VERSATILITY

Privileged Remote Access

Connect. Secure. Simplify.

Rahul Vaidya

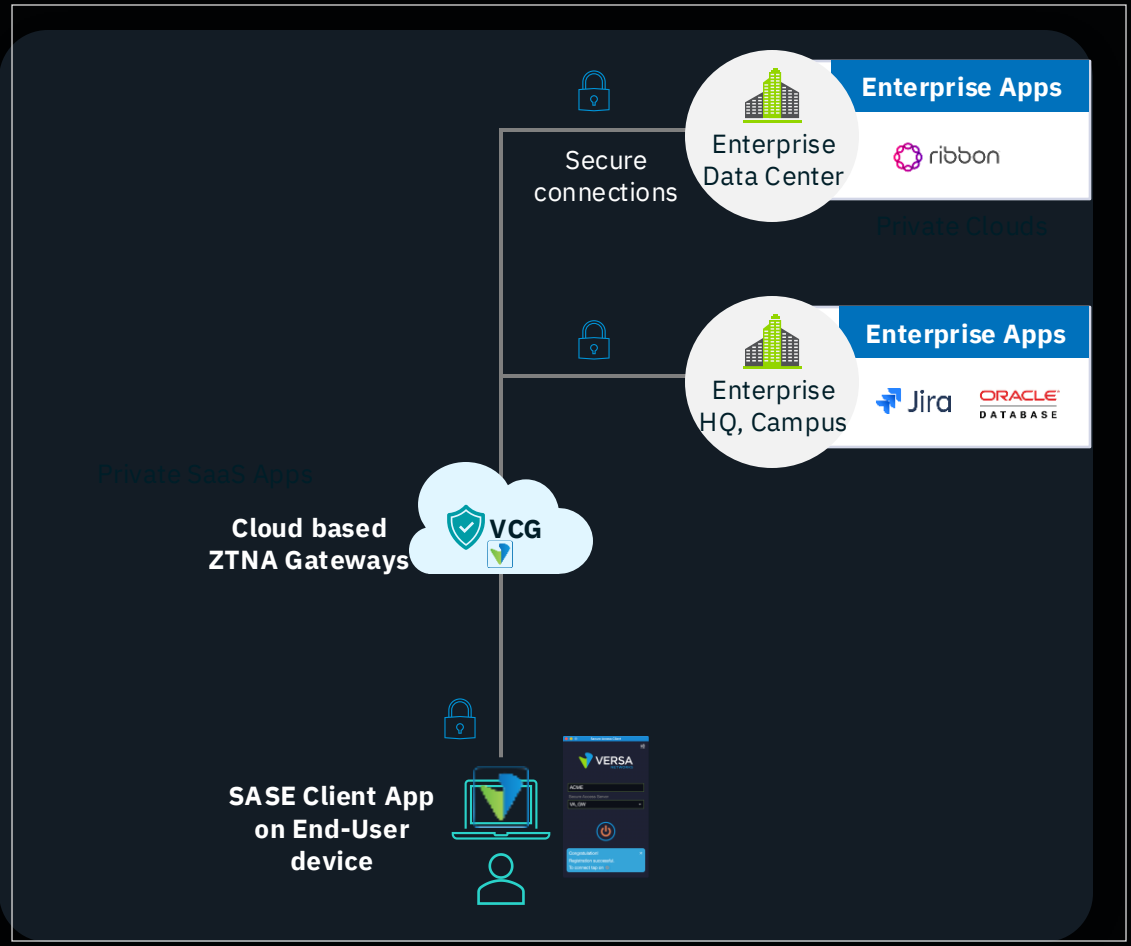
Director, Product Management

Purushothaman Balakrishnan

Senior System Test Manager

Characteristics of Zero Trust Architecture

- Identity and Context based Access
- Principle of Least Privilege
- Application Segmentation
- Continuous Posture Verification



