Cisco Zero Trust

Řízení přístupů uživatelů a zařízení do sítě

Andrej Jeleník

Systems Engineer, Cisco ČR

Complementary security approaches

Threat-Centric

Basic security maturity to prevent attacks via an intelligence-based policy – then detect, investigate, and remediate

Dynamic Context

Trust-Centric

Good security practice to verify before granting access via a identity-based policy – for any user, any device, any app, in any location

Three pillars of Zero Trust

Zero-trust people

Authenticate users and continuously monitor and govern their access and privileges. Secure users as they interact with the internet.

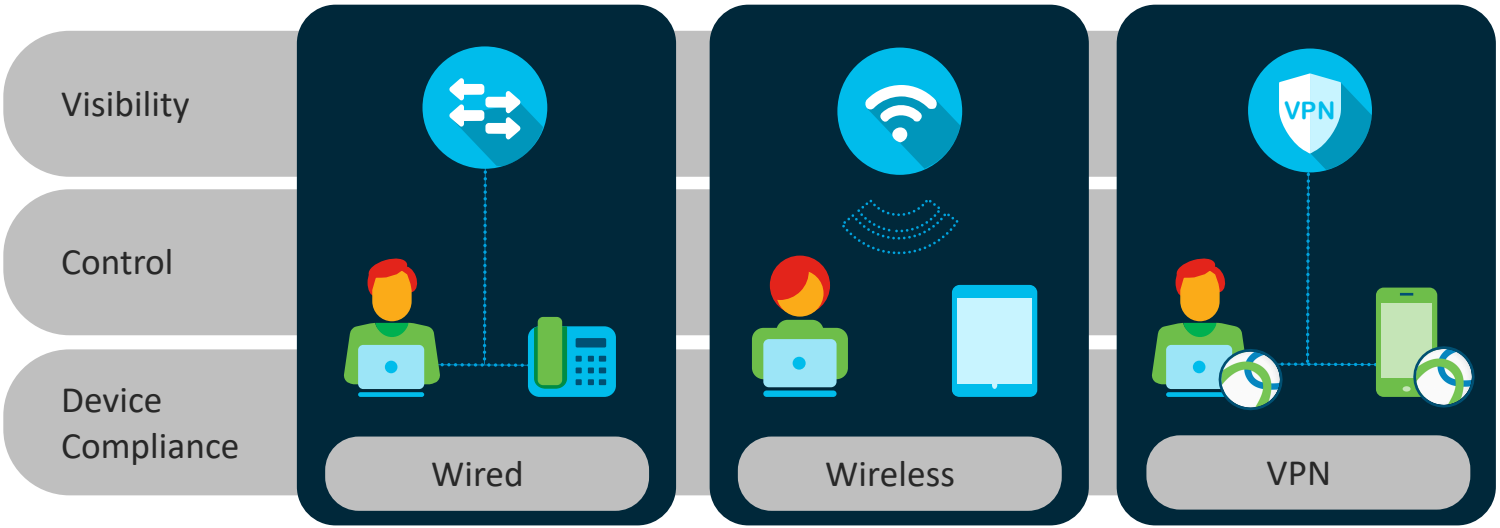
Zero-trust workloads

Enforce controls across the entire app stack, especially connections between containers or hypervisors in the public cloud.

Zero-trust data

Secure and manage data, categorise and develop data classification schemas, and encrypt data both at rest and in transit.

Smaller, more frequent, context-based decisions with **Identity Services Engine** (ISE)



