CISCO Engage | Tech Day Milwaukee

Ground the Cloud: Bring Zero Trust Back in your Control

Sarah Frisanco – SSE Solution Engineer

March 31 2026

Agenda

1. What is Zero Trust?
2. What is Universal ZTNA?
3. SSE & Hybrid Private Access
4. SDWAN & ISE
5. Identity
6. Cisco Live Teasers
7. Survey

About Me:

- 4+ Years at Cisco
- 6+ Years covering SASE
  - Deployed Zscaler and Palo Alto Firewalls
- Manufacturing, Healthcare, Education
- Green Bay, Wisconsin
- Find me on Linkedin:

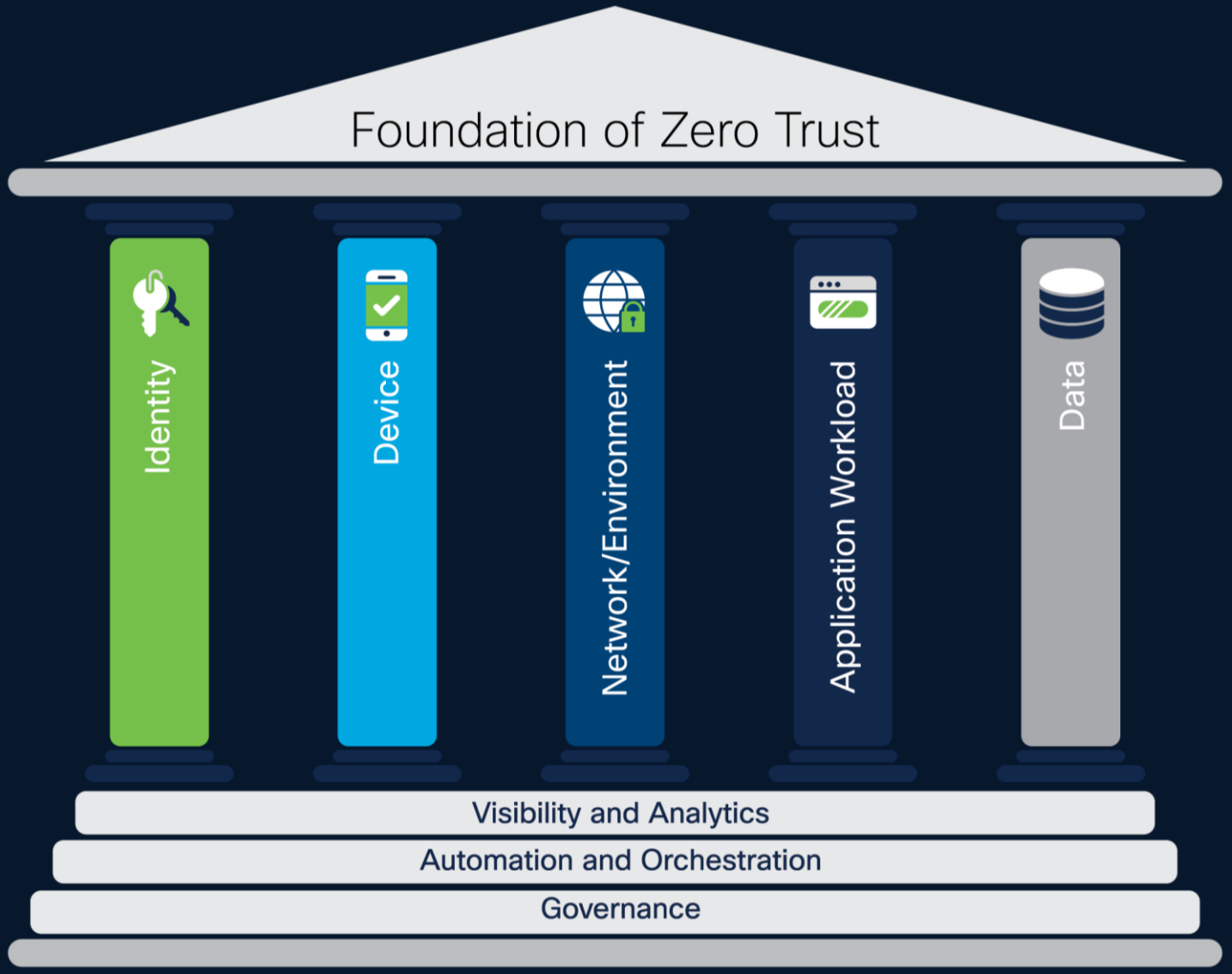
What are some things you've heard about Zero Trust?

Common Examples

- Never Trust, Always Verify
- “We have MFA therefore we have Zero Trust”
- Our Zero Trust journey is one and done
- Microsegmentation vs. Macrosegmentation
- No more firewalls, our SSE solution is our firewall

Zero Trust

Least Privilege Access is Key



US Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Pillars

The Nebula

The Nebula

The Network you Can Control

The Network you Can’t Control

Identity

Universal ZTNA

What is UZTNA?

