RSAC 2026 Conference

POWER OF COMMUNITY.

Beyond Zero Trust: Continuous Validation for Modern Enterprise Security

Sanjay Singh
Staff Software Engineer
LinkedIn Corporation
https://www.linkedin.com/in/singhsanjay12/

Mitendra Mahto
Engineering Manager
LinkedIn Corporation
https://www.linkedin.com/in/mitendra-mahto/

RSAC 2026 Conference

Sanjay Singh

Staff Software Engineer

POWER OF COMMUNITY.

RSAC 2026 Conference

Mitendra Mahto

Engineering Manager

POWER OF COMMUNITY.

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC (“RSAC”) or any other co-sponsors. RSAC does not endorse or approve, and assumes no responsibility for, the content, accuracy, or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio, and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Session Overview

What we'll cover

- Why traditional Zero Trust still leaves gaps
- How to enforce security without slowing users
- Designing for real-time verification and revocation
- Operating identity and policy at enterprise scale

Evolution of Enterprise Security

Global Access | Fortress Model (Everyone Inside) | VPN for Remote Access | SSO to Log Into VPN Once | SSO Per Application | Device Certificate Verification | Central Proxy for UI + CLI | Real-Time Policy Evaluation

Act 1: When the Perimeter Was Enough

- Harden the perimeter with firewalls and segmentation
- Trust everything once it’s inside
- Simple. Effective. Predictable.
- Then came cloud and remote work; and VPNs became the crutch

The Threat Is Sometimes Already Inside

Act 2: We Added Identity… Sort Of

- Identity checked to access the network
- SSO gates VPN or network segments
- Applications still authenticate independently
- No end-to-end identity model

Security Isn’t Just a UI Problem

Act 3: Access Is More Than Identity

- Verify device identity on every request
- Access decisions combine **user identity + device trust**
- Zero Trust in action!

Even Fortresses Fall

REVOKING ACCESS STILL TAKES HOURS

CAN WE MAKE ACCESS CONTROL CHECKS MORE DYNAMIC AND REAL TIME?

RSAC 2026 Conference

Beyond Zero Trust

Beyond Zero Trust

Policies evaluated in real time - not just at login

Context-aware decisions based on user, device, and behavior

Identical enforcement for UI and CLI

RSAC 2026 Conference

How We Built it?