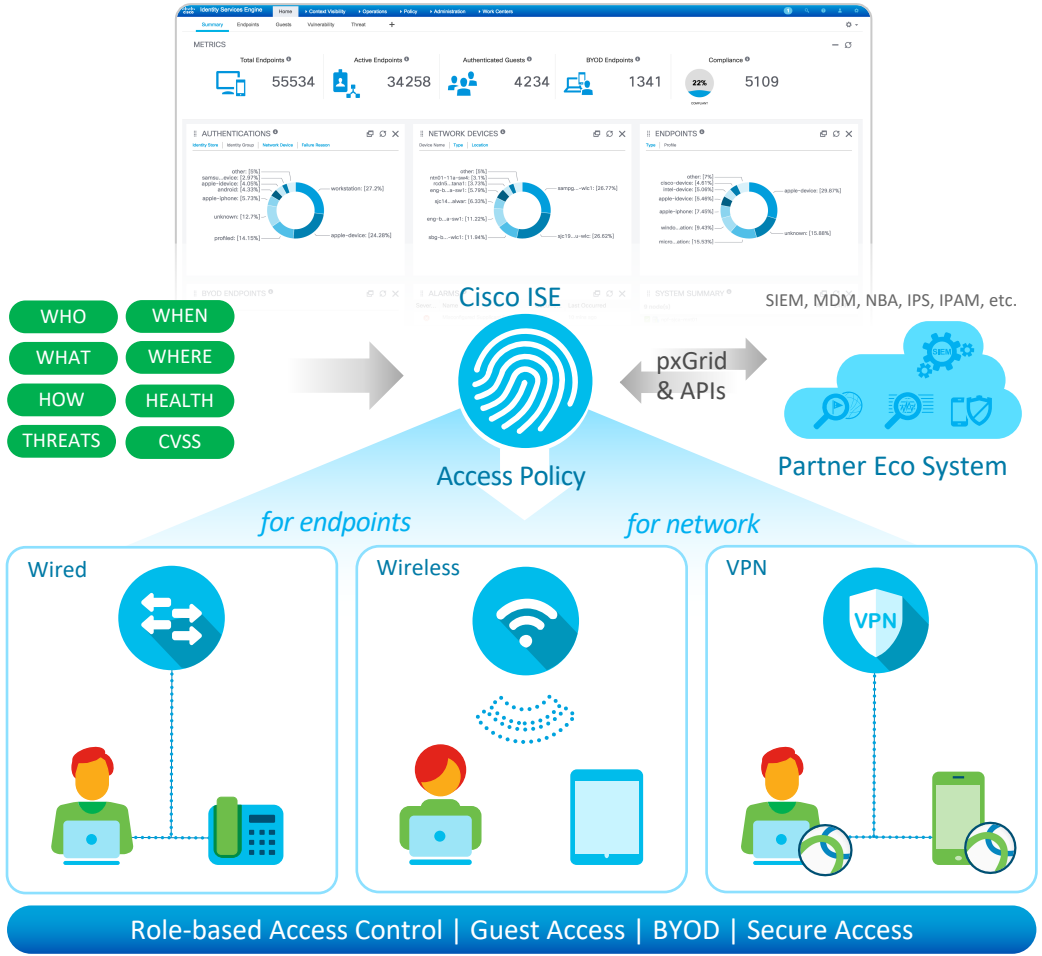
Cisco ISE Overview

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform, that lets you:

See
Users, endpoints and applications

Secure
By controlling network access and segmentation

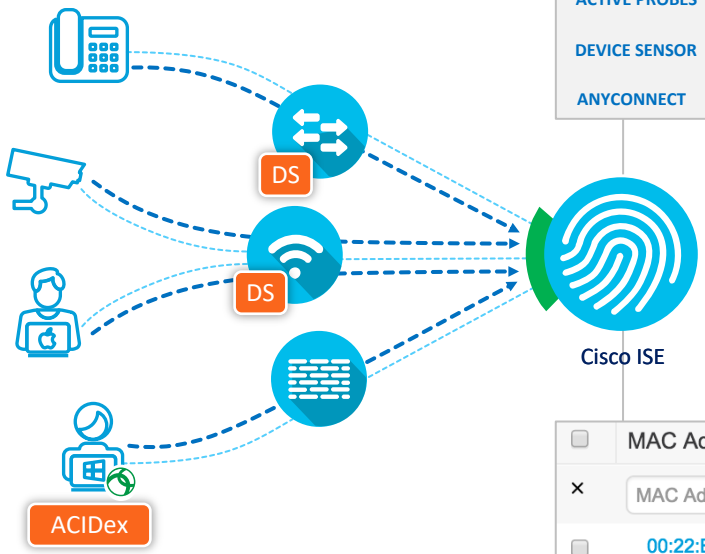
Share
Context with partners for enhanced operations



Visibility

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data, that reveal their device identity



ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

ISE data collection methods for Device profiling

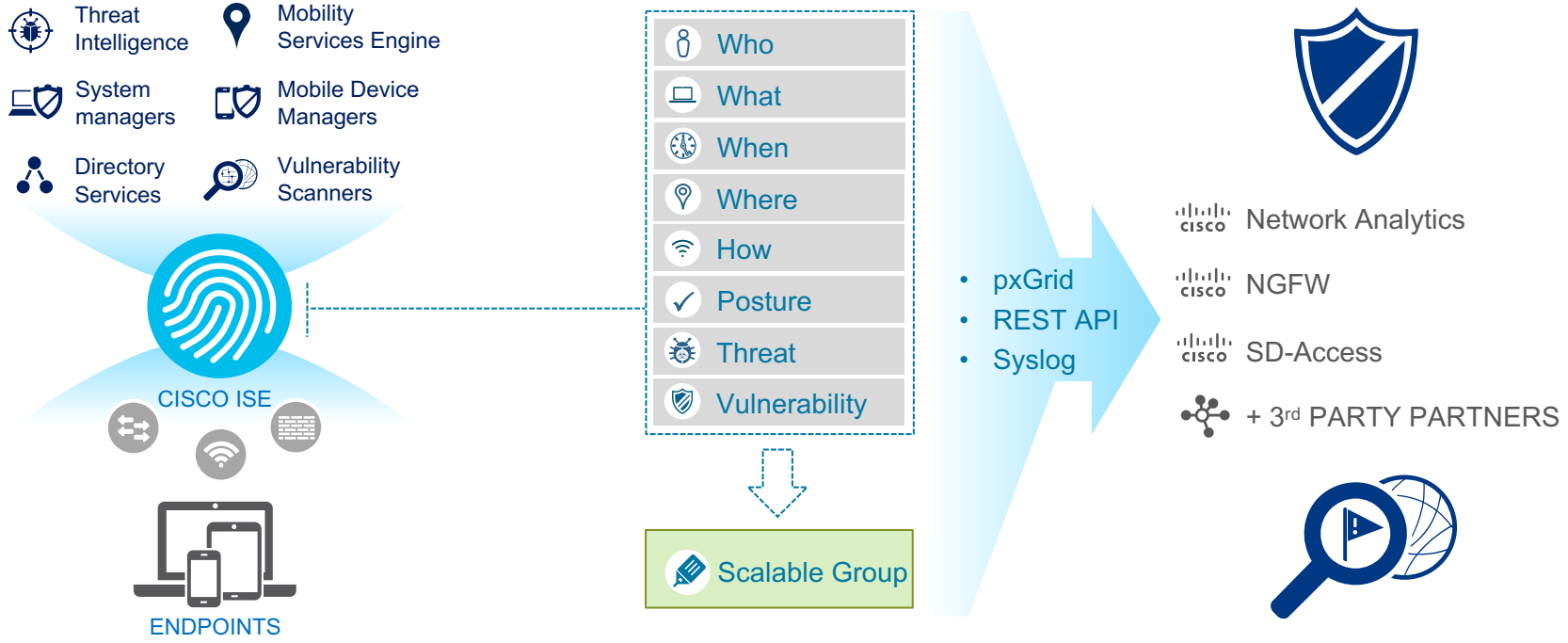
Cisco ISE

Feed Service
(Online/Offline)

MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

Context Build, Summarize, Exchange



Visibility and Access Control

ISE builds context and applies access control restrictions to users and devices

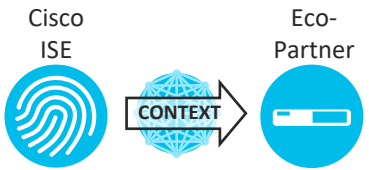
Context Reuse

by eco-system partners for analysis & control

External Services

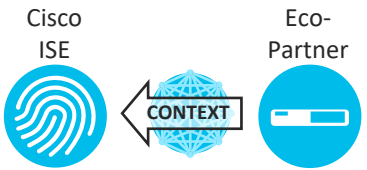
Eco system partnership to enrich, exchange context and enact

Context to Partner



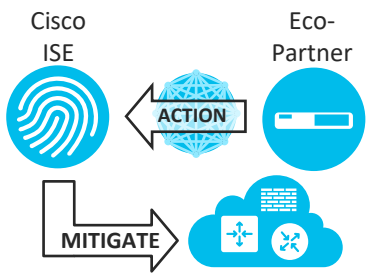
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Enrich ISE Context



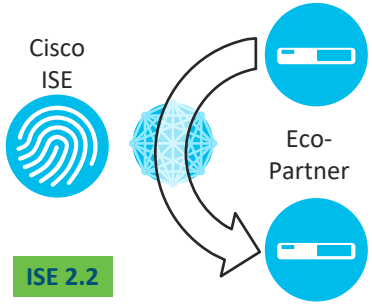
Enrich ISE context. Make ISE a better Policy Enforcement Platform

Threat Mitigation



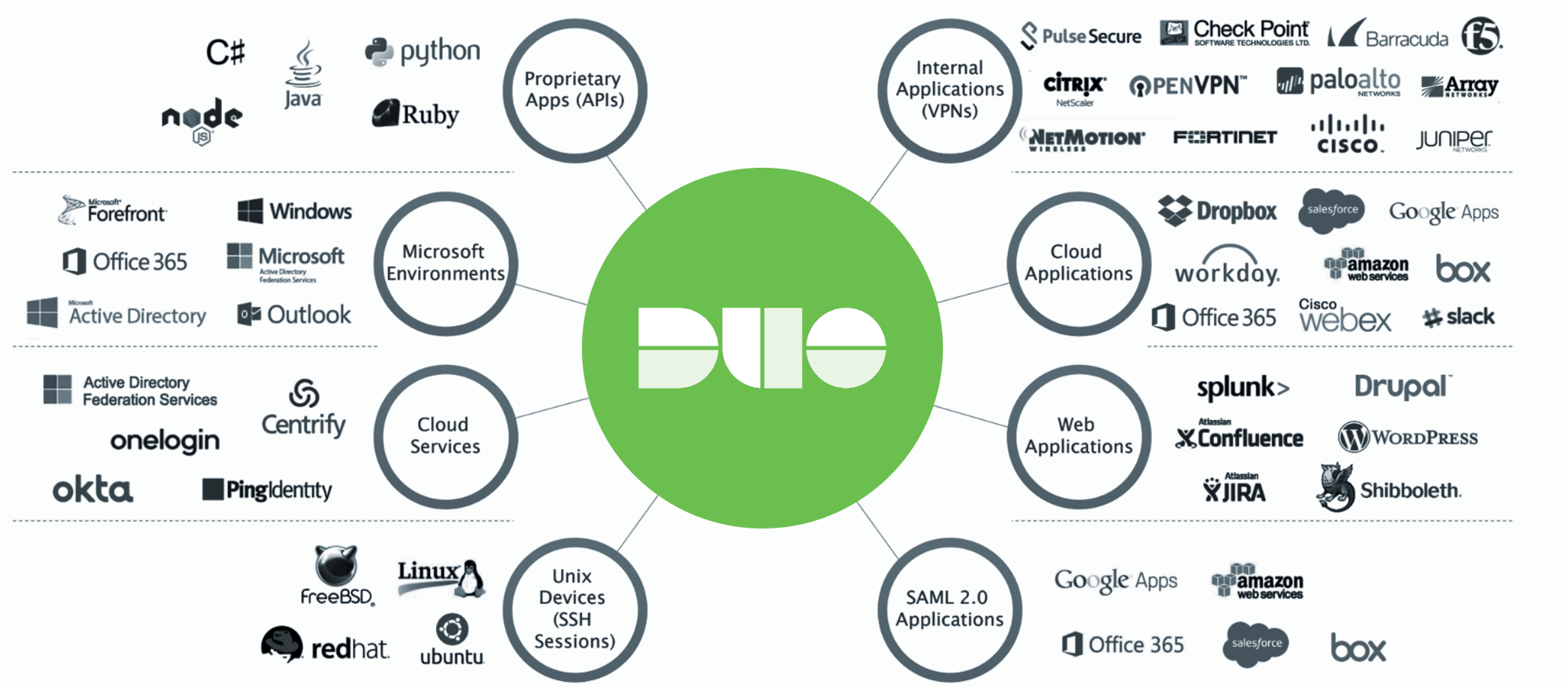
Enforce dynamic policies in to the network based on Partner's request