Cisco Universal ZTNA

Takes ZTNA to users and **devices**

Security Cloud Control

Secure SD-WAN + Secure Services Edge + **Continuous Trusted Identity for Everything**

Single vendor SASE

Digital Experience (ThousandEyes)”
“Threat Detection & Response (Talos, XDR, Splunk)”

cisco

Security Services Edge

Cisco Secure Access

- Go beyond core Secure Service Edge (SSE) to better connect and protect your business

Core SSE

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) and DLP
- Zero Trust Network Access (ZTA)
- Firewall as a Service (FWaaS) and IPS

Cisco delivers the core and more in a single subscription...

- DNS Security
- Multimode DLP
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring*
- Remote Browser Isolation*

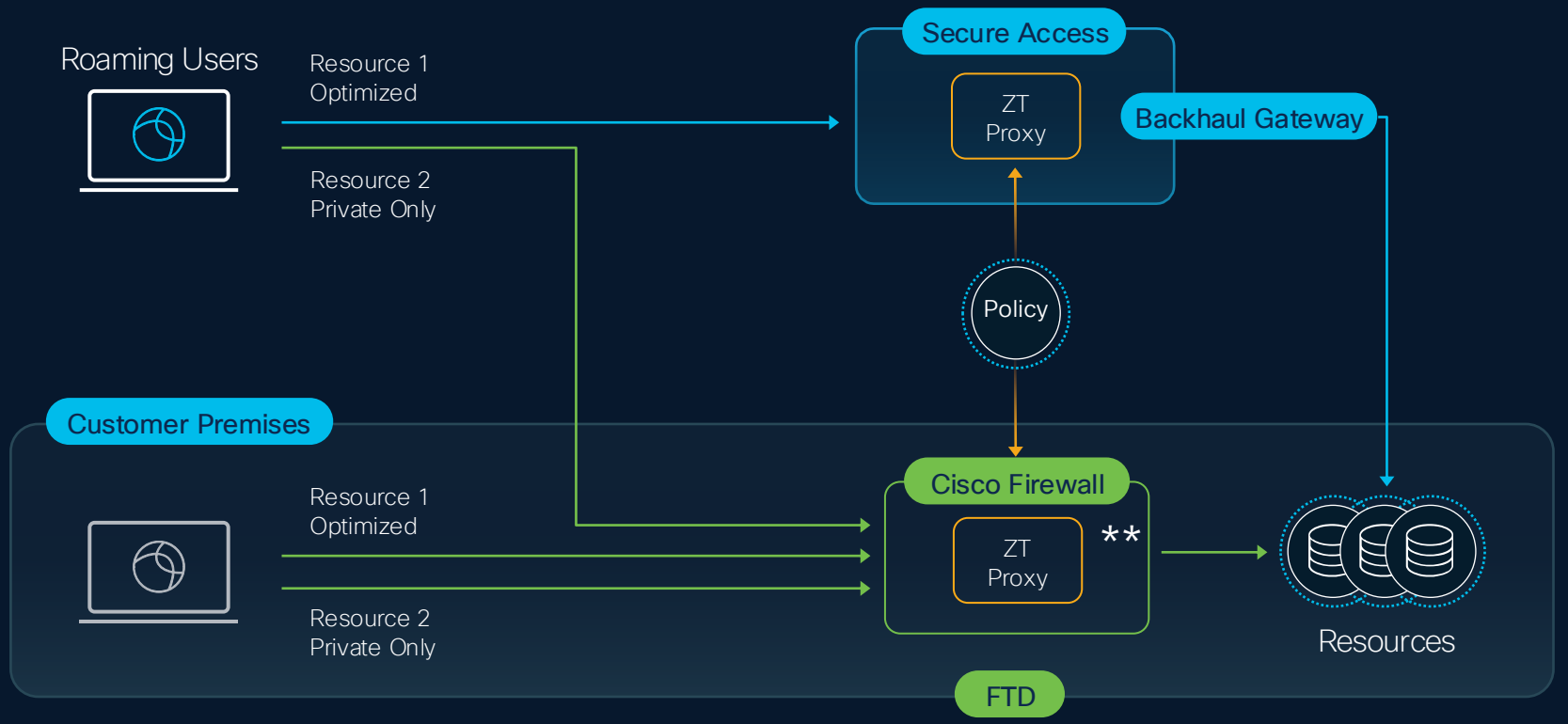
Add-on solutions

- SD-WAN
- XDR
- DUO MFA/ SSO
- CSPM

* Included in the unified experience / separate license (optional)

