CISCO

You make **possible**

Architecting Security for a Zero Trust Future

Jamey Heary, Distinguished Architect
Jamie Sanbower, Principal Architect
Jatin Sachdeva, Technical Solutions Architect

TECSEC-2609

Barcelona | January 27-31, 2020

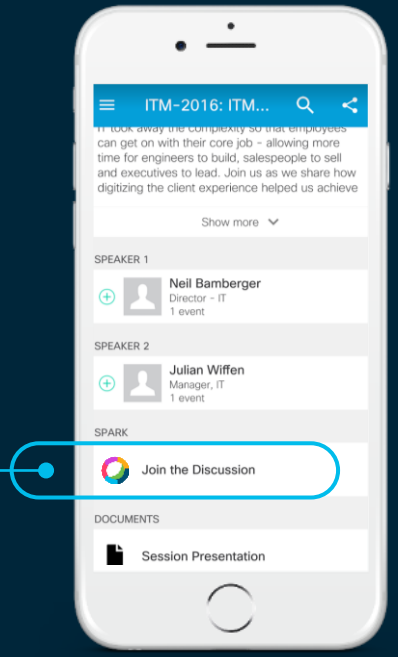
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



cs.co/ciscolivebot#TECSEC-2609

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

A little bit about Jamey…

Cisco role: Distinguished Systems Architect focused on Security at the architecture and cross-architecture level

Unofficial title:
"Cisco integrations enforcer"

Experience: 25yr+ in cyber security industry

Fun fact 1: Published 3 books, all on access control topics (No more!.. probably…)

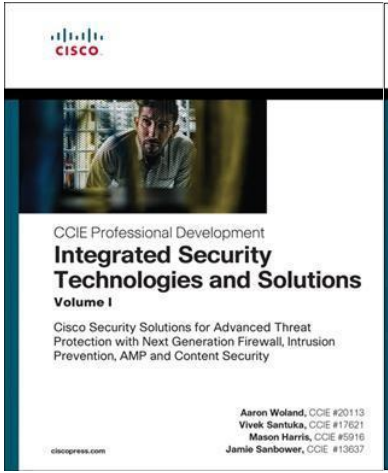
Fun fact 2: 8yr PCI Org Board of Advisors member 😮

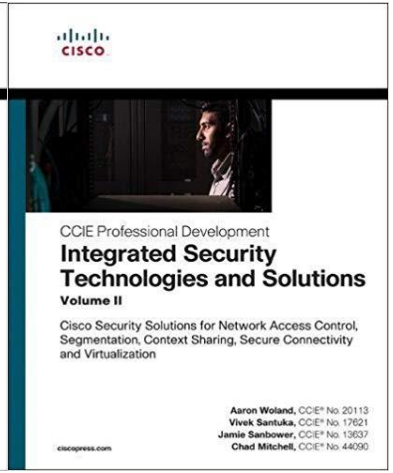
Fun fact 3: My "home" network has a power bill on par with a super target

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Jamie Sanbower

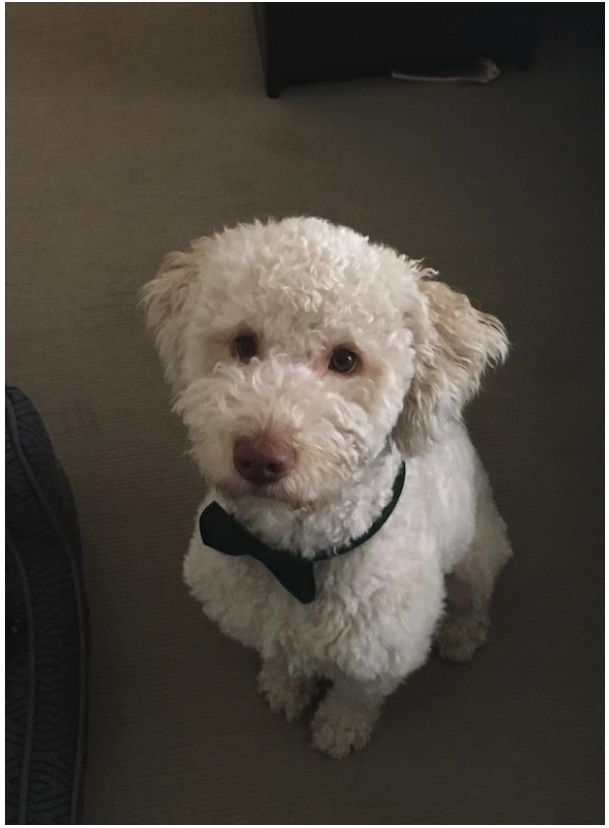
- Global Security Architecture Team
- 15+ years of security and networking experience
- Prior to Cisco…
  - Cisco Partner
  - Network and Security Consultant
  - Large Design, Deployments, Integrations, and Troubleshooting
- Live in Melbourne, FL





 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Jatin



- Global Security Architecture Team
- 18 years in security industry, 15 in Cisco.
- Prior to Cisco – security consulting, implementation and audit
- Fun fact – I am Indian but don't play cricket and can't take spicy food!
- Lives in Melbourne, Australia

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction to Zero Trust
- Cisco's Zero Trust Architecture
- Zero Trust for the Workforce
- Zero Trust for the Workload
- Zero Trust for the Workplace
- Conclusion

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction to Zero Trust

Shift in IT Landscape

Users, devices and apps are everywhere

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IT Challenges

Increased diversity in access & gaps in visibility

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Challenges

Increased attack surface, deficient access control & gaps in threat protection

Incident response way too slow 10K devices encrypted in <10mins!

300% Increase in malware for IoT devices

Business impact of a breach rising

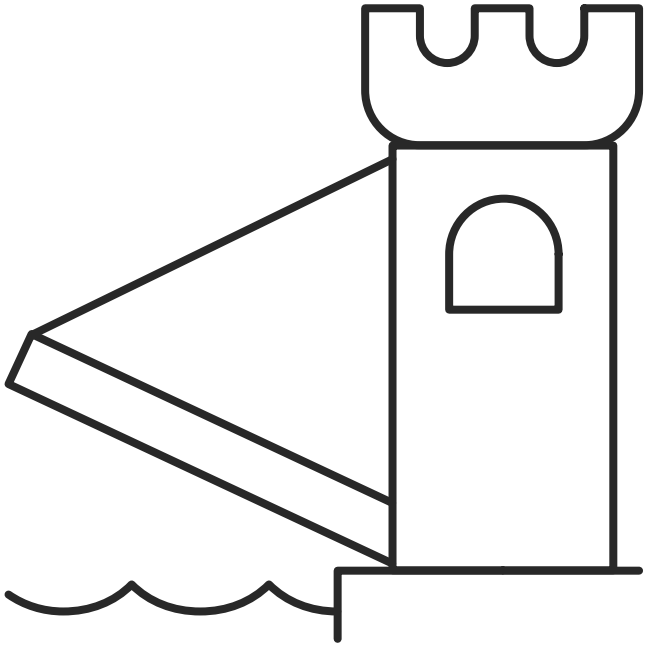
81% of breaches involved weak or stolen passwords

Security tools going blind due to privacy and encryption methods

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The traditional security model

Where was the trust boundary?

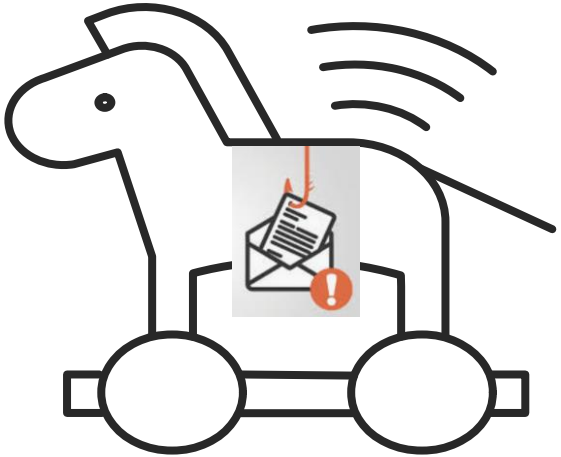


Perimeter-based defense

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

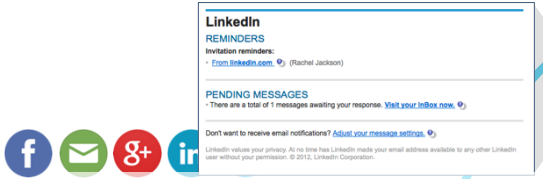
The age-old issue with this model

Changing Landscape, weapons & tactics



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

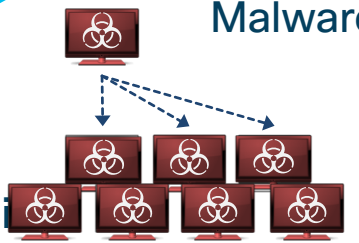
When we trust too much…



Victim clicks phishing email li

Information monetized

Perimeter bypassed
Malware exploits vuln



Lateral Movement

Pivot to DC, password harvesting

Data Exfiltration using
Admi rivilege

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Infection **Monkey**

1. Run Monkey Island Server ✔
2. Run Monkey
3. Infection Map
4. Security Report
5. Start Over

Configuration

Log

Powered by Guardicore

License

1. Monkey Island Server

Congrats! You have successfully set up the Monkey Island server. 👏👏

The Infection Monkey is an open source security tool for testing a data center's resiliency to perimeter breaches and internal server infections. The Monkey uses various methods to propagate across a data center and reports to this Monkey Island Command and Control server.

To read more about the Monkey, visit infectionmonkey.com

Go ahead and run the monkey.

Infection Monkey

Infection Monkey Version: 1.6.3

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   Ap5JVb-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUmZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

If you already purchased your key, please enter it below.
Key: _

Basic Tenant of Zero Trust

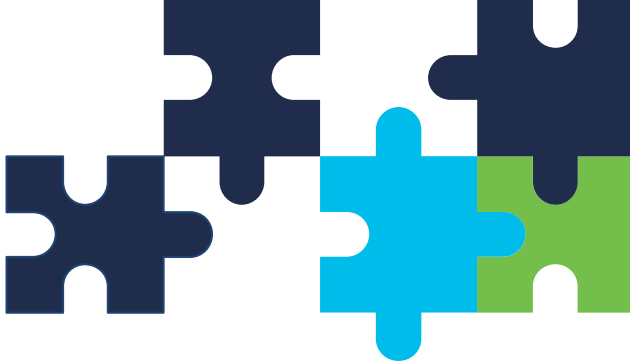
The effect of Zero Trust is

Ubiquitous Least-Privilege Access

(i.e. grant access, but make it specific!)

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

What's Different in a Zero-Trust Approach



The Traditional Approach

Trust is based on the network location that an access request is coming from. → Enables attackers to move laterally within a network to get to the crown jewels.

Doesn't extend security to the new perimeter.

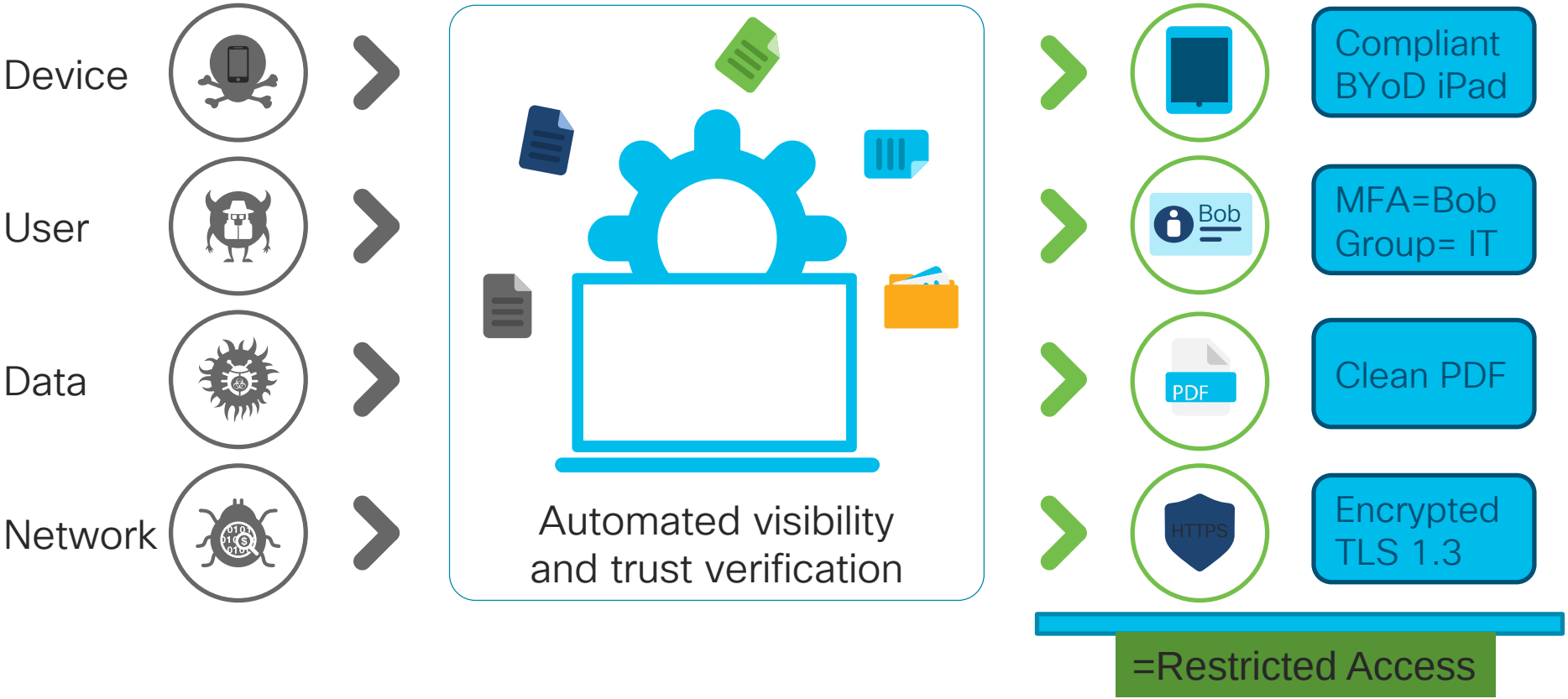
The Zero Trust Approach

Trust is established for **every access request**, regardless of where the request is coming from. → **Secures access** across your applications and network. Ensures only right users & devices have access.

Extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environments & more.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust: Malicious Until Proven Otherwise



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

A Little Bit of Zero Trust History

Jericho Forum	ZT	BeyondCorp	ZTX	ZTA
2004	2010	2014	2017	TODAY

De-perimiterization

An international group of corporate CISOs and vendors (Cisco hosted initial meeting)

Focused on solving “de-perimiterization” problem

Early output calling for “the need for trust”

Multiple models emerge

Forrester coined Zero Trust. NGFW biased

Google cloud first ZT arch, BeyondCorp

Forrester then expands to Zero Trust eXtended

Generalized

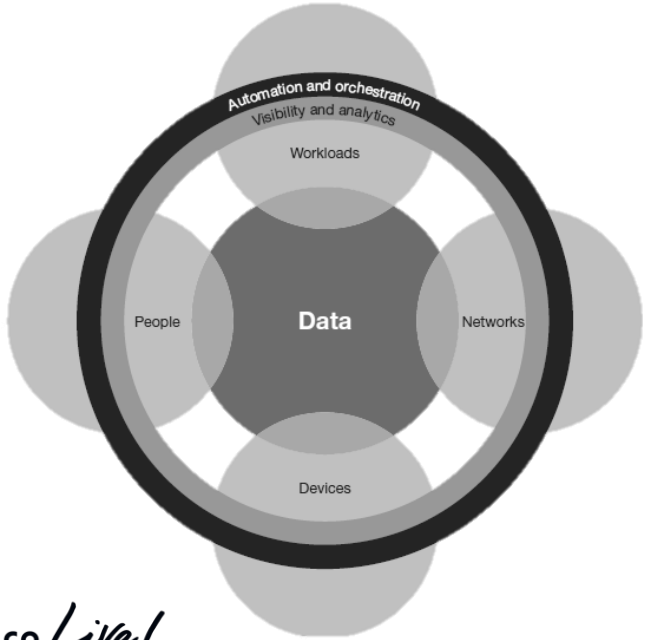
The industry has largely accepted Zero Trust Architecture as the general term

Interest

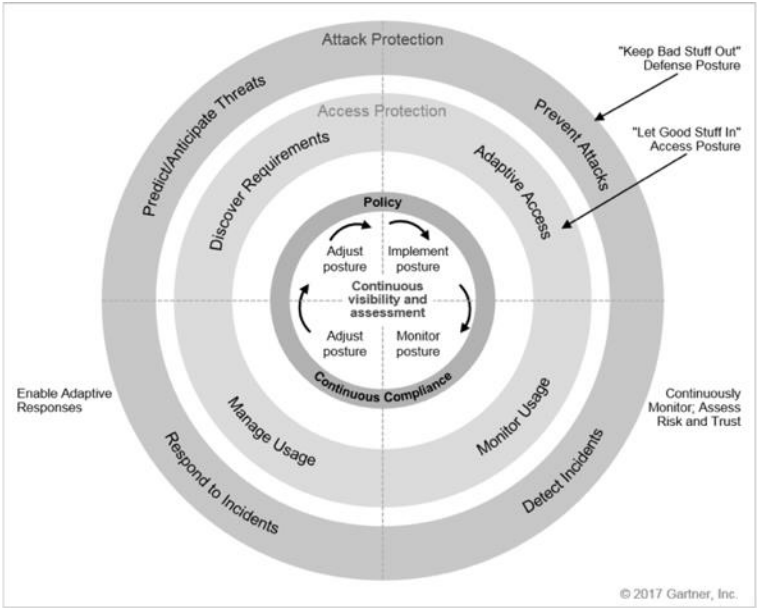
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The analysts shape the momentum… what's old is new again!

FORRESTER® Zero Trust eXtended



Gartner Continuous Adaptive Risk and Trust Assessment



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Marketing learns the term ZTA...

Everyone who had a security product magically has a zero trust solution now.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

…and many more

Everyone who had a security product magically solves Zero Trust now.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Forrester's Zero Trust models

2010 Model → **2017+ Model**

Originated with three tenets

Designed to have three pillars. He left Forrester in 2017.

Extended to six pillars

Forrester adds three more pillars. Includes automation & orchestration as well as visibility & analytics across the entire solution.

"Technology must have considerable and specific technical capabilities in at least 3 pillars of this framework AND a powerful API integration capability to be considered a ZTX platform." -Forrester

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The original three tenets of a Zero Trust network

Eliminate network trust

Assume all traffic, regardless of location, is threat traffic until it is verified that it is authorized, inspected, and secured.

Segment network access

Adopt a least privilege strategy and strictly enforce access control to only the resources users need to perform their job.

Gain network visibility and analytics

Continuously inspect and log all traffic internally as well as externally for malicious activity with real-time protection capabilities.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Three key new pillars of Zero Trust eXtended

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, categorize and develop data classification schemas, and encrypt data both at rest and in transit.

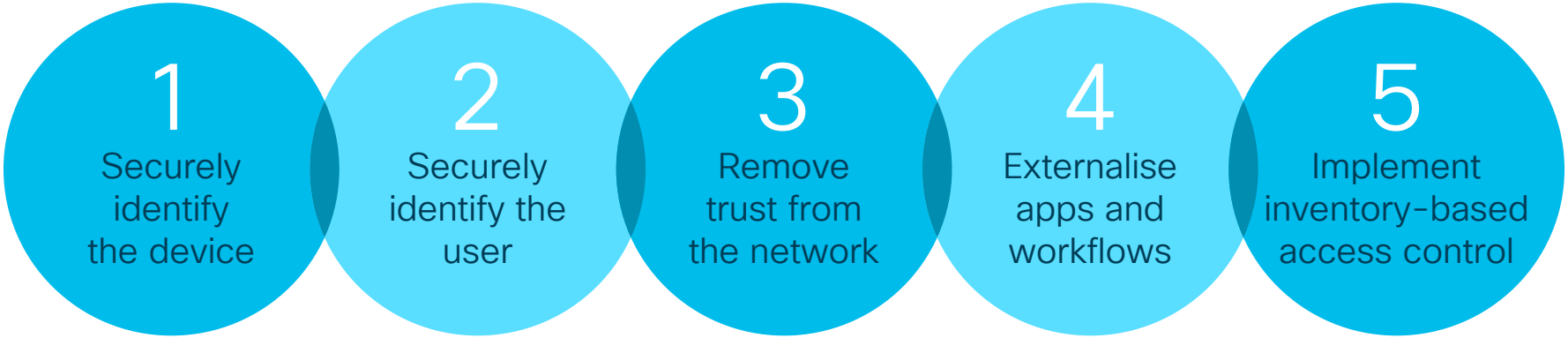
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Gartner's Continuous Adaptive Risk and Trust Assessment

- Security posture must constantly change
- Digital risk and trust vary over time
- Score and rate all entities
- Shift away from 1-time binary decisions
- Extend the approach outside the enterprise

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Google's BeyondCorp implementation of Zero Trust



Fun Fact: Cisco DUO Beyond was first commercial implementation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Google's BeyondCorp Implementation of Zero Trust

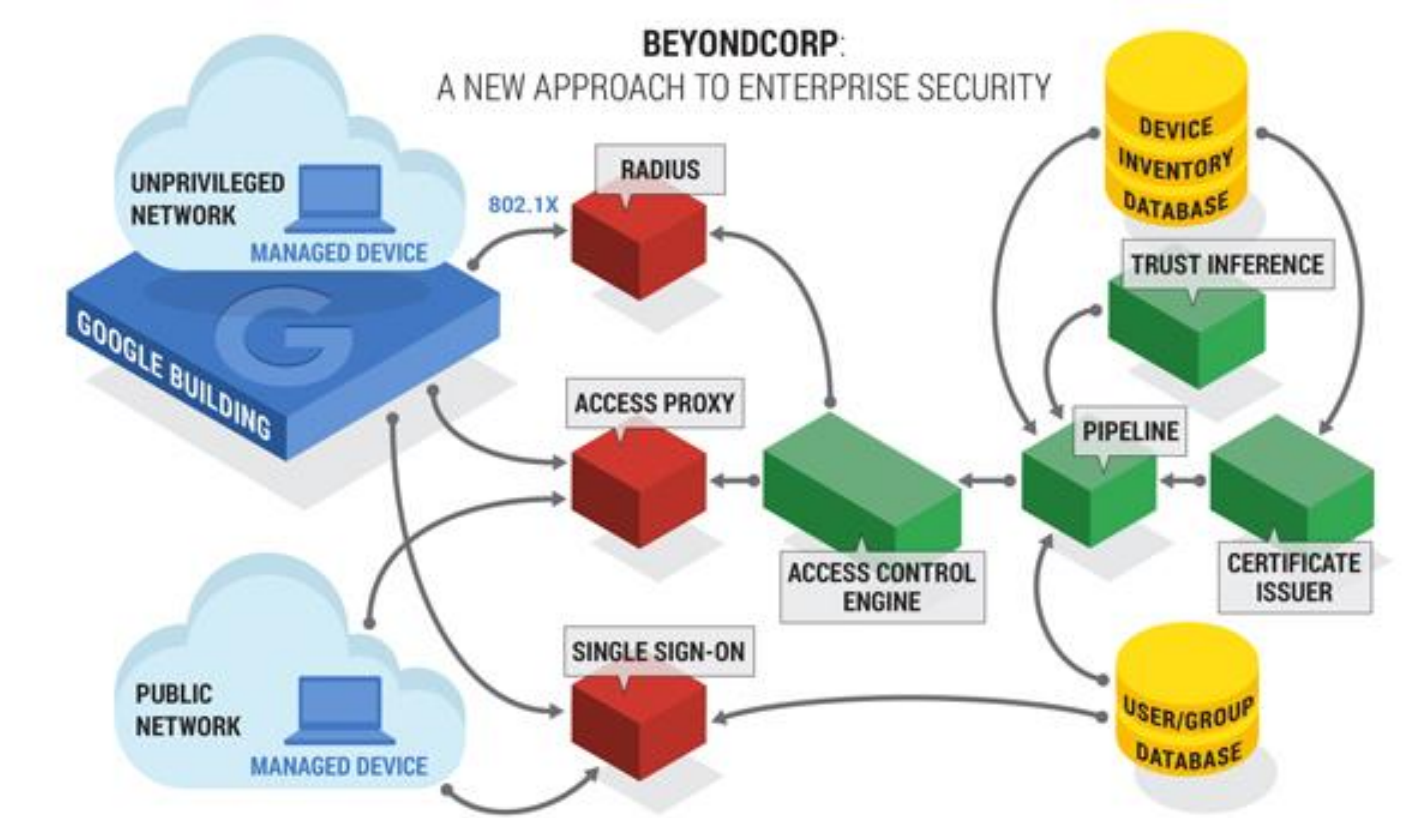


Image credit: Google

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco’s Zero Trust Architecture

Cisco Zero Trust Architecture

Simplifying the Journey: Cisco Zero Trust architecture in 3 critical areas

Workforce

Establish trust of users and devices to determine their application access privileges

Workplace

On networks you control, establish trust-based access control for users/devices and including IoT.

Workload

Minimizing the attack surface while enforcing least privilege access to/from our workloads

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

How does Cisco Zero Trust work?

3 Step Cyclical Process

We establish trust by verifying:

- Multi-factors of User Identity
- Device context and Identity
- Device posture & health
- Location
- Relevant attributes and context

We enforce least privilege access to:

- Networks
- Applications
- Resources
- Users & Things

We continuously verify:

- Original tenets used to establish trust are still true
- Traffic is not threat traffic
- Behavior for any risky, anomalous or malicious actions
- If compromised, then the trust is broken

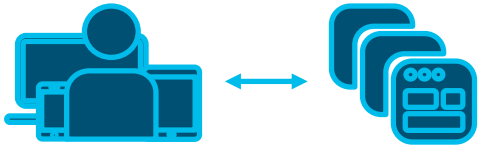
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Zero Trust Journey

Primary Solutions

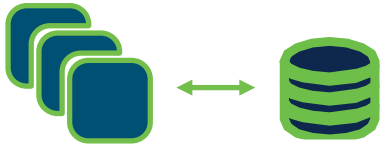
Duo for Workforce

Establish trust level for users and their devices accessing applications and resources



Tetration for Workload

Restrict access to workloads based on risk, contextual policy and verified business need



SD-Access for Workplace

Establish least privilege access control for all users and devices, including IoT, accessing your networks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Cisco Verifies Trust

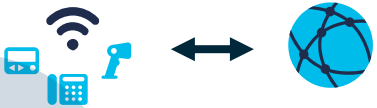
Establishing trust before granting access or allowing connections in your environment:

Workforce

+ Is the user who they say they are?
+ Do they have access to the right applications?
+ Is their device secure?
+ Is their device trusted?

Workload

+ What applications are used in the enterprise?
+ What is communicating with applications/data?
+ Is communication w/ the workload secure & trusted?



Workplace

+ Do users & devices authenticate for network access?
+ What access are they granted?
+ Are devices on the network secure?
+ Is their network segmentation based on trust?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Zero Trust Architecture Differentiators

- *Time to Value*
- *Leaders in networking and Access*
- *Unrivaled Integrated Architecture*
- Usability and Automation
- Broadest End-to-End ZT Coverage
- Broadest Visibility and control of hosts

Microsoft	Google	kubernetes	aws	UNIX
	vmware	IBM	vmware {api}	ORACLE
Symantec	MobileIron	Azure	Ping Identity	SDK
	okta	FORGEROCK	splunk>	

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extended Protection

Complementary products to extend trust for any app, any workload & any network.