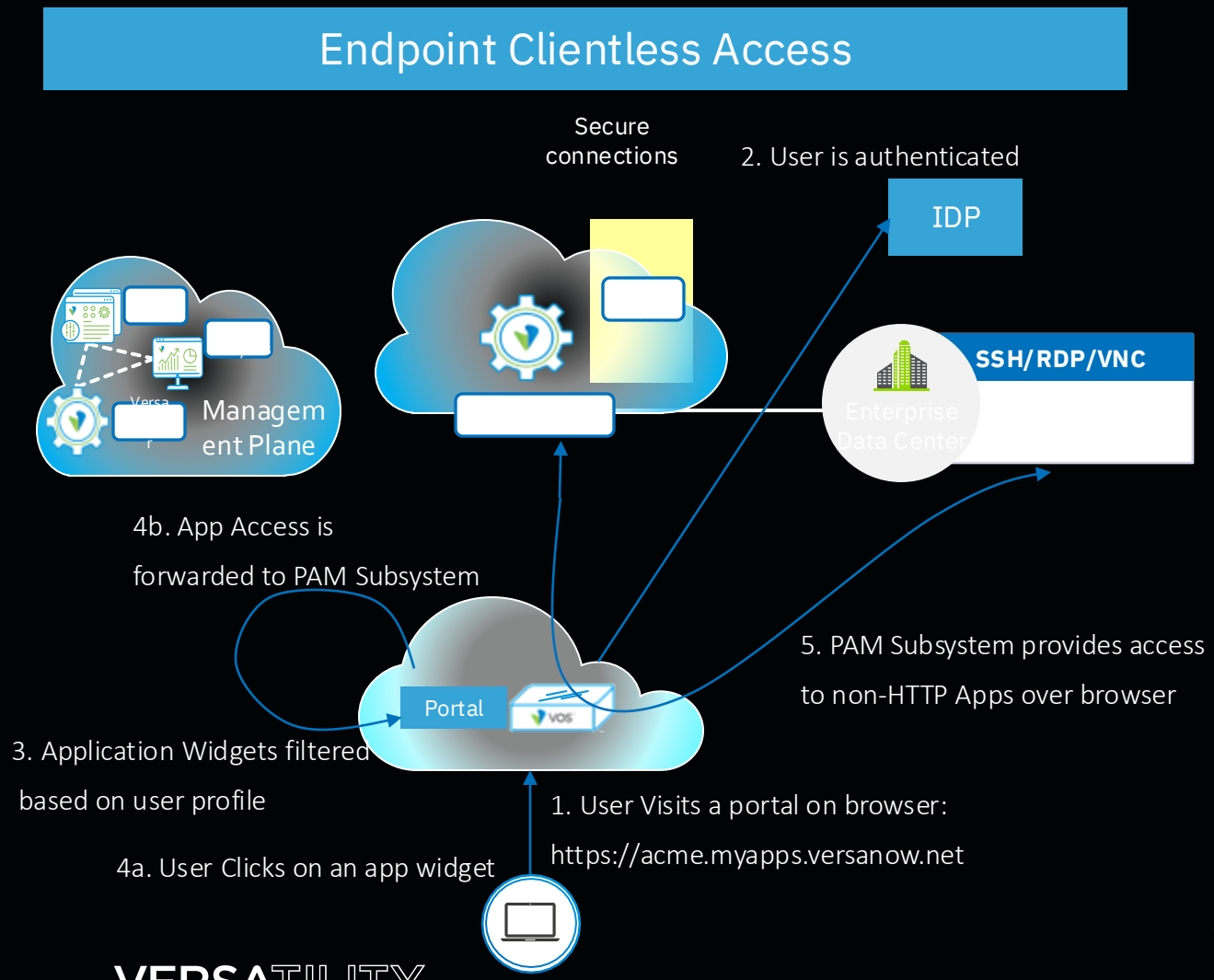
Need for Client-less Access to Private Applications

- Use Case 1: (In)Feasibility of Deploying Client
  - Example: Contract Employee using personal or employer device
- Use Case 2: (Un)Trustworthy-ness of the user –set
  - Auditors or consultants requiring to access only specific assets for short period of time
- Use Case 3: (Special) security for High Value Assets
  - Critical Applications which needs additional layer of security

Versa Privileged Remote Access Capabilities

- Client-less Browser based access to HTTP(s)*, SSH, RDP and VNC Applications
- Zero Trust Access without installing Client
- CASB functionality: Granular Control of actions allowed within SSH/RDP/VNC
- Credential Injection: SSH/RDP/VNC do not need to be integrated with IDP for each user