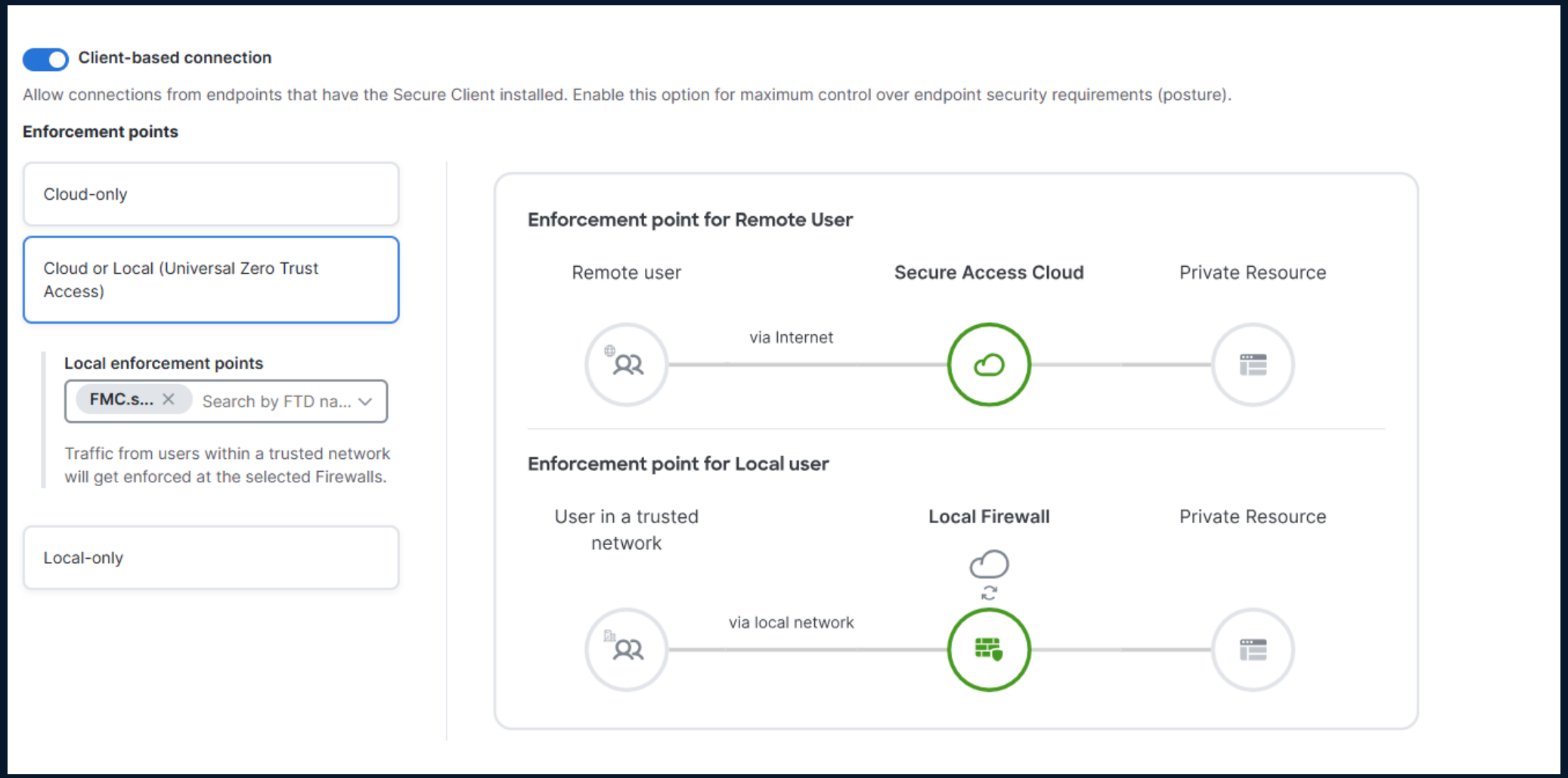
Hybrid Private Access for flexible enforcement

- Single set of ZTNA policies used in cloud and on-premise



** Roadmap: policy enforcement on 8k routers

Decide Per Application



Hybrid Private Access Demo

Organization
GSSO-GSAT
Home

Products
AI Defense
Firewall
Hypershield
Multicloud Defense
Secure Access
Secure Workload

Platform services
Favorites
Identity Intelligence
Security Devices
Shared Objects
Platform Management

Home

Set default homepage

Top Insights & Alerts

12 Active Insights

All Insights

Access Control Policy Anomalies

Data source: Test-abc | Cloud-delivered FMC

AIOps has detected 32 anomalies in Access Control policy 'Test-abc'.

28d ago — Details

Best practices and recommendations

Data source: ftdv-test6

AIOps has detected 6 needs review checks.

24d ago — Details

Best practices and recommendations

Data source: ftdv-test5

AIOps has detected 6 needs review checks.