Foundational Principle

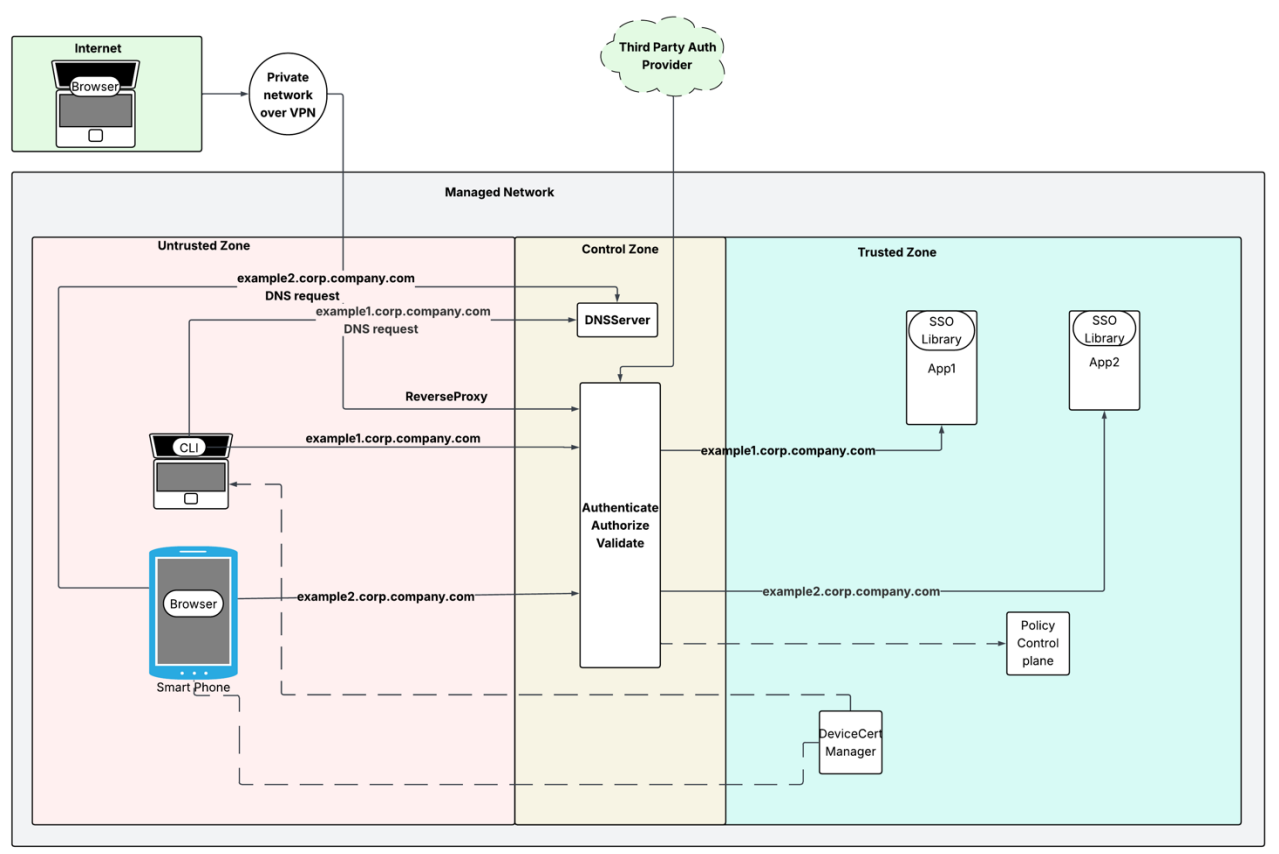
Open source + open standards first

No vendor lock-in for identity, policy, or enforcement

Portable across on-prem, cloud, and hybrid

Easier to evolve as architecture matures

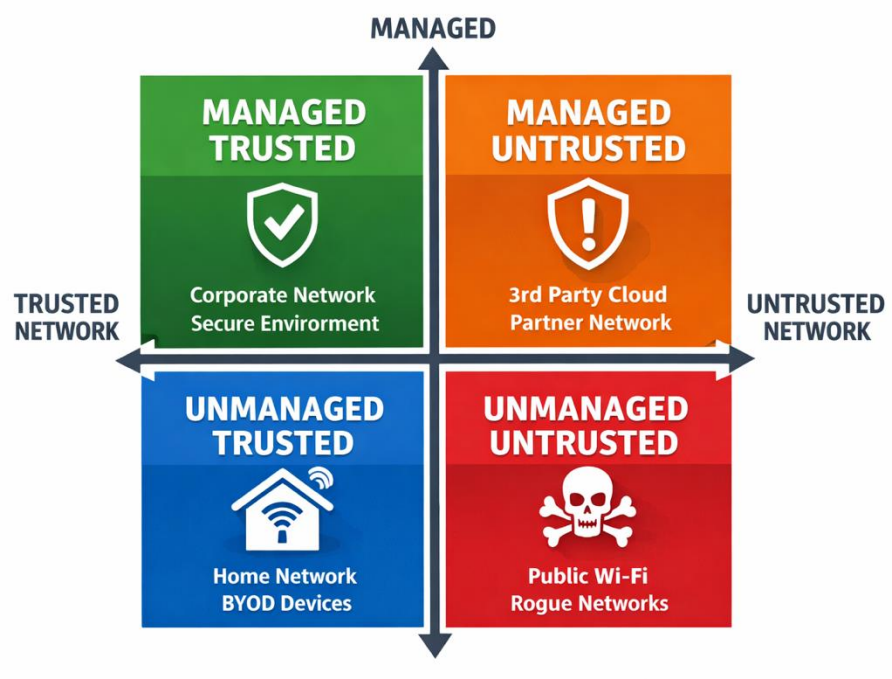
Architecture



Components

- Trust Zones
- Central Proxy
- Trust Verification : Identity + Device
- Control Plane

Trust Zones



- Two Dimensions
  - Trusted Vs Untrusted
  - Managed Vs Unmanaged
- Validation required for crossing trust boundaries