Context Brokerage



ISE brokers Customer's IT platforms to share data amongst themselves

Secure Any Corporate Application with Multifactor Auth



Integration documents are available at duo.com/docs

Workforce: Establish Trust

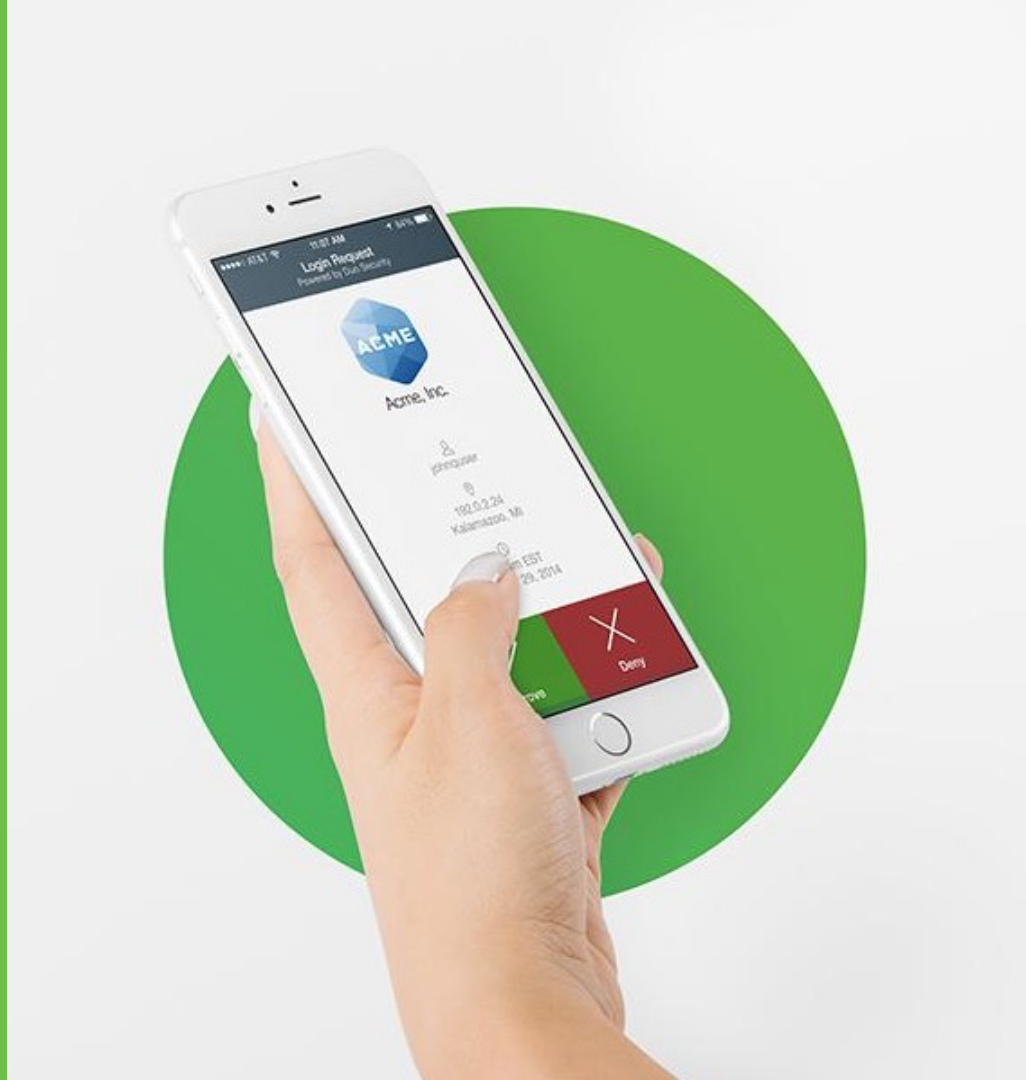
Verify User & Device Trust

Duo's Multi-Factor Authentication (MFA)

- Users authenticate in seconds – one-tap approval
- Scalable service that can be deployed in hours
- Natively integrates with all apps

Device Trust

- Check devices for vulnerable software & security features
- Identify managed vs. unmanaged
- Notify users of out-of-date devices