24d ago — Details

Multicloud Defense

Multicloud Defense

Account Resources

21 VPCS/ VNets	35 Security Groups	31 Route Tables	69 Subnets
8 Instances	1 Load Balancers	0 Tags	1 Applications

Security Considerations

- 1 Applications not protected
- 20 VPCs/VNets not protected
- 0 Service VPC/VNets without Gateways

Overall Inventory

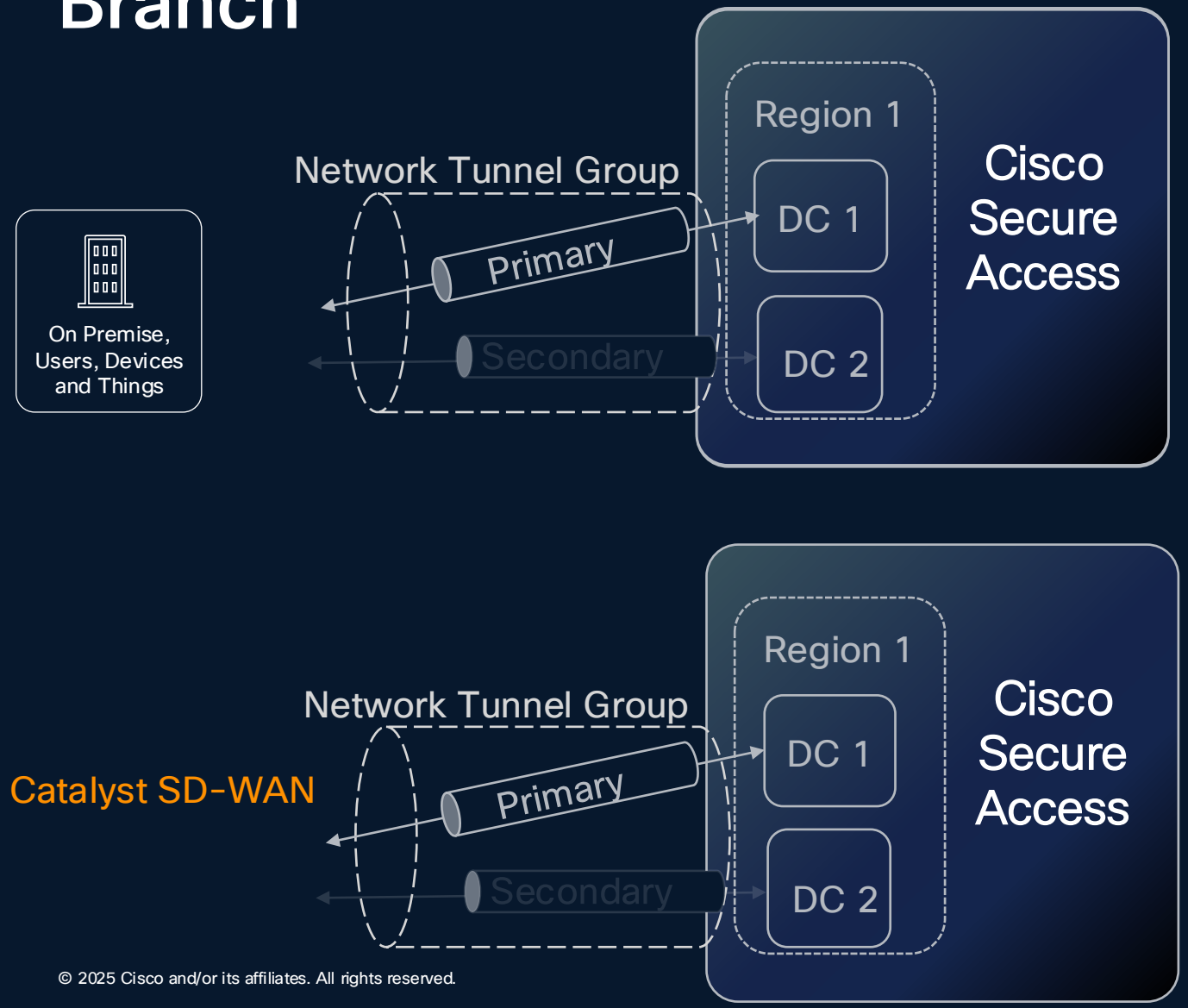
32 Total Devices

RA VPN Sessions

SDWAN

Secure Internet Access

