

Zero Trust Network Access

Integrating Identity for Secure Connectivity



October 2nd, 2025

Agenda

- 1 ZTNA and Identity
- 2 Enforcement Points of ZTNA
- 3 On-Prem Access Control
- 4 Cloud Security
- 5 Workloads and Applications

ZTNA and Identity

Shift in IT landscape

Users, devices, and apps are everywhere.

Security no longer can
rely solely on Location +
Devices for Policy



Zero Trust Platform Requirements

What it takes to get Zero Trust right



Establish
Trust



Enforce
Trust-Based
Access



Continuously
Verify Trust



Respond
to Change
in Trust

Focus Elements of a Zero Trust Platform

Establish Trust



Device Posture



Endpoint Security



Identity Authorization



Identity Access Policy



Multi-Factor Authentication



Mobile Device Management



SAML & SSO



Tagging

Enforce Trust-Based Access



Application Security



Clientless Remote Access



Cloud Security



DDoS Protection



Firewall



Intrusion Prevention



Micro-segmentation



SD-WAN



Web App Firewall

Continuously Verify Trust



Anomaly Detection



Anti-Virus



Anti-Malware



Data Loss Prevention (DLP)



Flow Analytics



Malware Sandbox



Network Anti-Malware



Vulnerability Scanning

Respond to Change in Trust



Security Orchestration Automation and Response (SOAR)

Zero Trust Pillars

Identity

Multi-factor authentication (MFA)
Enterprise single sign-on (SSO)
Role-based access control (RBAC)

Device

Continuous validation of users and devices
Endpoint detection and response (EDR)
Risk-based vulnerability management

Network and Workload

Network detection and response (NDR)
Micro-segmentation of application workloads

Automation and Orchestration

Orchestrated workflows
Automation and response
Security Orchestration and Automated Response (SOAR)

Strategy

CISA's Zero Trust Maturity Model (ZTMM)



Identity



Devices



Networks



Applications and
Workloads



Data

Visibility and Analytics

Automation and Orchestration

Good Governance

Enforcement Points of ZTNA

Enforcement Points of ZTNA

Focal points of Network Security

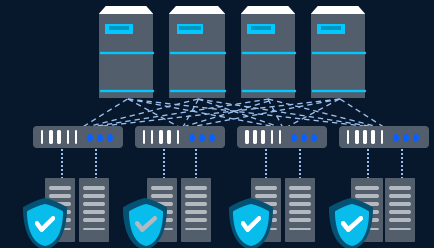
On-Prem,
Trusted Networks



Cloud Tenants
and Controls



Workloads \
Applications



On-Prem Access Control

What Makes On-Prem Security Difficult?

Managed, Secure Devices are the exception to the rule.

BYOD

- Unwanted devices or unauthorized users can introduce new network breaches.
- It isn't going anywhere, research talks about how an increase in a BYOD policy implementation "propels the market growth".

Post Covid 19 Impact

- Hybrid employees working from home and connecting to the corporate need to protect network data no matter where they are.
- Usually involves trusted devices in untrusted environments

IoT Devices

- As more IoT devices are deployed, there are more entrances for bad actors to infiltrate the network.
- IoT devices are routinely overlooked in terms of strong security and are sometimes needlessly attached to a part of the network that doesn't need access.

How Cisco Manages On-Prem Security

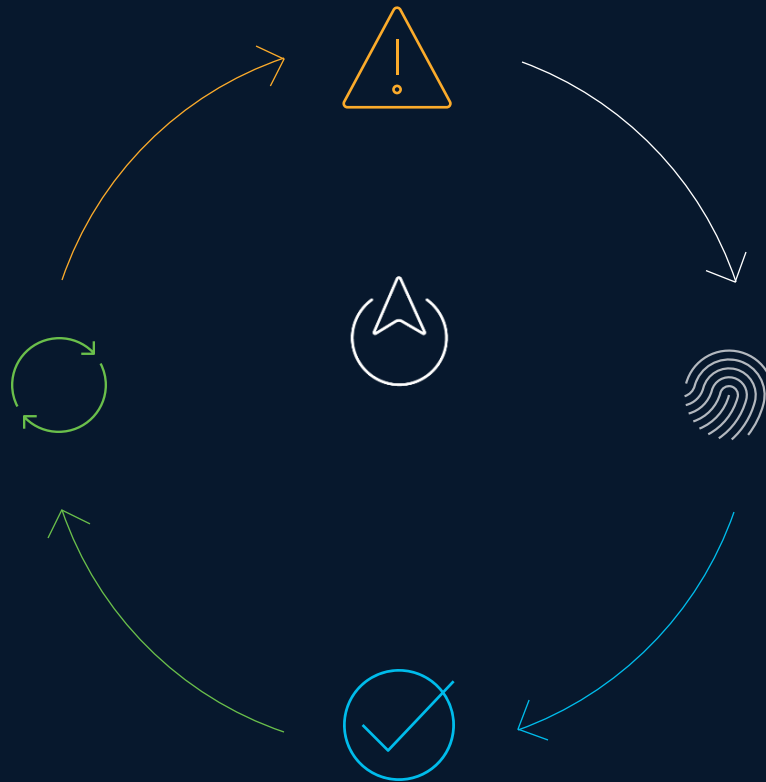
Secure Network Access via Classification and Authentication with Cisco Identity Services Engine

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy



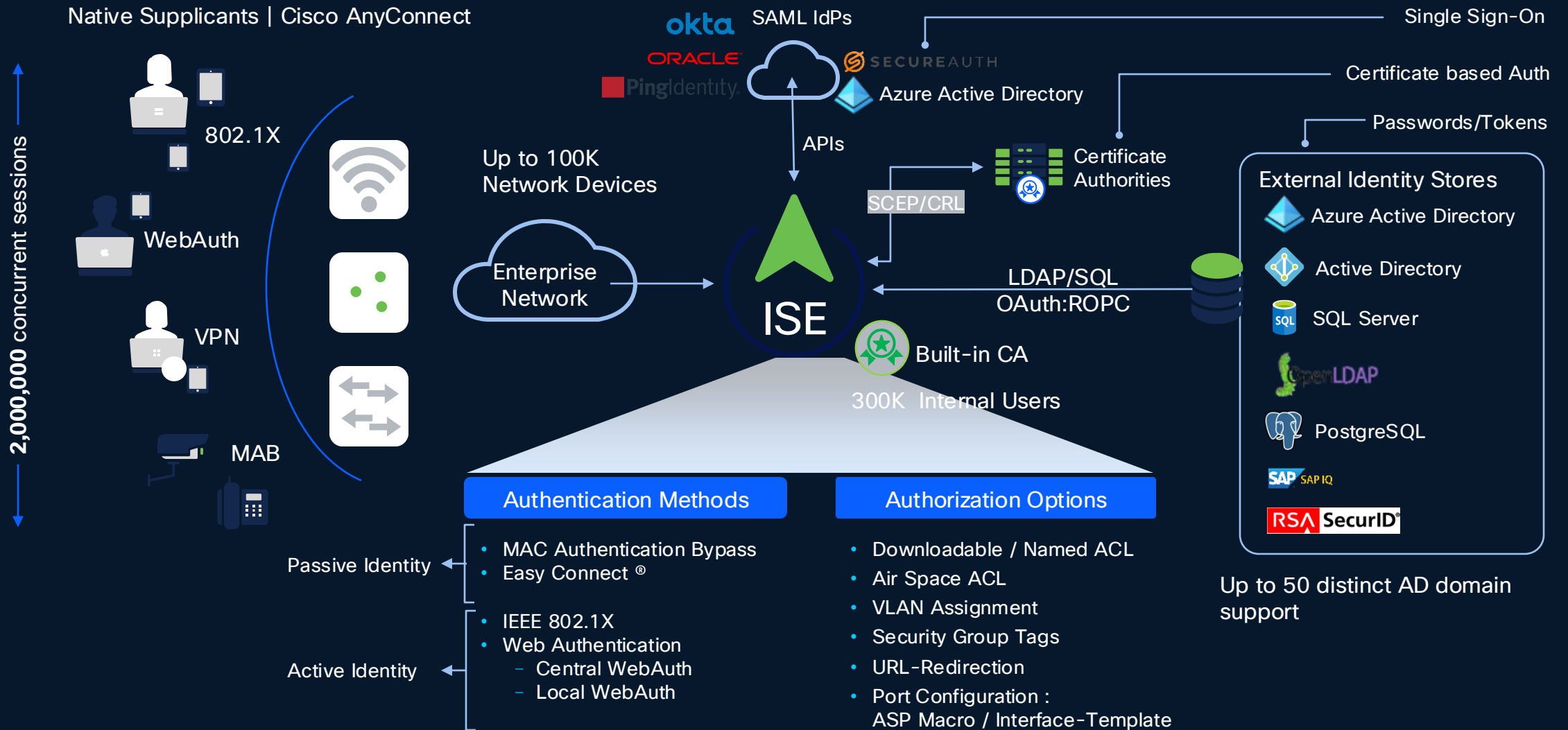
Endpoint classified, and profiled into groups

- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

NAC Powered by Cisco Identity Services Engine



The Key Role of Integration

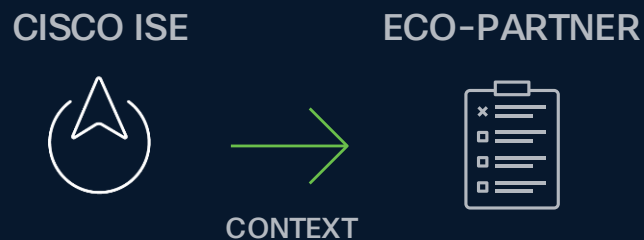
Enabling a “single source of truth” for Network Security starts with Integration

ISE CONTEXT IN



Enrich ISE context. Make ISE a better Policy Enforcement Platform

ISE CONTEXT OUT

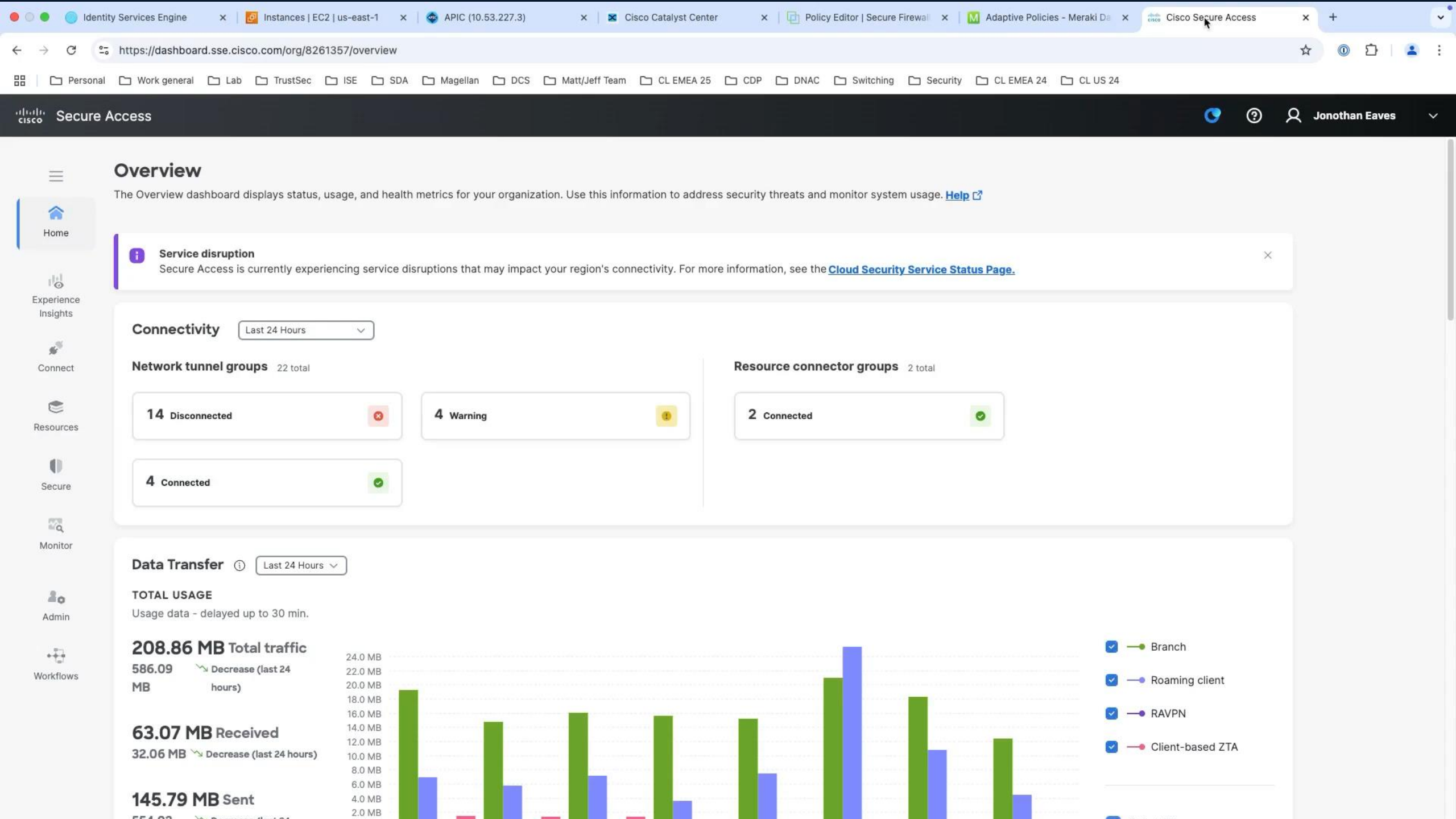


ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Rapid Threat Containment



Enforce dynamic policies into the network based on Partner's request

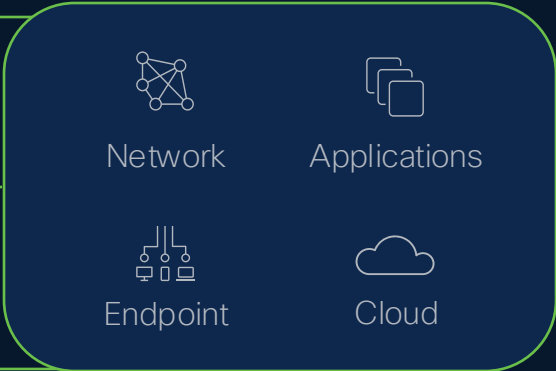


The power of integration, the simplicity of operations



More Cross-Team
Use Cases
Simplified with
Visibility and
Automation

Cisco Security



More Integrated
Products Across
Partner Ecosystem
and Beyond



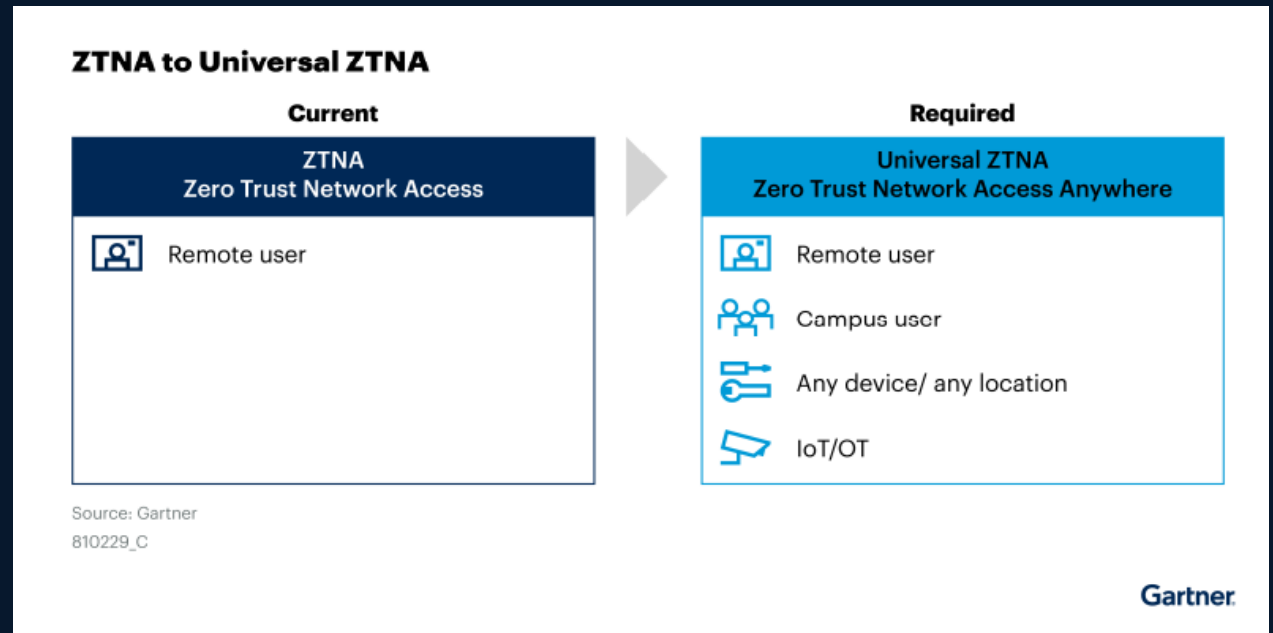
Your infrastructure