Workforce
Cloud & On-Prem Apps

Workload
Hybrid & Multi-Cloud

Workplace
LAN, WAN, SD-WAN, ACI

+ Extend Trust

- Umbrella
- AMP
- Next-Generation Firewall
- AnyConnect
- ACI
- CloudLock
- Meraki
- Email Security

+ Detect & Respond

- Cisco Threat Response (CTR)
- Stealthwatch

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application to Application Flows

East - West traffic between workloads

Business Use Case - Apps need to access other apps for business purposes (eg. web-app-db) and management functions (eg. DC for ntp, dns, domain, etc.)

Risks- Lack of Visibility, Policy mis-configuration, Policy Violations, Infection, Vulnerability

Application — Application

Capabilities – to mitigate identified risks

Application — Server Based Security | Anti Malware | Anti Virus | Flow Analytics | Application Dependency Mapping | Vulnerability Assessment & Software Inventory | Process Anomaly Detection & Forensics | Tagging/ Grouping For Software Defined Policy | Policy Generation, Audit & Change Mgmt | Micro Segmentation & Policy Enforcement | Anti Malware | Anti Virus | Server Based Security — Application

Workload Security

Product Mappings – to provide identified capabilities

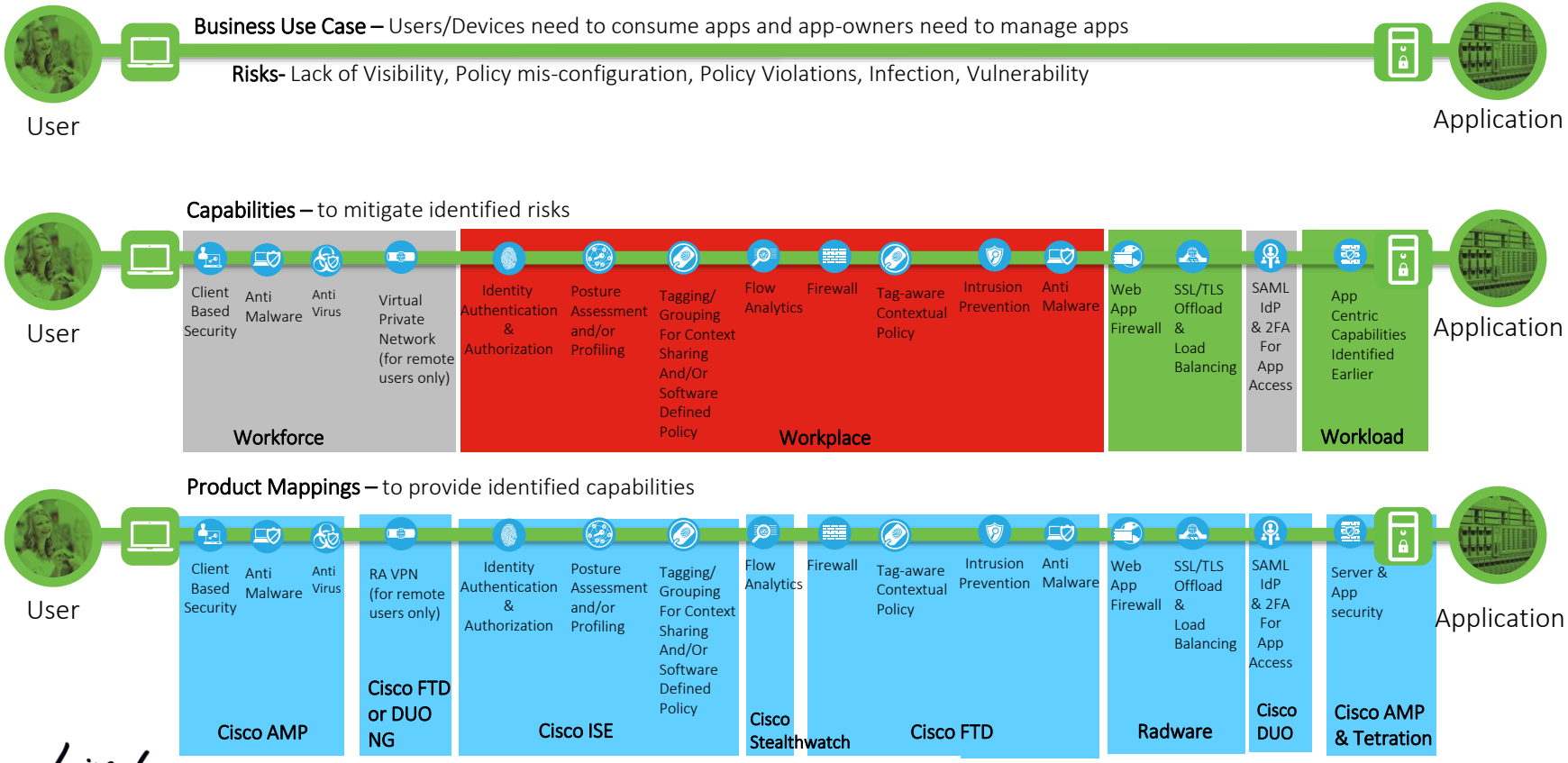
Application — Server Based Security | Anti Malware | Anti Virus | Flow Analytics | Application Dependency Mapping | Vulnerability Assessment & Software Inventory | Process Anomaly Detection & Forensics | Tagging/ Grouping For Software Defined Policy | Policy Generation, Audit & Change Mgmt | Micro Segmentation & Policy Enforcement | Anti Malware | Anti Virus | Server Based Security — Application

Cisco AMP — Cisco Tetration — Cisco AMP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Corp User to Application Flows

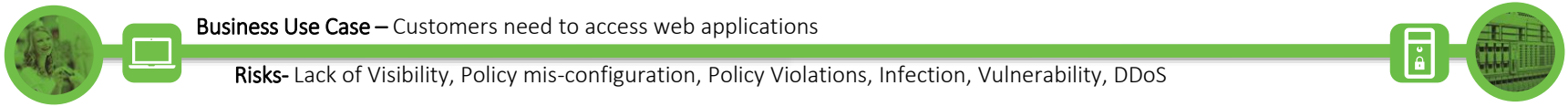
North - South from user to application

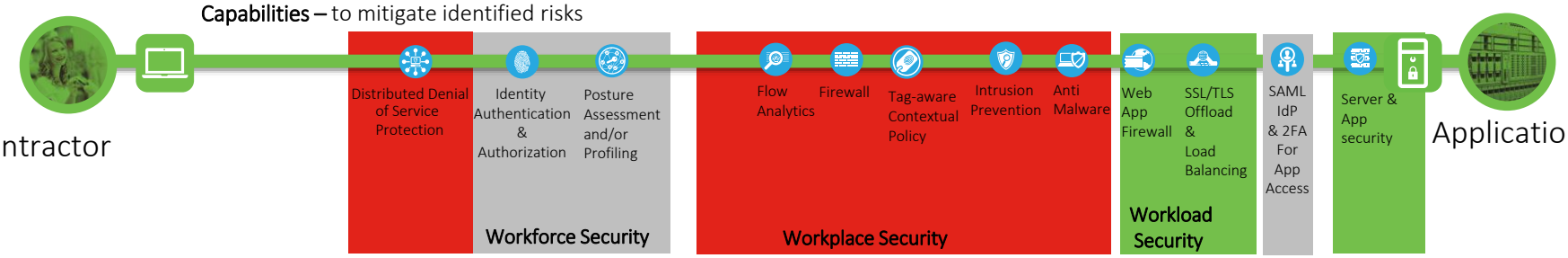


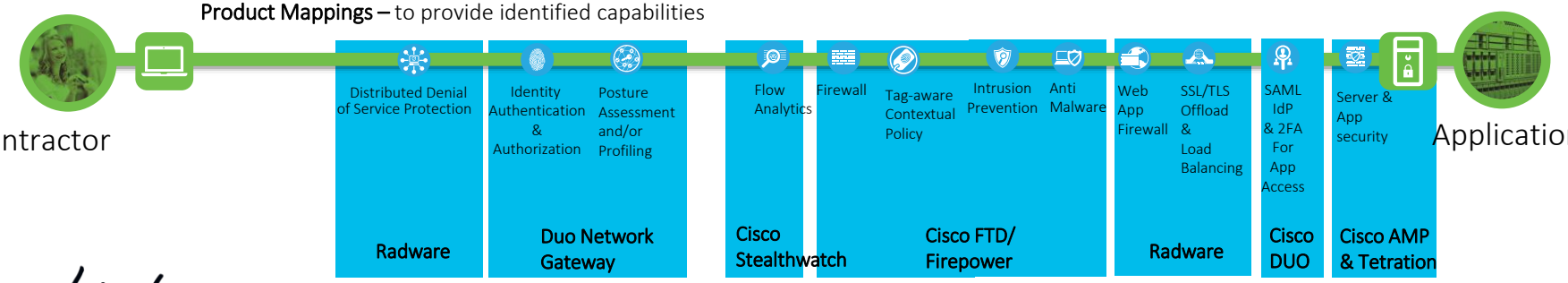
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

External Contractor to Application Flows

North - South from external user to application







© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: End-to-End Cisco Zero Trust Architecture

What's the problem?	How Cisco helps:
I need to discover and classify my devices and application everywhere	Cisco SDA, Tetration, Duo
I need zero trust access control policy everywhere	Cisco SDA, Tetration, Duo
I need constant verification my users, devices and applications are trustworthy	Cisco SDA, Tetration, Duo

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Domains and Transits

Choose a Fabric Domain or Transit below to manage, or add a new item by clicking "Add Fabric Domain or Transit".

Add Fabric Domain or Transit

Fabric Domains

Default LAN Fabric
LAN

Campus Fabric
LAN

Transits

No Transits Created

Make a Wish

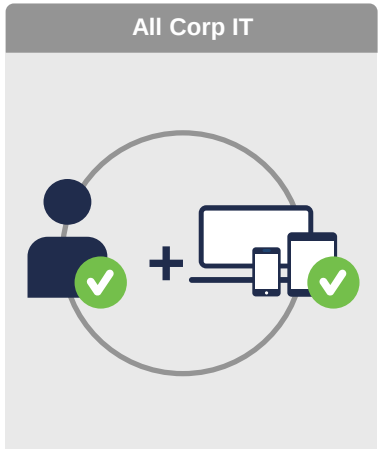
Let’s recap…

1. **Workplace: SD-Access**
   - DNAC and ISE really streamlines deployment,
   - New ML profiling
   - Dynamic SGT-based access rules, integrated NGFW.
2. **Workload: Tetration**
   - Auto-Clustered apps together including ISE context
   - Dynamic, least-privilege application policy with one-click
   - Continuous trust with dashboard attack surface report
3. **Workforce: Duo**
   - Simple, powerful setup
   - Built-in integrations with tons of applications
   - One-click app enforcement: MFA, Biometric, device health, device trust

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Cisco Zero Trust Journey

Secure the Workforce
With Duo

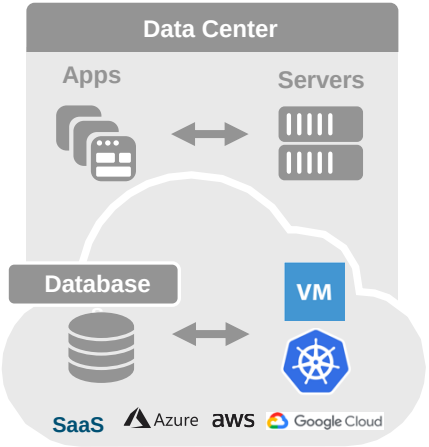


User & Device Access

MFA + Device Trust

Application Access

Secure Your Workloads
With Tetration

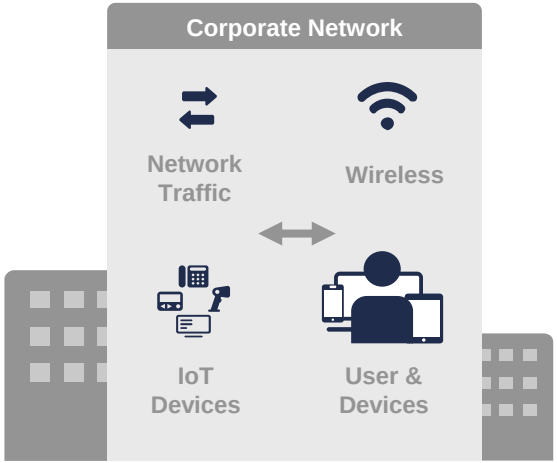


Workload Access

Application Micro-Segmentation

WAN Routing

Secure the Workplace
With Software-Defined Access



Network Access

Network Segmentation

Visibility | **Policy** | **Enforcement** | **Reporting**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust for the Workforce

Cisco Zero Trust for Workforce

How to establish trust with Duo

Verify identity of users

WITH

Multi-factor authentication (MFA)

Ensure trustworthiness of devices

WITH

Endpoint posture & context visibility

Enforce risk-based and adaptive access policies

WITH

Per application access policies that vary based on risk tolerance levels

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Risks Persist with Passwords

- Compromised credentials is a major security risk
- Cumbersome tokens and one-time passwords; not user friendly
- 8,418,474,549 stolen creds in the public domain; 2.2+ Billion YTD; HIBP
- Top reason bad actors phish - to steal credentials

81%

of breaches leverage stolen or weak passwords

Source: Verizon 2018 Data Breach Investigations Report

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multi-Factor Authentication (MFA)

Workforce: Establish Trust

How it works:

A user logs in using primary authentication (something they know = username + password).

Duo prompts the user with secondary authentication (something they have = push notification sent via Duo Mobile app on their smartphone).

What this does:

- ✓ Prevents identity-based attacks.
- ✓ Thwarts attackers using stolen or compromised passwords.
- ✓ Provides zero-trust access for applications.
- ✓ Creates less reliance on passwords alone.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MFA Options for Every Use

Workforce: Establish Trust

You can configure authentication:

- Per-application or user group
- Based on sensitivity of application data
- Or based on user scenario

Additionally, allow multiple options for ease of usability and flexibility:

- Push notification
- Mobile passcode
- Phone
- SMS
- HOTP token
- U2F/WebAuthn

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Enrollment

Workforce: Establish Trust

Automatic Enrollment

Admins can import users from existing Azure, LDAP and AD directories

Self Enrollment

Users can self-enroll into Duo in less than 1 minute

Import Users

Provision users using Duo's REST API or add users manual one at a time or through CSV

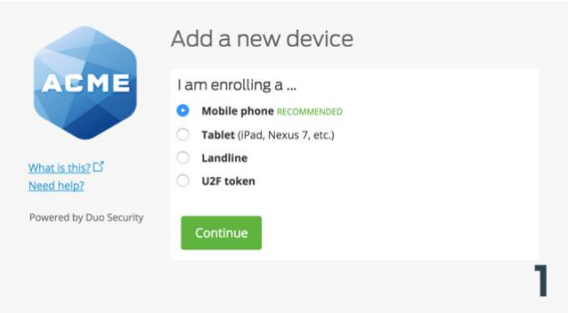
Learn more about Enrollment Options

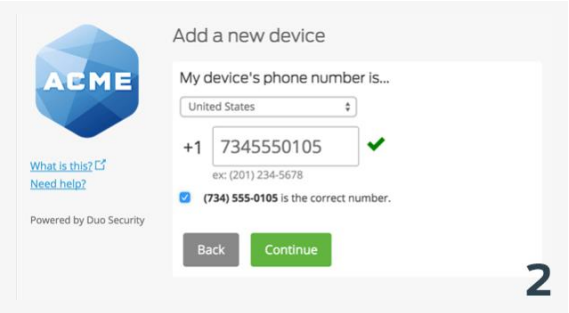
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

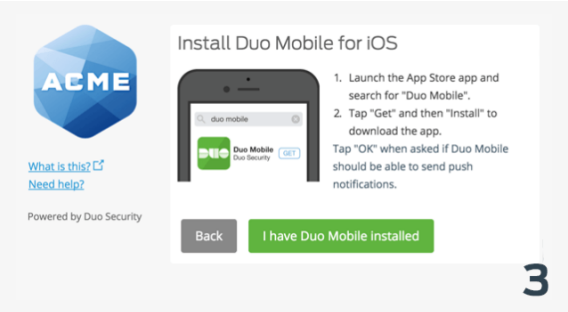
Removing Barriers to MFA: Self-Enrollment

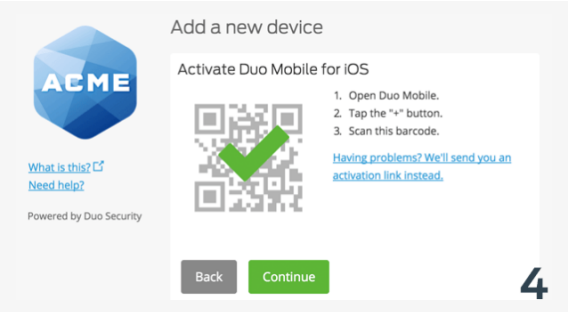
Workforce: Establish Trust

- Users easily self-enroll in minutes
- Users leverage their own device
- Enroll thousands of users in hours.
- Reduce TCO by enabling the user to easily enroll with no help needed







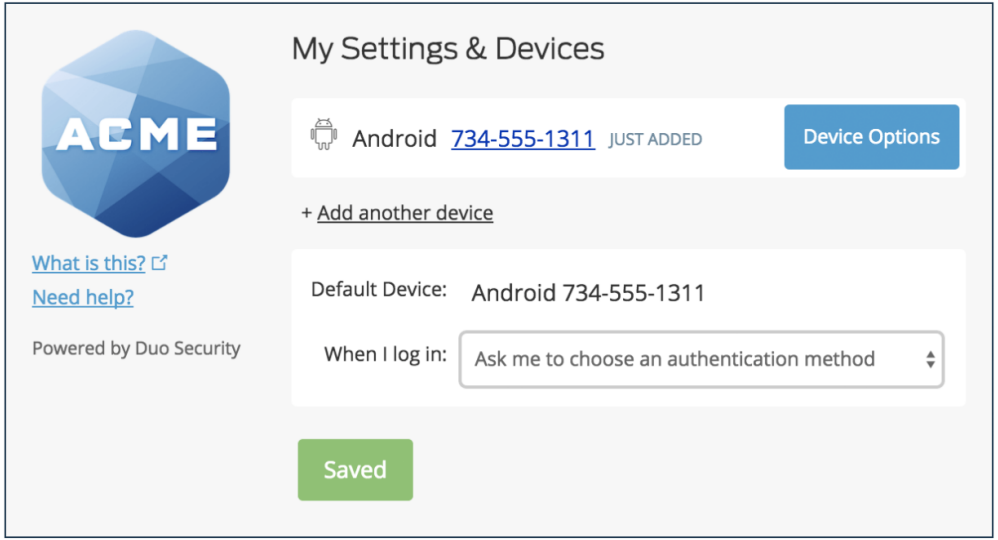


Learn more about self-enrollment

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Removing Barriers to MFA: User Self-Service

Workforce: Establish Trust



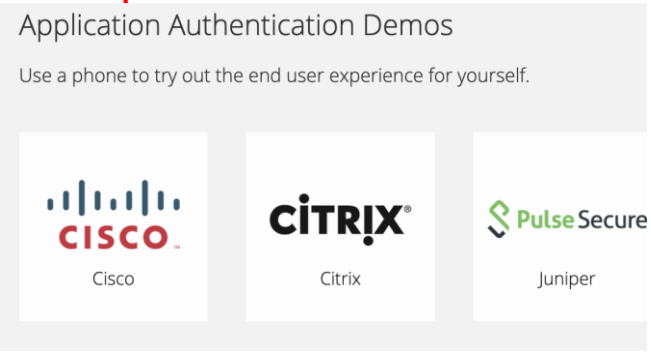
- Users can manage their own 2FA devices during login.
- Add, Remove and Configure Devices
- Reduce TCO by enabling the user to easily manage their own device.

Learn more about Device Management

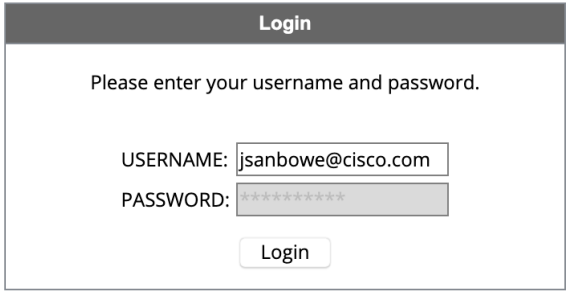
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Audience Duo Enrollment

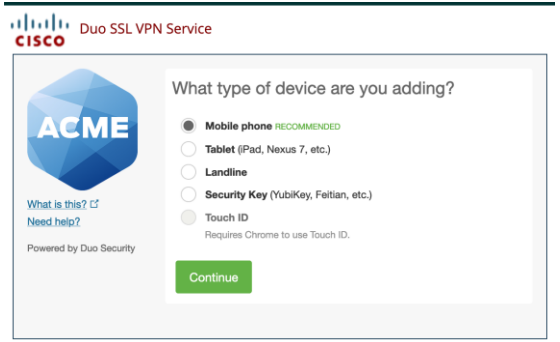
https://demo.duo.com/

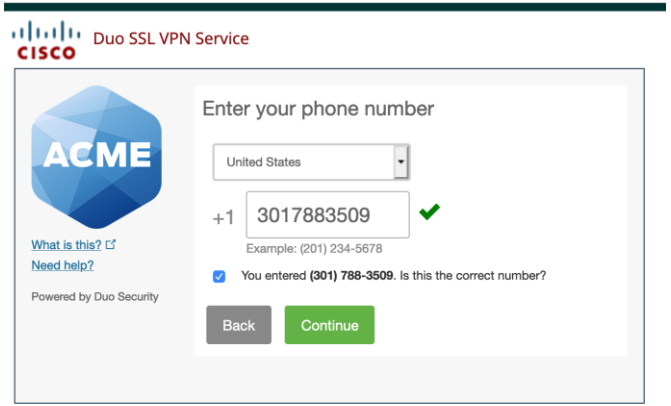


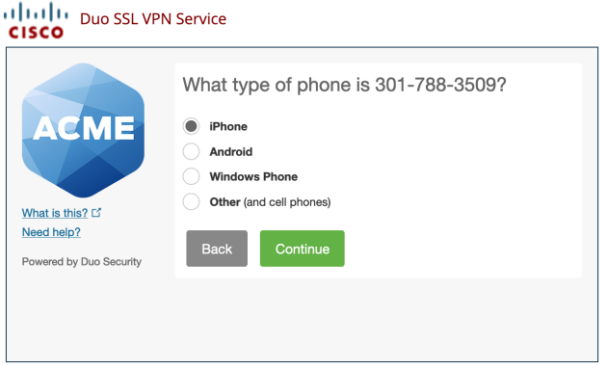
Enter Email

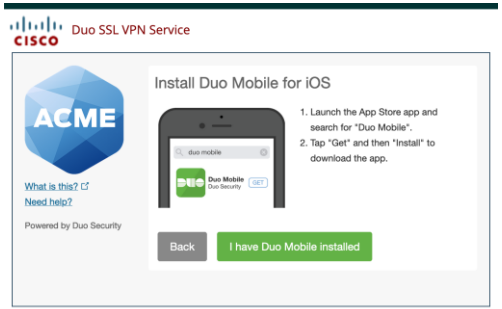


Mobile Phone





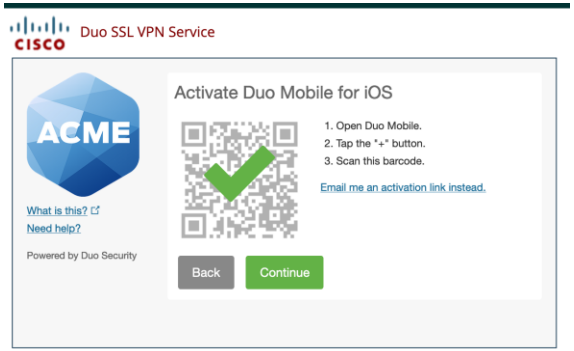


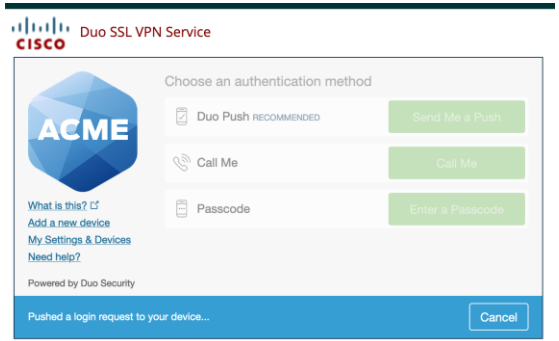


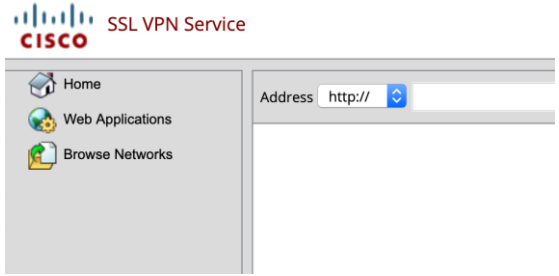
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Audience Duo Enrollment

https://demo.duo.com/







© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Protect Every Application – External and Internal

Workforce: Enforce Trust-Based Access

Start Here

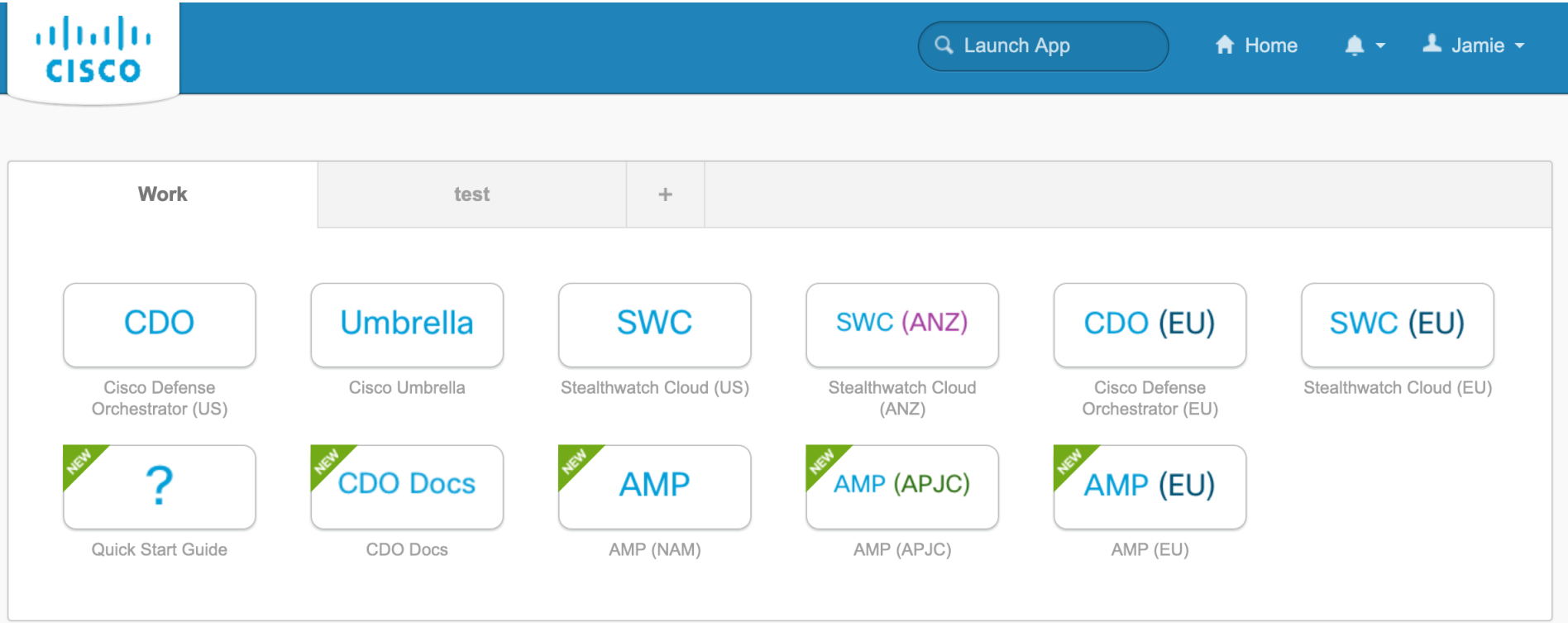
Then Expand

VPN RA	Multicloud	Email/MSFT	On-Prem	SSO	Custom
Cisco	Google Apps	Office 365	Epic	Microsoft Azure	REST APIS
Juniper Networks	salesforce	Outlook	Oracle PeopleSoft	AD FS	WEB SDK
Citrix	aws	Microsoft Remote Desktop Services	vmware Horizon View	okta	RADIUS
paloalto Networks	box	Windows Server	>_SSH	Centrify	SAML
Pulse Secure	Dropbox	RRAS	Shibboleth	onelogin	OIDC

Learn more about application integrations

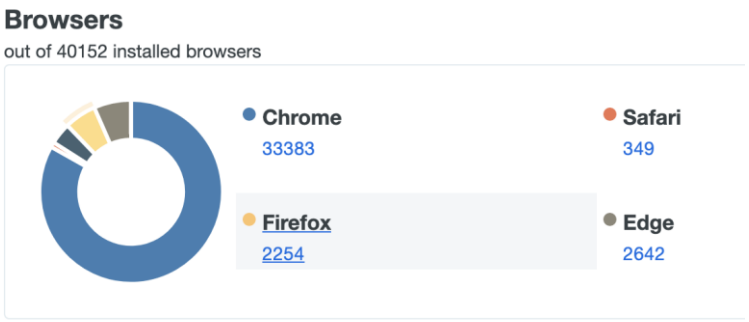
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

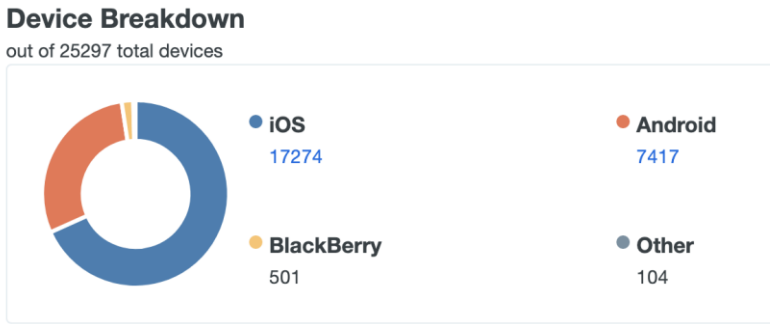
security.cisco.com



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ensure Trustworthiness of Devices





© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why Device Trust?