Branch



Site-to-site Tunnels with IPsec

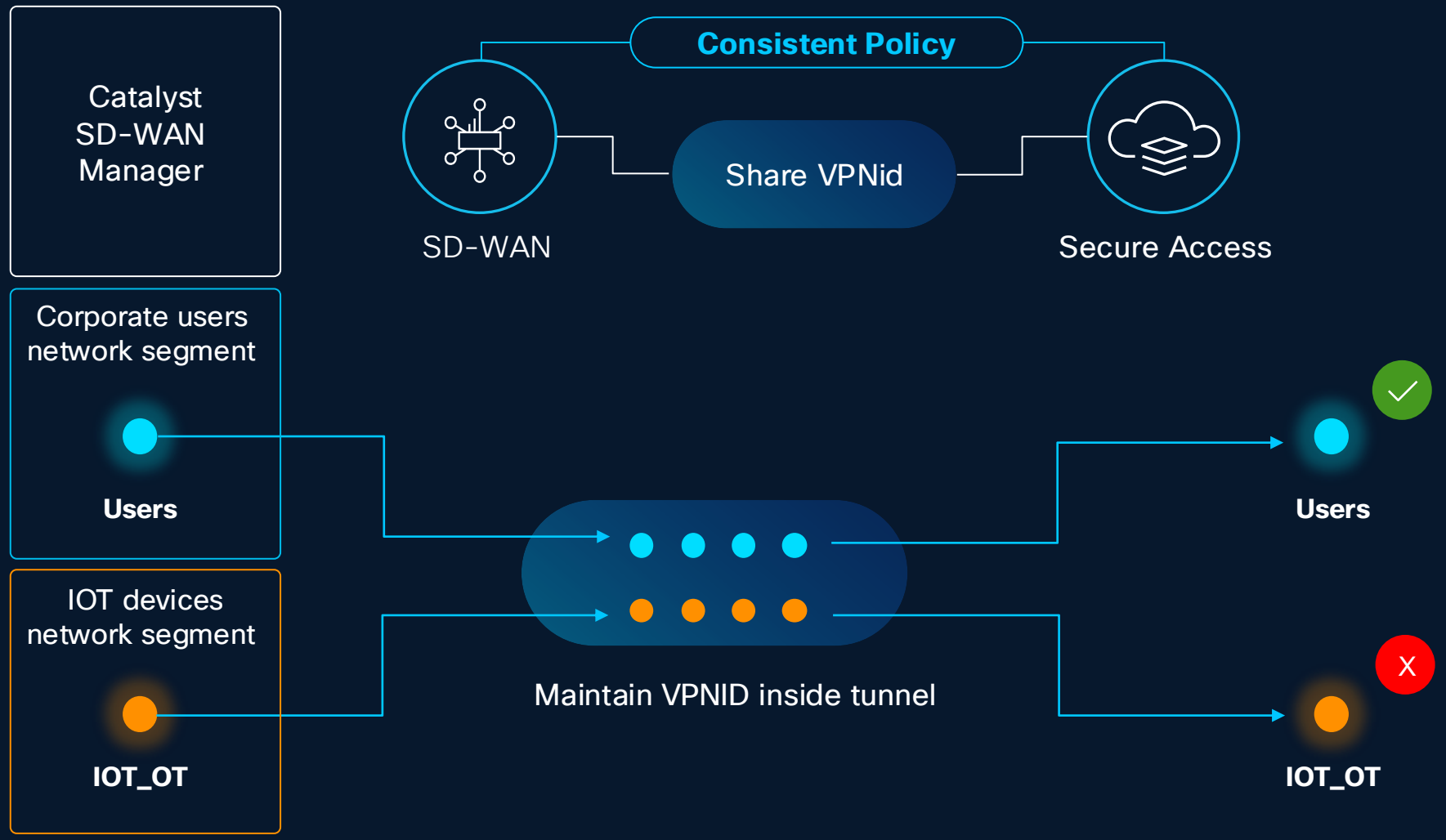
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Regional redundancy
- Outbound NAT support for internet only tunnels

Catalyst SD-WAN

- Auto-tunnel from Catalyst SD-WAN for Internet apps now
- Auto-tunnel from Catalyst SD-WAN for Private apps in 20.18
- 1GB per tunnel
- Up to 8 active, 8 backup per tunnel group
- SD-WAN tracker support for regional redundancy