From Flat Network → Enforced Trust Zones

Network Segmented Trust Zone

L2/L3 Isolation

Dedicated VLANs and unique subnets per zone

Access Controls : Cross Domain Not Allowed

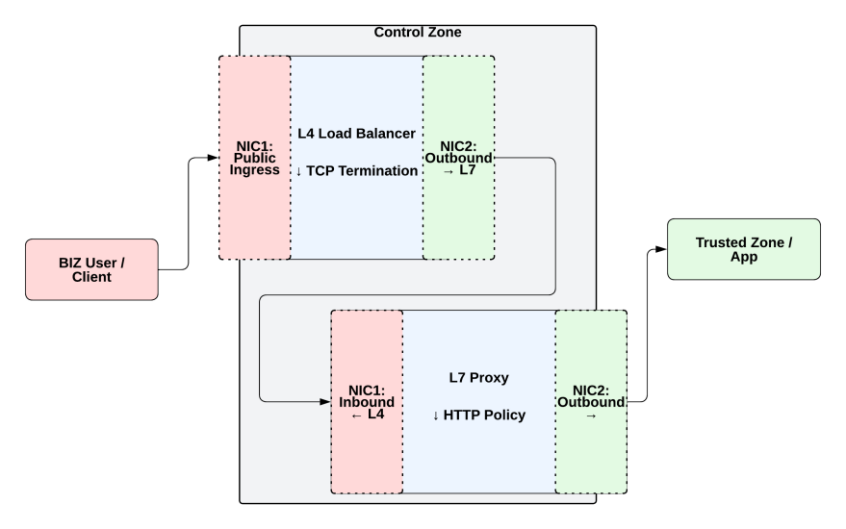
NACLs at every boundary + host-level firewalls

Protected Lateral Movements through Edge Control Zone

Protocol Break and Re-Origination

Policy Enforcement

Protected Lateral Movements through Edge Control Zone



Zone-Bound Interfaces (Dual-NIC Isolation)

- Servers dual-homed with NICs pinned to a single zone pair
- **L4 LB:** NIC1 = public ingress | NIC2 = outbound → L7 only
- **L7 Proxy:** NIC1 = inbound ← L4 only | NIC2 = outbound → trusted zone
- No cross-zone interfaces → forward-only traffic flow

Protocol Break & Re-origination

- TCP terminates at **L4** → inspected → new connection to L7
- HTTP terminates at **L7** → policies enforced → new connection to trusted zone
- Untrusted traffic never traverses end-to-end into trusted network

Open Source Tech

Control	Open-source Tech
Network Segmentation	Linux VLAN, Cilium/Calico, Open vSwitch, FRRouting (FRR)
Access Controls	iptables/nftables, Cilium NetworkPolicy
Layer 4 Proxy Stack	IPVS/LVS, Envoy, HAproxy

Central Access Proxy

Validate Clients

Connections : Approved Devices Only

Requests : Approved Users Only

No Bypass Paths

Consistent Validation

 UI ·  Web · 

CLI

Context Aware

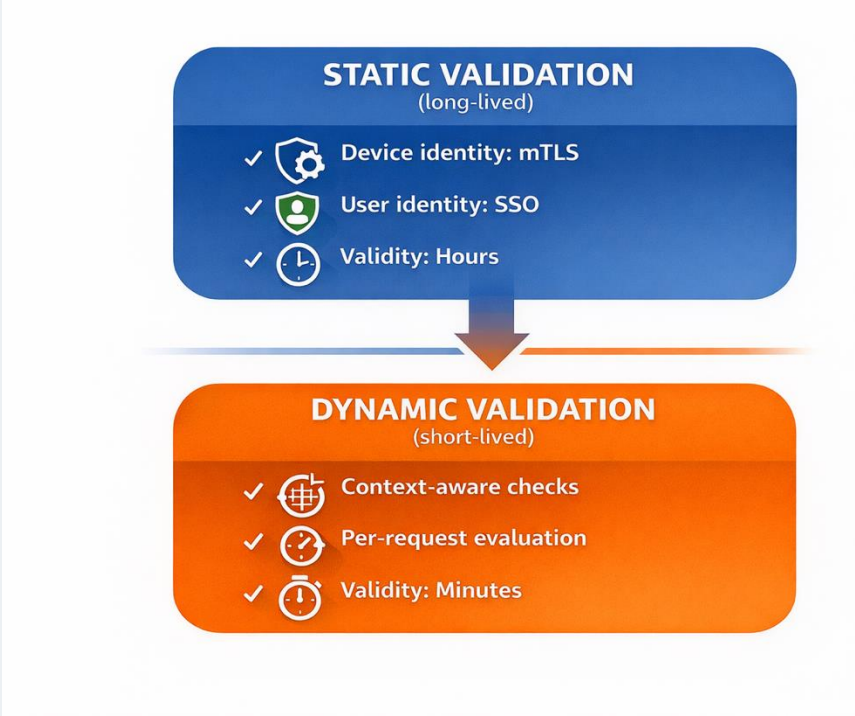
Session

Location

Duration

User Behavior

From Static Validation → Dynamic Policy Verifications



Device Verification

- mTLS with enriched X.509 client cert metadata

Identity Verification

- Proxy integrates with multiple external IdPs (OIDC, SAML, LDAP) — no app changes