Compromised devices can access your data

Attackers exploit known vulnerabilities

Patching devices (especially user-owned) is complex

Accessing critical data from vulnerable devices can be risky

99%

of vulnerabilities exploited will be ones known by security team for at least one year (through 2021)

Source: Gartner, Dale Gardner, 2018 Security Summit

How Duo Establishes Device Trust

Workforce: Establish Trust

Device Insight

Duo's Unified Endpoint Visibility inspects users' devices at login -- without installing any endpoint agents.

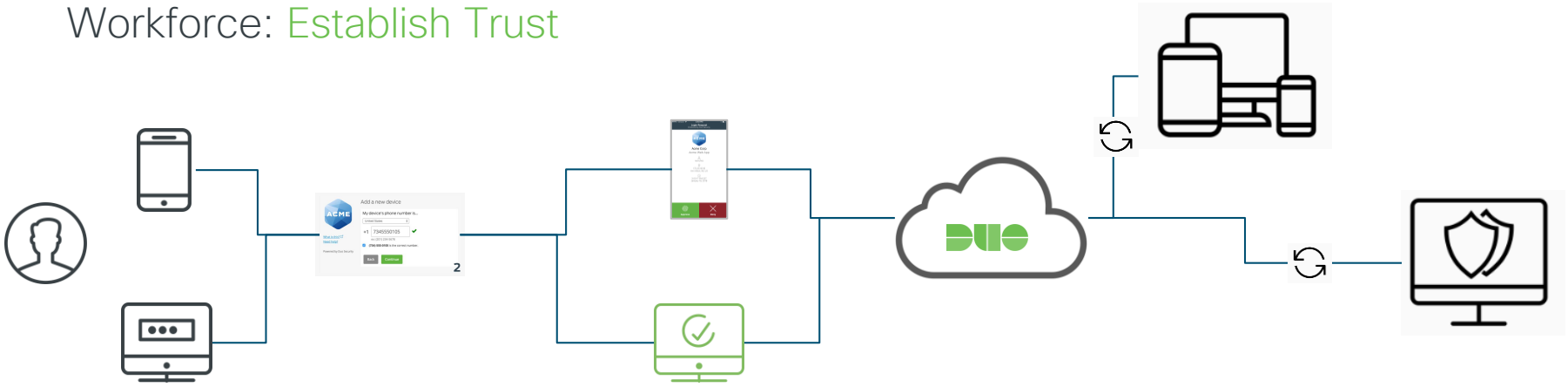
Managed or Unmanaged

Duo's Trusted Endpoints integrates with endpoint management systems to detect if the device is managed by your IT.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Duo Gains Device Visibility

Workforce: Establish Trust



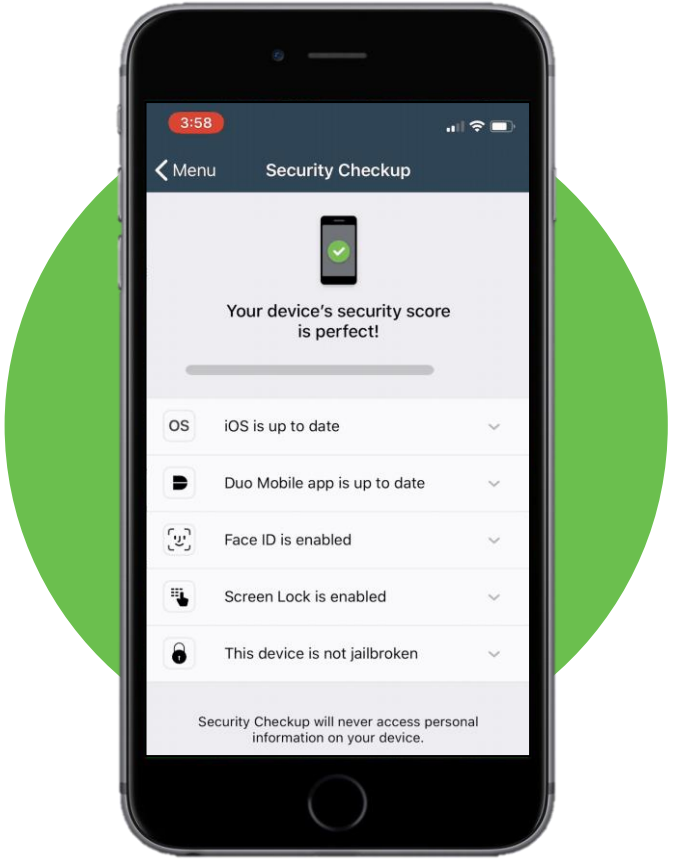
Visibility Source	Duo prompt in Web Browser	Duo mobile app Duo Device Health app	Device Manager (MDM/UEM)	EDR / EPP Agents+Services
Information Collected	Browser, OS, Plugins	Password, Disk Encryption, OS, Browser, (Mobile only: Jailbroken) (Desktop only:Firewall)	Device mgmt. Status (Managed/BYO)	Compromises, malware, viruses etc.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Assess Mobile Device Posture without MDM

Workforce: Establish Trust

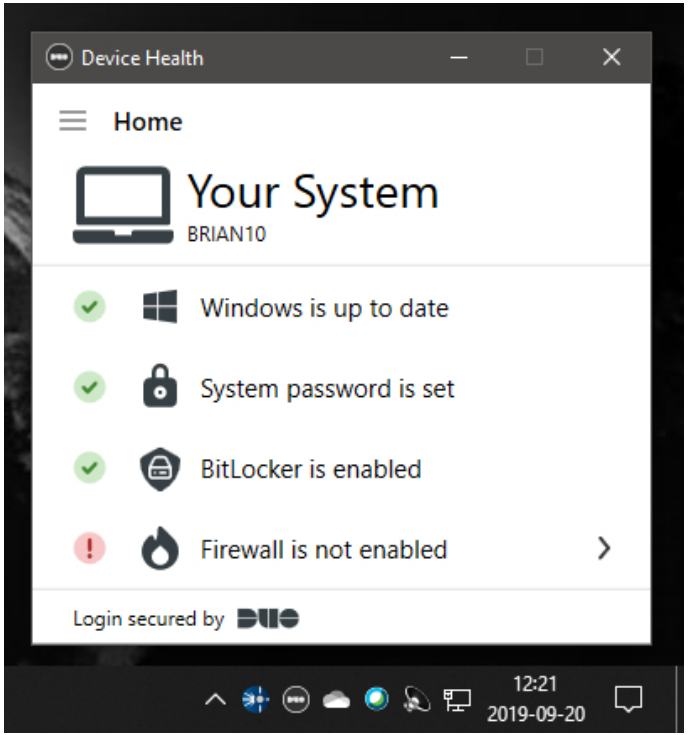
- Check if mobile devices are up-to-date
- Verify encryption and passcode lock
- Check if devices are jailbroken or tampered
- Works for MDM managed and unmanaged mobile devices



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deep Insights Into Laptops and Desktops

Workforce: Establish Trust



Duo Device Health Application:

- New functionality
- Laptop / desktop security health
- Check devices before they login
- Corporate managed and BYO devices
- Supports web-based applications
- Windows 10 and macOS
- Launches On-Demand
- Inspects for third party AV clients including AMP for endpoints*

*Public beta

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identify Managed vs. BYO Devices

Workforce: Establish Trust

1 A cloud service (PKI) Duo uses **generates a certificate** for user. It is then **distributed per device**.

2 When user logs into a protected app, Duo uses the Trusted Endpoints policy to **check for the presence of a certificate**.

3 User with a certificate is granted access and **her device is considered a Trusted Endpoint**. User without a certificate is blocked and her device not trusted.

Source: ***https://duo.com/docs/trusted-endpoints***

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identifying Managed Devices

Workforce: Establish Trust

Mobile

Duo: Duo Mobile app can be used to trust mobile devices. (Great for customers w/o MDM)

Native: AirWatch, MobileIron, Google G Suite, Sophos

Alternative: Duo has a generic cert deployment

Future: Meraki Systems Manager and Microsoft Intune

Windows

Native: Microsoft AD, Ivanti (Landesk)

Script based: Symantec Altiris, Chef, Microsoft SCCM, AirWatch, etc.

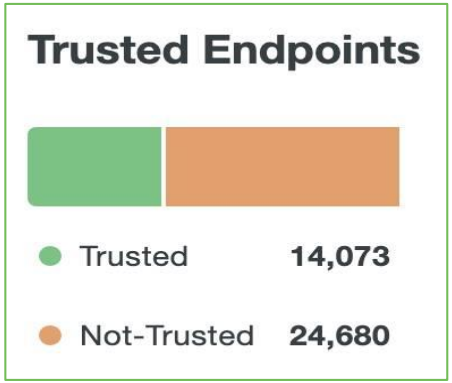
Alternative: Duo has a generic cert deployment

macOS

Native: Jamf

Script based: Symantec Altiris, Chef, AirWatch, etc.

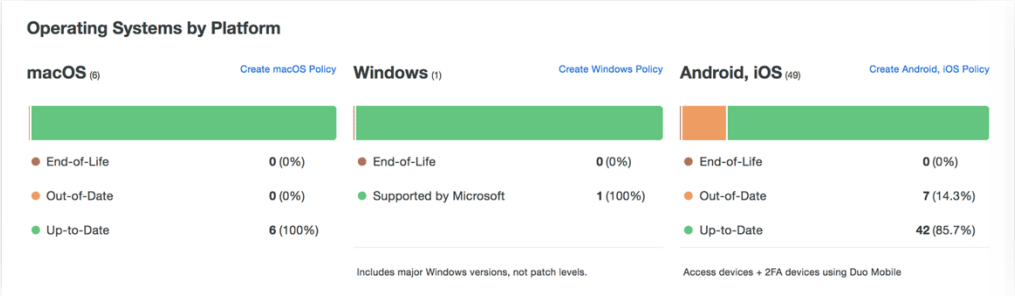
Alternative: Duo has a generic cert deployment

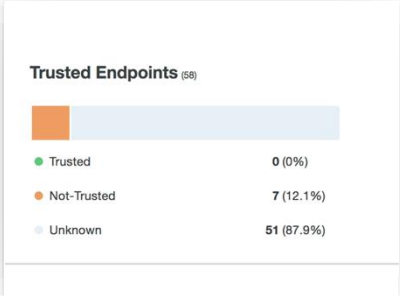


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unified Device Visibility

Workforce: Continuously Verify Trust





Get mobile device details:

- Corp-managed status
- Biometrics (Touch/Face) status
- Screen lock status
- OS condition (tampered) status
- Encryption status
- Platform type
- Device OS type & version
- Device owner
- Duo Mobile version

Get laptop/desktop details:

- Corp managed status*
- Device owner
- OS type & versions
- Browser type & versions
- Flash & Java plugins versions
- OS, browser and plugin(s) status
- Disk Encryption*
- Firewall*
- Anti-virus/Anti-malware*

*In public beta

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enforce Risk-Based Policies

- **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

Duo's Adaptive Policies

Reduce friction and risk to applications with customizable, granular access policies

Role-Based Policy

Based on individual users or groups, enforce policies to determine who can access what applications.

Device-Based Policy

Allow access by only secure, up-to-date or managed devices, and prevent access by risky devices.

Location-Based Policy

Prevent authorized access to your applications from any geographic location.

Network-Based Policy

Grant or deny access based on a set of IP address ranges or from anonymous networks like Tor.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enforce Device Policies

Workforce: Continuously Verify Trust

Require devices that access applications to be:

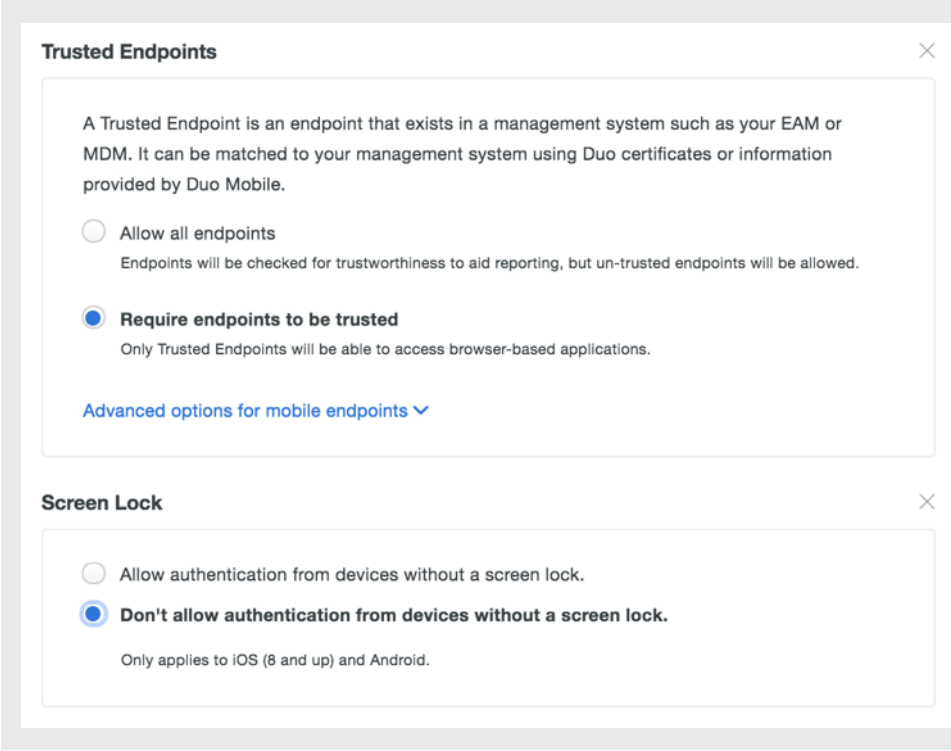
- Corporate-owned
- Up-to-date OS, browsers, Flash/Java

Require mobile devices to have:

- Screen lock
- Biometrics
- Encryption
- Not jailbroken/rooted

Remembered devices

- Allow trusted and known devices to automatically authenticate

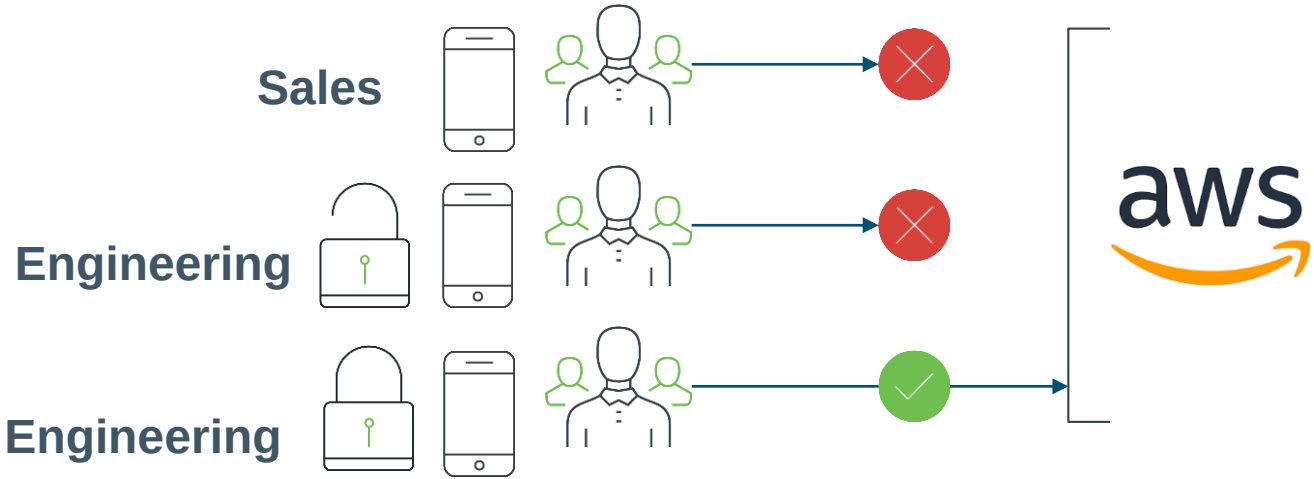


 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Role/Trusted Endpoint Policy Example

Workforce: Enforce Trust-Based Access

With application policy, only the engineering team using **trusted and corporate managed** devices are allowed to access AWS.
All others are blocked.



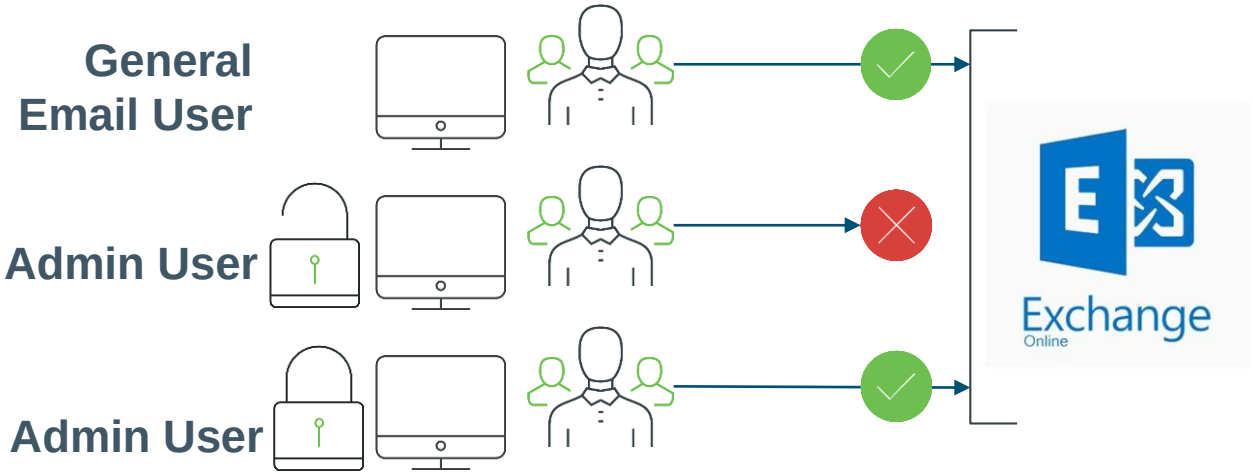
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

More Complex Role/Trusted Endpoint Policy

Workforce: Enforce Trust-Based Access

Normal email users can use personal devices, Exchange Online admins cannot use personal devices.

Exchange Online admins using **trusted and corporate managed** devices are allowed to access .



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

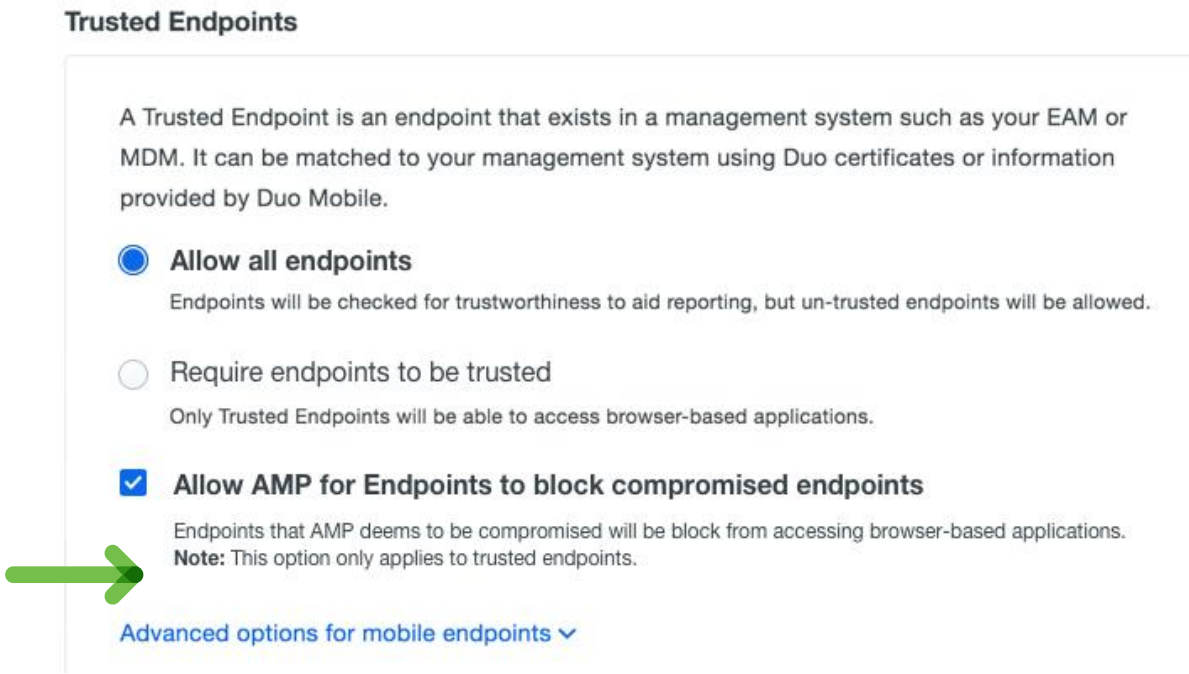
BETA

Detect Device Malware & Respond

Workforce: Continuously Verify Trust

Duo + AMP4E (Advanced Malware Protection for Endpoints) Integration*

Prevent compromised devices from accessing Duo-protected applications.



*Currently available to select customers for private beta

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

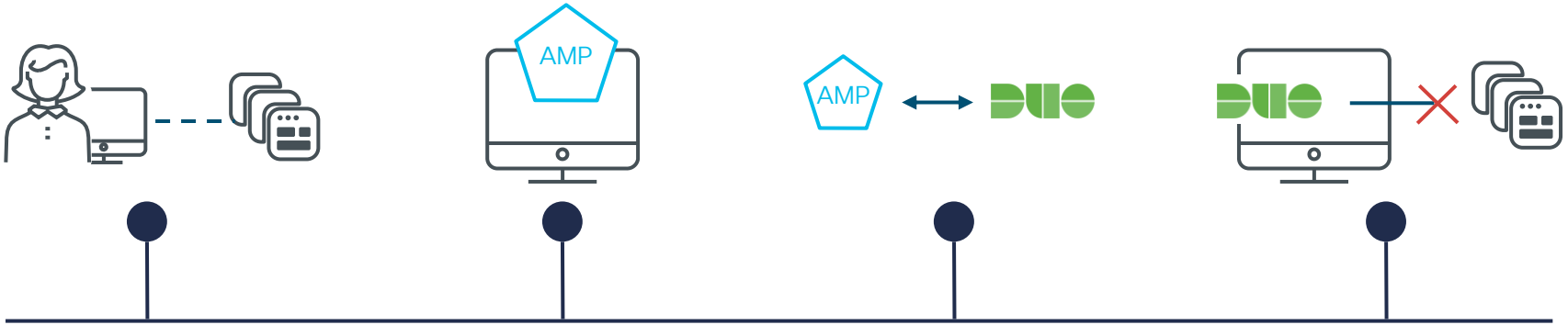
BETA

Detect Device Malware & Respond

Workforce: Continuously Verify Trust

How It Works:

Block malicious devices from accessing applications with Duo and AMP.



Users use their devices to access application.

Cisco AMP running on the device detected malware.

AMP notifies Duo about the infected device.

Duo blocks that device from accessing apps.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo + AMP Setup

BETA

Dashboard > Trusted Endpoints Configuration > AMP for Endpoints

AMP for Endpoints

Remove Integration

1. Generate AMP Credentials

1. Login to the AMP console.
2. Navigate to "Accounts > API Credentials".
3. Click "New API Credentials".
4. Give the credentials a name and make it read-only.
5. Click "Create".
6. Copy the **Client Id** and **API Key** and return to this screen.

2. Enter AMP Credentials

Client ID

Enter Client ID from Part 1.

API Key

Enter API Key from Part 1.

Hostname

Hostname will be auto-selected

Test Integration

Hostname

https://api.amp.cisco.com/

Test Integration

Save Integration

Success!

3. Enable AMP Integration

Enabled

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

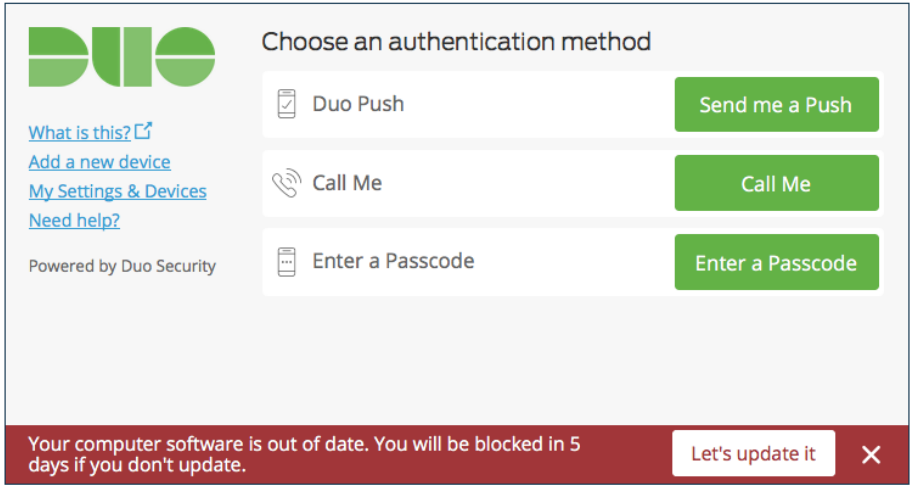
Inform Users

Workforce: Establish Trust

If users do not update by a certain day, the endpoints are blocked.

