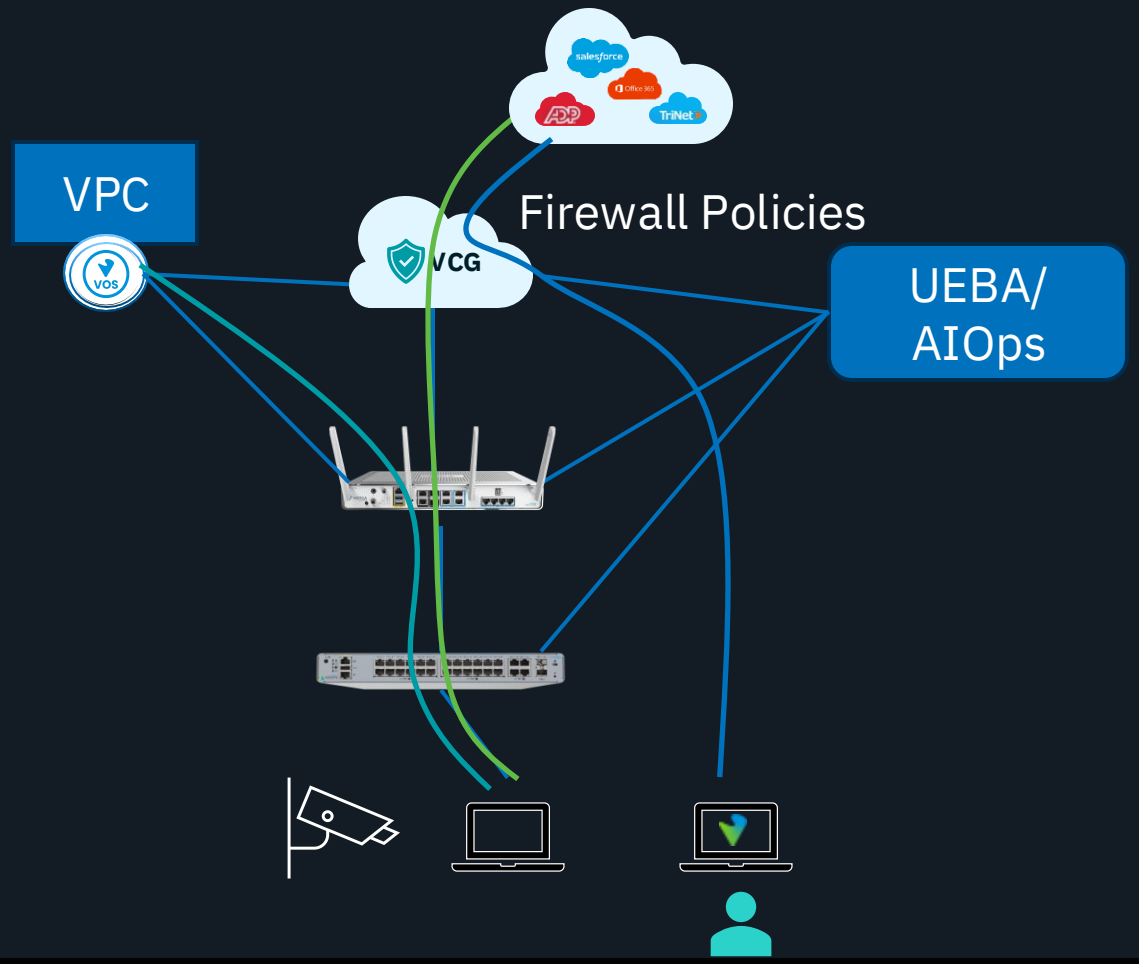


Identify

- User Authentication
  - User ID, IMSI (Mobile)
  - Group Membership
- Device Authentication
  - Device Authentication
  - MDM
- Agent Authentication

Policy follows the User

- User/Device is Remote
  - SSE for Internet Security
  - SSE for ZTNA Policies
- User/Device/Agent is in branch
  - LAN, CPE or SSE for Internet Security
  - LAN, CPE for ZTNA Policies
  - LAN or CPE for Segmentation
  - CPE for QoS and Traffic Steering