Client-less Access: User View



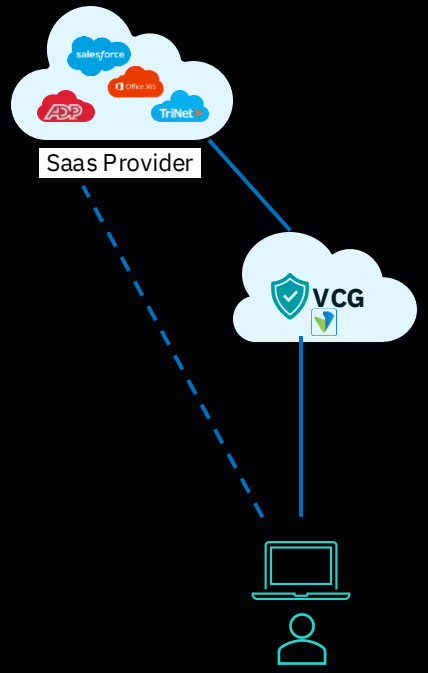
1. User visits into Portal using a browser (e.g., https://acme.versanow.net)
2. User gets authenticated with Enterprise IDP
3. User gets presented with applications authorized for specific user. Each app is a widget
4. User clicks on the widget to access the application
5. User is allowed access to the application via the browser
6. Any activity (within the application) not authorized for the user is automatically blocked.

* PRA Portal – Privileged Remote Access Portal

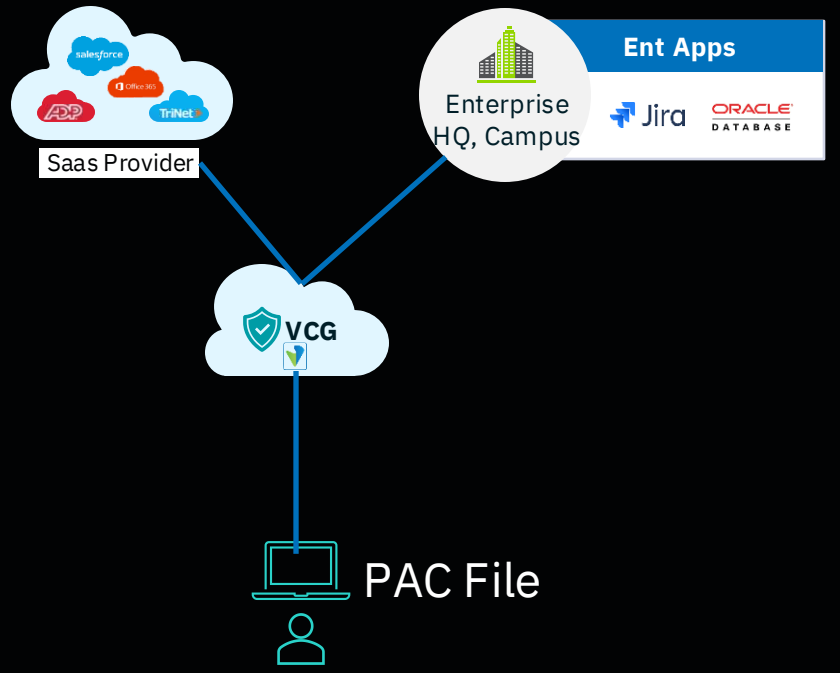
VERSATILITY

Other Client-less features (not relevant to this topic)