Cloud Security

How does the industry define Universal ZTNA?

“Universal ZTNA extends ZTNA technologies to use cases beyond remote access, to support local enforcement in campus and branch on-premises locations.”

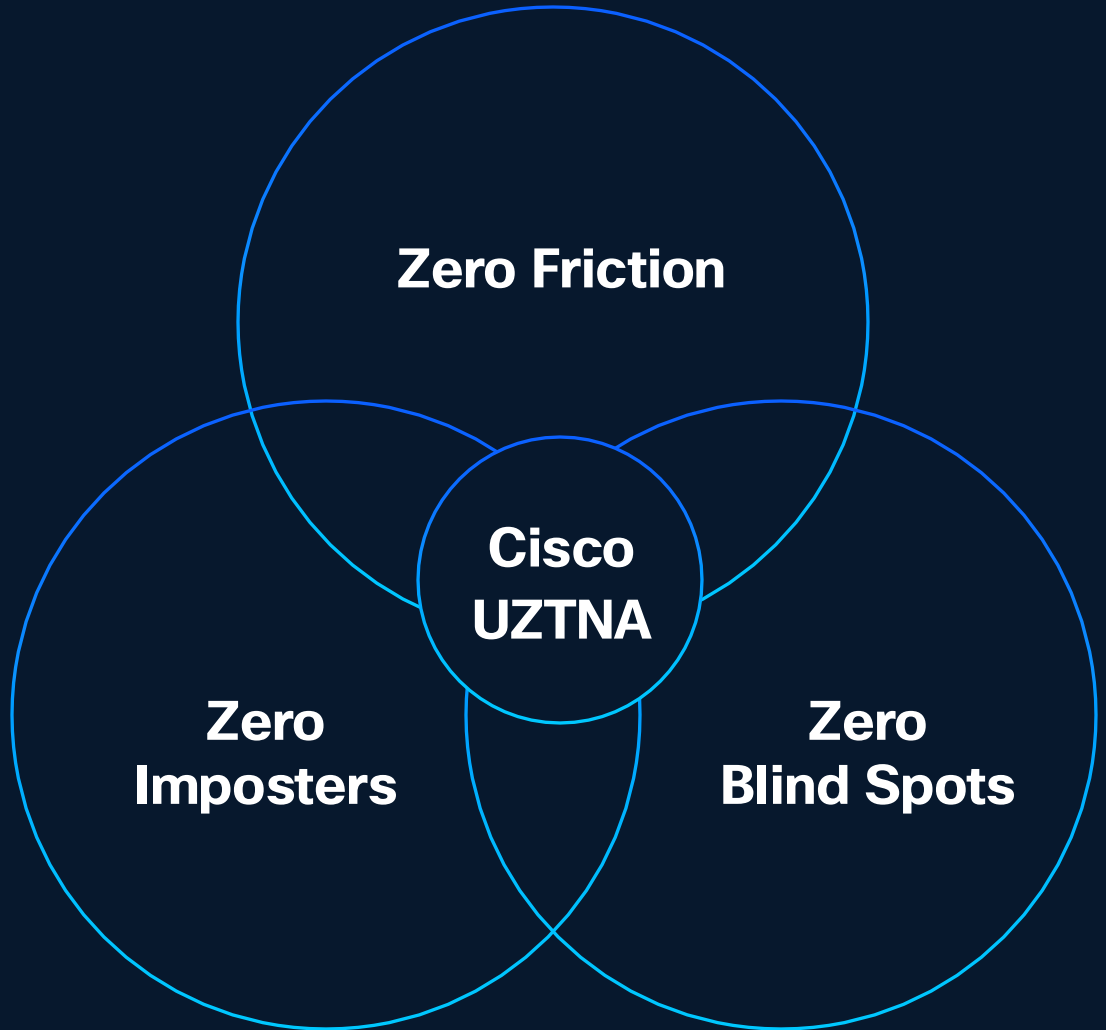
“That means providing a seamless experience to the user and delivering a consistent security posture across the entire network, whether remote or on-premises.”



**Source: Gartner – Emerging Tech: Universal ZTNA Drives Secure Access Consolidation – Dec 2024*

Cisco Universal ZTNA is built on 3 core concepts

- **Zero Friction** – Seamless access for users and integrated operations for admins.
- **Zero Imposters** – Continuous identity and trust verification that stops Identity attacks.
- **Zero Blind Spots** – Complete visibility and protection across users, devices, apps, and *now AI*.