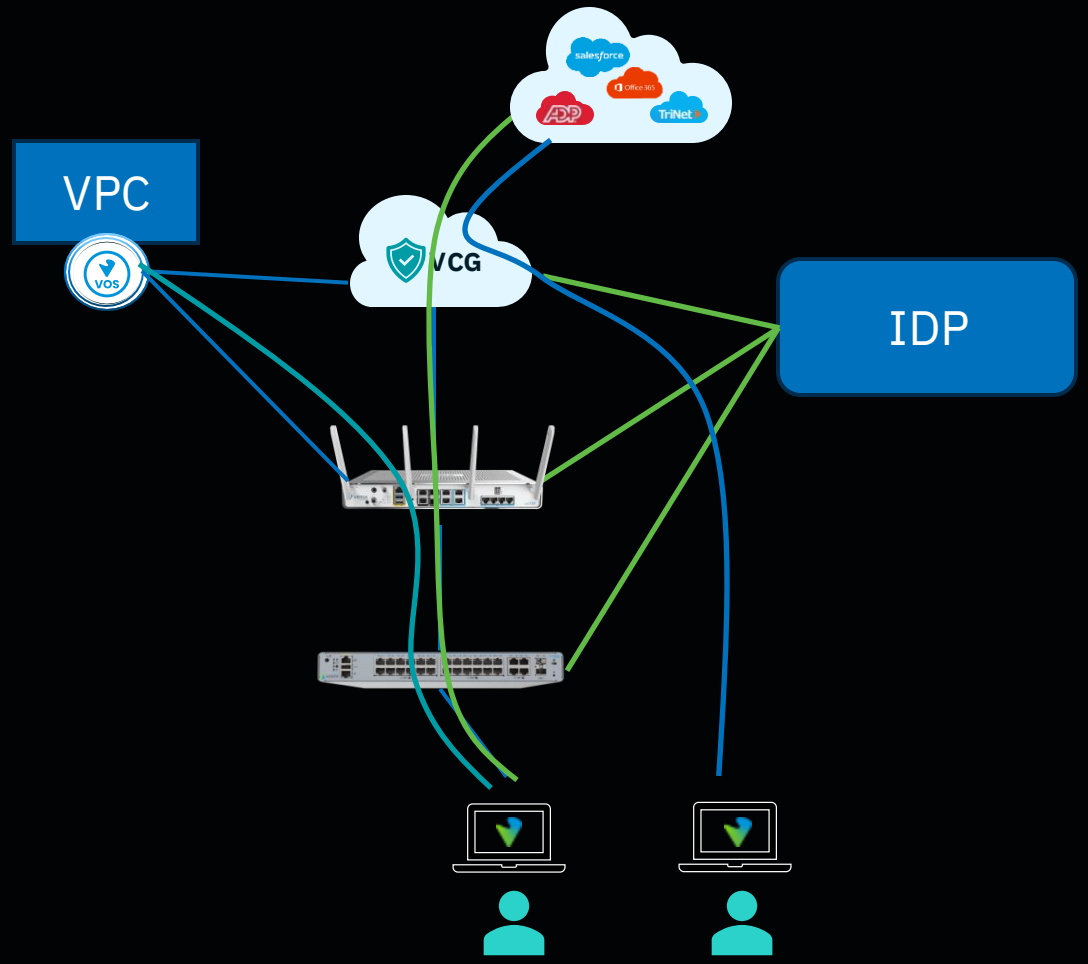


User Auth

VERSATILITY

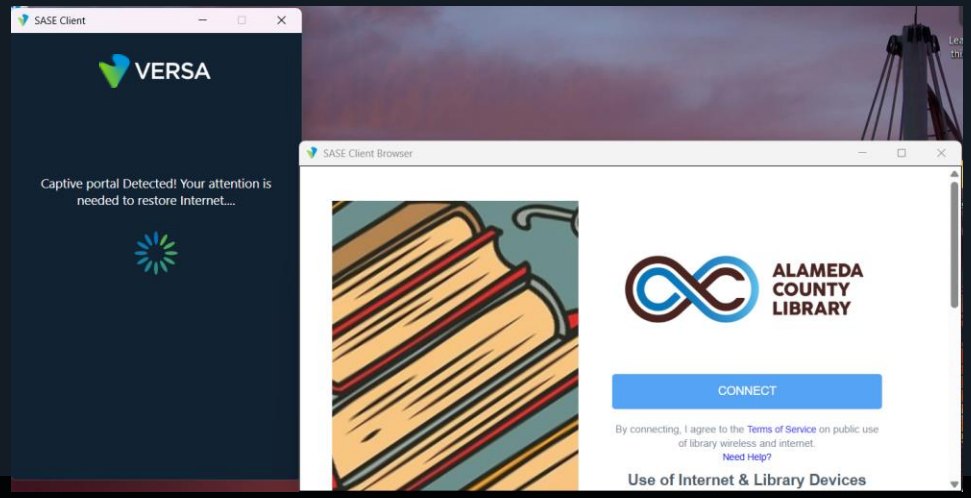
Versa Client based Authentication

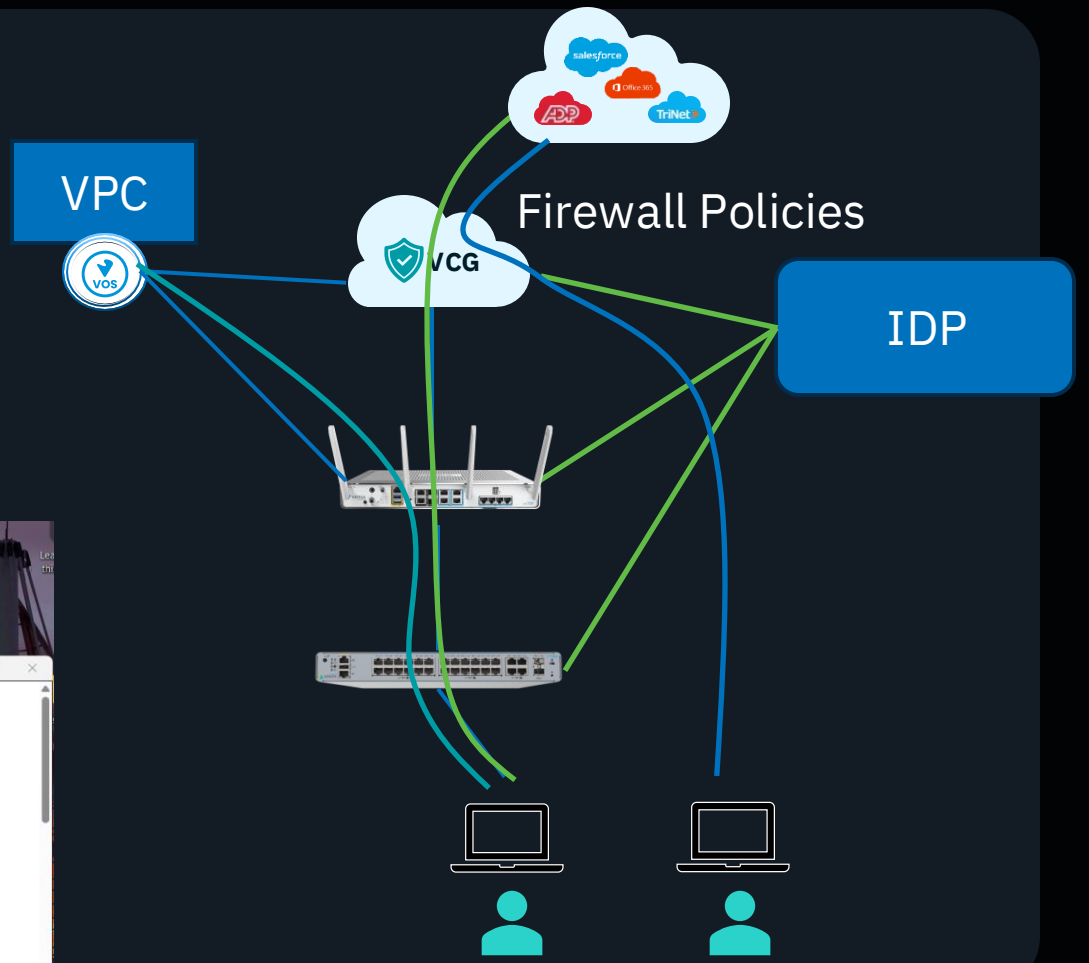
- Device has Versa Client
- LDAP, SAML or RADIUS based authentication
- VOS configured as Registrar. TND disables tunnel if user in trusted domain
- Client authenticates with the first VOS on the network (Switch, CPE, VCG in that order)