Catalyst SD-WAN
VPNid support for consistent segmentation

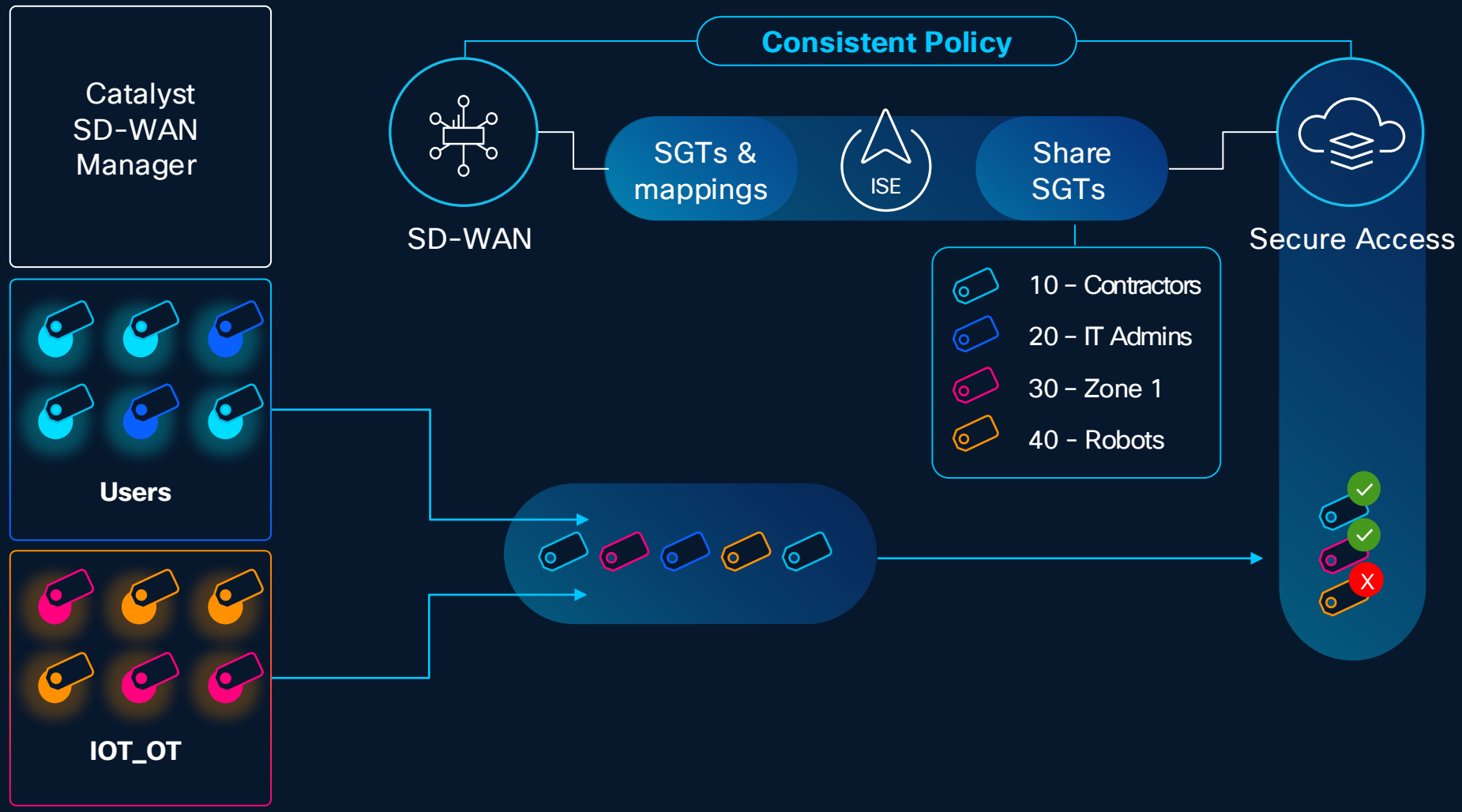
- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Identity Services Engine (ISE)

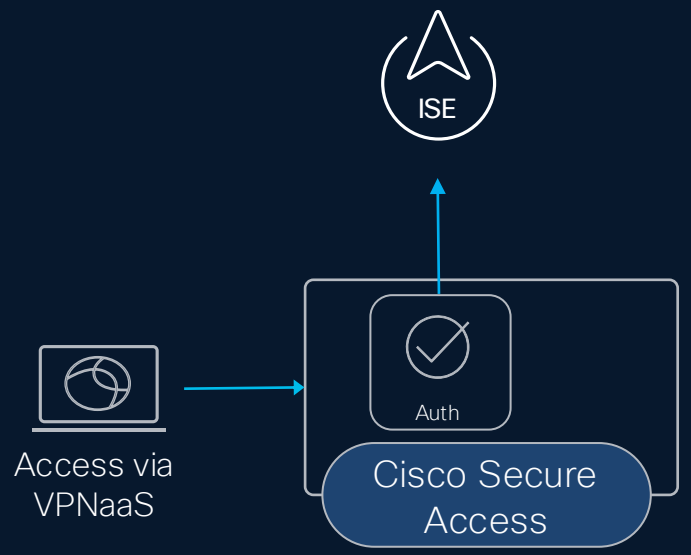
Leverage SGTs for granular access control

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



ISE integration with Secure Access VPNaaS

RADIUS authentication, in addition to SAML authentication



- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- ISE posture supported (optional)
- SGT assignment via authorization