From complex choices to zero friction flexibility

Architectural consolidation and seamless integration

Cisco Universal Zero Trust Network Access

SD-WAN

- Catalyst
- Meraki
- Firewall

SSE

- Secure Access
- Secure Connect*

Identity

- Duo
- ISE
- TrustSec

Policy Management

- Cloud Control
- Meraki
- Catalyst Manager

Single vendor SASE

All use cases
supported

One SSE platform

Identity
differentiates SSE

Unified Policy plane

Zero Friction UZTNA Admin Experience!

Zero Imposters: Meet the NEW Cisco Duo!

Redefining and restoring trust in identity

Phishing Resistance

Proximity Verification

True Passwordless

Session Theft Protection

Identity Verification

Secure by Default IAM

Directory

Identity Broker

Device Trust

MFA + SSO

Identity Intelligence

Unifies Identity Signals

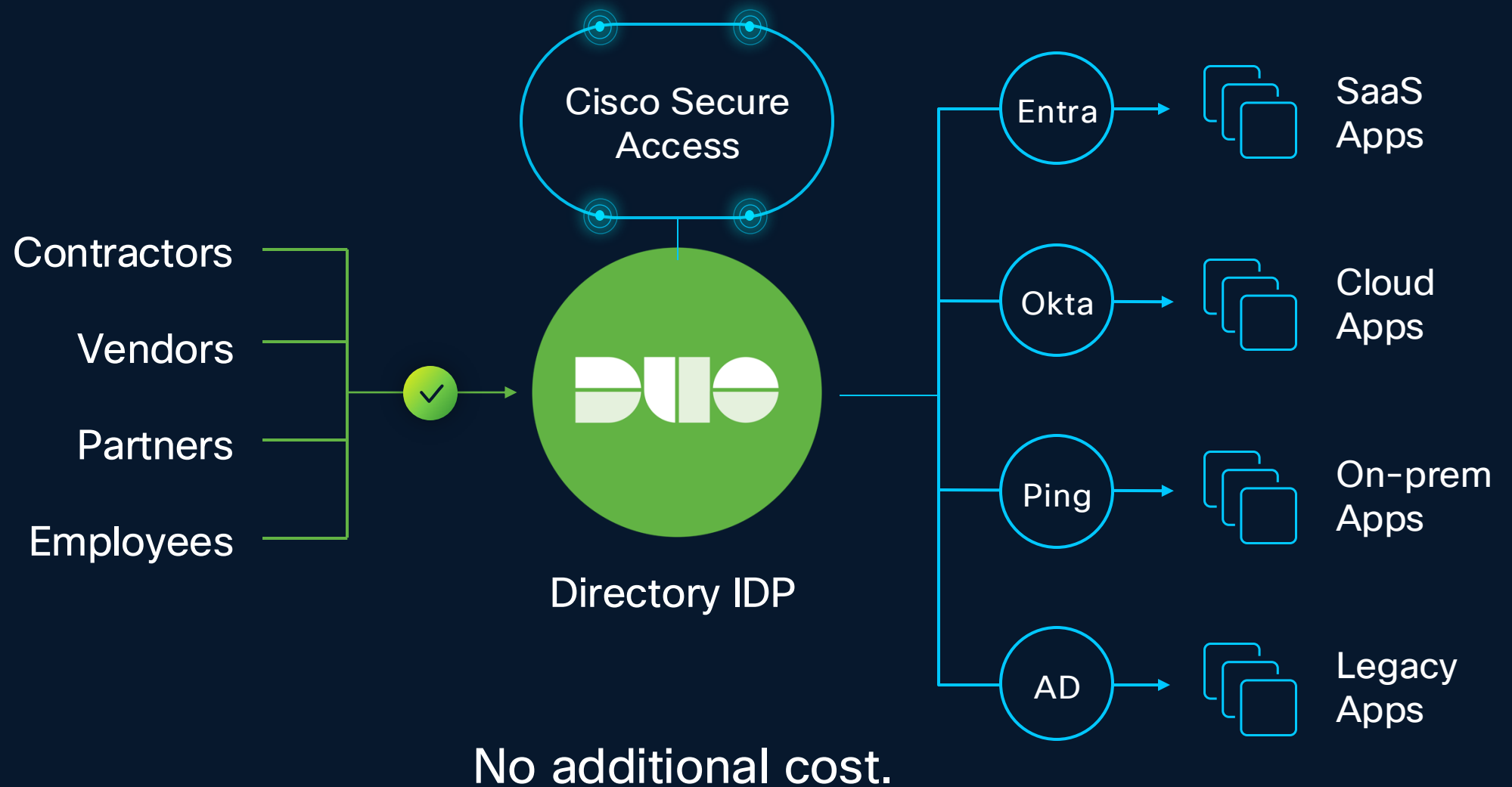
Detects Anomalies/Threats

Enforces with User
Trust Score

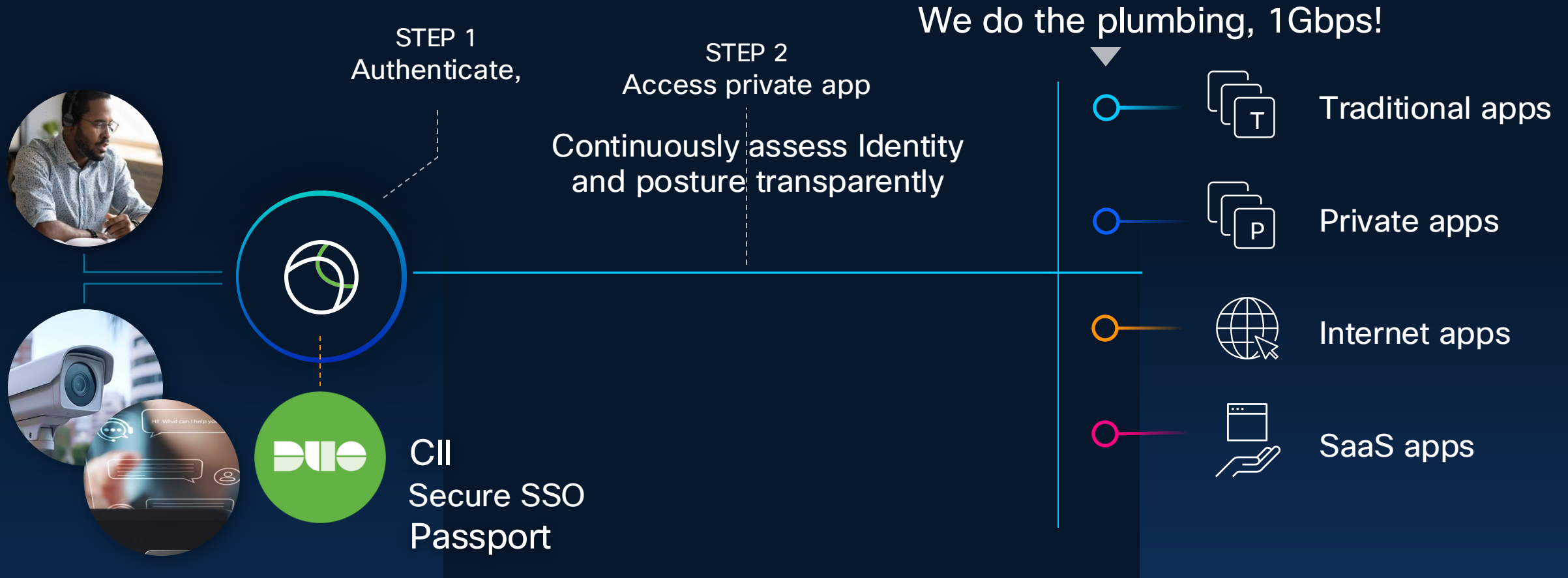
Standalone IAM
when required

Identity broker
for existing IAM

Alternate directory
for third-party users



Zero Friction: Transparent UZTNA



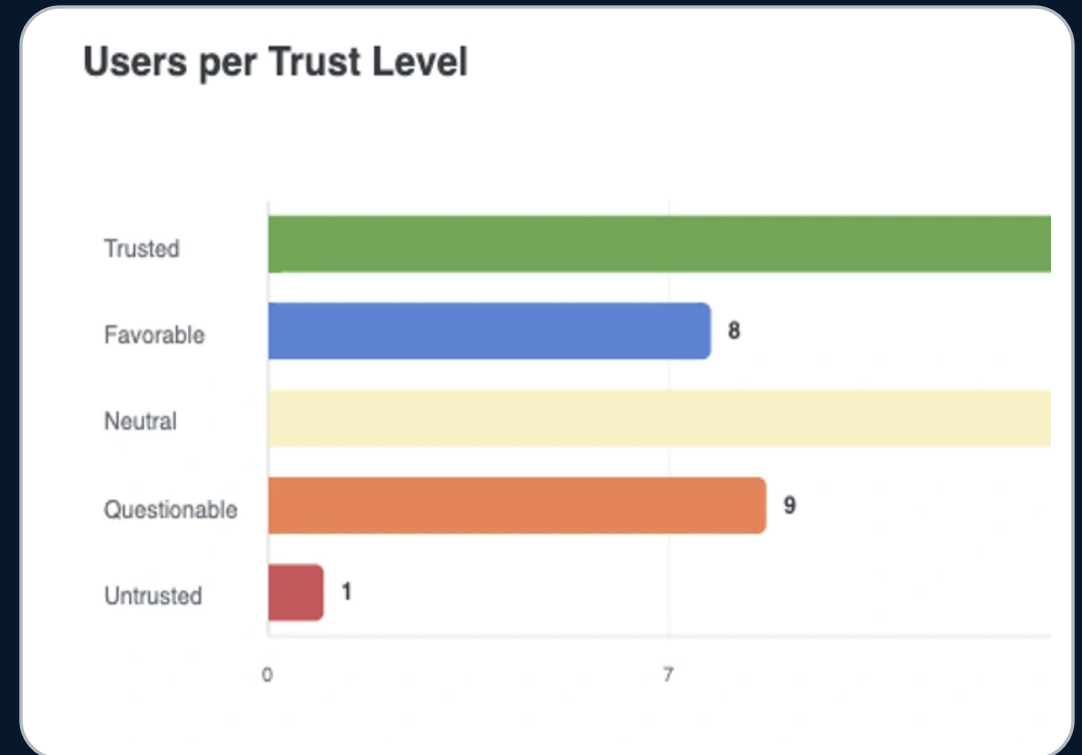
Zero imposters: Identity-based user trust level

- In Duo and Secure Access
- A user's trust level is determined via risk inputs
- Score dynamically changes

User risk inputs

- Inherent Risk (exec/admin roles)
- Posture Risk (MFA, password strength, device posture)
- Behavior Risk (recent activity, anomalies)
- Action Risk (real-time signals: IP, location, app)

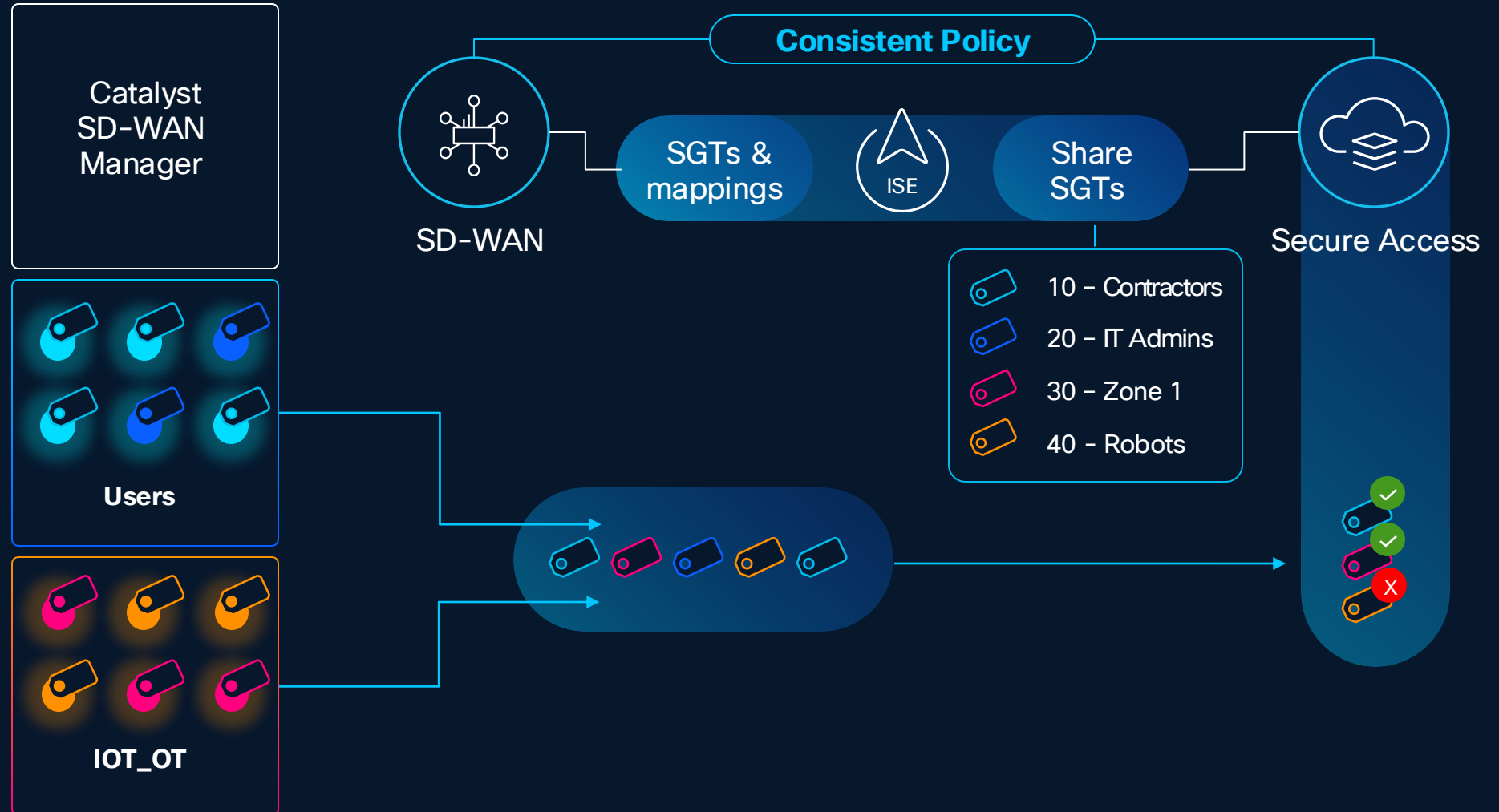
Trust level output



Identity Services Engine (ISE)