Captive Portal Based Authentication

- Captive Portal Detection on Browsers and IOS/Android
- Use SAML, LDAP or RADIUS to authenticate the user





SCIM: Automated User Provisioning

What It Is

System for Cross-domain Identity Management — an open standard (RFC 7643/7644) for syncing user identities between your IdP and downstream apps via REST + JSON.

How It Works

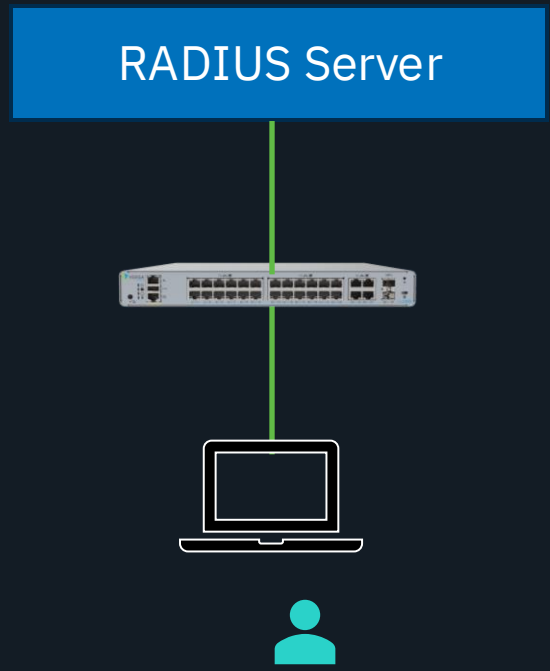
When HR or IT changes a user in the source of truth, SCIM pushes create, update, and delete events to every connected app — keeping accounts, attributes, and group memberships in sync automatically.

Why It Matters

Eliminates manual onboarding/offboarding, closes the gap on orphaned accounts after termination, and cuts identity admin overhead — critical for security, compliance, and scale.

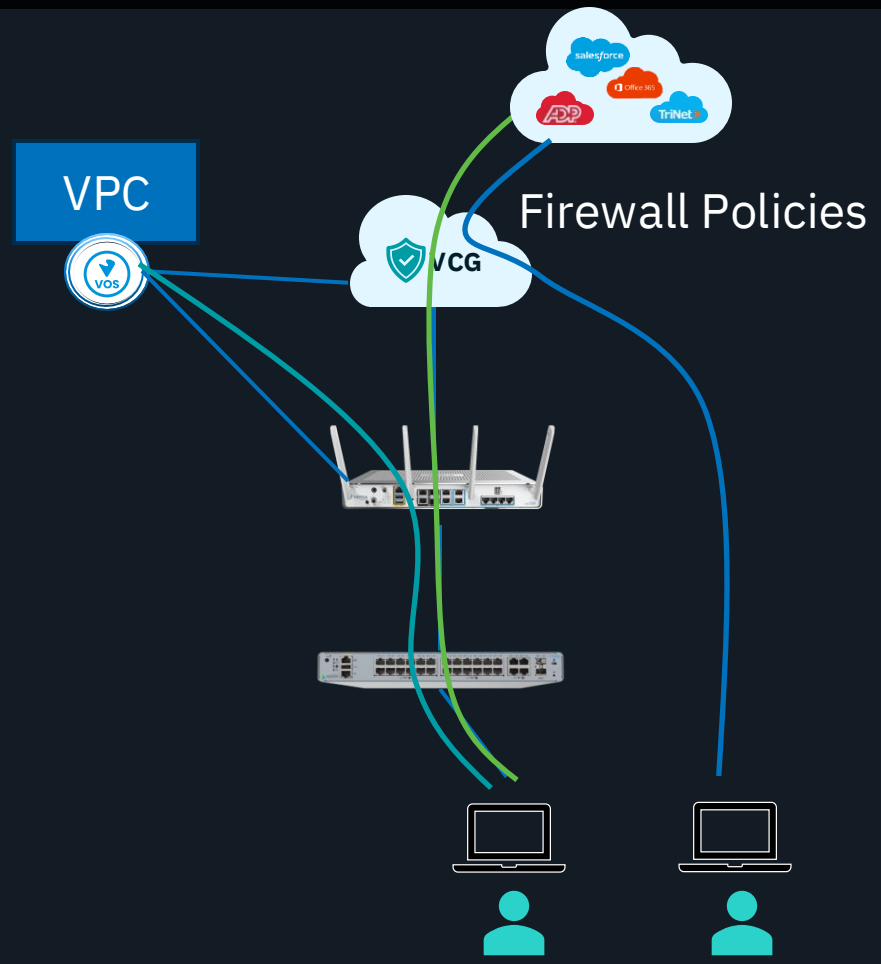
802.1x Authentication

- Use 802.1x/RADIUS to Authenticate users
- MAC Address Bypass to allow Non-User Devices