SGT Demo

Home
Connect
Resources
Secure
Monitor
Admin
Workflows

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help

Rule Defaults and Global Settings

Search by rule name | Intent | Objects | Settings

Add Rule

13 Rules

Customize view

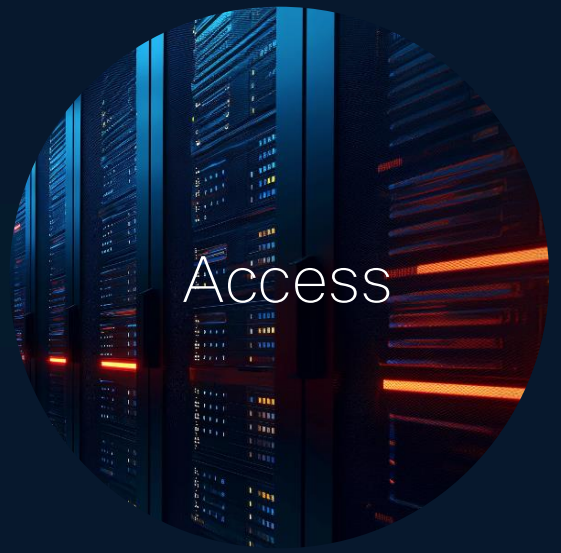
	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
	1	AllowTunnelToInternet	Internet	Allow	testLogicalA... +1	Any		-	
	2	AllowSGTtoAnyInternet	Internet	Allow	Any Security...	Any		-	
	3	AllowAnySGTtoAnyprivate	Private	Allow	Any Security...	Any		-	
	4	AllowSGT8ToSGT9	Private	Allow	SGT-8	SGT-9	-	-	
	5	AllowSGT9TOSGT8	Private	Allow	SGT-9	SGT-8	-	-	
	6	allowTun1ToTun2	Private	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services +3	-	-	
	7	TunnelAllow8888	Internet	Allow	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	
	8	TunnelBlock8844	Internet	Block	testLogicalA... +1	1 IP Address/CIDR AND 1 Services		-	
	9	AllowSGT2ToSGT1	Private	Allow	SGT-2	SGT-1	-	-	
	10	AllowSGT2SGT	Private	Allow	SGT-1	SGT-2	-	-	
	11	DenyPing8844	Internet	Allow	SGT-5	Any		-	
	12	AllowSGT6toAny	Private	Allow	SGT-6	Any		-	