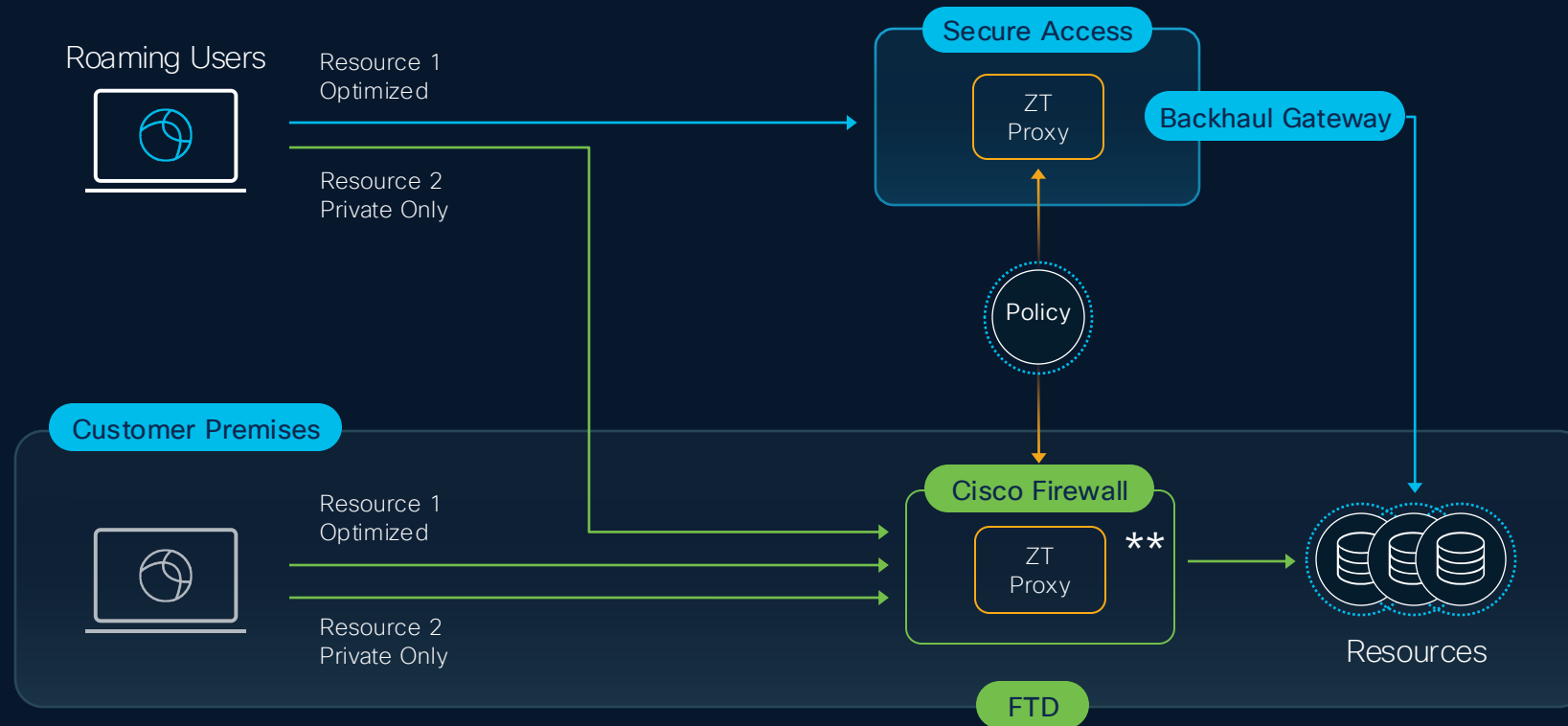
Leverage SGTs for granular access control

- 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



Hybrid Private Access for flexible enforcement

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



** Roadmap: policy enforcement on 8k routers

Workloads and Applications

Segmentation doesn't need to look like this



Simplifying and automating segmentation with Cisco



Cisco Cloud Protection for Workloads

Secure Workload | Isovalent | Hypershield

Visibility sources for discovery



User Identity

Discover user and endpoint telemetry from multiple sources



Application Dependency Mapping

Policy Discovery – User Identity Microsegmentation on Workloads!

Scope

Full Name

Primary App

Query

Finance Users

Root:CSW-SBG-Org:Campus:Finance Users

Invoice-App

* LDAP_memberOf contains Finance

or

* ISE_tag contains Finance

View Scope Details

Services 0

Pods 0

Workloads 2

IP Addresses 2

2 of 2 inventory

Address ↑↓

* ISE_tag ↑↓

* LDAP_memberOf ↑↓

10.40.100.56

Finance_Users

CN=RDS - All Devices Access,OU=Groups,OU=INSBU,DC=insbu,DC=lab, CN=RDS - Local Admin.