Certificate based User Authentication

- Why Certificate based Authentication is superior
  - No password on the wire
  - Prevents MITM attacks
  - Protects against attacks on the OS
- Disadvantages
  - Enrollment complexity

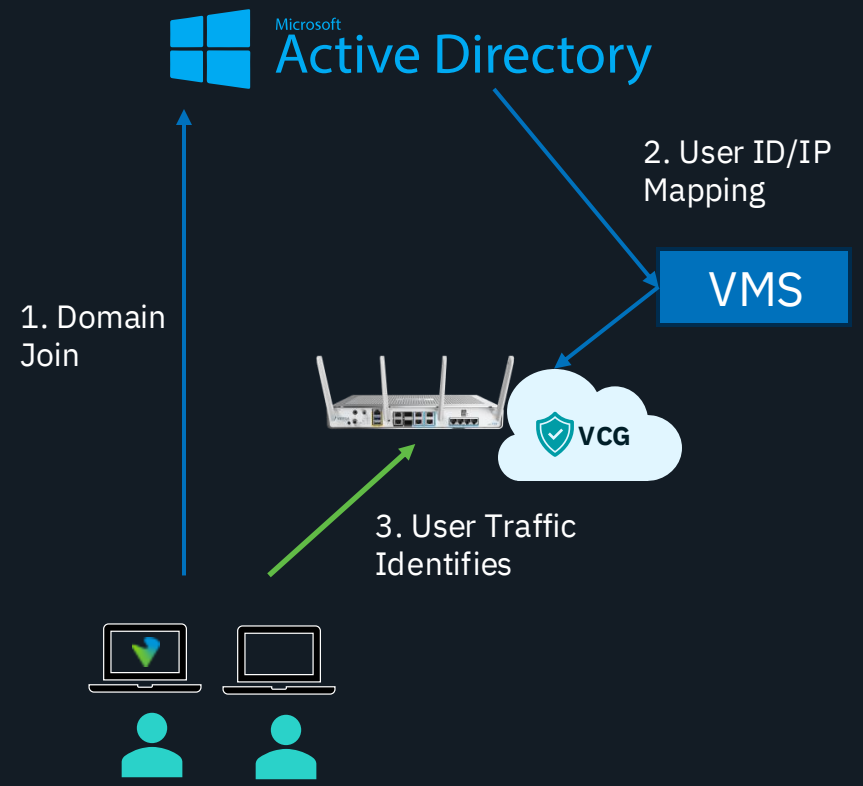


Passkey/CAC

- Overcomes the enrollment shortcoming of Certificate based authentication
- Uses hardware based assurance for storing keys
- Passkey is based on FIDO2 standard. Suitable for Enterprise/Consumer
- CAC is based on NIST standard. Suitable for Federal, Regulated space

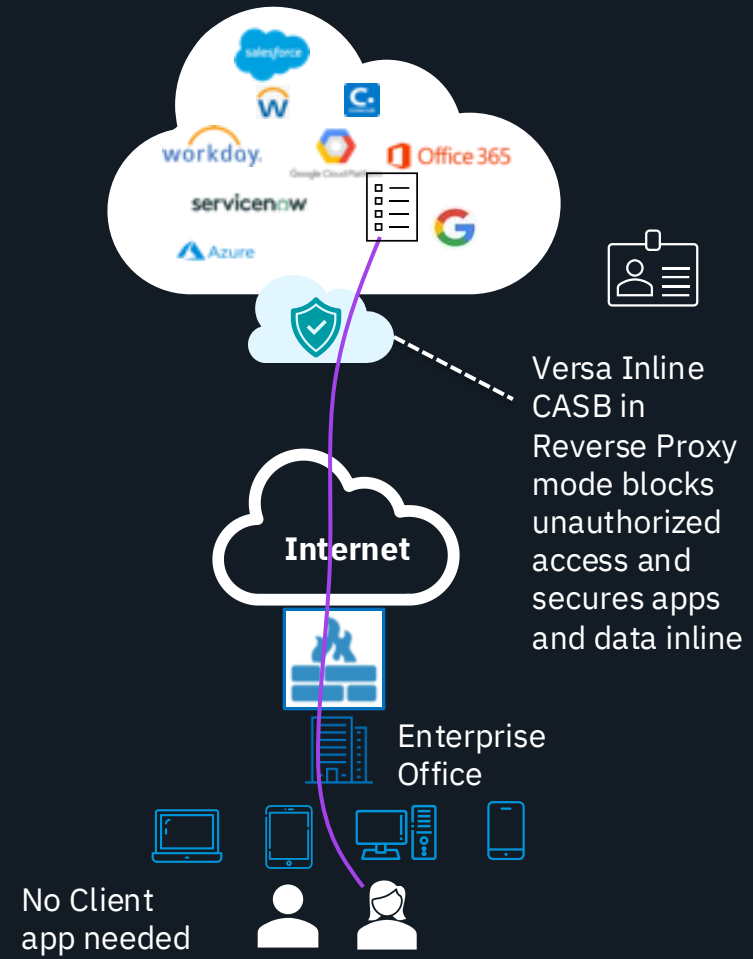
Passive Authentication

- Applicable for domain joined devices
- CPE/VCG automatically obtain User ID to Private IP mapping
- Leverages VMS for scalable distribution
- Supported for AD, Panorama