Workforce: Enforce Trust-Based Access

Enforce Policies for Every App

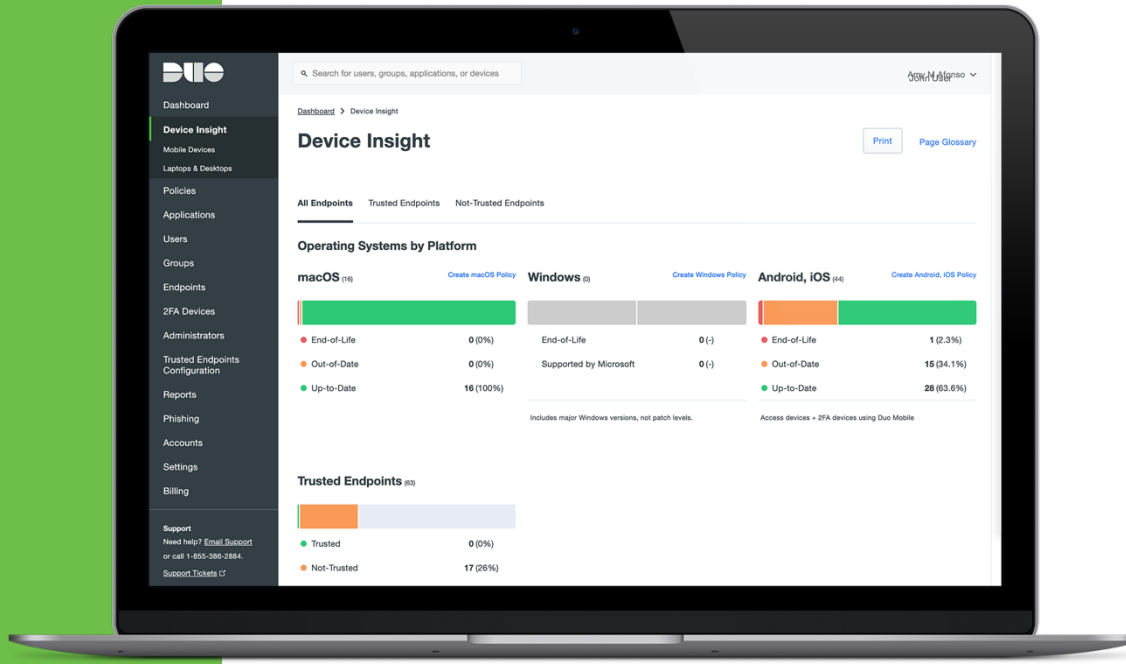
- Custom security policies based on user & device trust. Examples:
  - Block users logging in from anonymous networks
  - Block access by unencrypted devices
- Integrates to protect every application

Workforce: Continuously Verify Trust

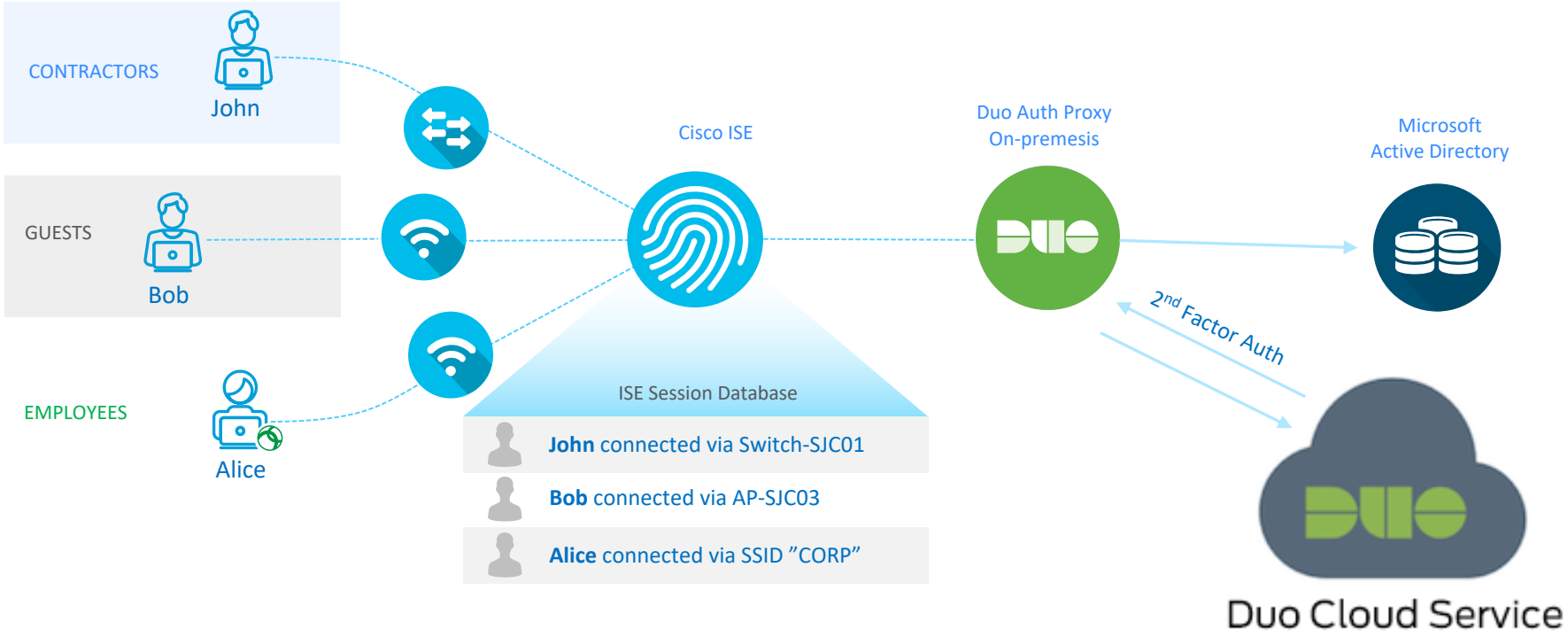
Monitor Risky Devices

Duo's Device Trust:

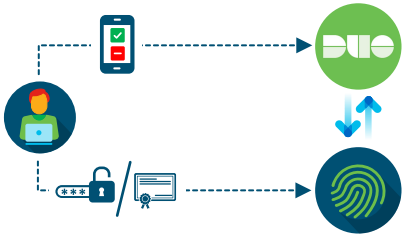
- At every login, Duo checks users' devices for security health & status
- Duo detects managed and unmanaged mobile & desktop devices
- Enforce device-based access policies to protect against vulnerable devices



ISE and Duo Integration for MFA

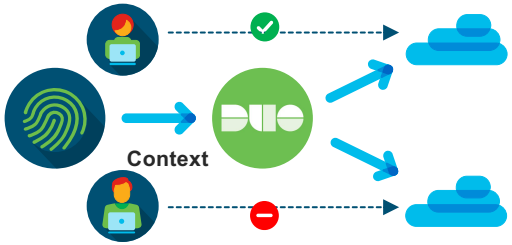


2FA for network access



Chain ISE RADIUS / Web authentications with 2nd factor authentication from Duo for secure network access.

Granular policies

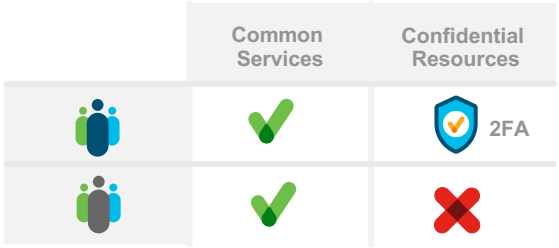


Duo consumes contextual data from ISE to make better access control decisions

Zero Sign-on

Duo trusts ISE authorization to provide access to cloud applications without MFA

Step-up Authentication

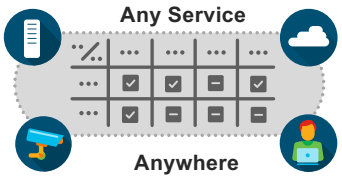


Specific network / application access is subject to additional screening

Duo Context to ISE

ISE receives endpoint telemetry from Duo

Consistent Access Policies



Network through Application, Group based policies

Duo never touches the primary authentication

Primary Authentication
Performed by you. Duo never sees users' passwords.

Server Communication
Duo integrations

Request Sent to Duo
Core service and policy engine is always in the cloud

Secondary Authentication
User verifies login on their device.

- Duo Push
- Mobile Passcode
- Phone, SMS
- HOTP Token
- U2F/WebAuthN
- Bypass

Success!
User is logged in.

Zero Trust Story

Job 1

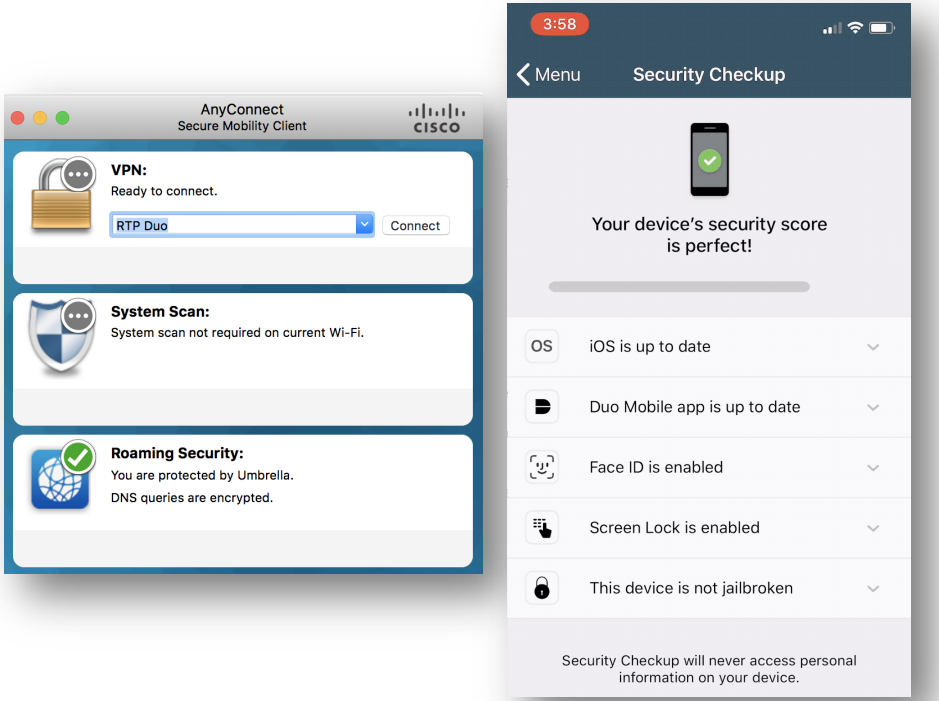
Establish User Trust

2FA is one of the easiest and most effective ways to immediately **reduce security and compliance risk**.