End users get notified about out-of-date OS, browsers, Flash and Java.

Quickly improve security without support desk help

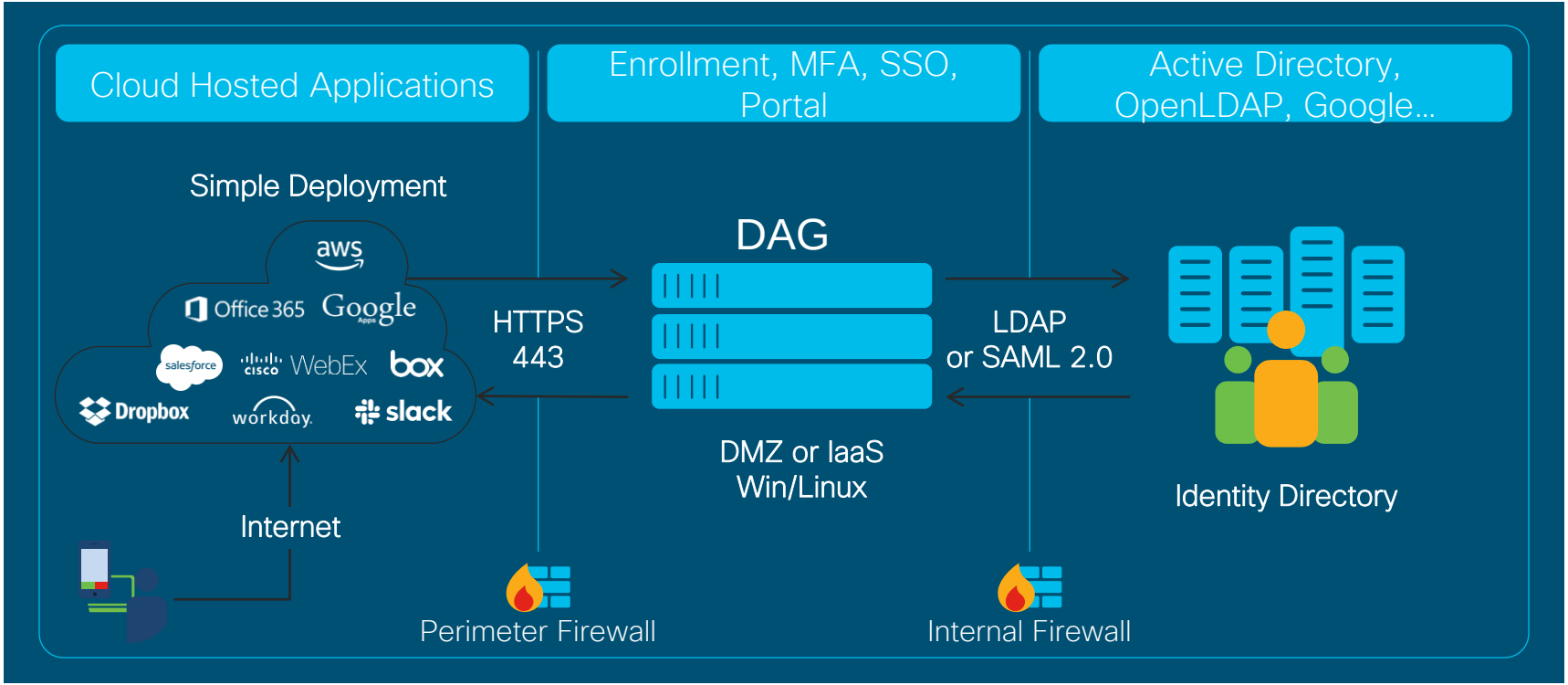


Improve your security posture & notify users of out-of-date devices

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Easily Secure Cloud Application Access

Duo Access Gateway (DAG)



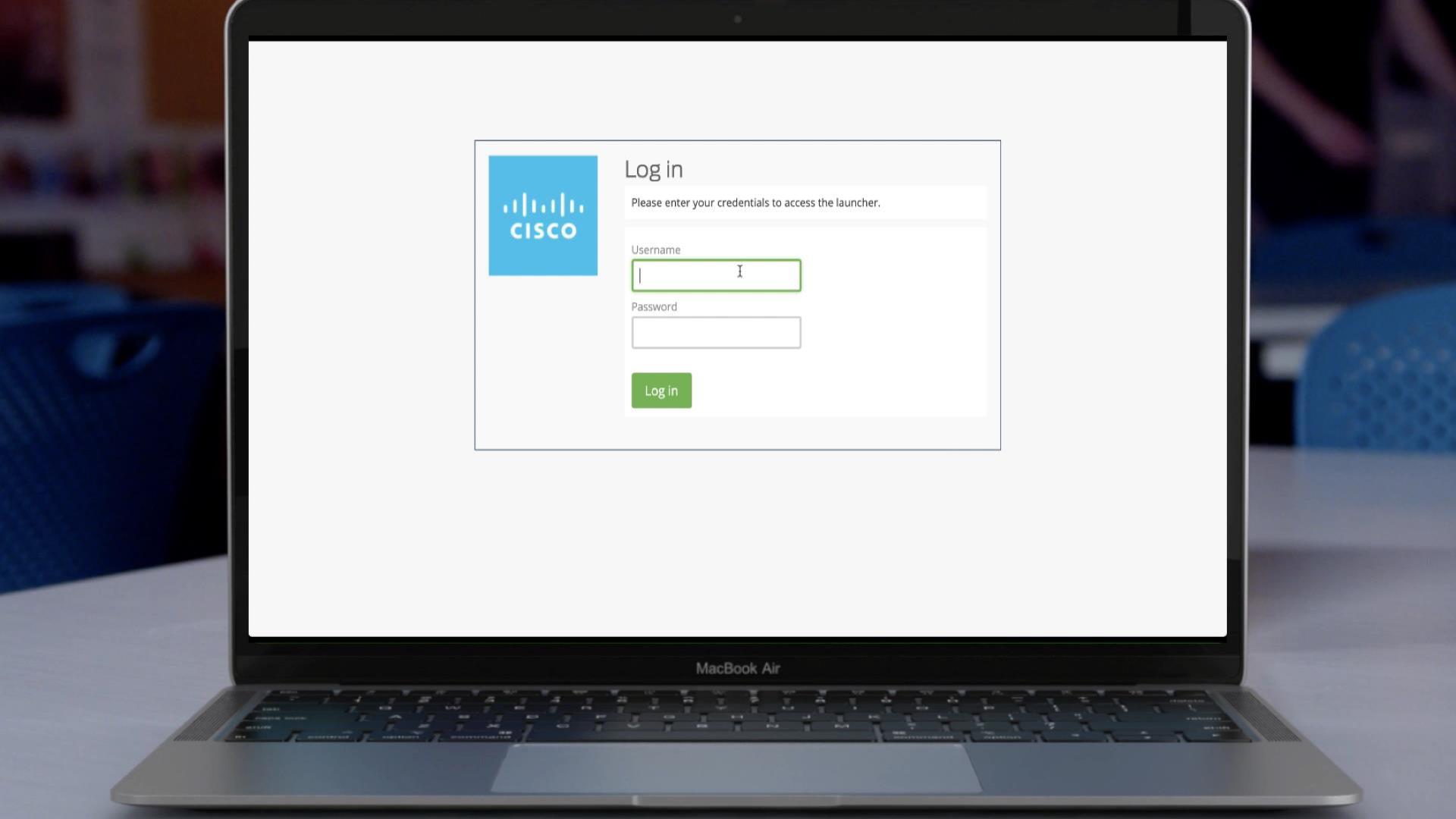
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Workforce- Employee Off-Prem to SaaS

What's the problem?	How Cisco helps:
Protect against stolen or compromised credentials	DNG, Duo MFA, Biometric, Location awareness
Provide simple but strong access control to applications and resources anywhere	Duo endpoint health, Group based application policies, SSO, DNG
Protect users from threats while they are remote	Duo health, Umbrella DNS and web security, AMP

Log and Audit Everything

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

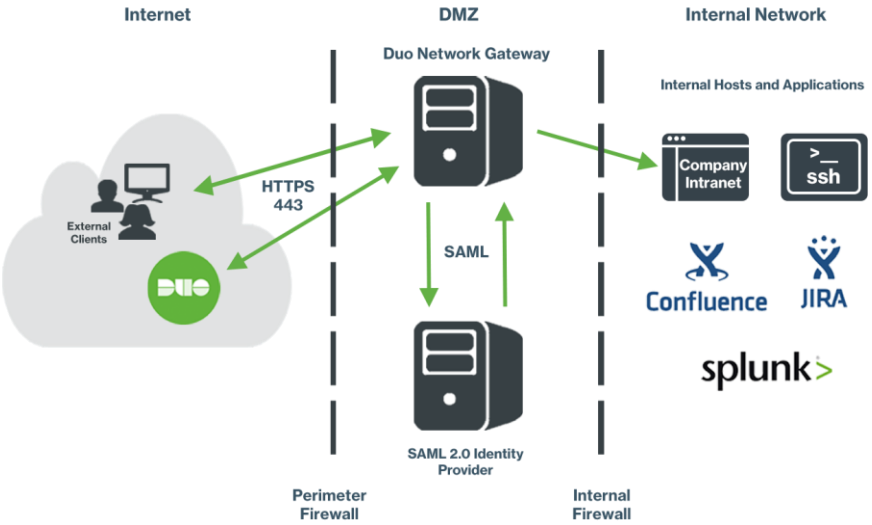

Log in
Please enter your credentials to access the launcher.
Username
Password
Log in
MacBook Air

Demo Recap…

- Workforce: Duo – Remote employee on trusted client to SaaS
  - DAG app portal provided MFA, biometric, SSO, device health, device trust
  - New Duo endpoint health for firewall, disk encryption, system password
  - Umbrella remote protection: blocked phish, blocked unapproved apps, policy to reduce shadow IT risk with new app discovery

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

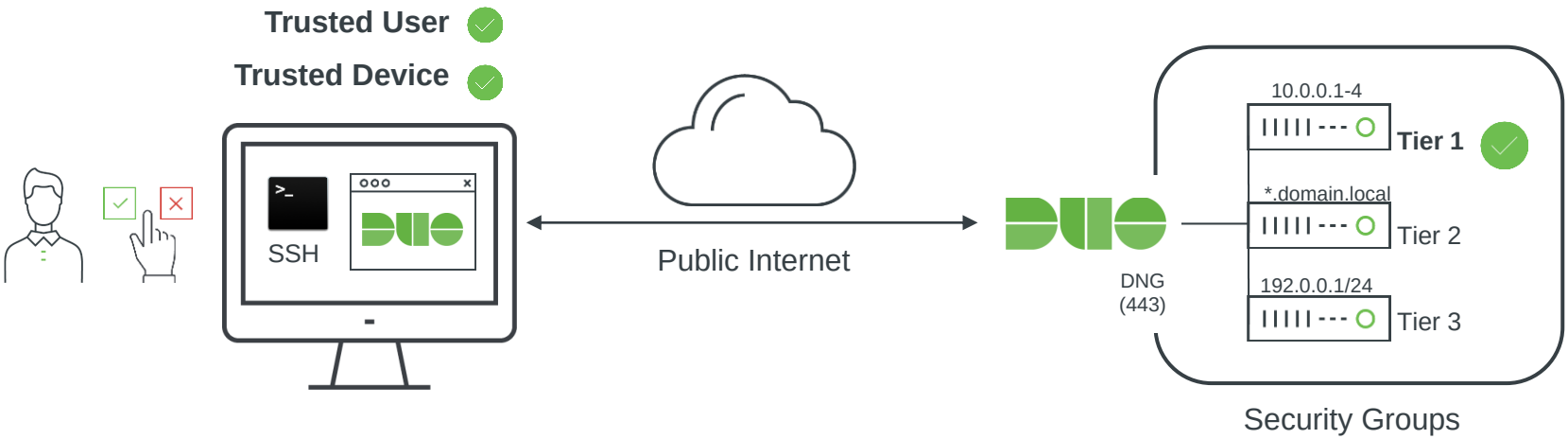
Securely Providing Access to Internal Applications from the Internet



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Network Gateway

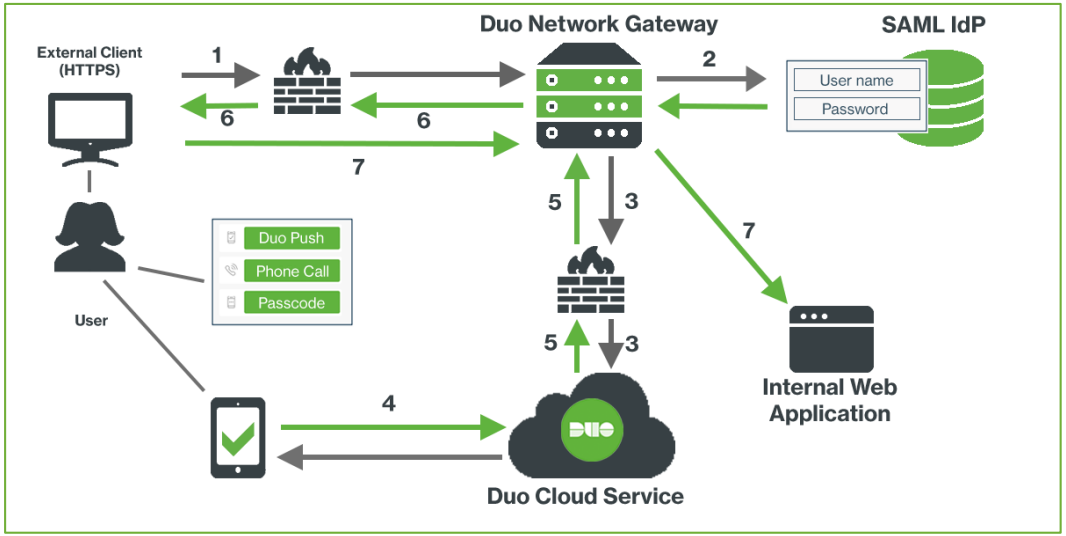
Detect user & device context for internal HTTP/S and SSH apps



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is the Duo Network Gateway?

- Deployed on Linux operating systems using Docker
- A reverse proxy that adds strong authentication before allowing users to access services protected by the Duo Network Gateway
- Supports HTTP, HTTPS and SSH traffic



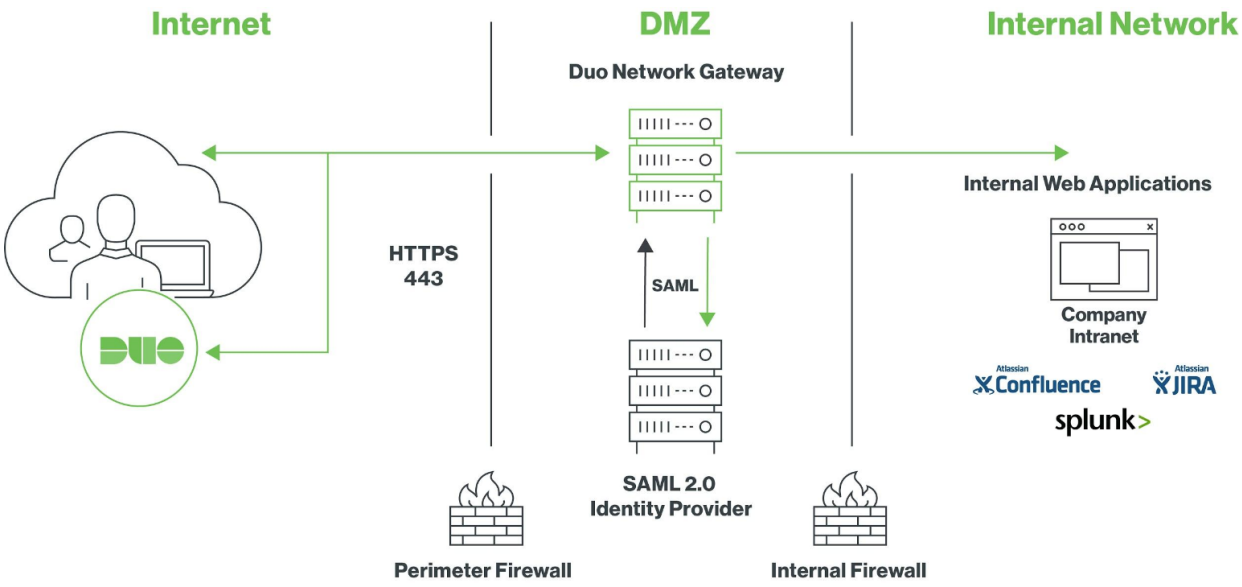
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example of Protected On-Prem Applications?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

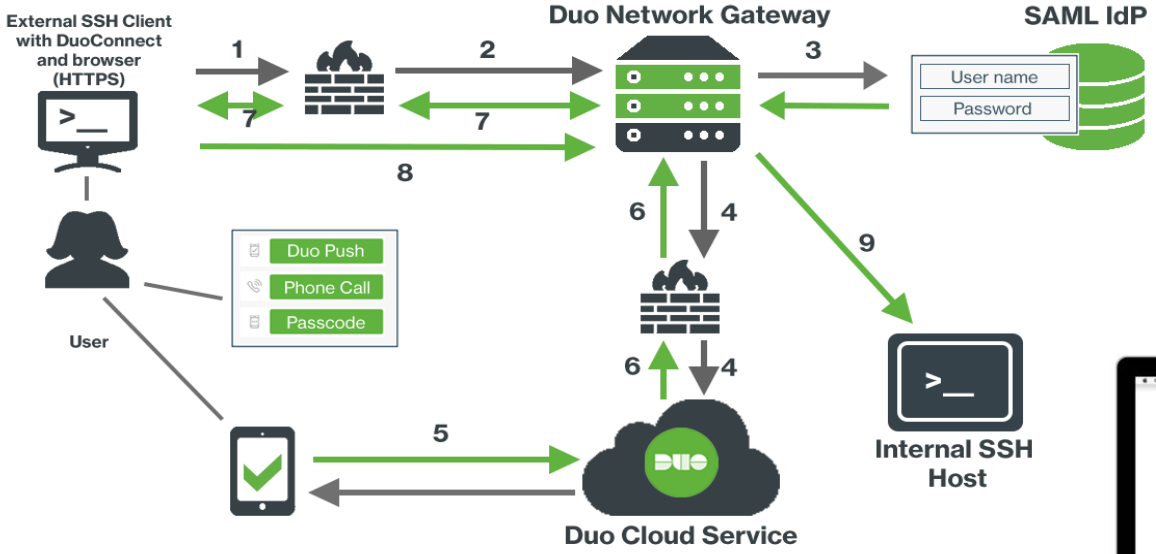
Setting Up Duo Network Gateway (DNG)

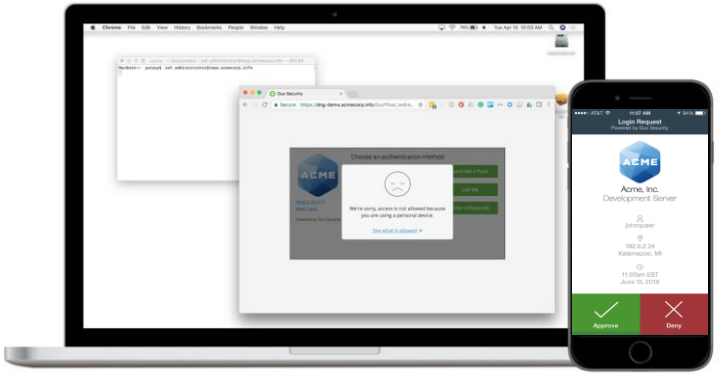
- Deploy a DNG in the DMZ
- Configure your **SAML IdP** for primary auth
- Create public DNS entries for your protected internal web apps to point to the DNG's public interface.
- Users access the "internal" app using their browser.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SSH Workflow





© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Workforce- Application Remote Access

What's the problem?	How Cisco helps:
Provide secure clientless external access to internal applications	Duo network gateway proxy, MFA
Determine trustworthiness of users/devices (managed & unmanaged)	Duo MFA, device health checks, Location, Tor check
Make the experience great for admins and users	Duo DAG Portal, MFA, SSO

Log and Audit Everything

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Welcome

Primary Authentication

Applications

Settings

Documentation

Logout

Applications

Add New...

Web Applications | **SSH Servers**

Show 25 entries

Name	Internal URL	External URL	
apc1.sanbower.net	http://10.28.20.30/	https://apc1.sanbower.net/	Remove

Showing 1 to 1 of 1 entries

1

Duo Network Gateway v1.5.0 · © 2019 Duo Security. All rights reserved.

Duo Network Gateway

Demo Recap…

- Workforce: Duo – Remote contractor, personal client to internal apps
  - DNG Deployment and Policy was simple, straightforward and quick
  - Awesome user experience, clientless self-enrollment MFA and SSO
  - Contractor specific, per app policy included device health OS, browser, plug-in, even geo-location restrictions and deny sources from Tor

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recap: Zero Trust for the Workforce

Duo helps reduce the risks of phishing, malware & unauthorized access to your applications.

Establish user + device trust

- Multi-factor authentication (MFA)
- Device visibility & policies

Enforce access policies

- For every app
- Adaptive & role-based controls (location, device type, network type, etc.)

Continuously monitor risky devices

- Device health
- Managed/unmanaged device status

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust for the Workload

Workloads

Zero-Trust Security

Gain visibility into what's running & critical by identifying workloads & enforcing policies

Contain breaches & minimize lateral movement with application micro-segmentation

Alert or block communications by continuously monitoring & responding to indicators of compromise

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Legacy Zero Trust for Workload Approach

Doesn't Scalable – Highly Error Prone

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Zero Trust for Workload

How to Establish Trust with Tetration

Visibility and behavior modeling

Application discovery and dependency maps

All Processes, cmds, files, users and network comms

Per workload, micro-segmentation policy

Automated, context-based, segmentation policy

Consistent policy: Any workload, Anywhere

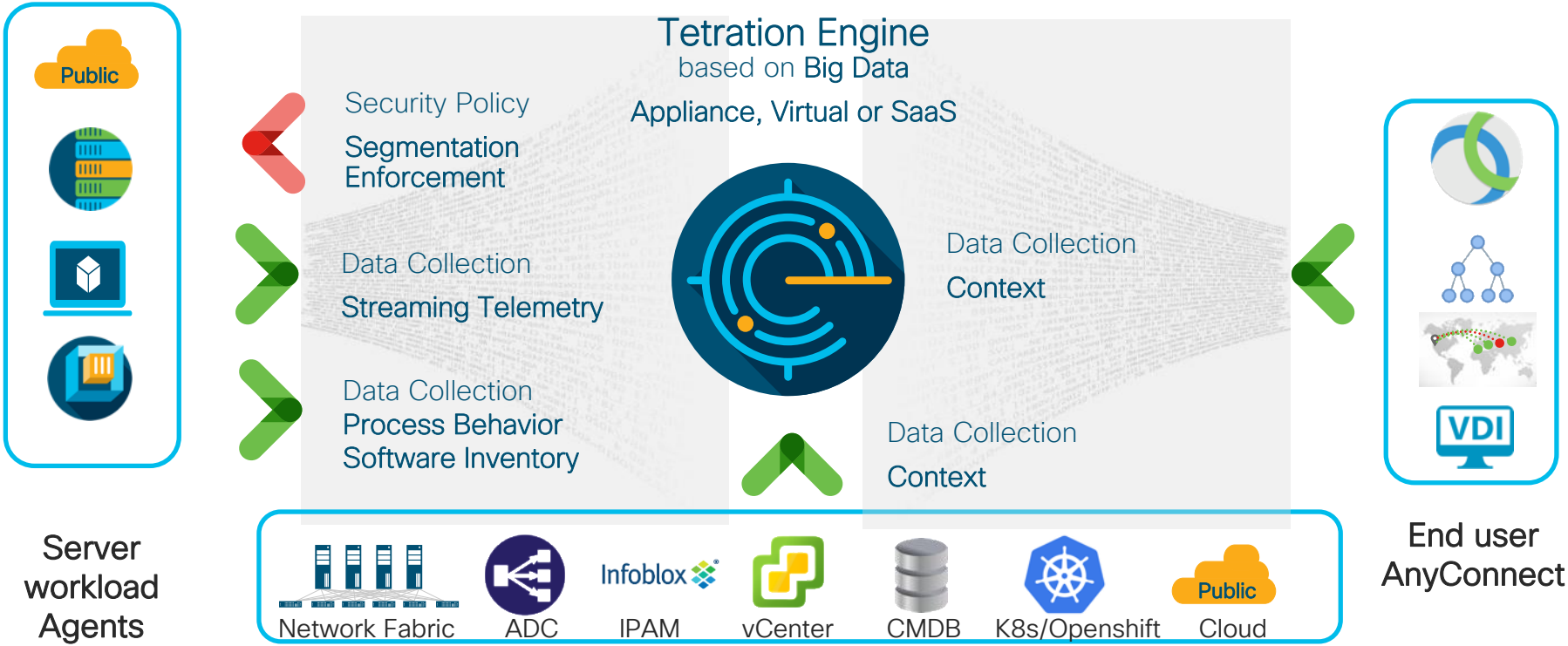
Real-time security health of workloads

Security visibility and health score

Vulnerability, anomaly, forensic and threat data

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

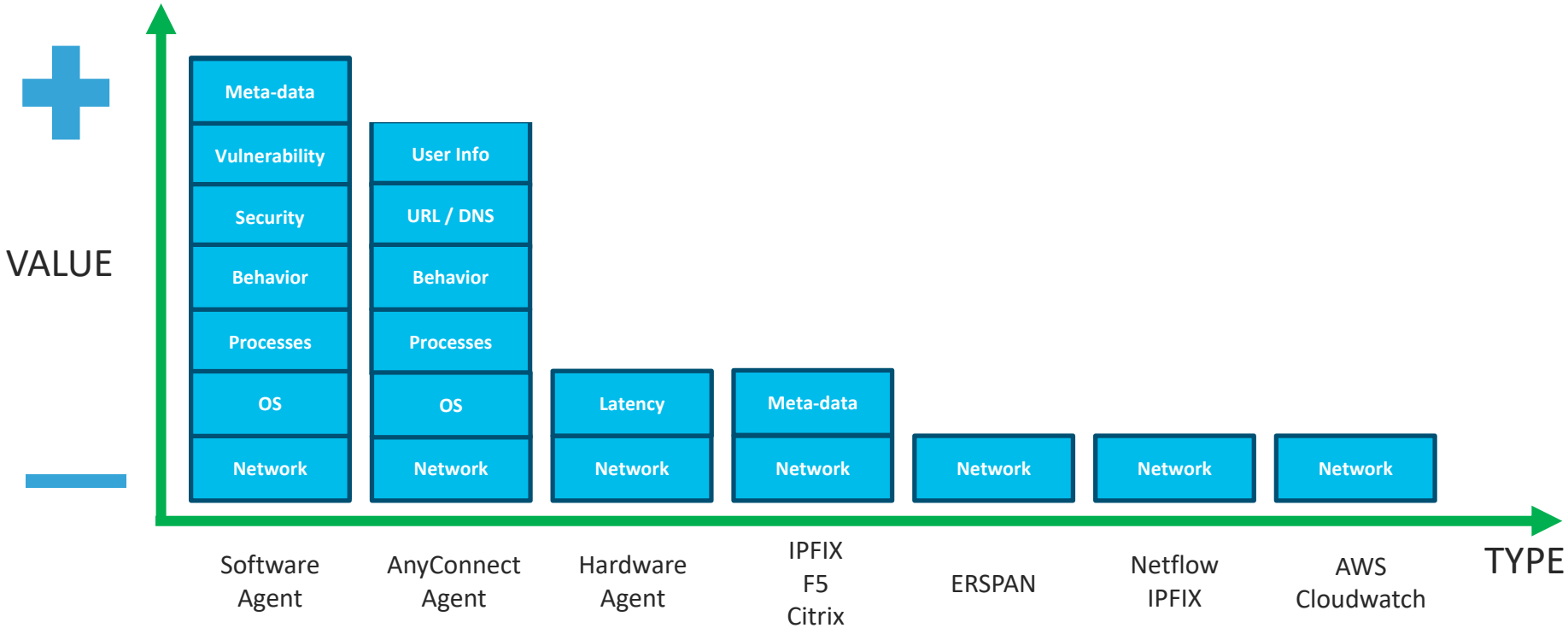
Tetration workload protection



Any vendor's infrastructure. Any data center. Any cloud

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Different Data Sources provide different value