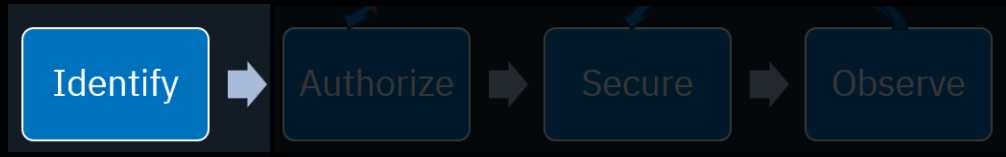
Securing Clientless connection to SaaS

- Problem Statement: User uses personal device to access SaaS. How to force the access to be authorized by firewall?
- Answer: Reverse Proxy and Identity proxy



Device Auth

VERSATILITY

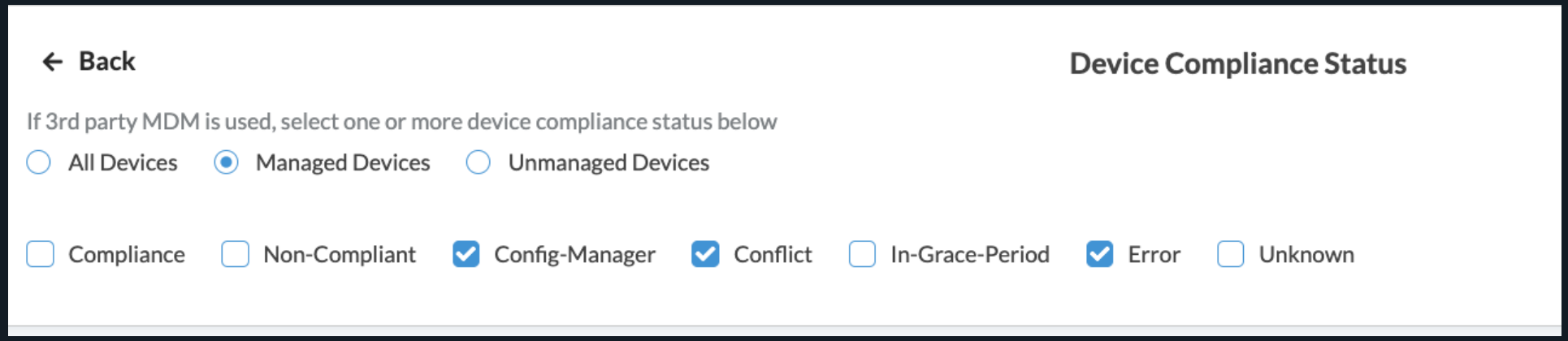


Device Authentication as MFA

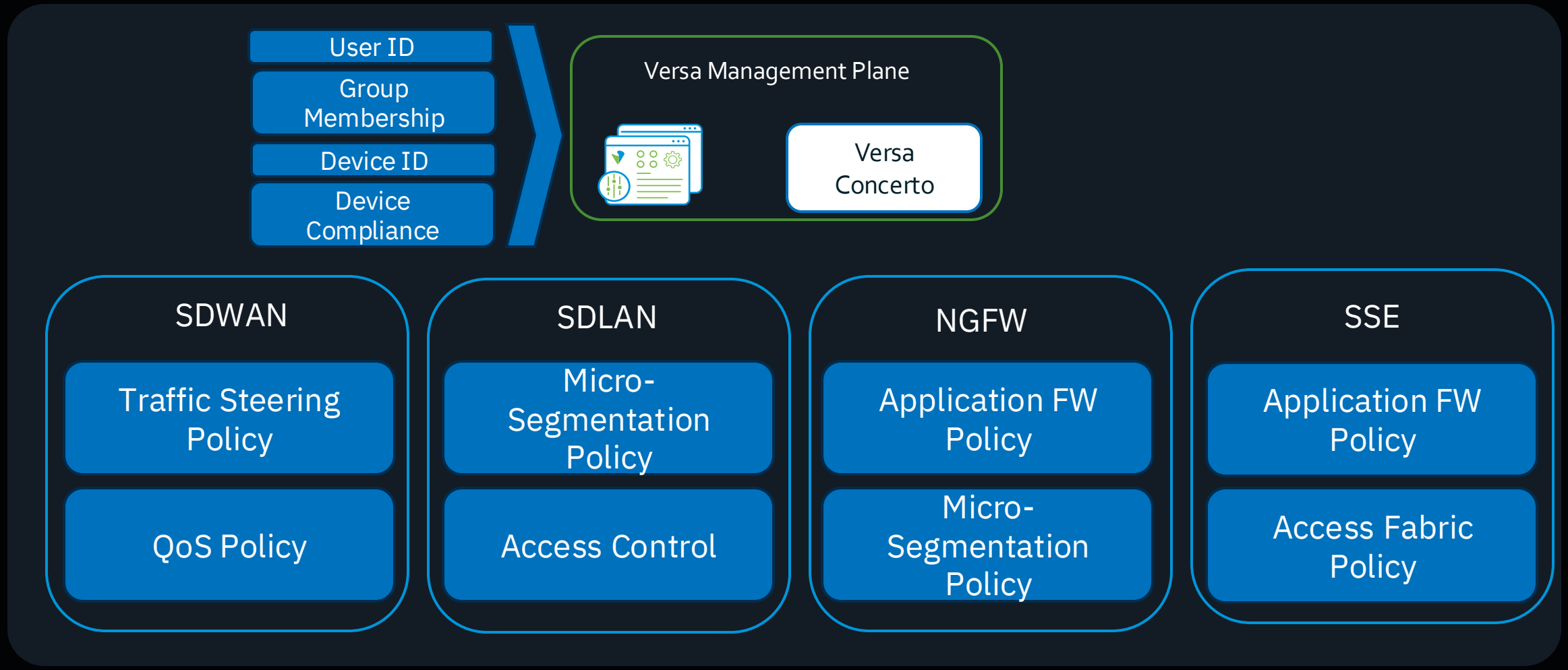
- In addition to user authentication, you can enable device authentication
- Define policies based whether authorized device is used to access the network
- Certificate based Authentication/MTLS