Identity

Identity Intelligence

Continuously assess you are
who you say you are

BLINK TRUST



Works with existing IDPs

cisco

Cisco Identity Intelligence

SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

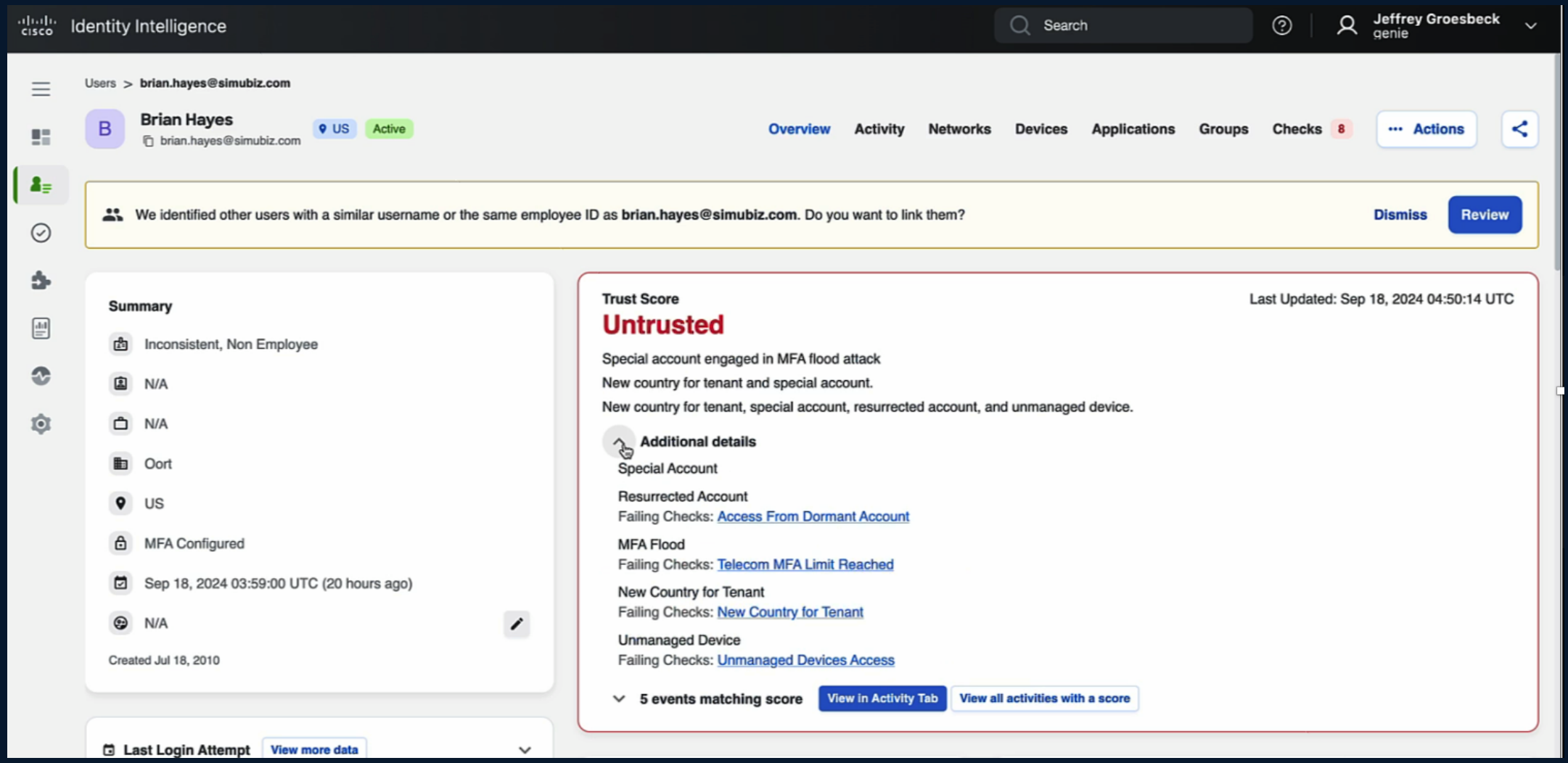
Microsoft

Google

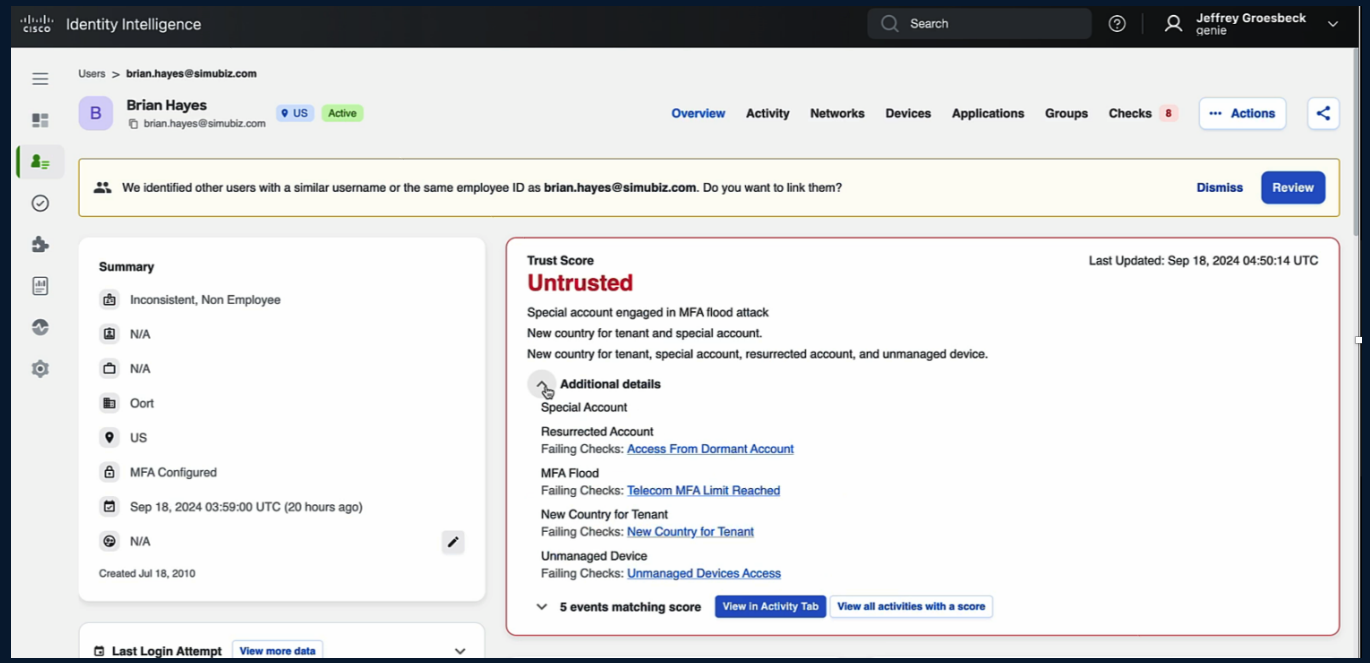
Cyberark

Amazon

User trust timeline



User Trust Score



User Trust Score

Identity Intelligence will be providing a user trust score for integrating solutions to leverage. Will be a single score, determined by a user's behaviors, actions and posture

Easy Workflows

After assessment, seamlessly take response action from the console.

Key Scores

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown

Bringing It All Together

There is no universal zero trust
without ubiquitous, shared identity across the enterprise

Cisco Universal ZTNA

Every device, person, thing, everywhere

Zero impostors:
Identity Trust

Zero downtime:
Experience and Policy Assurance

Data Loss Prevention	Remote Browser Isolation	AI Access
Firewall as a Service	Secure Web Gateway	Zero Trust Network Access
Cloud Access Security Broker	DNS Security	VPNaaS

Consistent Security:
Security Service Edge

Zero friction:
We do the plumbing.