Scope

Full Name

Query

Sales Users

Root:CSW-SBG-Org:Campus:Sales Users

* LDAP_memberOf contains Sales

or

* ISE_tag contains Sales

View Scope Details

Services 0

Pods 0

Workloads 1

IP Addresses 1

1 of 1 inventory

Hostname ↑↓

Address ↑↓

Agent Type ↑↓

* ISE_tag ↑↓

* ISE_username ↑↓

TME-CSW-ALICE.tme-csw.lab

192.168.25.33

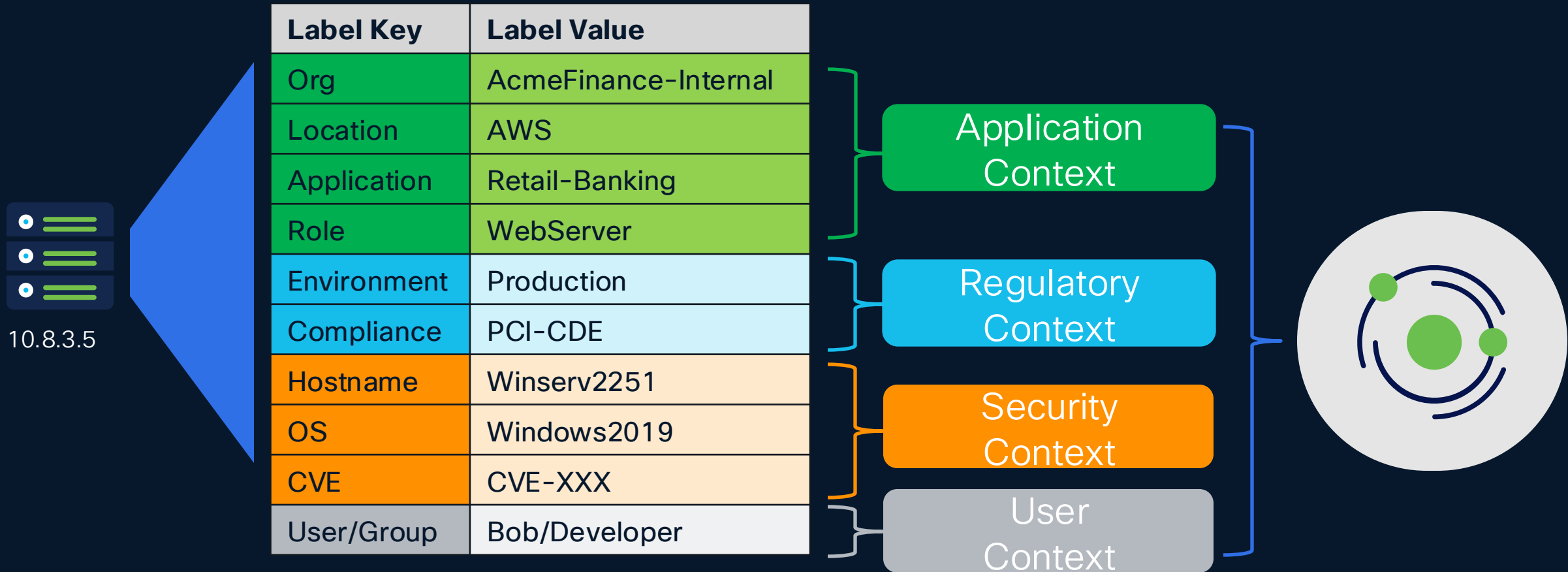
AnyConnect

Sales_Users

alice

Identifying workloads with context

Labels/tags/annotations



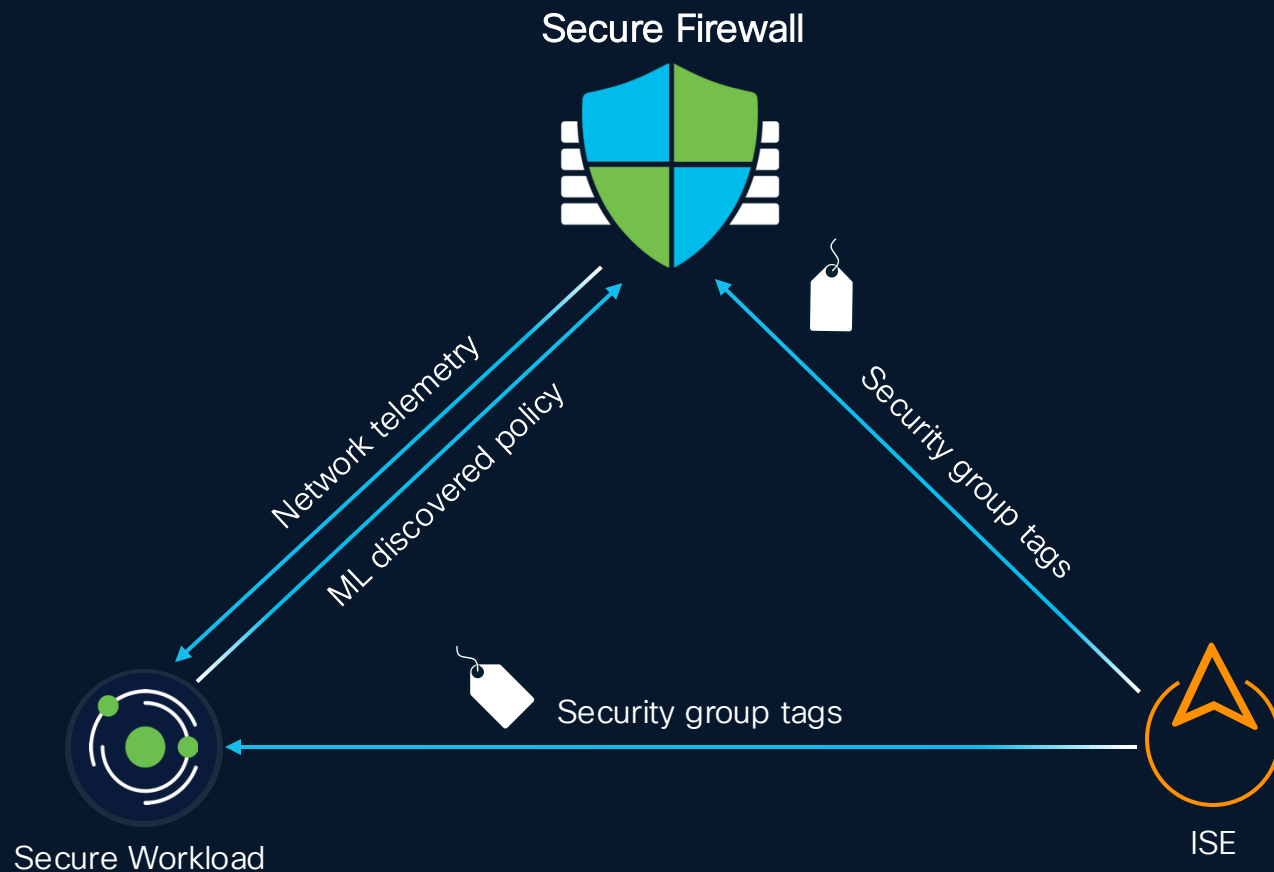
Policy Analysis

Comprehensive Toolkit for: Policy Validation, Versioning and Compliance



Share identity to apply consistent policies

Native integration



User based policy using ISE tags inline

ML powered policy discovery

Policies evolve as users and apps change

Application identity discovery

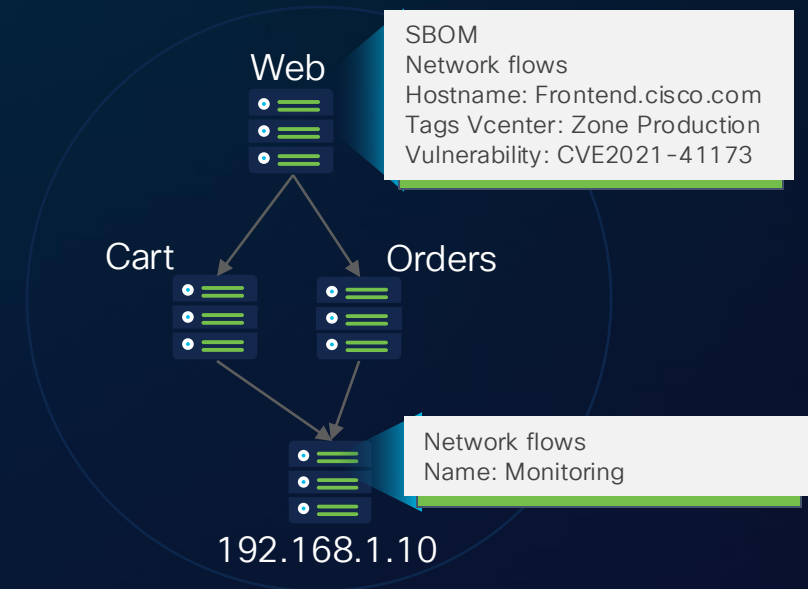
Discovering the application runtime identities!