- Client-less SaaS Access

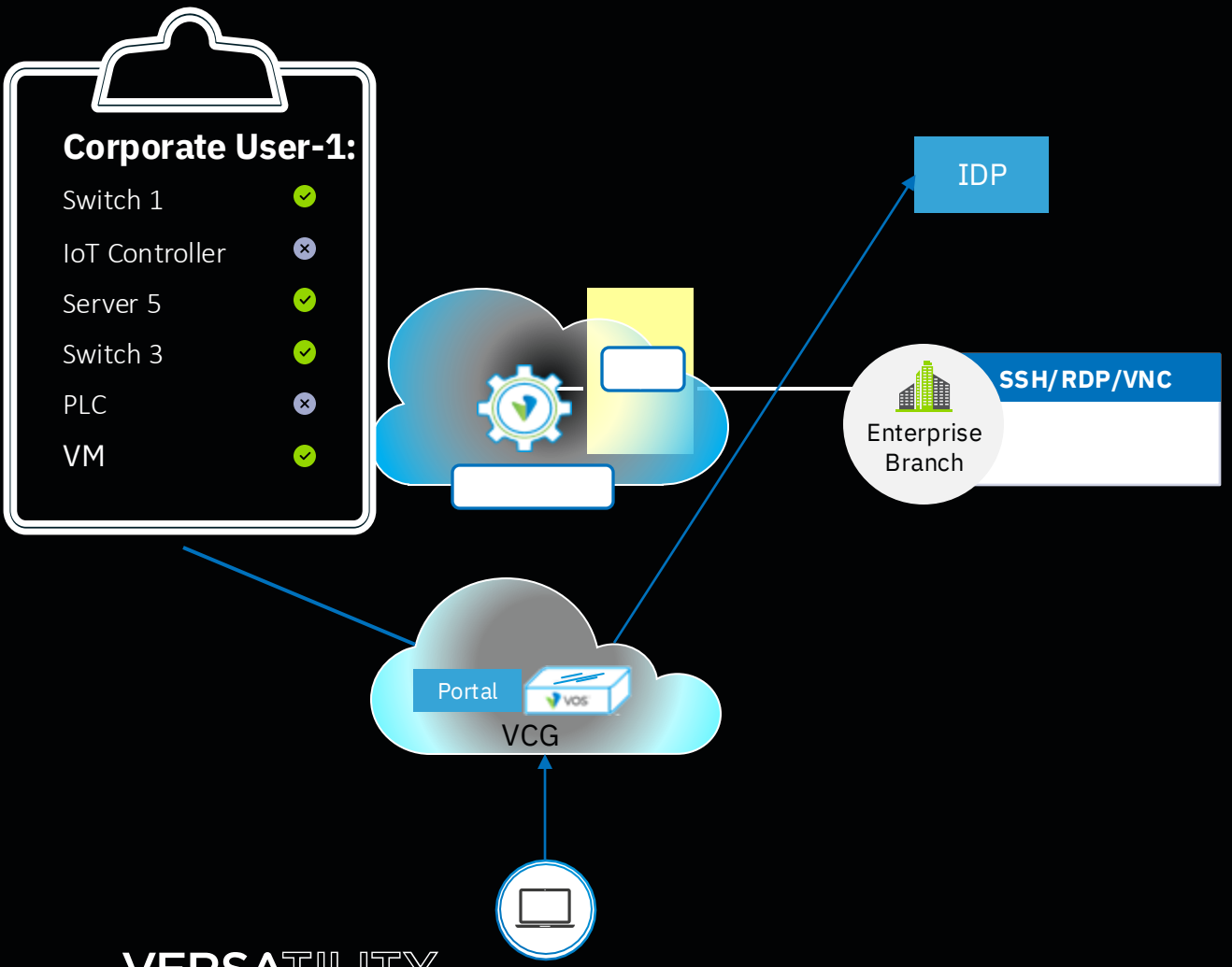


- PAC file based Remote Access



* PAC - Proxy Auto Config

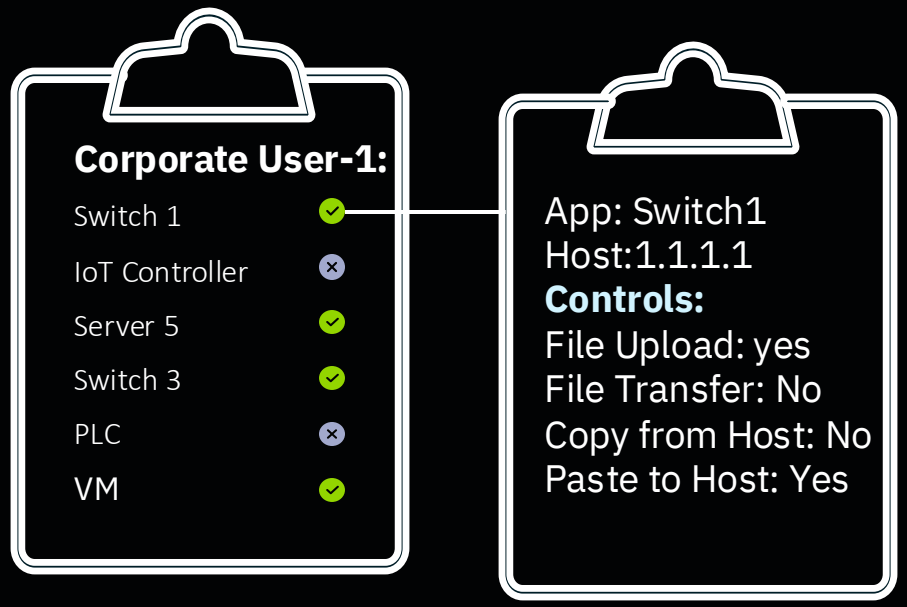
Zero Trust Access to Applications



- Integrated with Corporate IDP server
- IDP based Multi-factor Authentication
- Role Based Access Control based on User/User Group membership
- Dynamic policy decisions for every application
- Zero risk of lateral movement