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Identify Workloads

With Tetration's workload visibility, gain insight into:

- Application components
- Communications
- Processes & network flows
- Dependencies

Get visibility:

- Across the data center & multi-cloud infrastructure
- Private/public clouds

Workload Visibility

Workload: Establish Trust

Visibility:

- Every packet & data center flow
- East-west communication
- Users and user groups accessing application
- Process info & installed software
- Long-term data retention for telemetry & forensics
- Application Dependency Maps

How Data is Collected:

- Software sensors for bare-metal, virtual machines & containers
- Endpoint & flow visibility through Cisco AnyConnect & Identity Services Engine (ISE)
- Other telemetry collection option includes Nexus 9000 series hardware, ERSPAN and Netflow sensors

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tetration Software Sensor Overview

Workload: Establish Trust

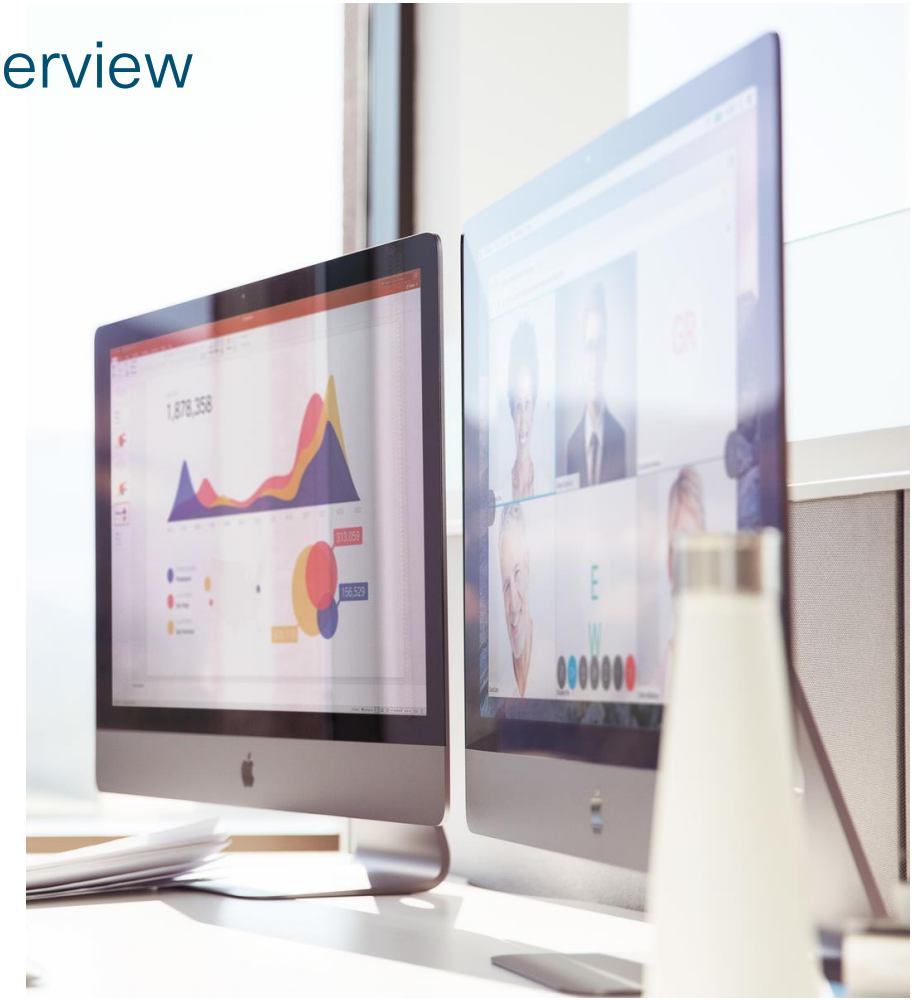
Installs and runs as a user process in the operating system

Enables telemetry collection and policy enforcement for segmentation

- Collects metadata from packet headers (no payload), process information, and installed software
- Enforces policies for segmentation through IPsets for Linux and Windows advanced firewall for Windows servers

Software sensors thresholds:

- Low CPU overhead (<1%)
- Default set to 3% CPU overhead



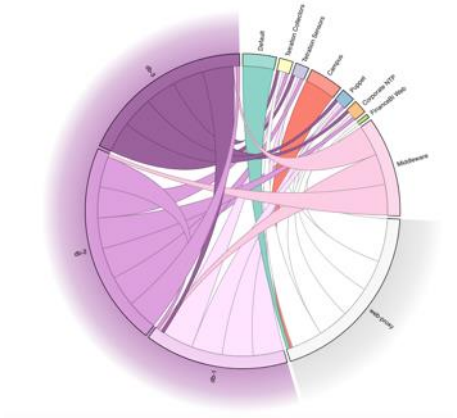
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

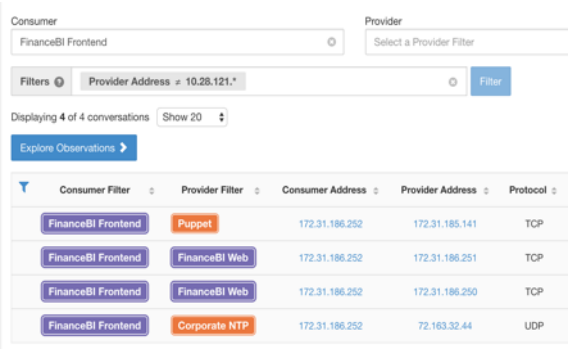
Tetration Demo

Application Insight

Workload: Establish Trust

Tetration maps your application dependencies, giving you insight into app communications.





Cluster View

Snapshot of communication between app components, grouped into clusters (VM, bare-metal)

Conversation View

All communication details between different app components

Shared Services

Services commonly shared among multiple apps (orchestration, DNS, AAA servers, etc.)

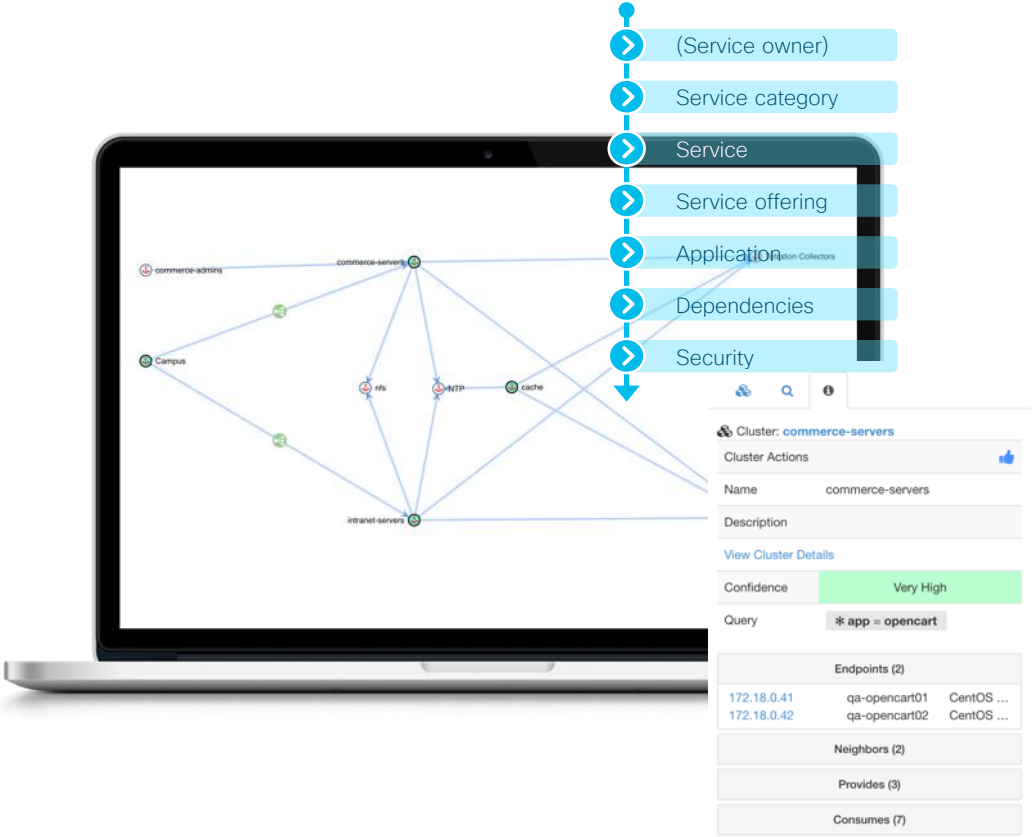
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Application Insight Dependency Map

Workload: Establish Trust

Get visibility into:

- How different application tiers are communicating
- About direct connections to database servers
- Communications through load balancers
- If there are outgoing connections that shouldn't be allowed



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workload Profile

Workload: Establish Trust

Any host with a Tetration software agent or an endpoint registered through an AnyConnect Proxy contains the workload profile information

Based on the agent type, information includes

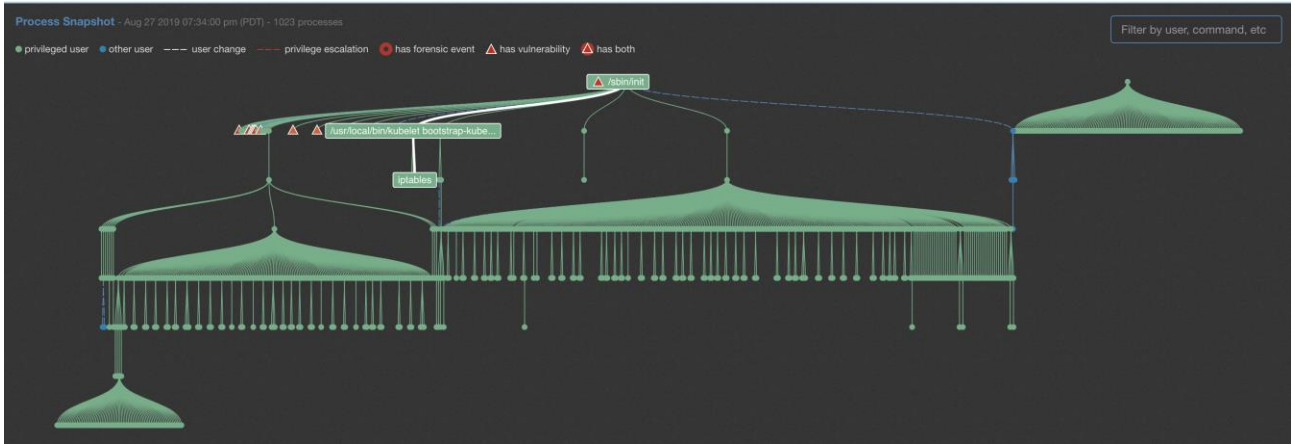
Long-lived processes	Enforcement policies	File hashes
Installed packages	Interface details	Visit history
Process snapshot	Data leaks	Agent statistics

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workload Profile – Process Snapshot

Workload: Establish Trust

- Process details collected in near real-time and process snapshot is updated with this information
- Full time-series view to go back and visualize process hierarchy and behavior information
- Correlated with vulnerability information to indicate if a process is started by a software package with known vulnerability
- Indicates process behavior history such as a past forensic event or privilege escalation



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workload Profile – Software Package Details

Workload: Establish Trust

VESX3-KUBE5

Filters: CVE Score v3 ≥ 9 | Filter

Displaying 12 of 487

Name	Version	Architecture	Publisher
wget	1.17.1-1ubuntu1.5	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
vim	7.4.1689-3ubuntu1.3	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
systemd	229-4ubuntu21.22	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
rsyslog	8.16.0-1ubuntu3.1	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
rsync	3.1.1-3ubuntu1.2	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
python	2.7.12-1~16.04	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
perl	5.22.1-9ubuntu0.6	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
openssl	1.0.2g-1ubuntu4.15	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
libxml2	2.9.3+dfsg1-1ubuntu0.6	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
git	2.7.4-0ubuntu1.6	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
curl	7.47.0-1ubuntu2.13	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
bzip2	1.0.6-8ubuntu0.2	amd64	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>

VESX3-KUBE5

Filters: Package Name = openssl | Score (V3) ≥ 9

Displaying 3 of 454

CVE	Package Name	Package Version	Score (V2)	Score (V3)	Severity (V2)	Base Severity (V3)	Access Vector (V2)	Access Complexity (V2)
CVE-2016-6303	openssl	1.0.2g-1ubuntu4.15	7.5	9.8	HIGH	CRITICAL	NETWORK	LOW
CVE-2016-2182	openssl	1.0.2g-1ubuntu4.15	7.5	9.8	HIGH	CRITICAL	NETWORK	LOW
CVE-2016-2177	openssl	1.0.2g-1ubuntu4.15	7.5	9.8	HIGH	CRITICAL	NETWORK	LOW

- See all the software packages installed on that workload
- Search for specific packages based on various parameters including vulnerability data
- Identify the vulnerabilities associated with a particular software package and its details

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

User & Endpoint Visibility

Workload: Establish Trust

AnyConnect

- Get information on devices, OS, interface, flow details
- Collect telemetry from AnyConnect Network Visibility Module (NVM)
- Integrate with LDAP for additional user context

Identity Services Engine (ISE)

- Get device type (IP phone, printer, etc.), usernames, tags, device posture, flow records
- Collect endpoint/inventories from ISE
- Using LDAP for additional user context

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workload: Enforce Trust-Based Access

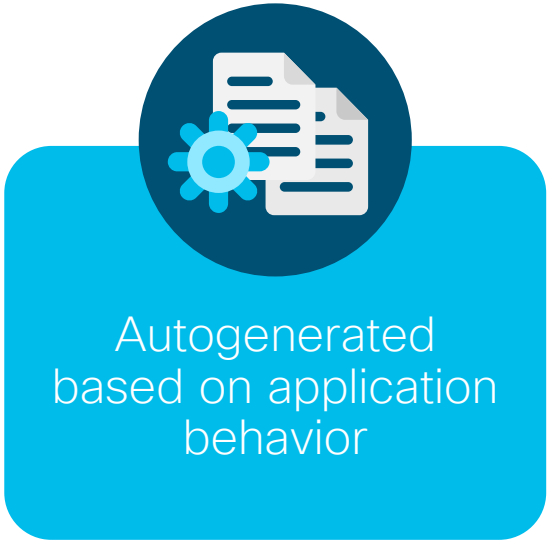
Application Micro-Segmentation

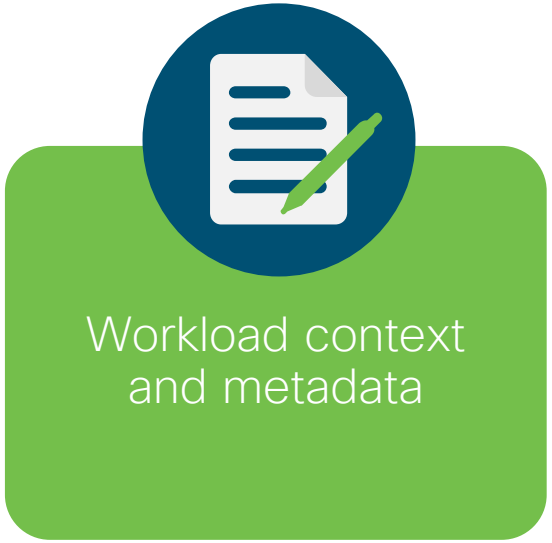
Tetration's micro-segmentation works by:

- Defining policies to restrict application access
- Enforcing segmentation policy across data centers and the multi-cloud
- Containing breaches & minimize lateral movement

Zero Trust Policy: Sources and Context

Workload: Enforce Trust-Based Access

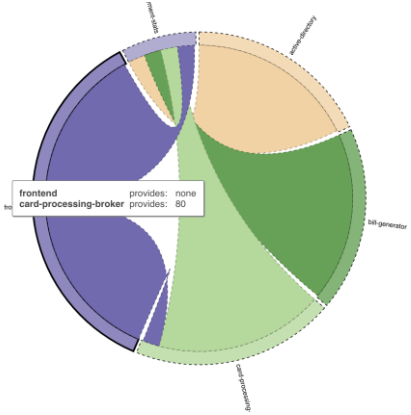


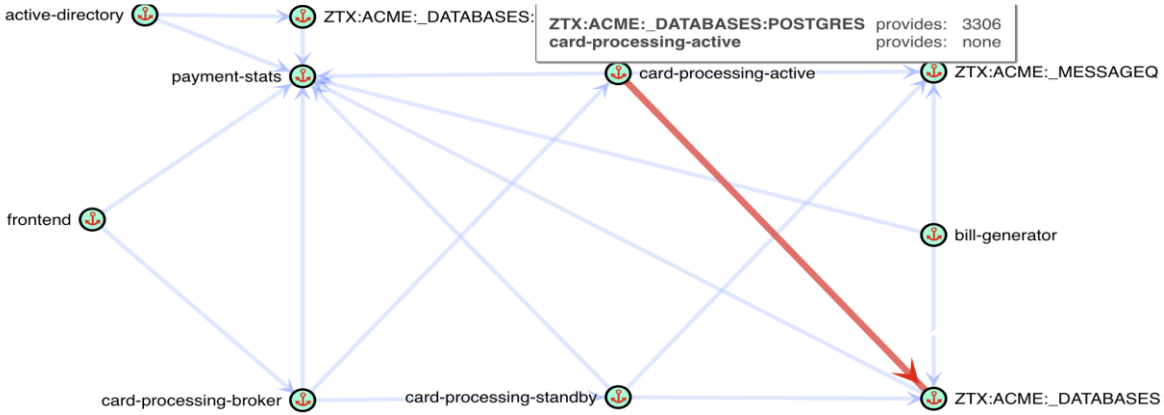


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Automated discovery, clustering and policy generation

Workload: Enforce Trust-Based Access





Priority	Action	Consumer	Provider	Services
10	DENY	client posture=non-compliant	ZTX : ACME : DC : PAYMENT PROCESSOR	Any
10	DENY	SGT=Quarantine	ZTX : ACME	Any
90	ALLOW	LB Internal Interface	ZTX : ACME : DC : PAYMENT PROCESSOR	TCP : 80 (HTTP)
100	ALLOW	active-directory	ZTX : ACME : _DATABASES : ORACLE	TCP : 3306 (MySQL)
100	ALLOW	card-processing-active	ZTX : ACME : _DATABASES : POSTGRES	TCP : 3306 (MySQL)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

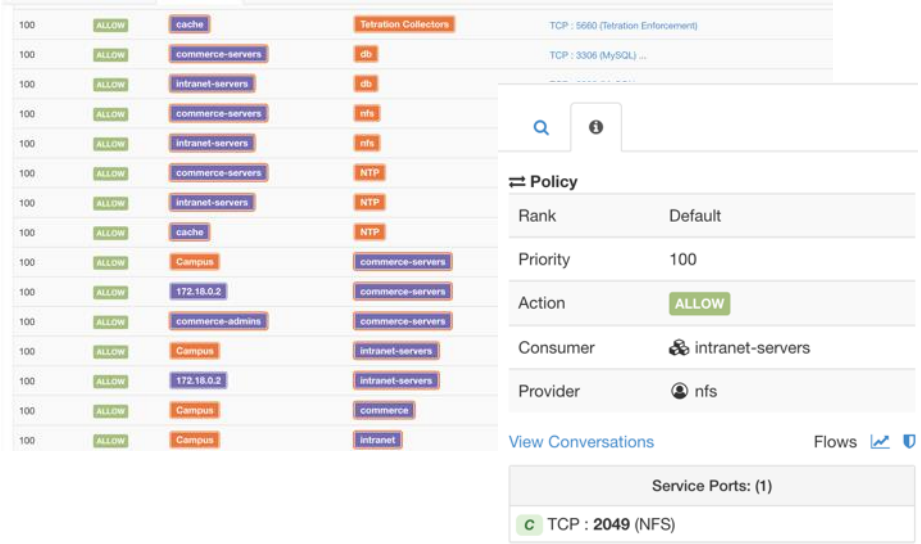
Zero Trust Policy: Application Segmentation

Workload: Enforce Trust-Based Access

Tetration generates policies based on application behavior.

For example:

- Production may not talk to non-production
- Certain applications are not accessible via the internet
- Allow or deny traffic between app components & infrastructure elements



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Enforcing Micro-Segmentation Policies

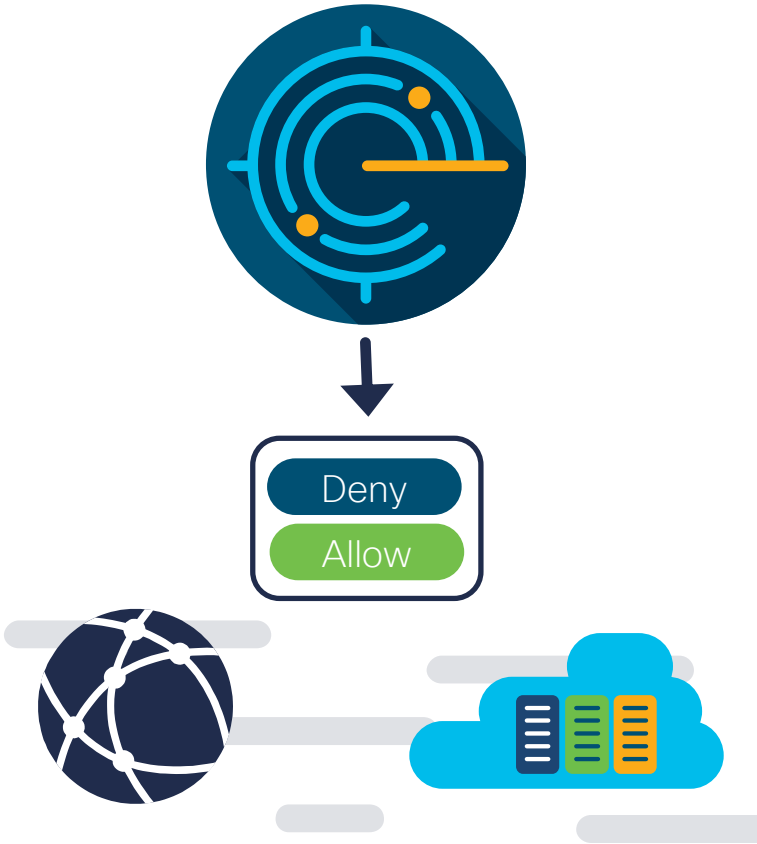
Workload: Enforce Trust-Based Access

Intent informs trust-based policies.

Intent is rendered as security rules in native OS firewalls.