Job 2

Establish Device Trust

Establish **device trust**



Job 3

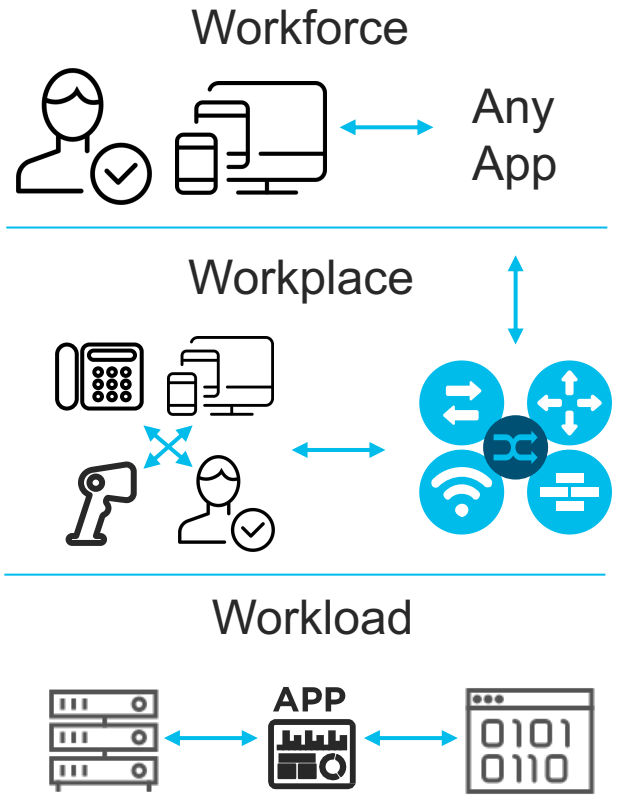
Gain Visibility

Gain **visibility** into **users**, **devices** and **workloads**

Job 4

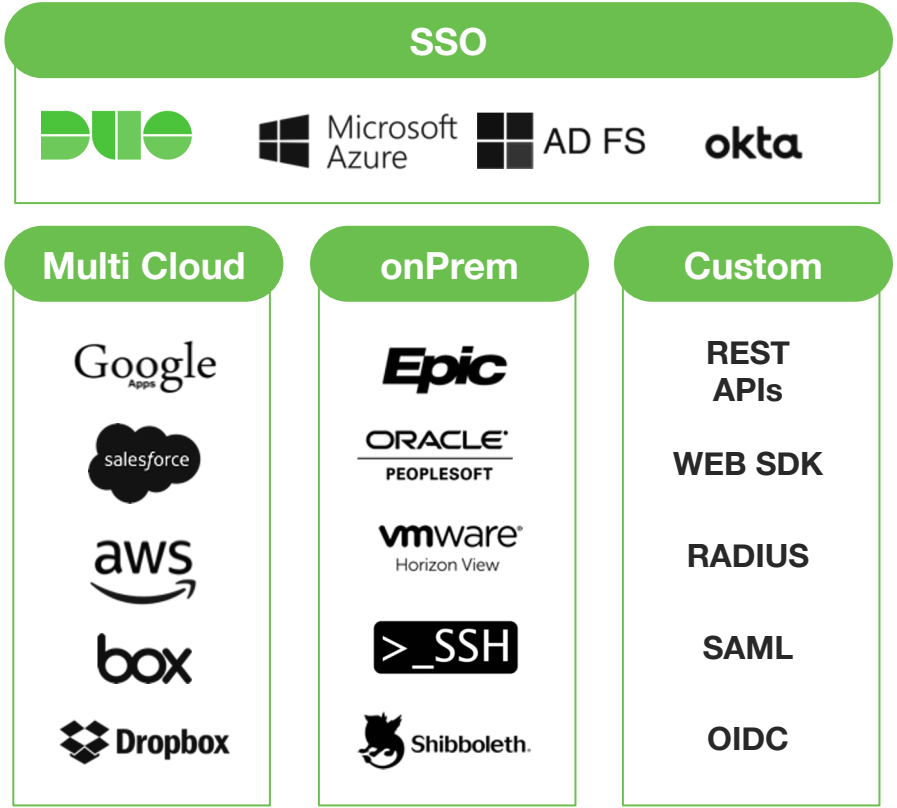
Enforce Adaptive Access Policies

Customized policies based on workforce, workplace and workload



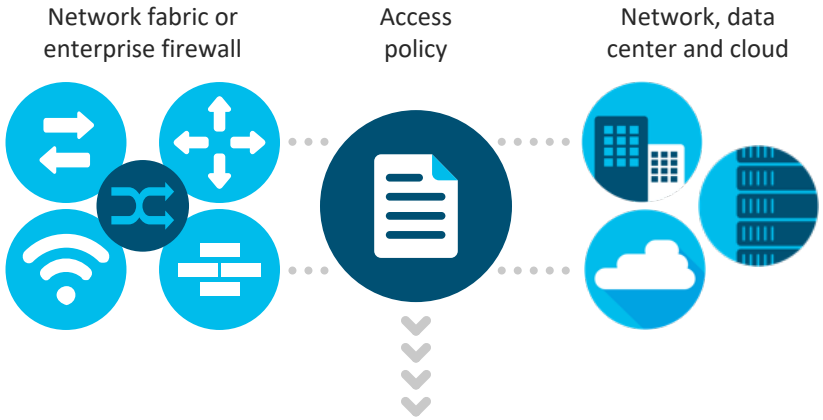
Job 5 - Workforce

Grant workforce easier, safer access to specific work apps

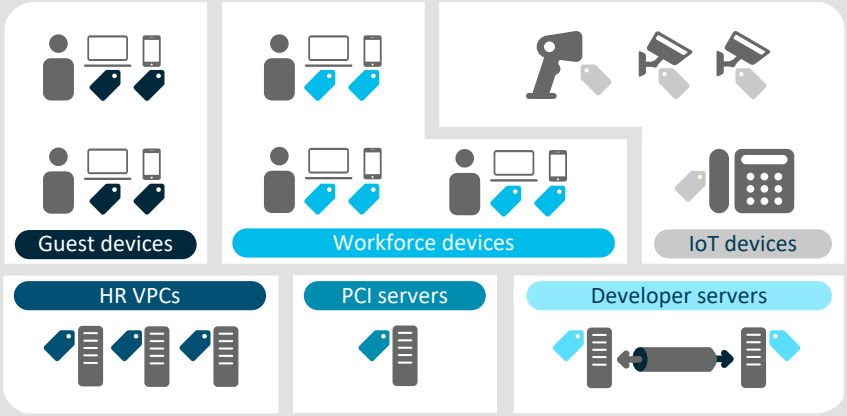


Job 5 - Workplace

Grant secure access to the Network with Segmentation