Auto-discovery of application runtime inventory

- Network endpoints and workloads
- Network flows and processes
- Filesystem and others

Enrichment

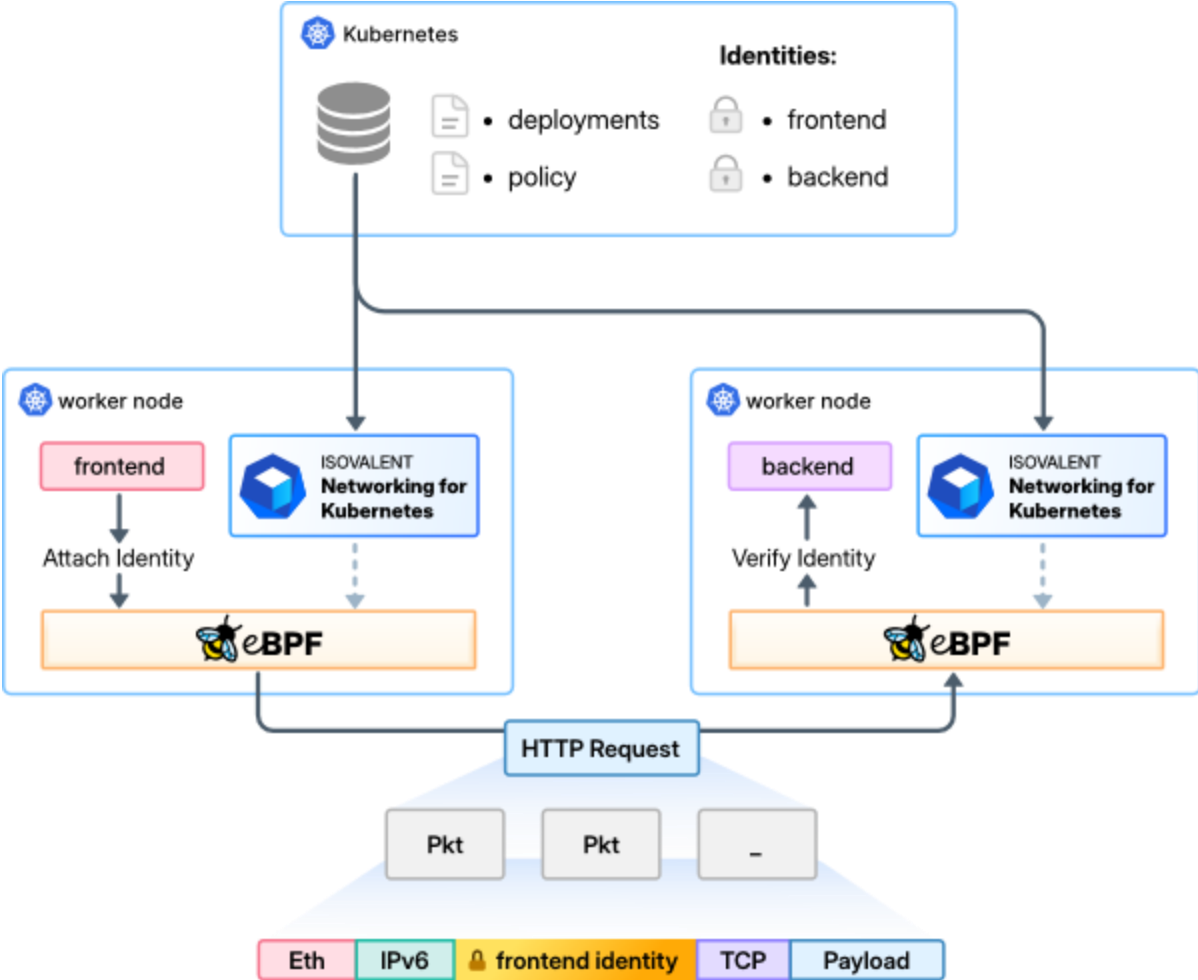
- Software bill of materials (SBOM)
- Vulnerabilities
- User defined
- External systems



Application Identity Discovery



Identity-based Security for Kubernetes



Flexible segmentation enforcement

Enforce closest to the application with whichever control point is right for YOU!



Network

Smart Switches

ACI

Load Balancers



Host

Windows

Linux

Bare Metal

etc



Kubernetes

Isovalent



Public Cloud

Native controls in

AWS

Azure

etc



Firewalls

Cisco Firewalls

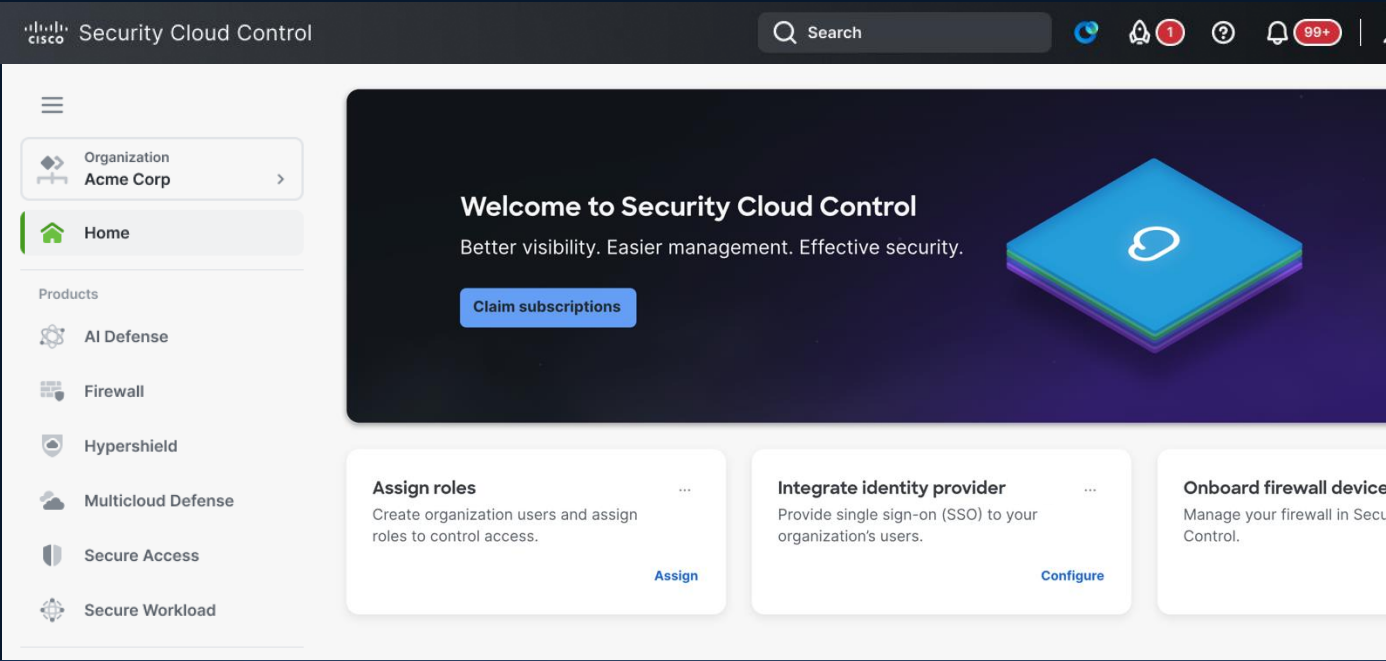
Multicloud Defense

3rd Party

Wrap-up

Security Cloud Control

AI-native unified security management



Secure Firewall

Multicloud Defense

Hypershield

Secure Workload

Secure Access

AI Defense