Real-Time Policy Enforcement

- Control plane-driven policies enforced per request (user, path, device)
- Dynamic policy refresh at intervals + continuous session re-validation
- Supports multi-device sessions with anomaly detection

Open Source Tech

Control	Open-source Tech
Reverse Proxy	Envoy, HAproxy
SSO	Ext_authz (Envoy), SPOE_Auth (HAproxy)
Custom Policy Enforcement	Xds Control Plane (Envoy), Haproxy DSL with runtime API

Control Plane

Responsibilities

- Defines and manages access policies
- Acts as the authoritative metadata source for allowlists and denylists *(devices and users)*

Mechanisms

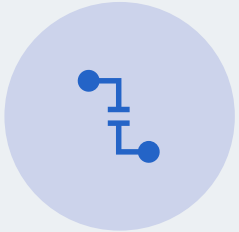
- Periodic policy and metadata synchronization
- Emergency control mechanisms for rapid enforcement

Open Source Tech

Control	Open-source Tech
Control Plane Service	gRPC / Rest Endpoint, XDS

Scaling the System : Production-Ready

Geo-distributed, multi-datacenter architecture



Built-in redundancy across proxies and auth providers

Automatic and controlled failover

Progressive rollouts with instant rollback

RSAC™ 2026 Conference

POWER OF COMMUNITY.

Challenges

Fragmented SSL and certificate support across languages

OS-dependent certificate management limitations

Limited SSO support in non-UI tools (CLI)

Proliferation of authentication and SSO standards

Challenges → Resolutions

Standardized access libraries across **4 core languages**

Updated our standard libraries to support certificate handling using **OS-native key stores like MAC keychain**

Invoke browser-based SSO with **tokens stored locally to reuse across CLI sessions**

Proxy-centric multi-IdP integration **abstracting identity from applications** via custom token headers

Working With Legacy Systems

Inconsistent security baselines

Added audit logging to scope gaps

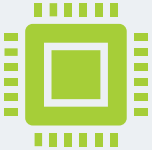
Stop the Bleeding

Prioritize major use cases and tail end to be handled later

Legacy authentication and identity mechanisms

Temporary dual-auth support for safe transition

Not ideal but enabled us to move without breaking existing setup



Siloed and non-standard access implementations

Built IDP-agnostic abstraction layer

Working With Legacy Systems (Contd)

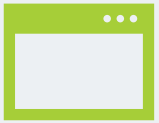
Inefficient client behavior

Partnered with teams to correct patterns

Protocol/payload assumptions from Old System

Audit the outliers

Enhanced current system to support most of the existing assumptions and rest of were asked to fix the apps



Migration safety

Split-DNS + incremental rollout (per app / per path)

Provided easy kill switch to go back to old behavior

APPLY : IMMEDIATE ACTIONS

Identify

Identify your weakest revocation path

- Measure time to fully revoke access after user/device compromise
- Check if internal apps still work after SSO logout or cert revoke

Map

Map your enforcement gaps

- List apps (including CLIs) without SSO + mTLS enforcement
- Identify tools reachable from unmanaged devices or VPN

APPLY : WITHIN 3 MONTHS

Move enforcement to request time	Add proxy/gateway enforcing identity + device per request
	Reduce reliance on long-lived sessions and static checks
Reduce revocation latency	Shorten cert/session TTLs
	Implement continuous re-validation for active sessions
Standardize access controls	Centralize policy in a control plane
	Remove app-specific auth logic
Improve visibility	Add audit logs for **who accessed what, from where, and with which device**
	Track access after termination or role change

Key Takeaways

- Zero Trust is the **starting point**, not the solution
- Trust expires every request
- Revocation must be real-time
- UX and scale decide **adoption and success**

RSAC | 2026 Conference

Thank You!

For more information:

Reach out on LinkedIn

LinkedIn @ Sanjay Singh

LinkedIn @ Mitendra Mahto