Converted into blacklist/whitelist rules

Intent	Rules
Block nonproduction applications from talking to production applications	SOURCE 10.0.0.0/8 DEST 128.0.0.0/8
Allow HR applications to use the employee database	SOURCE 128.0.10.0/24 DEST 128.0.11.0/24
Block all HTTP connections that are not destined for web servers	SOURCE * DEST 128.0.100.0/24 PORT = 80
	SOURCE * DEST * PORT = 80

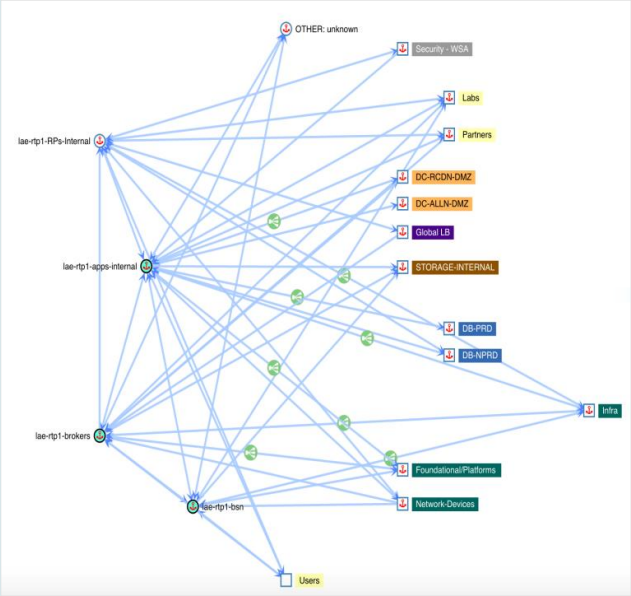


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

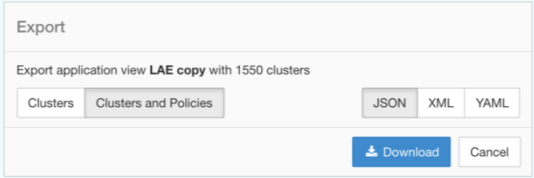
Zero Trust Policy: Exportable Policies

Workload: Enforce Trust-Based Access

Application discovery



Whitelist policy recommendation (export in Kafka, JSON, XML, and YAML)
Import into ASA, NGFW




```
{
 "src_name": "App",
 "dst_name": "Web",
 "whitelist": [
  {
   "port": [0, 0],
   "proto": 1,
   "action": "ALLOW"
  },
  {
   "port": [80, 80],
   "proto": 6,
   "action": "ALLOW"
  },
  {
   "port": [443, 443],
   "proto": 6,
   "action": "ALLOW"
  }
 ]
}
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Real-time and historical policy simulation

Workload: Enforce Trust-Based Access

Validate policy impact assessment in real time

Simulate policy changes over historic traffic

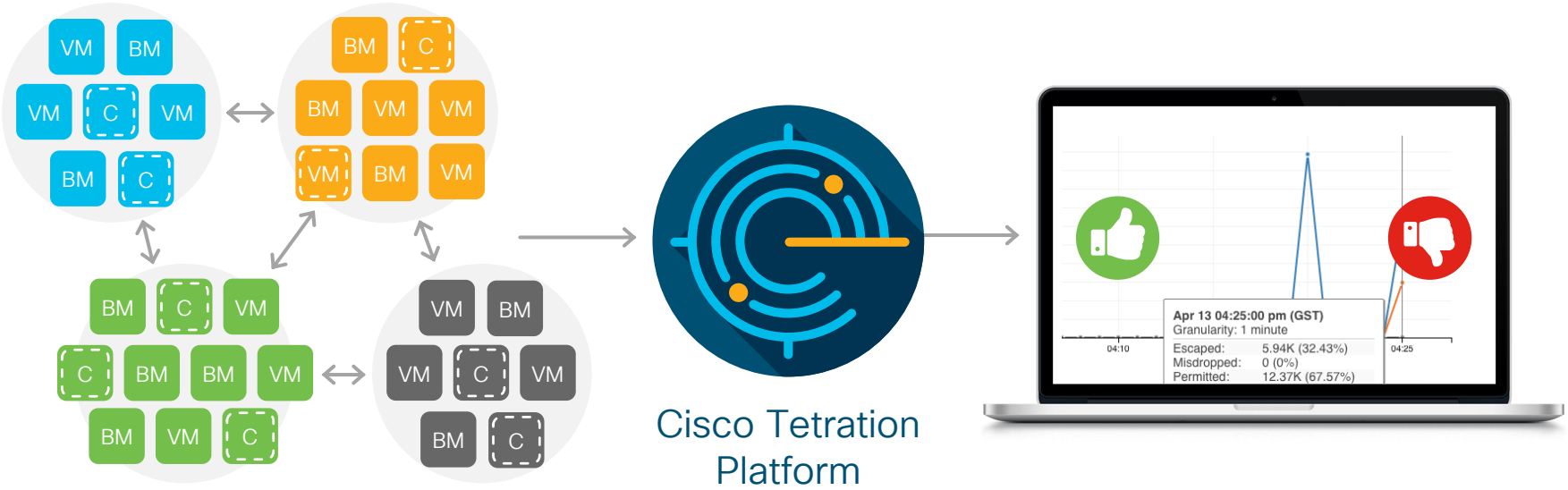
View traffic outliers for quick intelligence

Audit becomes a function of continuous machine learning

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Compliance Assessment

Workload: Enforce Trust-Based Access



Identify policy deviations in real time

Review and update whitelist policy with one click

Perform policy lifecycle management

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Workload Context

Workload: Enforce Trust-Based Access

Cisco Tetration can connect to external systems to get workload context

- vCenter, for VM info
- Kubernetes or OpenShift, for container tags (pod information, service tags, etc.)
- AWS, for security tags
- IP address management system, for IP/subnet info
- DNS servers, for domain name info

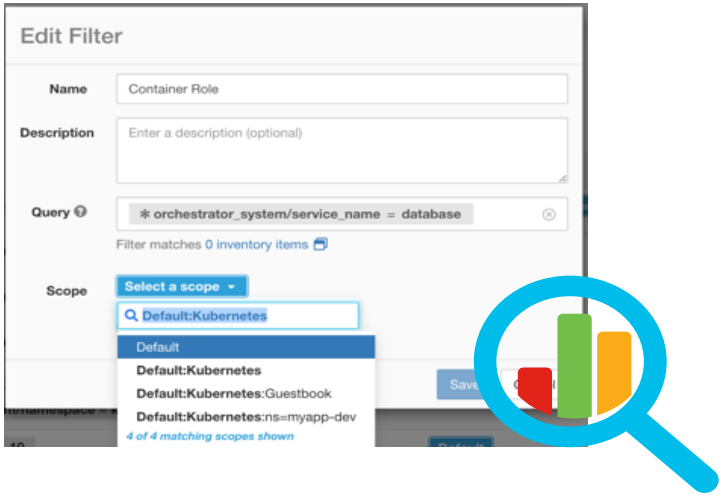
Using:

- Standard APIs to query info
- Periodic data collection
- Read-access only

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: Workload Context-aware Segmentation

Workload: Enforce Trust-Based Access



Priority	Action	Consumer	Provider
10	DENY	AWS:Web-prod	LondonDC:DB-prod

Tetration identifies, inventories and defines workloads, & continuously updates as new servers are added, existing servers moved or IP addresses change

Using this info, Tetration enforces context-aware policies.

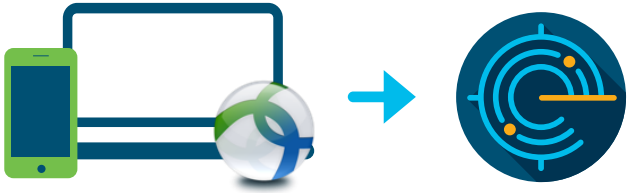
Example Context : Web production is in AWS and DB is on-prem

Example Policy : Public cloud Web can't talk to on-prem database servers

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: User & Endpoint

Workload: Enforce Trust-Based Access



DENY

client posture=non-compliant

ZTX : ACME : DC : PAYMENT PROCESSOR

Tetration gets insight from external sources

- User & endpoint context
- From AnyConnect, ISE, LDAP

And through using this insight, generates policies

Example: Only finance users can access financial reporting system.

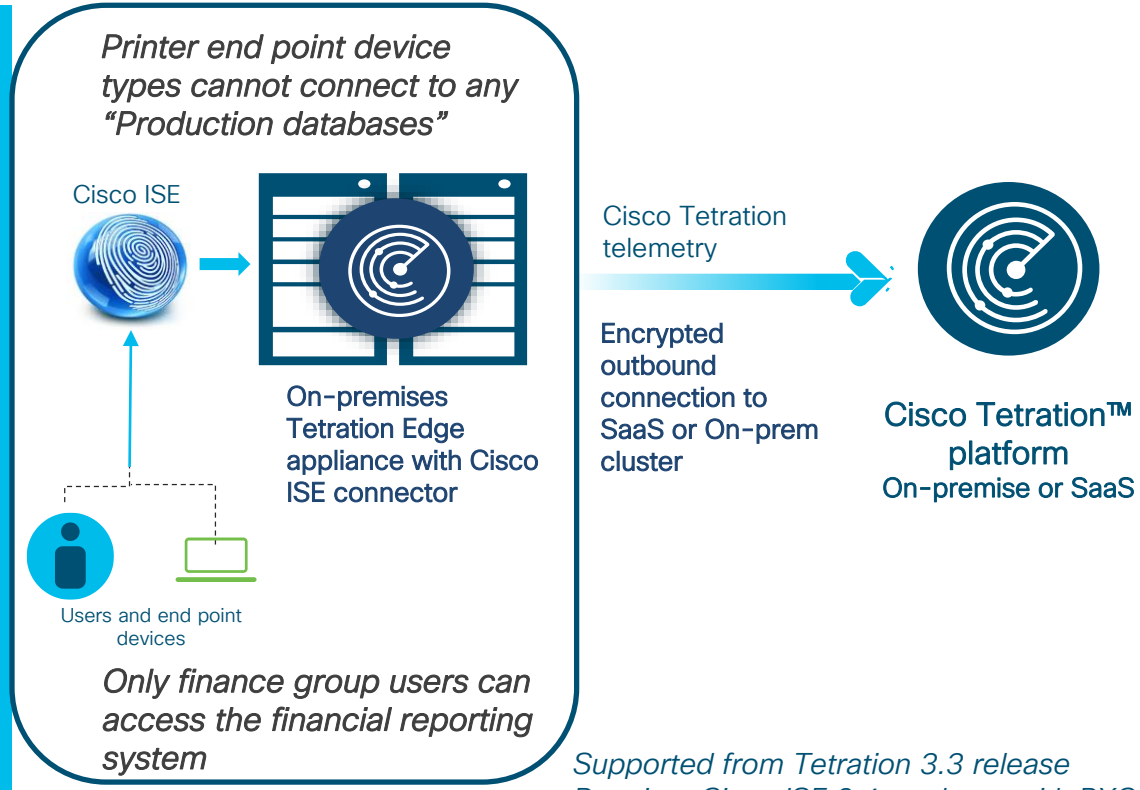
Or, printers can't connect to any database servers

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust Policy: User & Endpoint context

Workload protection policy based on endpoint device attributes

- Authenticated machine or not
- Source Group Tags (SGT) - Name and Id
- Mobile Device Management attributes
  - Compliant, Disk encrypted, Jail broken, Pin locked device, etc.,
- End point profile
  - Workstation or Mobile device or Laptop or Printer
  - End point device names
- User and device memberships are maintained and updated in real time



Supported from Tetration 3.3 release
Requires Cisco ISE 2.4 or above with PXGrid enabled

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case: Segmentation for the Hybrid Cloud

Workload: Use Case

Consistent ZT Policies:

- Enforce granular controls everywhere
- Control lateral movement across east-west traffic to minimize damage

Address customer problems:

- Need to discover workloads & application behavior & traffic
- Create and enforce adaptable ZT app segmentation policy
- Limit workload access to only users/devices that require it

Dynamic, ZT Segmentation Policies:

- Segmentation policy moves with the workload
- Policy auto-updates as app dependencies & communications evolve

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Workload – Hybrid Cloud Segmentation

What's the problem?	How Cisco helps:
Discover, model and baseline my applications behavior and traffic	Tetration Visibility and analysis
How can I create and enforce a ZT segmentation policy that adapts	Tetration ADM, contextual policies, dynamic attributes
I need to limit workload access to only users/devices that require it	Tetration integrations with SD-Access/ISE/Anyconnect

Log and Audit Everything

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public


Untitled - Notepad
File Edit Format View Help
SGT: Employee
Windows (CRLF)
Ln 1, Col 14
100%
Host Name: 172-17-16-111
OS Version: Windows 10
IP Address: 172.17.16.111
MAC Address: 00-50-56-A2-70-E2
DNS Server: 172.16.1.98
Default Gateway: 172.17.16.1
Boot Time: 8/14/2019 5:18 PM
Recycle Bin
Google Chrome
PuTTY
Visual Studio Code
WinSCP
Microsoft Edge
tetration_in...
msi_installer
Type here to search
12:28 PM
8/16/2019
MacBook Air

Let's recap…

- Workload: Tetration – Hybrid-DC multi-tier invoicing application
  - Started with flat network, clean slate in tetration
  - Integrated ISE for context (SGT, users, device profiles and health…)
  - Tetration performed discovery, security health assessment, ADM, baselining
  - Automated creation of dynamic rules and one-click policy enforcement

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workload: Continuously Verify Trust

Continuous Monitoring & Response

Tetration's proactive response

Baseline process behaviors for:

- Faster detection of indicators of compromise

Identify software vulnerabilities & exposures:

- Quarantine servers
- Block communication when policy violations are detected
- Reduce attack surface

"Gartner predicts that, through 2020,
99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year."

Reduce attack surface

Reduce your attack surface

Software vulnerabilities

Identify known vulnerabilities associated with the installed software packages

Define actions proactively to restrict communication or quarantine workloads

Stale processes and ports

Identify unused process and port bindings that could potentially be exploited

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detect Policy Compliance

Workload: Continuously Verify Trust

Verify and simulate policy compliance with Tetration's analytics

Identify policy deviations in real time

Review and update whitelist policy with one click

Policy lifecycle management

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detect Workload Vulnerabilities

Workload: Continuously Verify Trust

Limit your attack surface & prevent lateral movement

Cisco Tetration Analytics

- Inventories software packages
- Identifies software with known vulnerabilities

Take Action

Set up policies to respond:

- Quarantine a host
- Or block vulnerable systems

Workload policy is auto-updated when vulnerability resolves

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

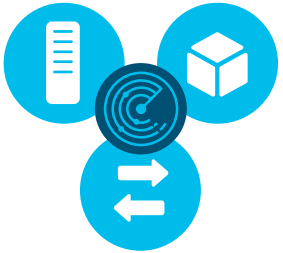
Protect from Workload Vulnerabilities

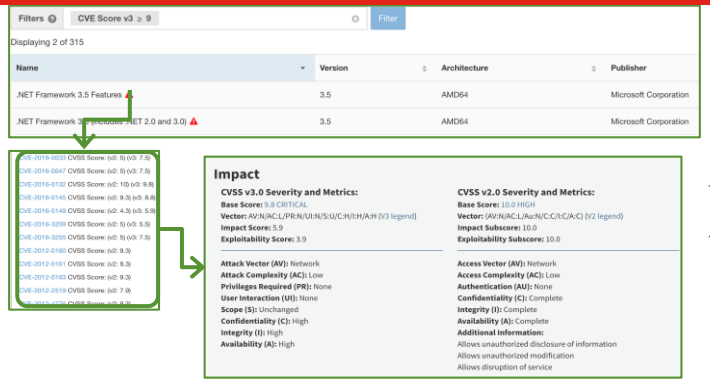
Reduce attack surface

Workload: Continuously Verify Trust

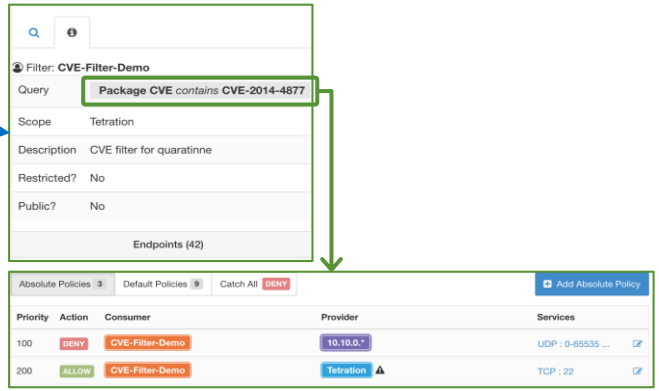
Limit the attack surface & prevent lateral movement

Workloads (VM, Baremetal and containers)





- Identify the vulnerability details in minutes
- Vulnerability details include:
  - Severity
  - Impact subscore
  - Exploitability subscore
- Quickly identify all servers that are running specific software package version



- Set up filters to search for one or more vulnerabilities
- Set up policy through UI or API to take specific action
- Quarantine a host when servers are identified with the vulnerability

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detect Server Behavior Deviations

Workload: Continuously Verify Trust

Baseline server behavior & detect deviations to help identify malware faster

Collect server details:

- Server process inventory (process, process execution details, process hash)
- See hierarchy of servers, historical hierarchy & behavioral info

Identify behavior deviations:

- Match server processing behavior to typical malware behavior
- Detect potential indicators of a compromise (privilege escalation, shell-code execution, etc.)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

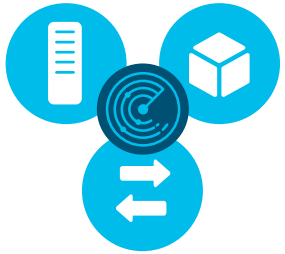
Detect Server Behavior Deviations

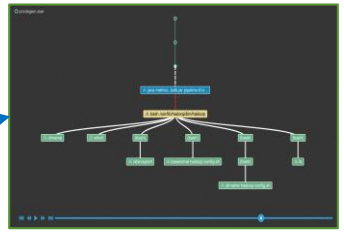
Detect behavior anomalies

Workload: Continuously Verify Trust

Baseline server behavior & detect deviations to help identify malware faster

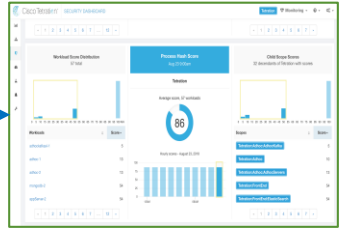
Workloads (Container, VM or Baremetal)



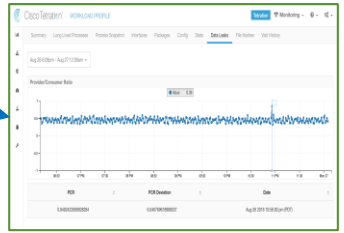


Process behavior deviations

- Privilege escalation
- Shell-code execution
- Side channel attack
- Raw socket creation
- MITRE ATT&CK tactics
- User login activities



Check process hash sanity based NIST RDS database and hash consistency

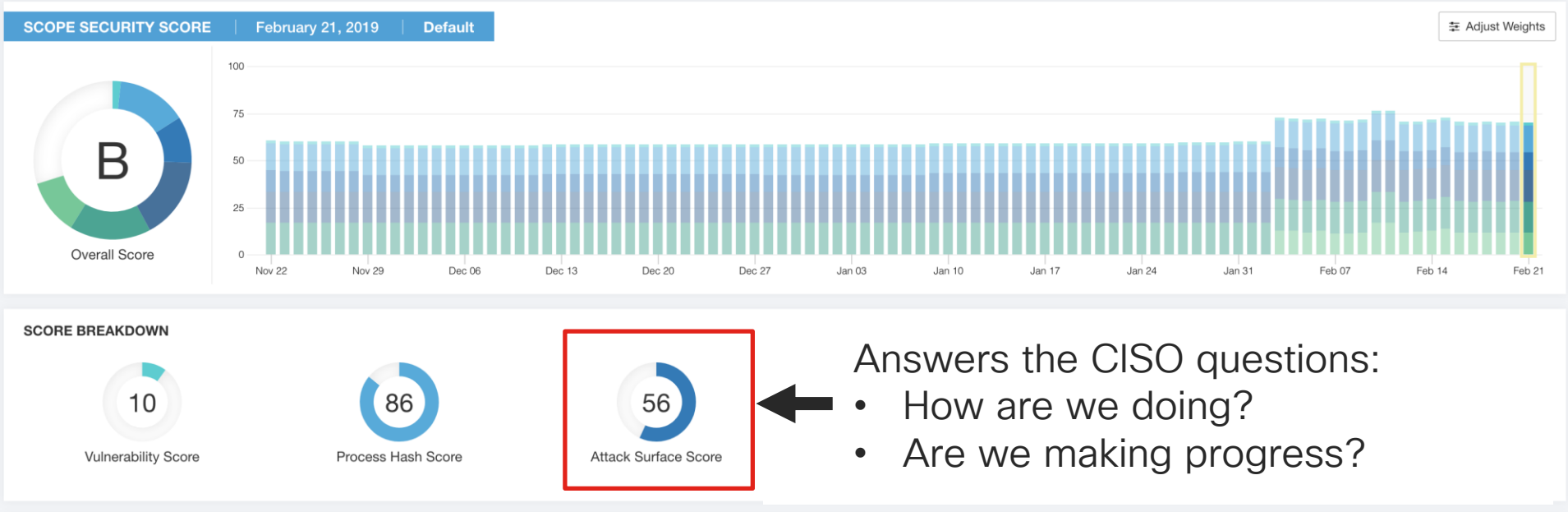


Detect anomalies in traffic volume between the workloads

- Temporal analysis to baseline the behavior to address seasonality

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Bringing all this together – Security dashboard



Answers the CISO questions:

- How are we doing?
- Are we making progress?

Overall Security posture

Visualize security trend

Identify areas to improve

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Case: Continuous Trust Verification

Address customer problems:

- Ongoing, real-time security of workloads
- Need to defend workloads from threats & risks
- Leverage other tools to protect workloads

Priority	Action	Consumer	Provider	Services
10	DENY	client posture=non-compliant	ZTX : ACME : DC : PAYMENT PROCESSOR	Any
10	DENY	SGT=Quarantine	ZTX : ACME	Any
90	ALLOW	LB Internal Interface	ZTX : ACME : DC : PAYMENT PROCESSOR	TCP : 80 (HTTP)
100	ALLOW	active-directory	ZTX : ACME : _DATABASES : ORACLE	TCP : 3306 (MySQL)
100	ALLOW	card-processing-active	ZTX : ACME : _DATABASES : POSTGRES	TCP : 3306 (MySQL)

Security dashboard for continuous workload monitoring.

- **Set policies to respond to a breach of trust (deviations, vulnerabilities)**
- Quarantine servers
- Block communication

Integrate with SD-Access/ISE, Cisco firewalls, Stealthwatch & Cisco Threat Response (CTR) for insight, policy & alerts.

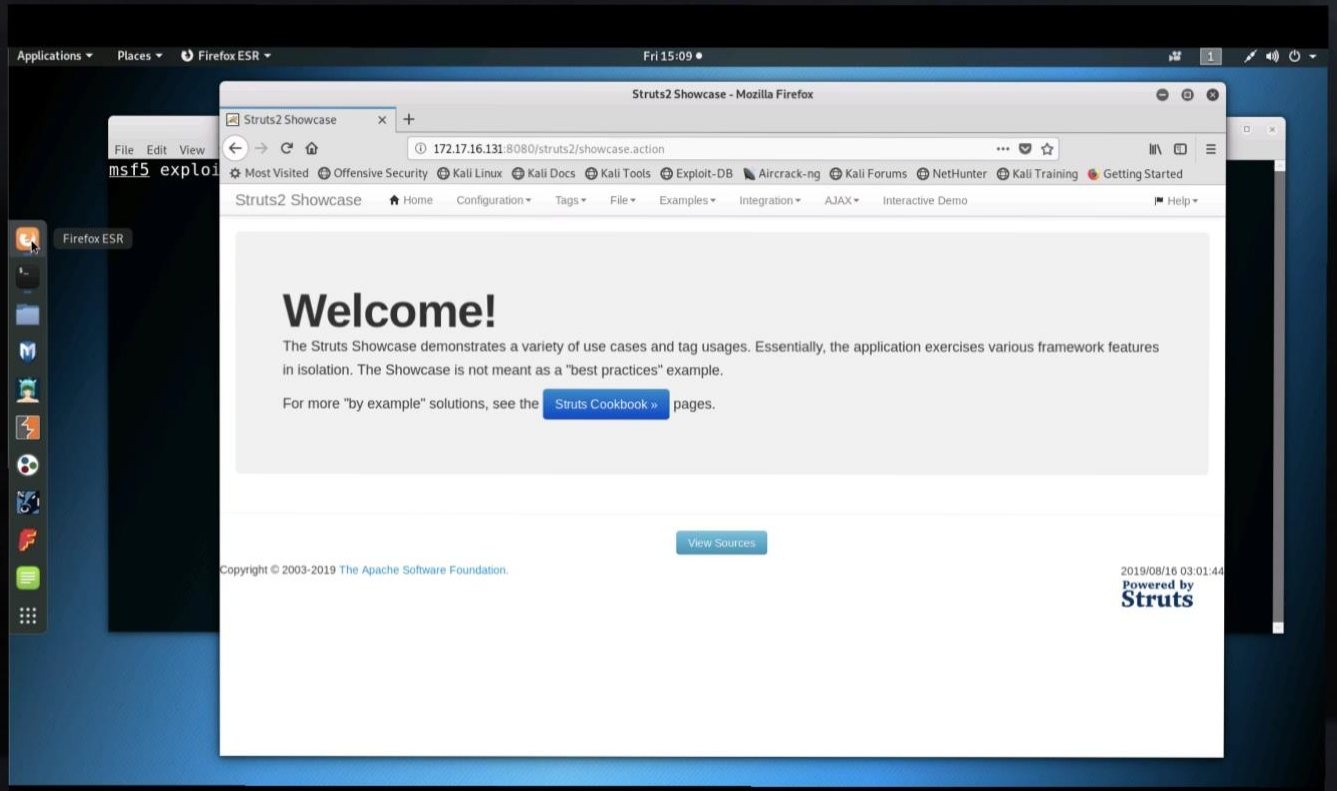
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Workload – Continuous Trust Verification

What's the problem?	How Cisco helps:
What is the real-time security health of my workload environments?	Tetration Security Dashboard
I need to defend my workloads from attacks	Tetration Forensics rules Automate segmentation rules based on threat/risk data
How can I leverage my other security tools to protect my workloads?	Tetration integration with SD-Access/ISE, CTR, NGFW, Stealthwatch, etc.

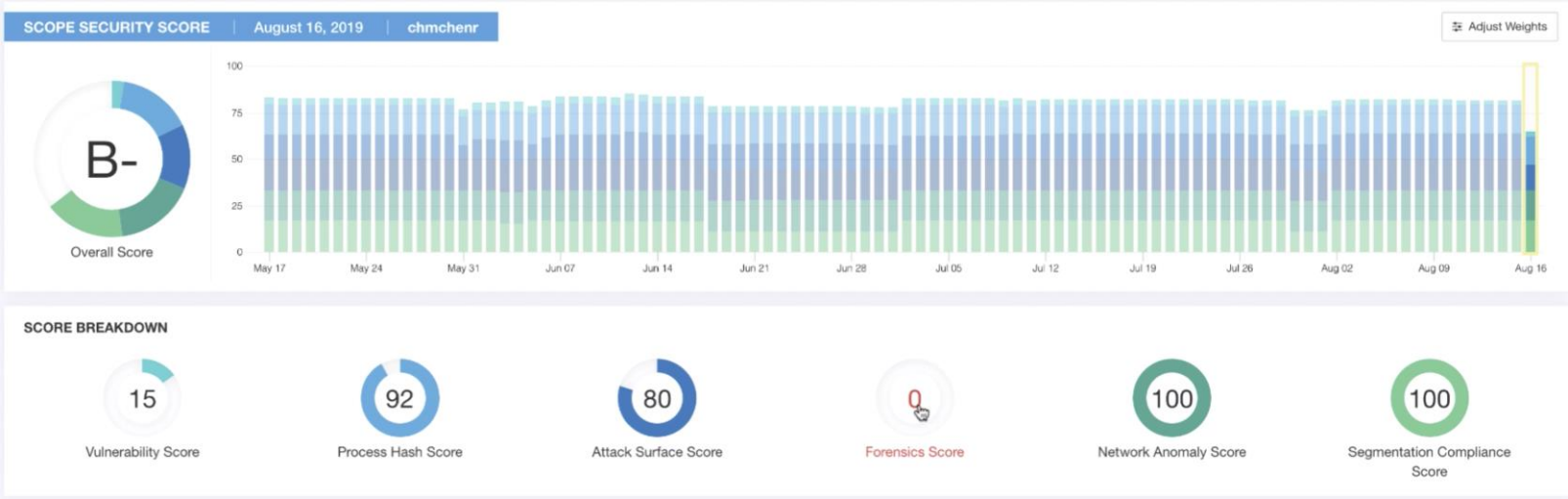
Log and Audit Everything

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public


Applications
Places
Firefox ESR
Fri 15:09
Struts2 Showcase - Mozilla Firefox
Struts2 Showcase
172.17.16.131:8080/struts2/showcase.action
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Struts2 Showcase
Home
Configuration
Tags
File
Examples
Integration
AJAX
Interactive Demo
Help
Welcome!
The Struts Showcase demonstrates a variety of use cases and tag usages. Essentially, the application exercises various framework features in isolation. The Showcase is not meant as a "best practices" example.
For more "by example" solutions, see the
Struts Cookbook »
pages.
View Sources
Copyright © 2003-2019 The Apache Software Foundation.
2019/08/16 03:01:44
Powered by
Struts
File Edit View
msf5 exploi
Firefox ESR

Let’s recap…

- Workload: Tetration – Workload Security
  - Security dashboard provided an overall health score
  - New vulnerability dashboard showed what was most critical to patch
  - Detailed forensics with new MITRE ATT&CK tactics rules & mitigation



Recap: Zero Trust for Workloads

Tetration secures all connections within your apps – get complete application visibility, prevent lateral movement and contain breaches.

Gain visibility:

- Identify workloads, dependencies, app behavior
- Create & enforce policies

Enforce policies:

- For application micro-segmentation
- To minimize lateral movement

Continuously monitor:

- Respond to indicators of compromise
- Alert or block communication

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust for the Workplace

Zero Trust for the Workplace

How to Establish Trust with SD-Access & ISE

Discover and classify devices

WITH

IoT device profiling
BYOD lifecycle management
User device Posture

Context-based network access control policy for users and things

WITH

Dynamic precise policies Group-based (SGT)

Continuous security health monitoring of devices

BY

Continuous Posture
Vulnerability assessments
Indications of compromise

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

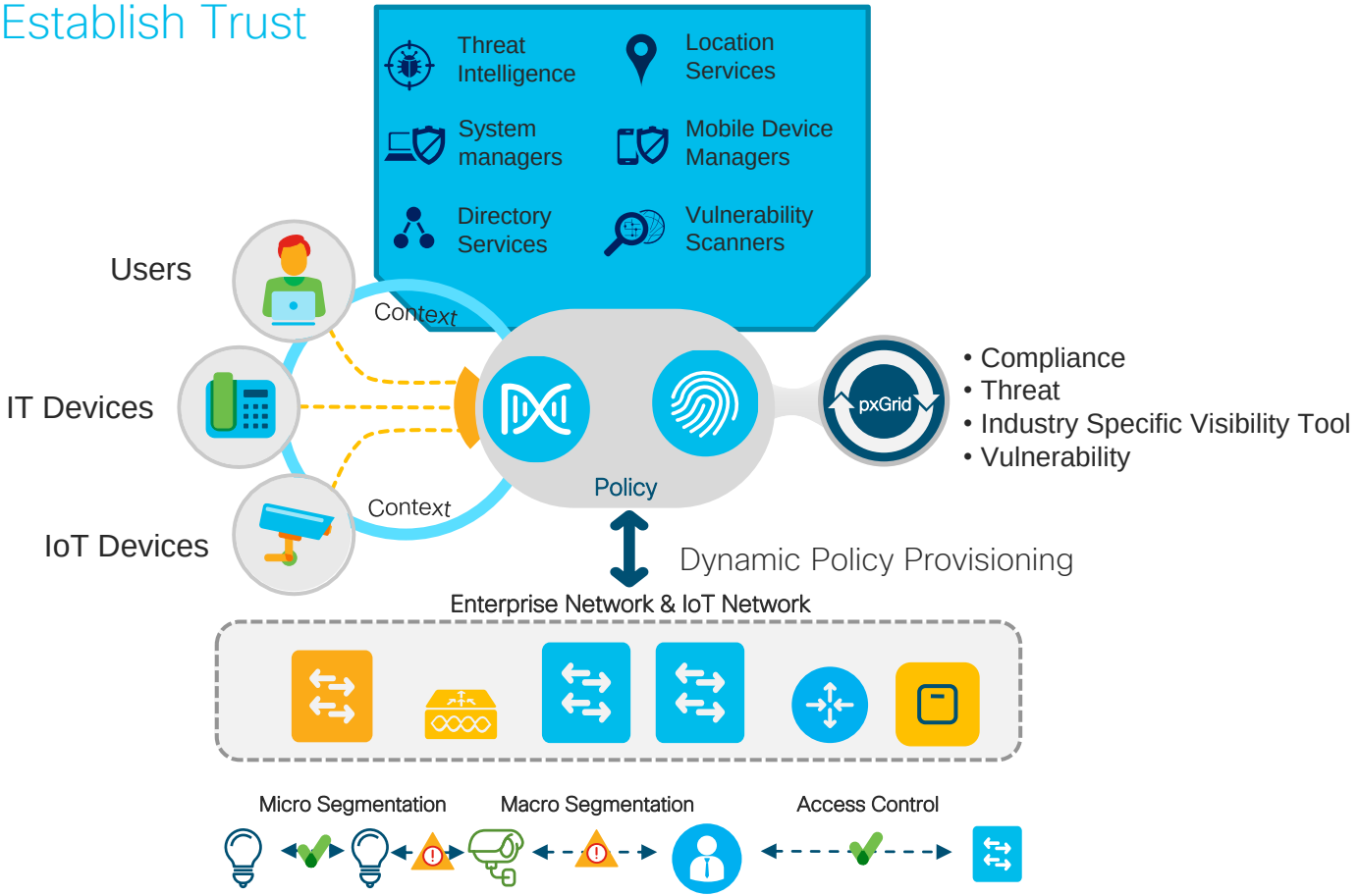
ISE is the foundation for ZT in the Workplace

- Asset & IoT Visibility
- Guest and Secure Wireless Access
- Device Administration
- Secure Wired Access
- Segmentation
- Device Compliance
- Security Ecosystem Integrations
- Rapid Threat Containment
- BYOD

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Access Overview

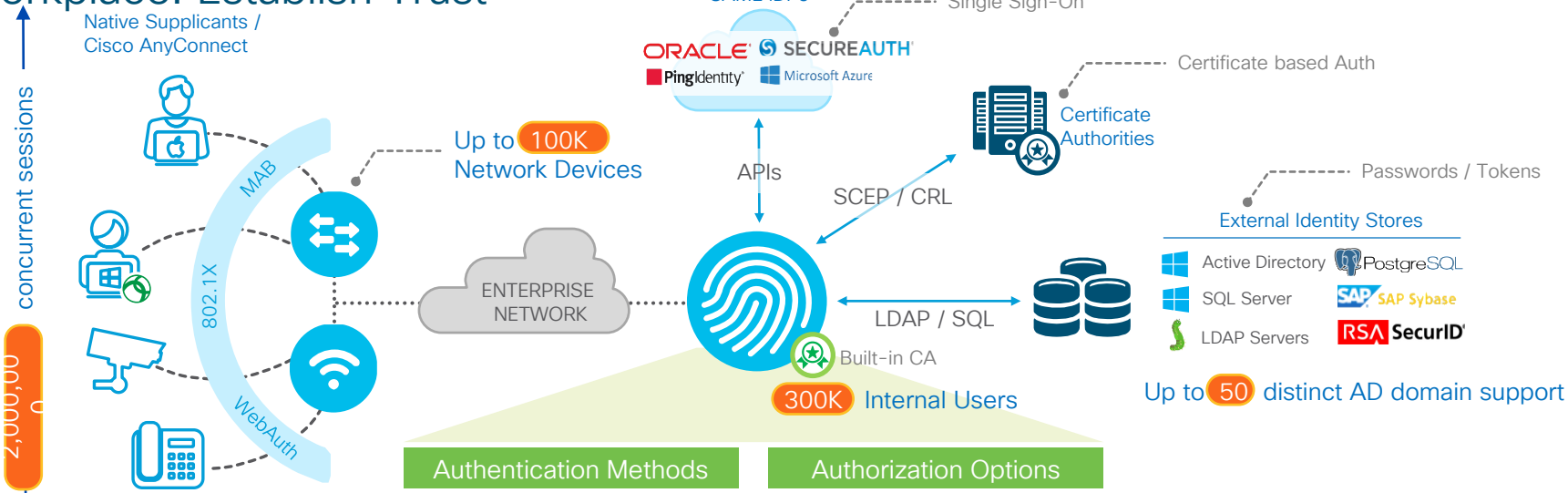
Workplace: Establish Trust



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 'Access Control' Overview

Workplace: Establish Trust



Authentication Methods		Authorization Options
PASSIVE IDENTITY	▪ MAC Authentication Bypass ▪ Easy Connect ®	▪ Downloadable / Named ACL ▪ Air Space ACL ▪ VLAN Assignment ▪ Security Group Tags ▪ URL-Redirection ▪ Port Configuration (ASP Macro / Interface-Template)

ACTIVE IDENTITY	▪ IEEE 802.1X
	▪ Web Authentication
	  ▪ Central WebAuth
	  ▪ Local WebAuth	

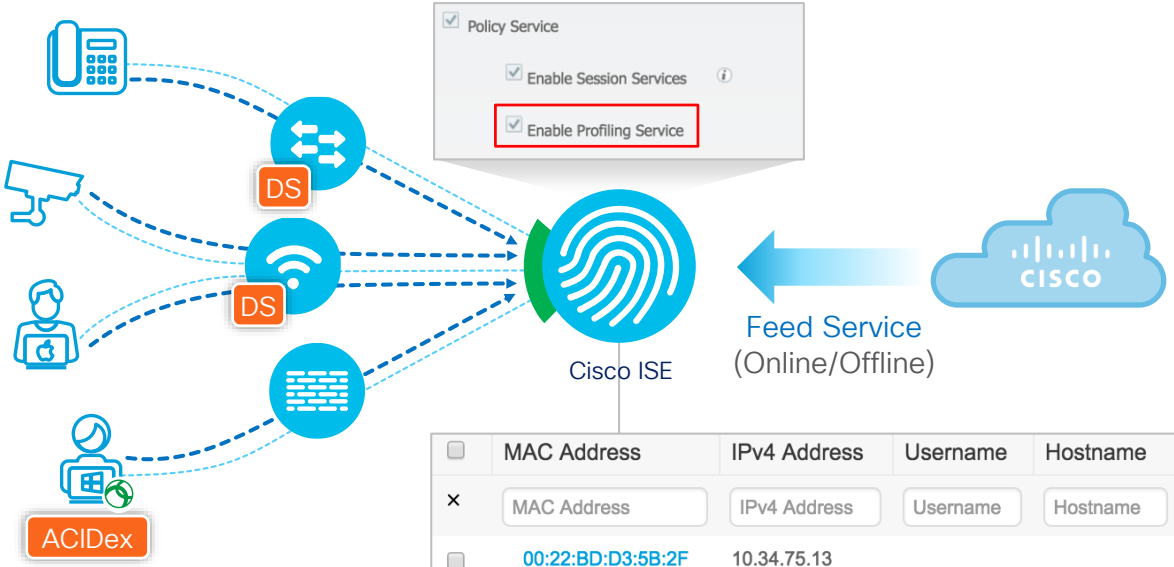
ASP: Auto Smart Port

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Visibility: Cisco ISE Profiling identifies devices

Workplace: Establish Trust

Endpoints send interesting data, that reveal their device identity



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

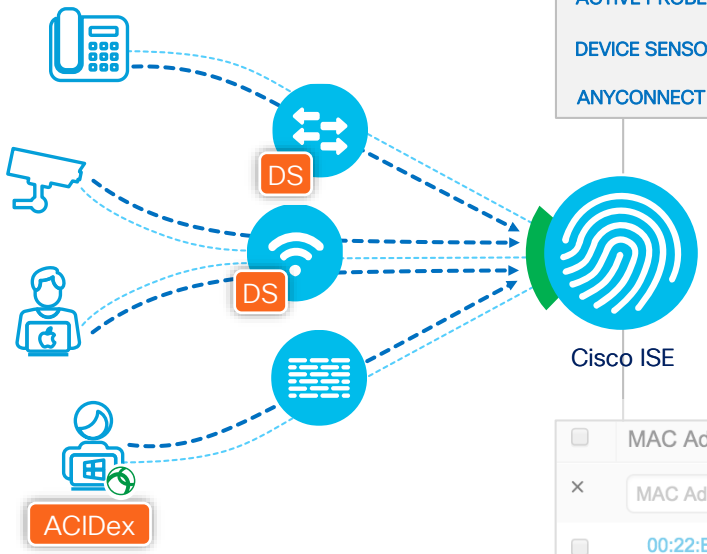
AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Visibility Data: Sources

Workplace: Establish Trust

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 (D

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Visibility and context gathering

I have no idea who and what is really on my network

→

Cisco ISE Profiler

ISE ➢ Fabric & Security

I'm blind to the risk of the users, devices and apps on my network

→

Cisco ISE Threat-centric NAC

ISE ➢ AMP, MDM, Anyconnect, 3rd party vuln. scanners

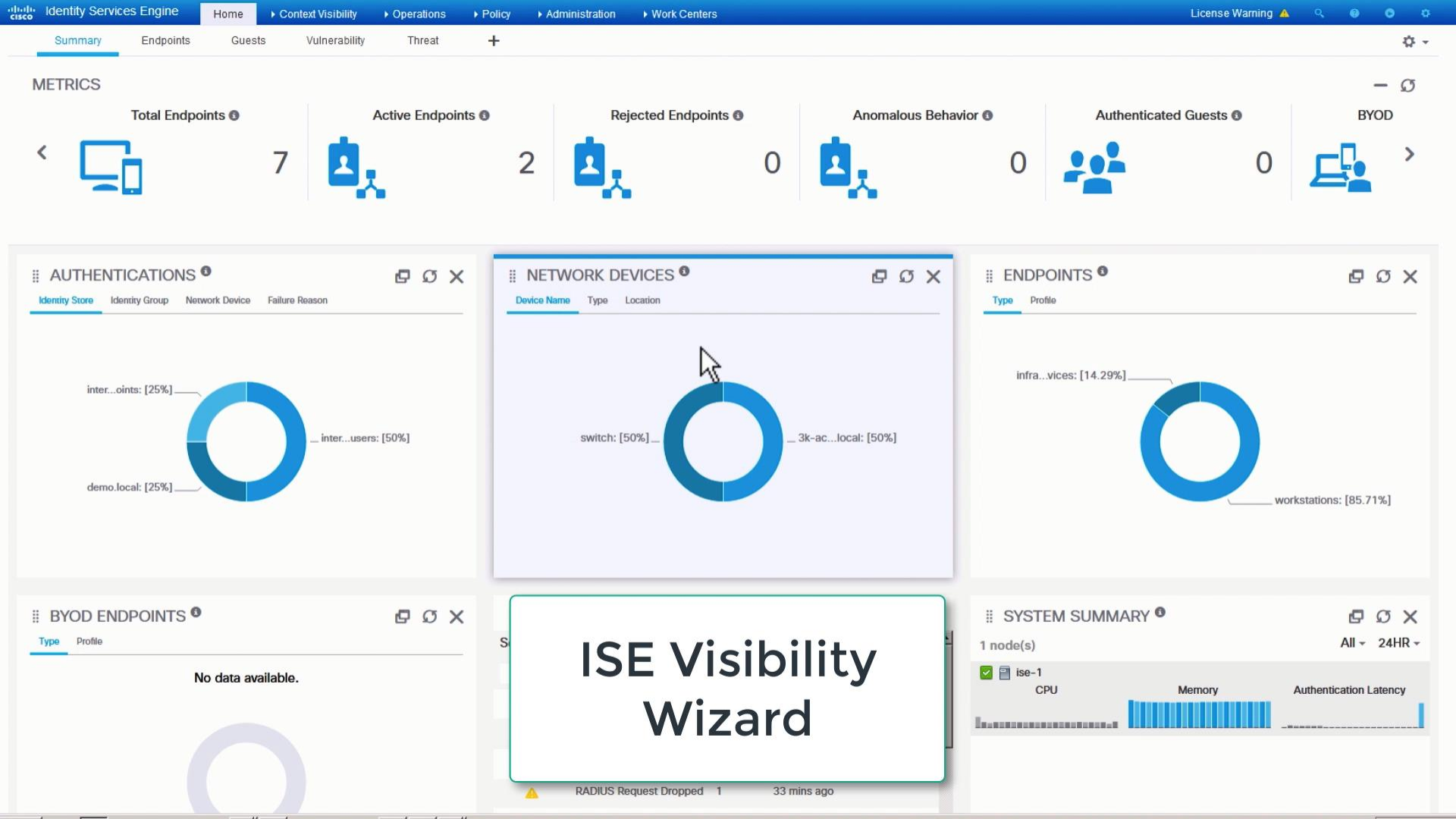
Collecting and maintaining an inventory is complex, unreliable and tedious

→

Cisco ISE

Visibility Wizard ➢ Fabric & Security

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public



ISE Visibility Wizard

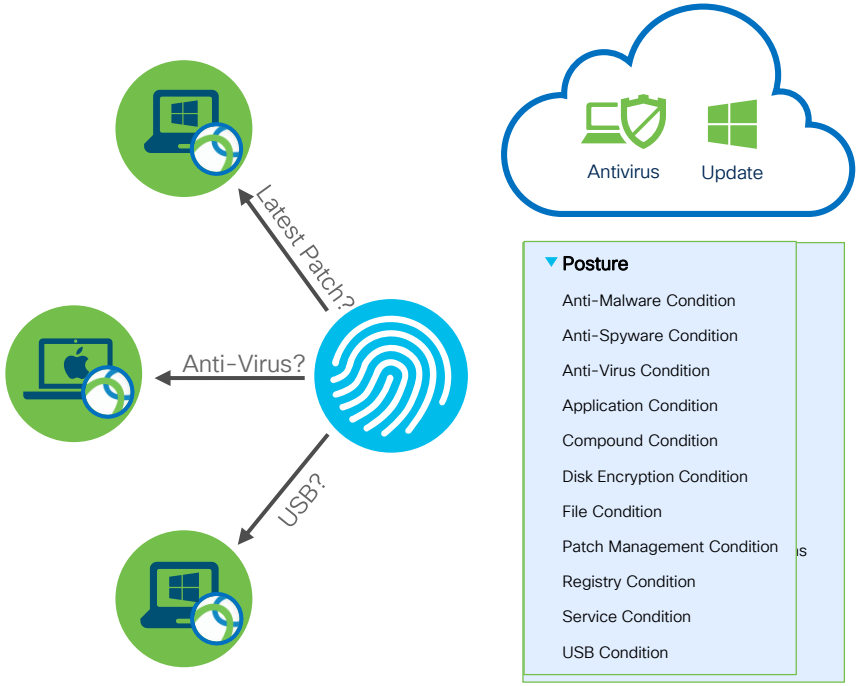
Posture Compliance

Workplace: Establish Trust

Posture defines the state of compliance with the company's security policy

Posture Flow

- **Authenticate User/Device**
  Posture: Unknown/Non-Compliant ?
- **Quarantine**
  Limited Access: VLAN/dACL/SGTs
- **Posture Assesment**
  Check Hotfix, AV, Pin lock, USB Device, etc.
- **Remediation**
  WSUS, Launch App, Scripts, MDM, etc.
- **Authorization Change**
  Full Access – VLAN/dACL/SGTs.



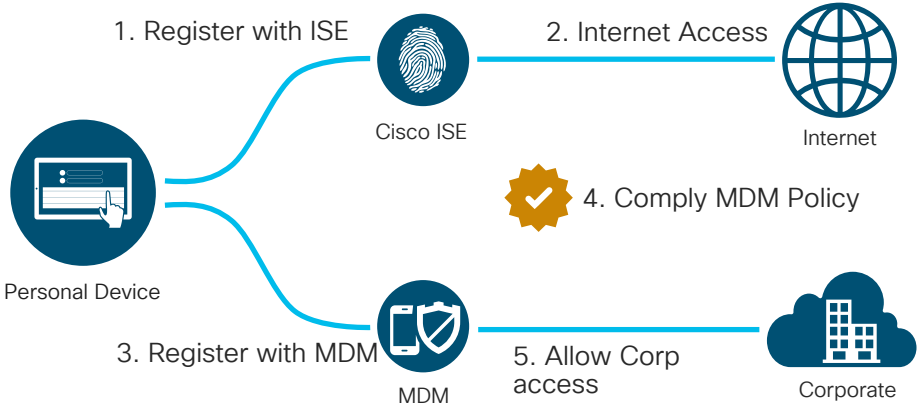
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mobile Device Compliance

Workplace: Establish Trust

MDM Policy Checks
Device registration status
Device compliance status
Disk encryption status
Pin lock status
Jailbreak status
Manufacturer
Model
IMEI
Serial number
OS version
Phone number

Posture Compliance assessment for Mobile devices



GOOD Absolute Software SAP IBM cisco Meraki AirWatch

Tangoe MobileIron Globo Jamf software Symantec MaaS360

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Centric NAC

Workplace: Establish Trust

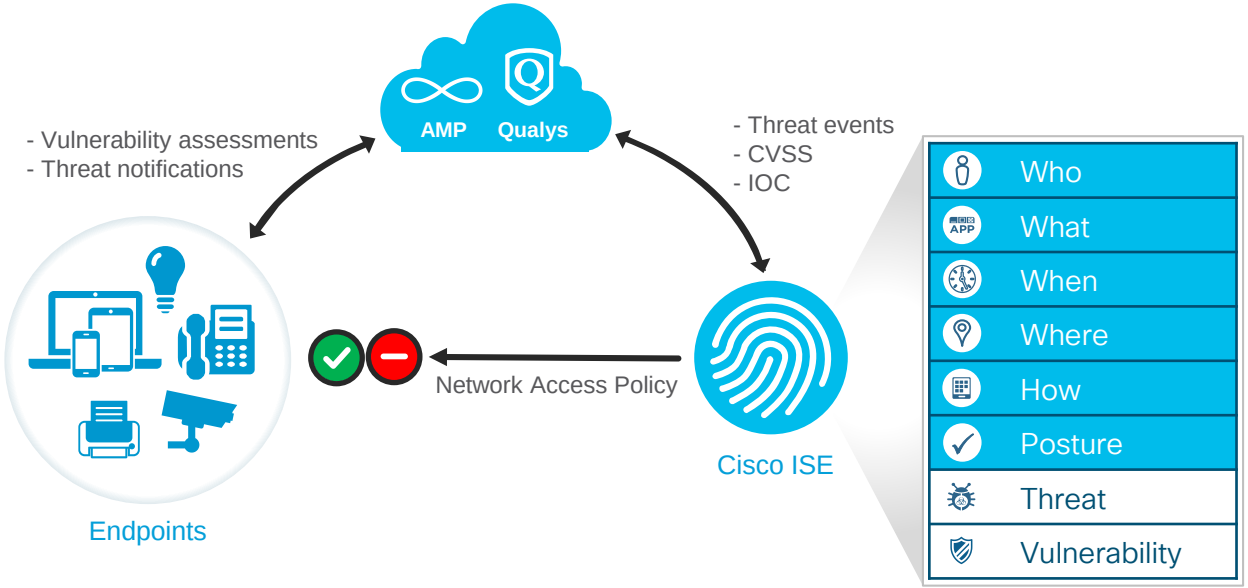
Cisco ISE protects your network from data breaches by segmenting compromised and vulnerable endpoints for remediation.

Compliments Posture
Vulnerability data tells endpoint's posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes



Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Grant access, but make it specific!

Guest | Contractor | Doctor

What data privileges do these users require?

Doctor | Unknown ID | Multi-User Kiosk

Surveillance | Telcom | Sales | Inventory

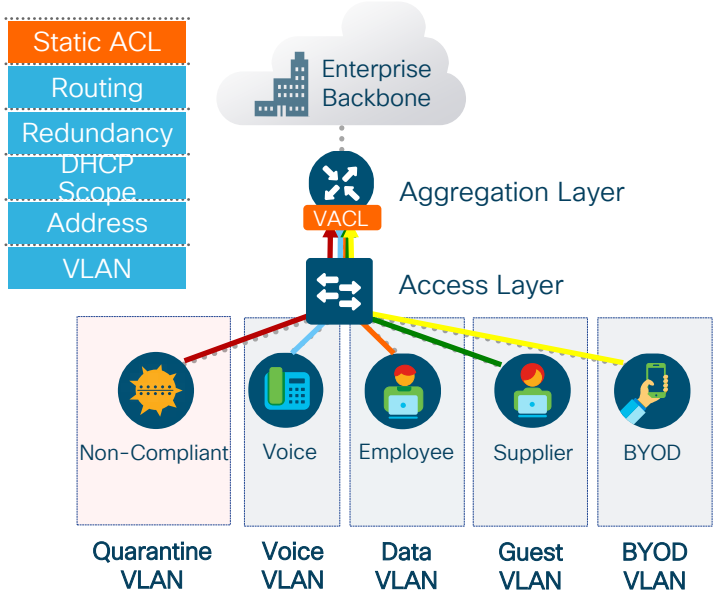
What data privileges do these devices require?

Medical | Infrastructure | Office

Network Segmentation: Policy

Workplace: Enforce Trust-based Access

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

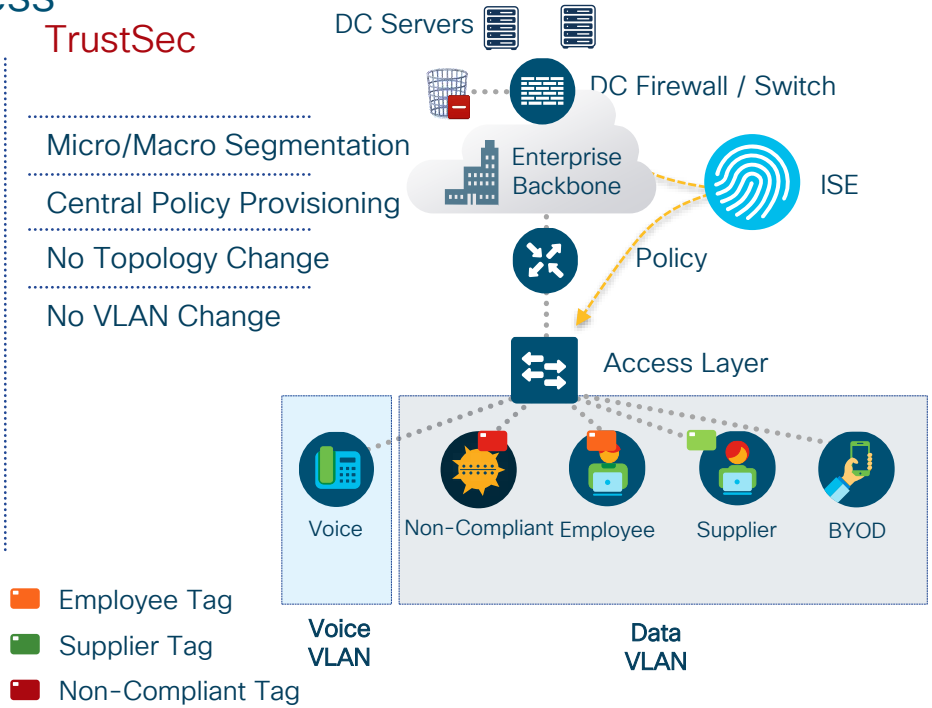
TrustSec

Micro/Macro Segmentation

Central Policy Provisioning

No Topology Change

No VLAN Change



Use existing topology and automate security policy to reduce OpEx

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Segmentation: Policy

Workplace: Enforce Trust-based Access

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | PassiveID

Overview | Components | TrustSec Policy | Authentication Policy | Authorization Policy | SXP | Troubleshoot | Reports | Settings

Egress Policy

Matrices List

Matrix

Source Tree

Security Groups ACLs List > MalwareBlock

Security Group ACLs

* Name: MalwareBlock

Description: SGACL to contain lateral movements

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```
deny icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
permit ip
```