MDM Integration

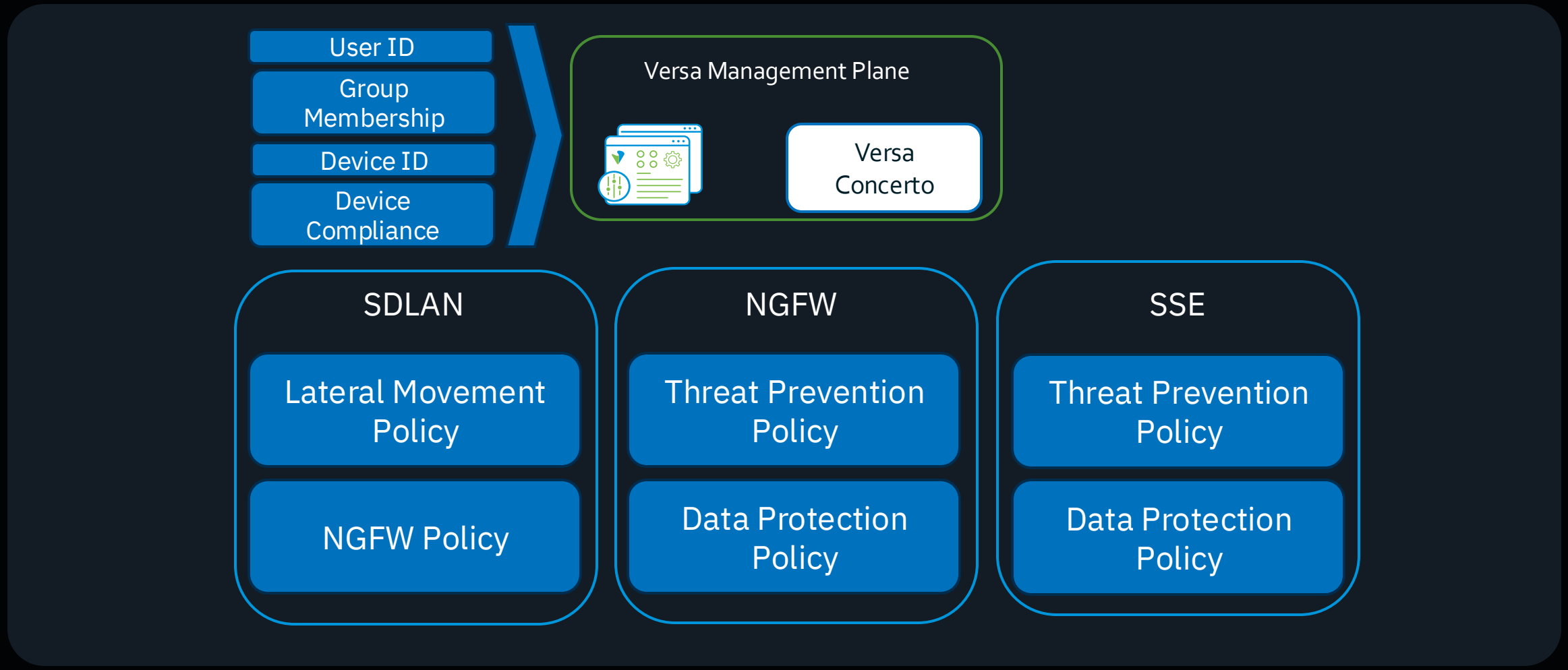
- Device Serial Number is used to “Authenticate” device with MDM
- Validate the device status using MDM
- Supported for Intune