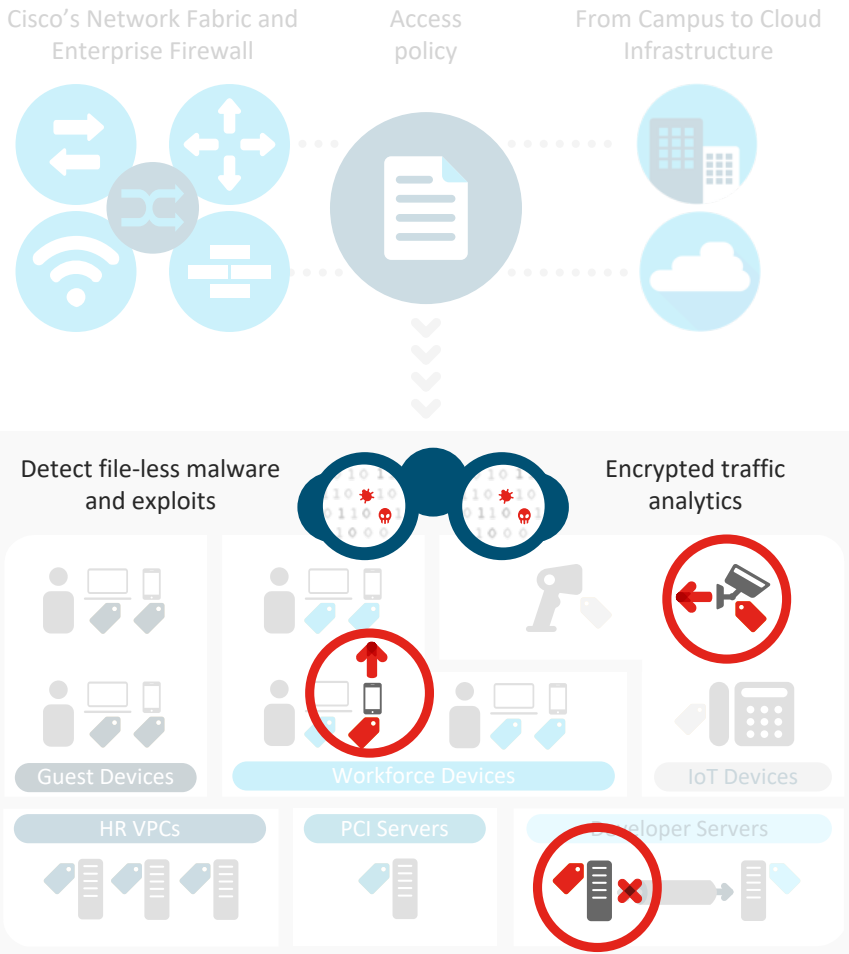


Reduced attack surface based on business intent; not network topology (e.g. VLANs)



Job 6

Continuous Monitoring & Response



Cisco Trusted Access – Guided Progression

1 User Trust

2 Device Trust

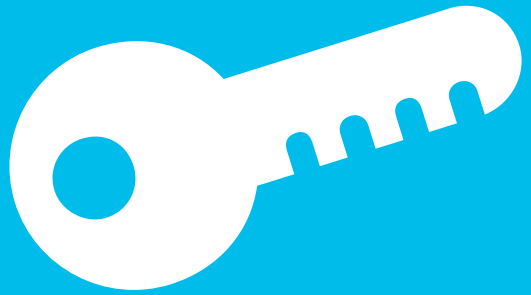
3 Visibility

4 Enable Access

5 Enforce Contextual Policies

6 Continuous monitoring and Response

Using a practical Zero Trust approach to security



Key point: User ID is extremely important, but so is the trustworthiness of the endpoint.


CISCO