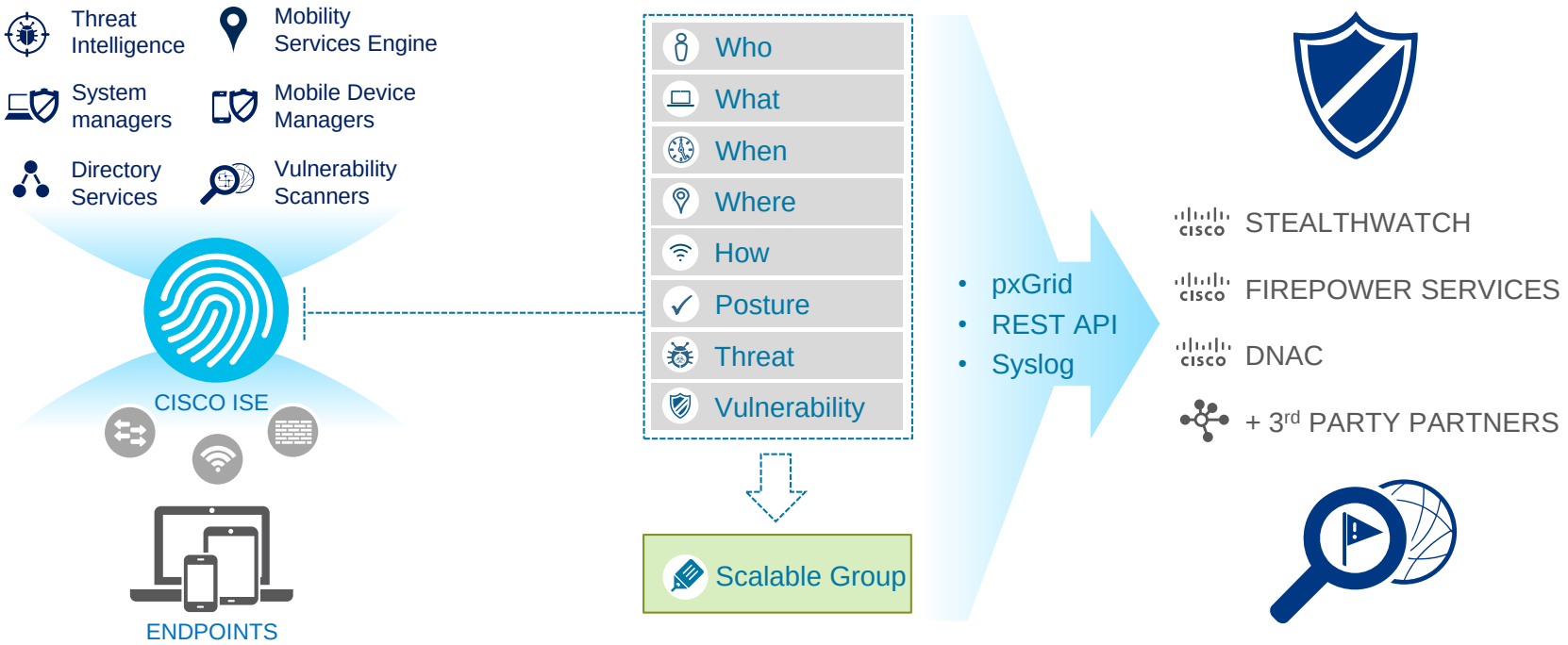
Production Matrix — Populated cells: 69

Edit | Add | Clear | Deploy | Monitor All - Off | Import | Export | View | Show CorpPolicy