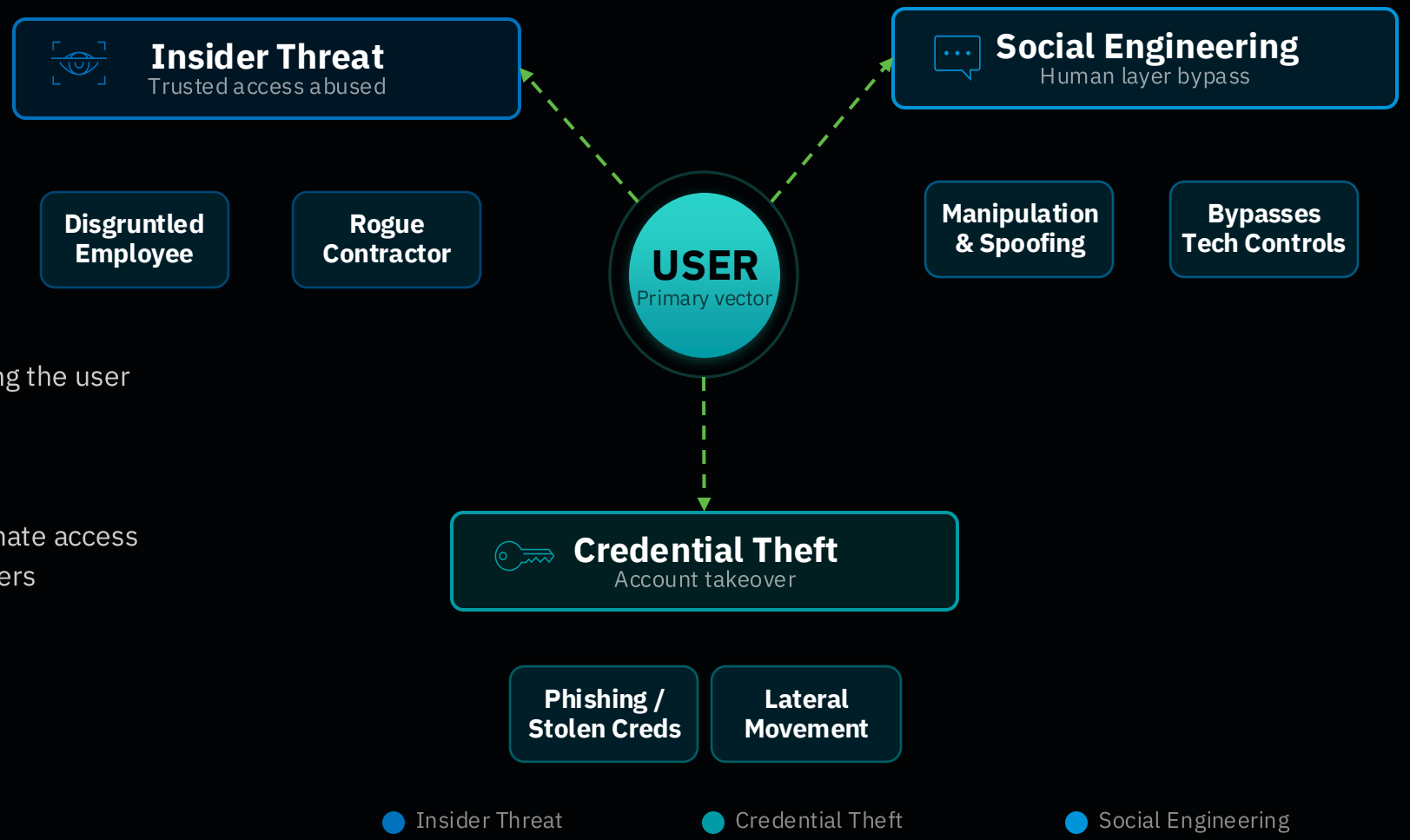
Authorization & Prioritization



Secure



User: The Most Critical Attack Vector



Why is the User Identity important?

Every attack vector converges on user behavior. Monitoring the user is the single most effective detection strategy.

- Users are the weakest link in the security chain
- Malicious or compromised insiders already have legitimate access
- User accounts are the primary target of external attackers