VERSATILITY

Granular Control



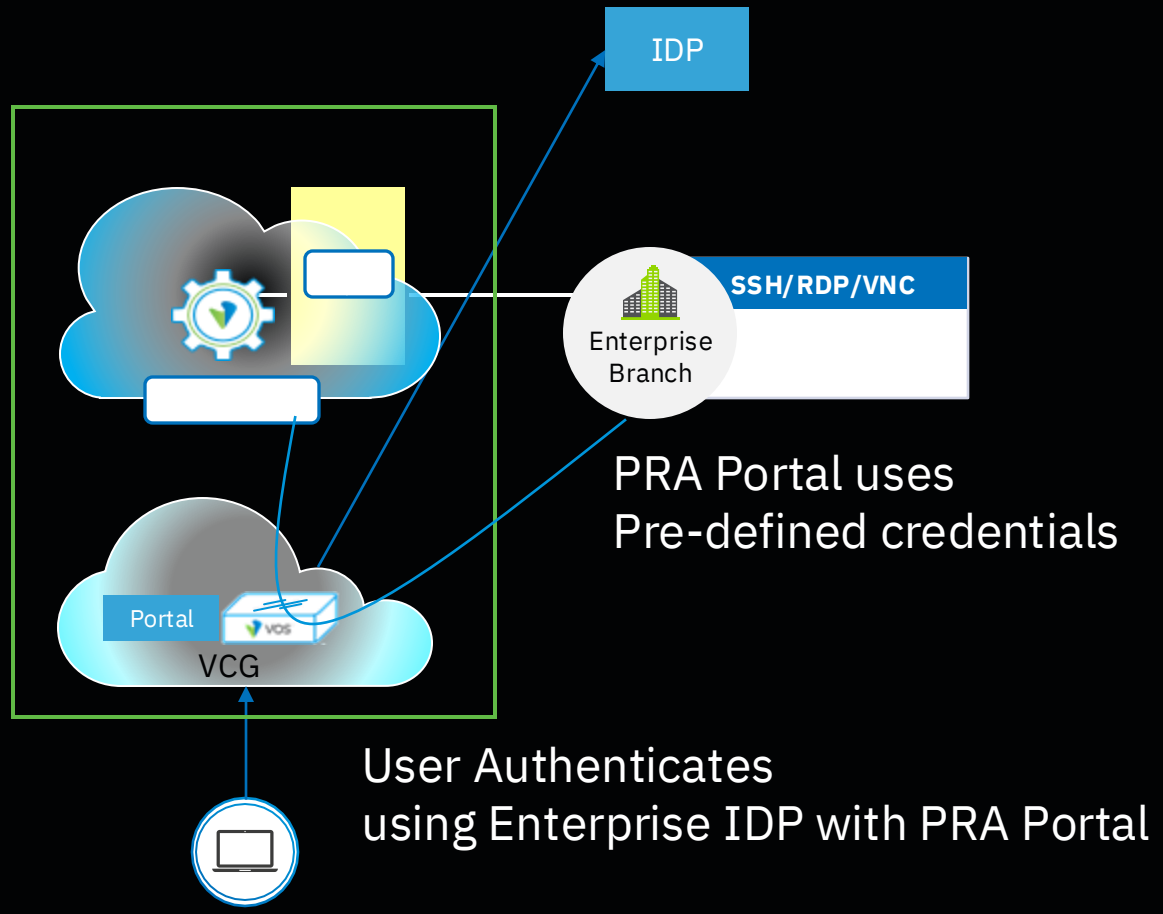
- Principle of Least Privilege
- Admins can create granular policy based on individual users or group memberships
- Provide access to only those actions required by the user role

How to prevent Credential Sprawl

- User Workflow
- User connect to Versa PRA Portal
- User logs in user enterprise IDP
- User clicks on SSH Server:1.1.1.1
- User logs in to SSH Server: 1.1.1.1
- User executes commands

- Problems with this workflow:
- Connecting every host with IDP is cumbersome and OPEX heavy
- Legacy systems do not support modern IDP protocols like SAML

Credential Injection: Solution



- Administrator create Pre-defined credentials with the Applications
- User Access to these applications are controlled by Enterprise IDP on PRA Portal
- Once PRA Portal authorizes the application access, User session is automatically authenticated on the application

Benefits

- Provide access to critical applications without compromising security

Secure your most critical applications by granular control of user activity

- Accelerate Productivity by reducing friction

Onboarding contractors, consultants is frictionless. Users become productive faster

- Lower Opex and Capex

Single pane of policy management for all remote users. Enable PRA without additional infrastructure on-site

VERSATILITY