82% of breaches involve the human element

Source: Verizon DBIR 2024

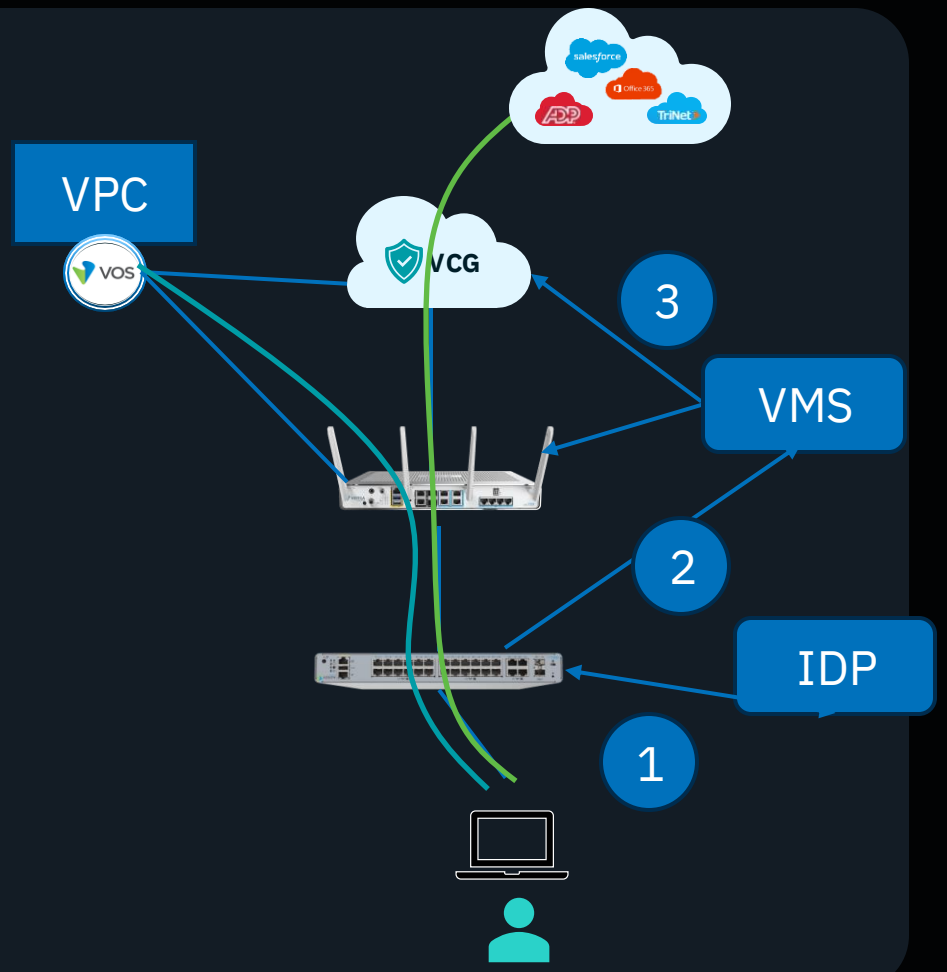
VERSATILITY

Roadmap

VERSATILITY

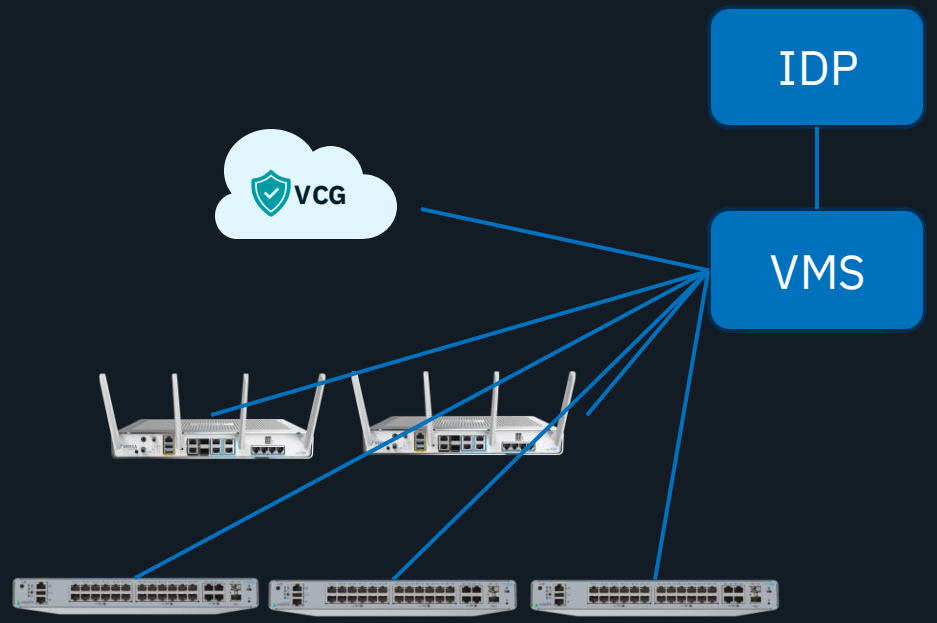
Seamless Authentication

- User Authenticates with SD-LAN
- User ID to IP Address mapping is shared with rest of Versa Ecosystem (SDWAN, SSE)
- SD-WAN and SSE apply user specific policy for traffic



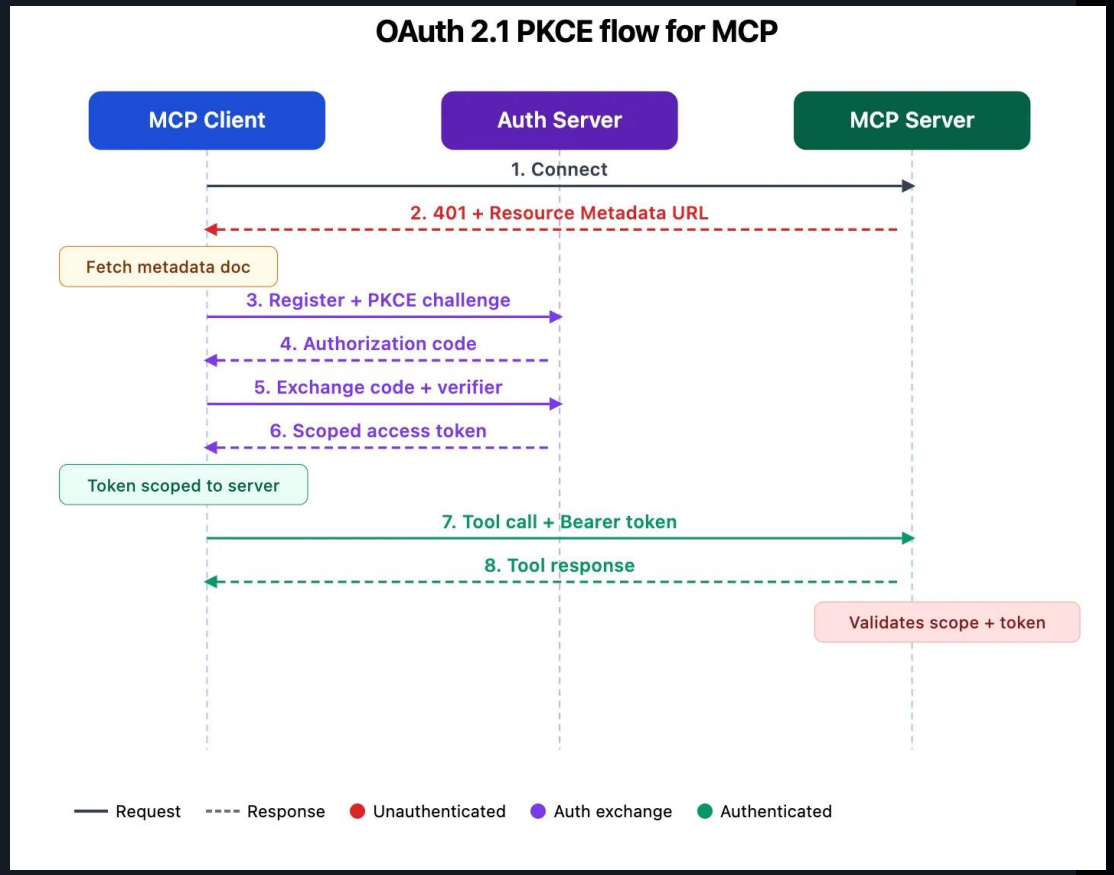
Authentication Proxy

- Integrating individual elements with IDP is configuration intensive
  - Certificate management is cumbersome
  - Migration to IDP is complex
- VMS as Auth Proxy will simplify Ops
- VMS is single point of integration with IDP



Agentic Security

- Oauth 2.1 enforces centralized authentication and authorization
- Integrates with Enterprise IDP
- Role based scopes per MCP Server
- Short lived tokens with restricted scope



* https://www.truefoundry.com/blog/mcp-authentication

Agentic Identity Security

Securing the lifecycle of every AI agent on your network

Discover & Inventory

Auto-detect every AI agent, MCP server, and tool call traversing the network. Build a real-time inventory of human, machine, and agent identities.

Authenticate & Authorize

Issue cryptographic agent identities. Enforce least-privilege scopes per tool, per dataset, per task — with delegation chains tied to the originating user.

Runtime Enforcement

Inline policy on every agent action: block prompt injection, exfiltration, and unauthorized tool use. Inspect MCP and API traffic at line rate.

Audit & Forensics

Full session lineage — prompts, tools invoked, data accessed. Tamper-evident logs ready for SOC, compliance, and incident response.

Conclusion

- Versa offers different mechanisms to authenticate the users and device
- You can Implement user authentication in Secure SDWAN, SSE and SD-LAN
- Implement User/Group based policies for SDWAN And Security

VERSATILITY