Source \ Destination	Employees 4/0004	Contractors 5/0005	Development_Ser... 12/000C	PCI_Servers 14/000E	Point_of_Sale_S... 10/000A
Employees 4/0004	MalwareBlock	MalwareBlock	Permit IP	Deny IP	Permit IP
Contractors 5/0005	MalwareBlock	MalwareBlock	Deny IP	Deny IP	Deny IP
	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extending Trust



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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

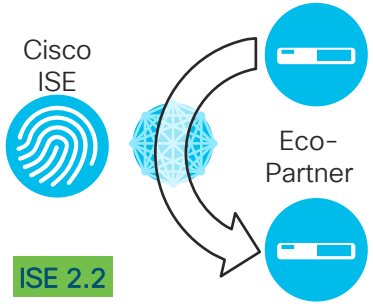
Enrich ISE Context

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

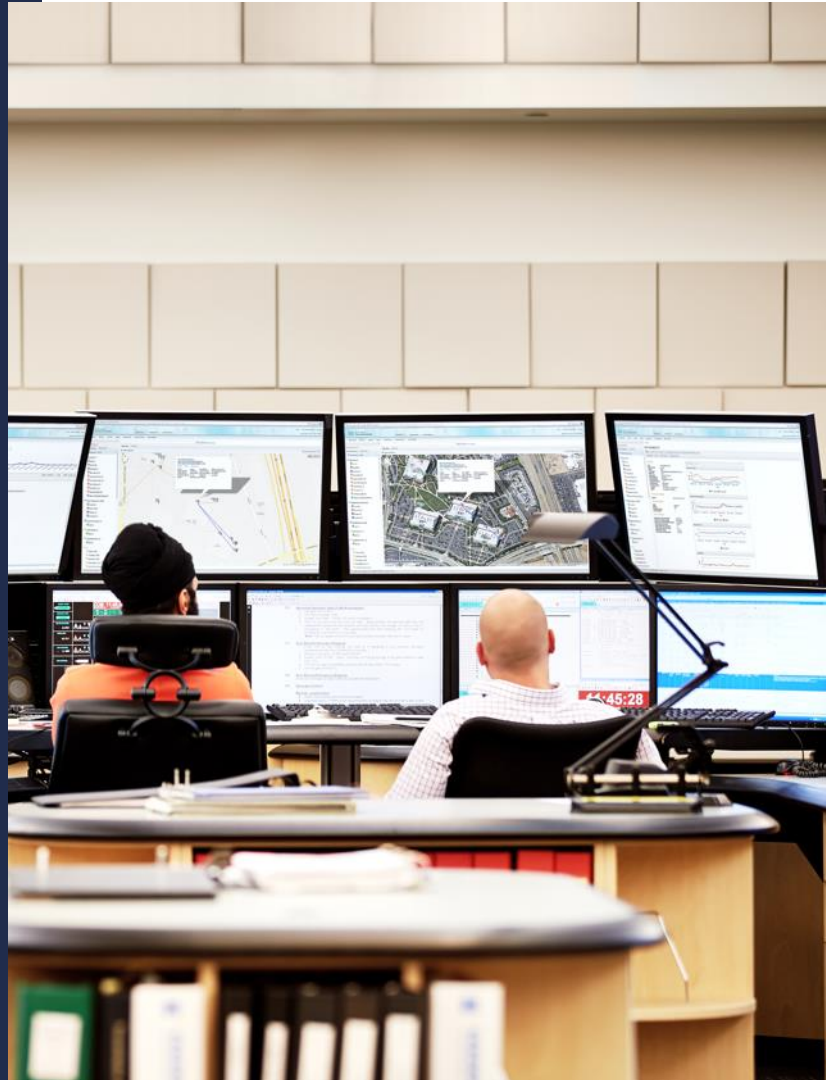
Continuous Monitoring & Response

With SD-Access, get complete network visibility into:

- Users' behavior
- Application performance
- Network threats

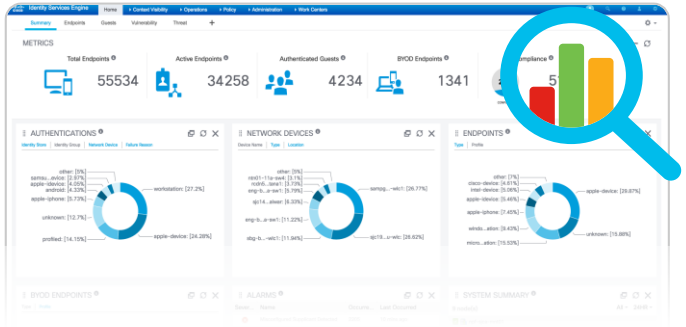
Get simplified network control:

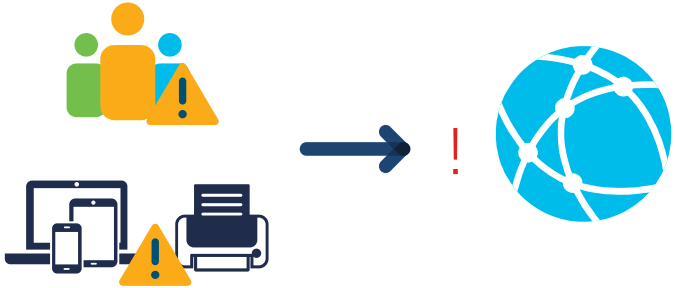
- Enforce network policies for network access & security
- Monitor networks across all network domains



Continuous Monitoring & Response

Workplace: Continuously Verify Trust





Continually analyze network traffic, get alerted of indicators of a compromise*.

Take action if:

- An endpoint is behaving differently than intended/classified
- Anomalous behavior matches attack behavior

Respond by:

- Quarantining users & devices with one click
- Revoking access to the network
- Changing access policies immediately

*Requires ISE integration with Cisco Stealthwatch

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continuous Monitoring & Response

Workplace: Continuously Verify Trust

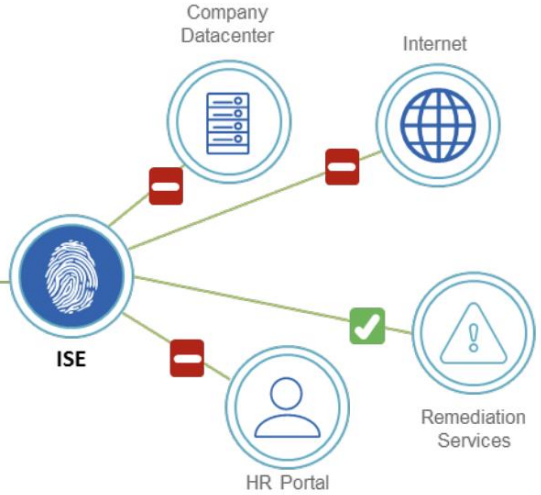
Detect indicators of compromise & take action with Stealthwatch + ISE

Quarantine users and devices with a single click

Change access policies immediately

Empower admins to make better security decisions

Stealthwatch Management Console

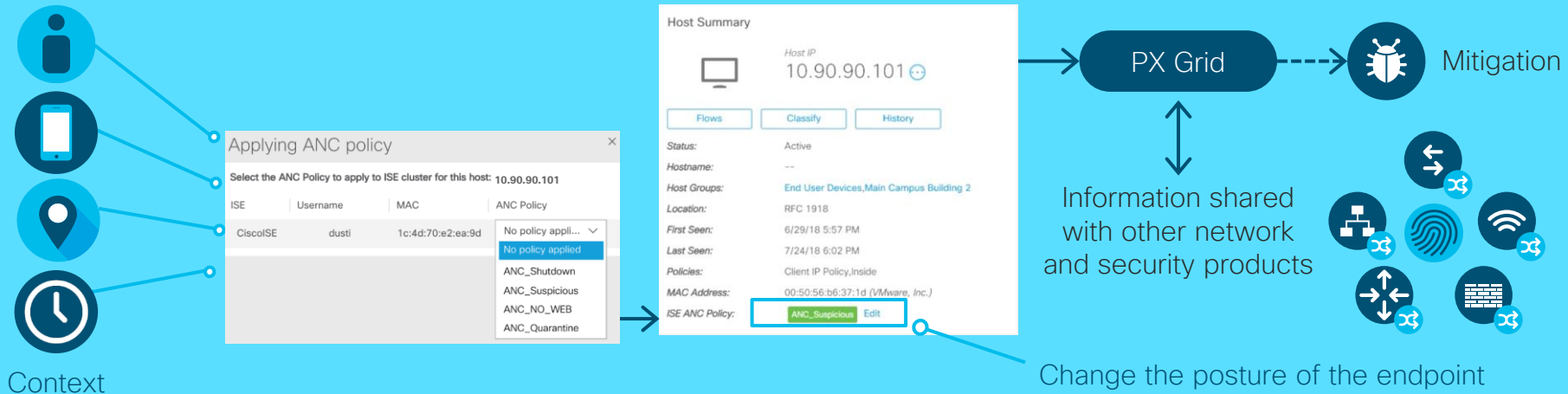


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Context Aware Rapid Threat Containment

Workplace: Continuously Verify Trust

Without any business disruption



Stealthwatch Management Console

Cisco® Identity Services Engine

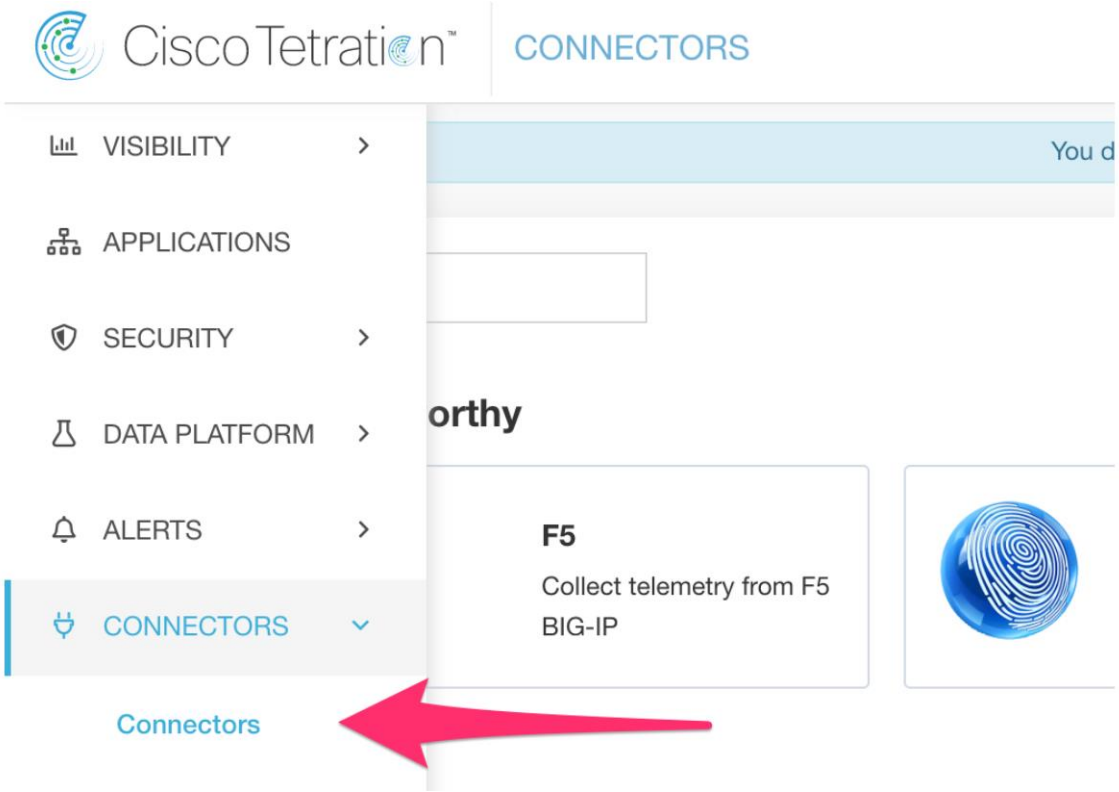
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE context sharing with Tetration

Workplace: Extend Trust

Ecosystem Integrations

2.4+



<u>Context sharing</u>
User
Endpoint
Compliance
MDM

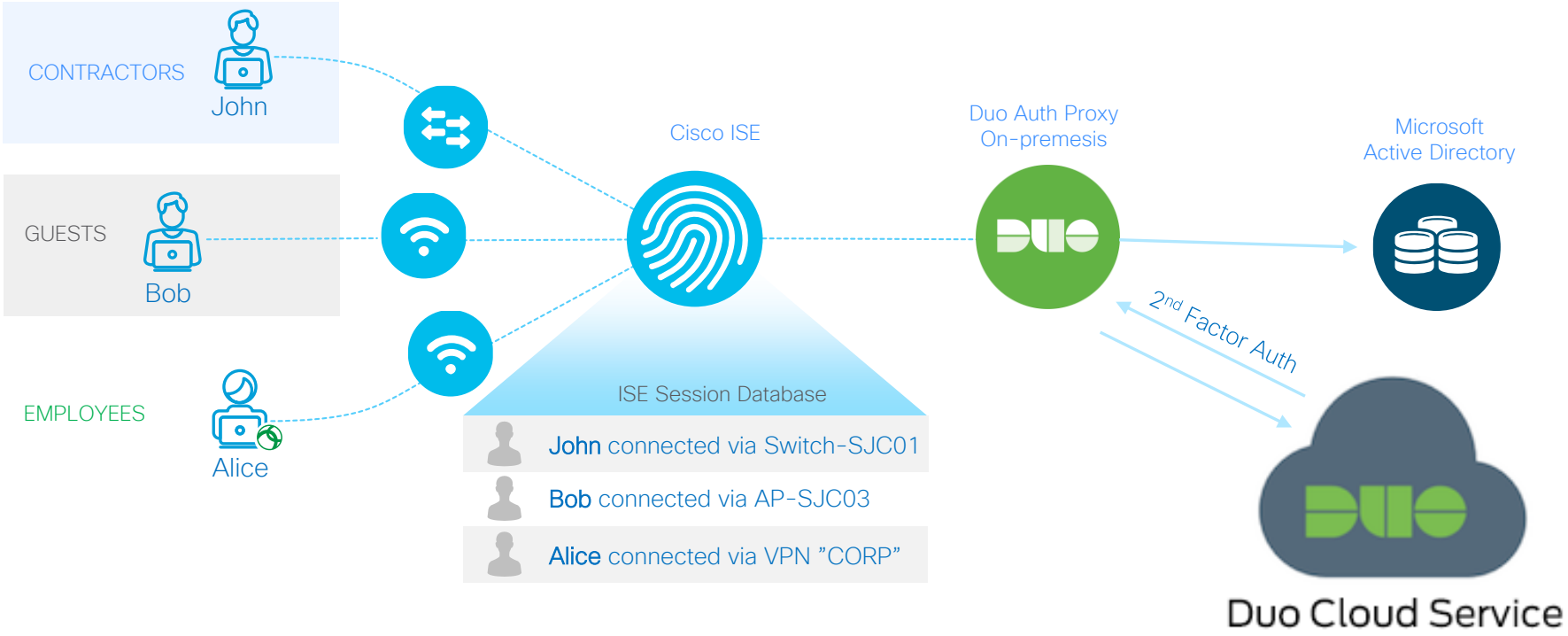
No Policy enforcement

https://kb.tetr.at/articles/ise-integration/

Supported in ISE 2.4+ and Tetration 3.3

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE and Duo Integration for MFA (VPN)



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Workplace Zero Trust: The need for Automation

- “Wired 802.1X and Segmentation is DIFFICULT”
- “My network is flat; campus segmentation is unmanageable and static but my business is dynamic”
- Options:
  1. Use Automation
  2. Start with Wireless

One Cat9300 48 port switch
Best practices deployment
Manual # config lines: 1400+!!!

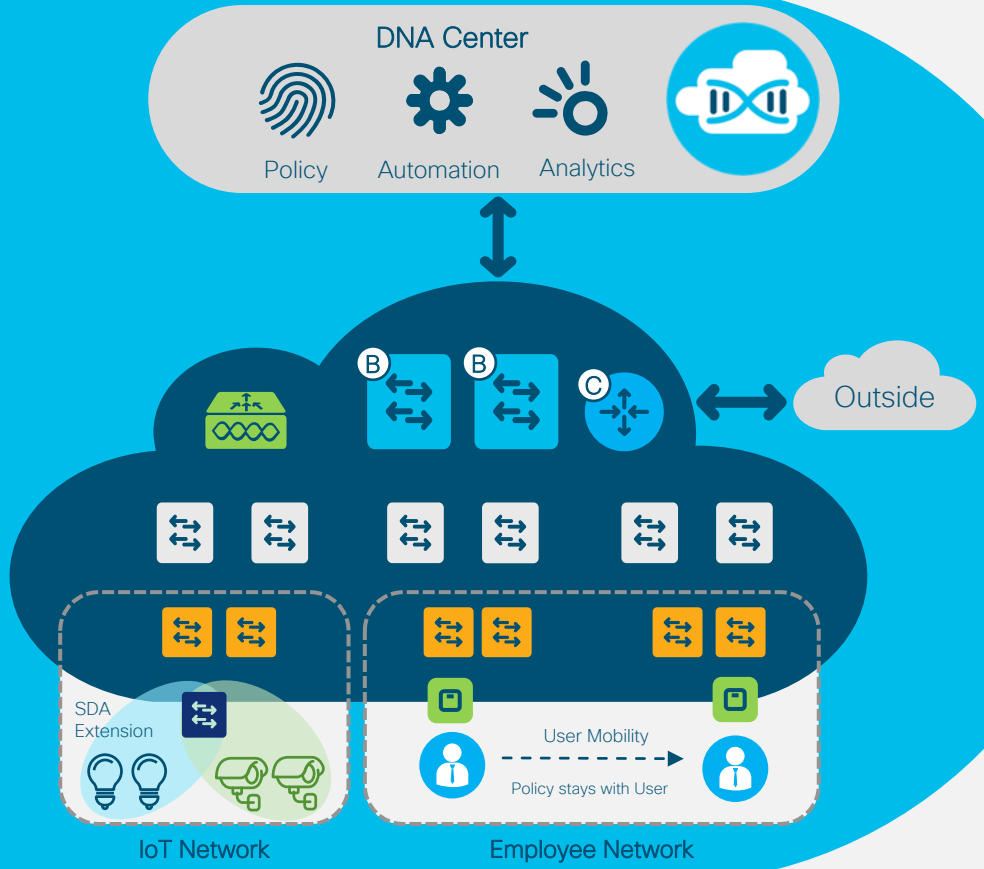
```
Current configuration : 47251 bytes
!
! Last configuration change at 18:30:12 edt Thu Aug 2 2018
! NVRAM config last updated at 18:53:21 edt Wed Aug 1 2018 b
!
version 16.6
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
 action b1020 cli command "conf t"
 action b1030 cli command "iox"
 action b1040 syslog msg "Enabled IOX.  Waiting 45 seconds for
 action b1050 wait 45
 action b1060 cli command "end"
 action c1010 cli command "guestshell enable"
 action z1010 syslog msg "IOX and GuestShell enabled."
 action z1020 syslog msg "Stop: 'enable-guestshell' EEM applet.
end
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco DNA & SD-Access

Networking at the Speed of Software!



Automated Network Fabric

Single Fabric for Wired & Wireless with simple Automation

Identity-Based Policy & Segmentation

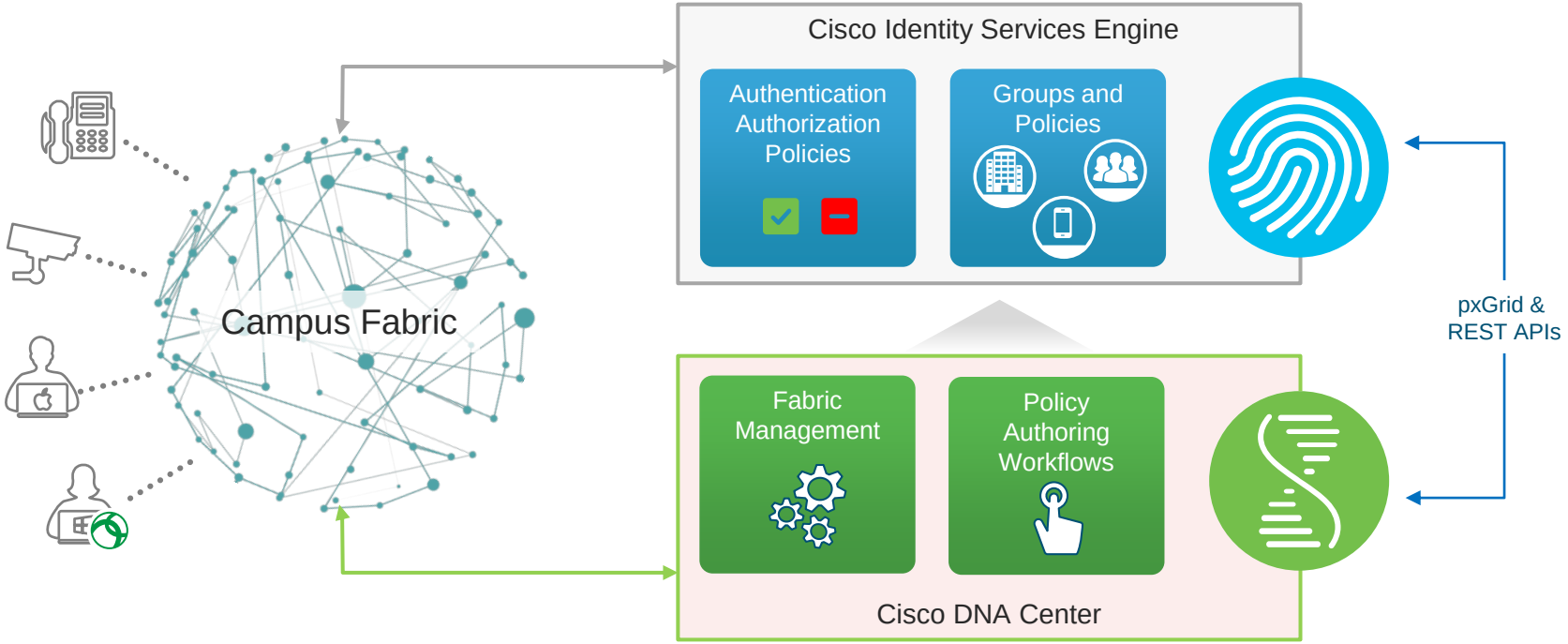
Decouples Security & QoS from VLAN and IP Address

Insights & Telemetry

Analytics and Insights into User and Application behavior

ISE and DNA-C Integration

Policy Automation and better usability



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

DNAC: Making ZT practical in the workplace

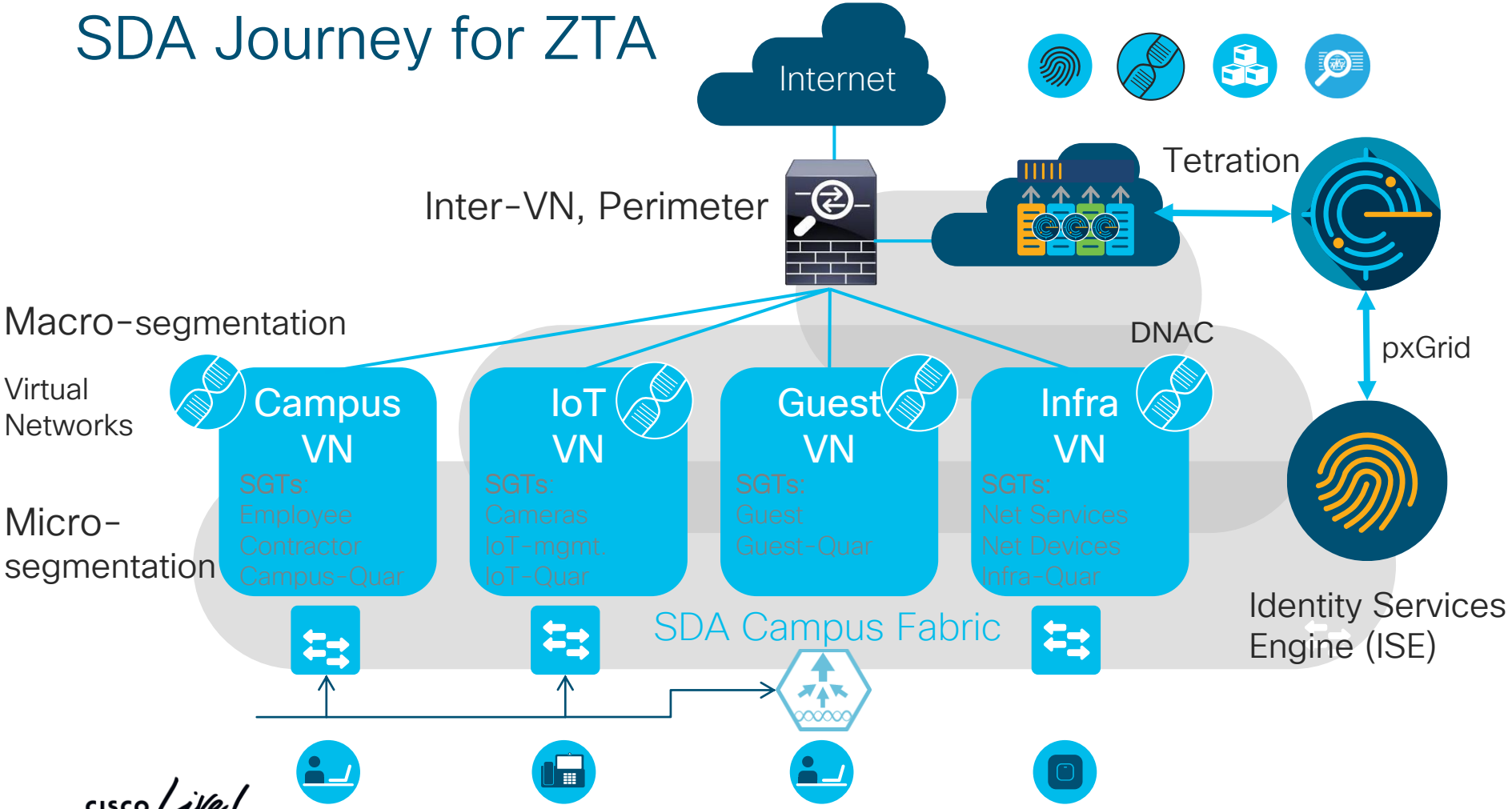
- Automated, best practice grounded, deployment of Zero Trust capabilities.

Simple SDA Fabric creation:
VLANs, VXLANs, lisp, routing, BGP, ECMP, VRFs

Easy setup of access control capabilities:
- 802.1x configuration
- ISE integration and policies
- SGT TrustSec
- Switch device sensor
- Profiling configuration
- AAA and device administration

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SDA Journey for ZTA



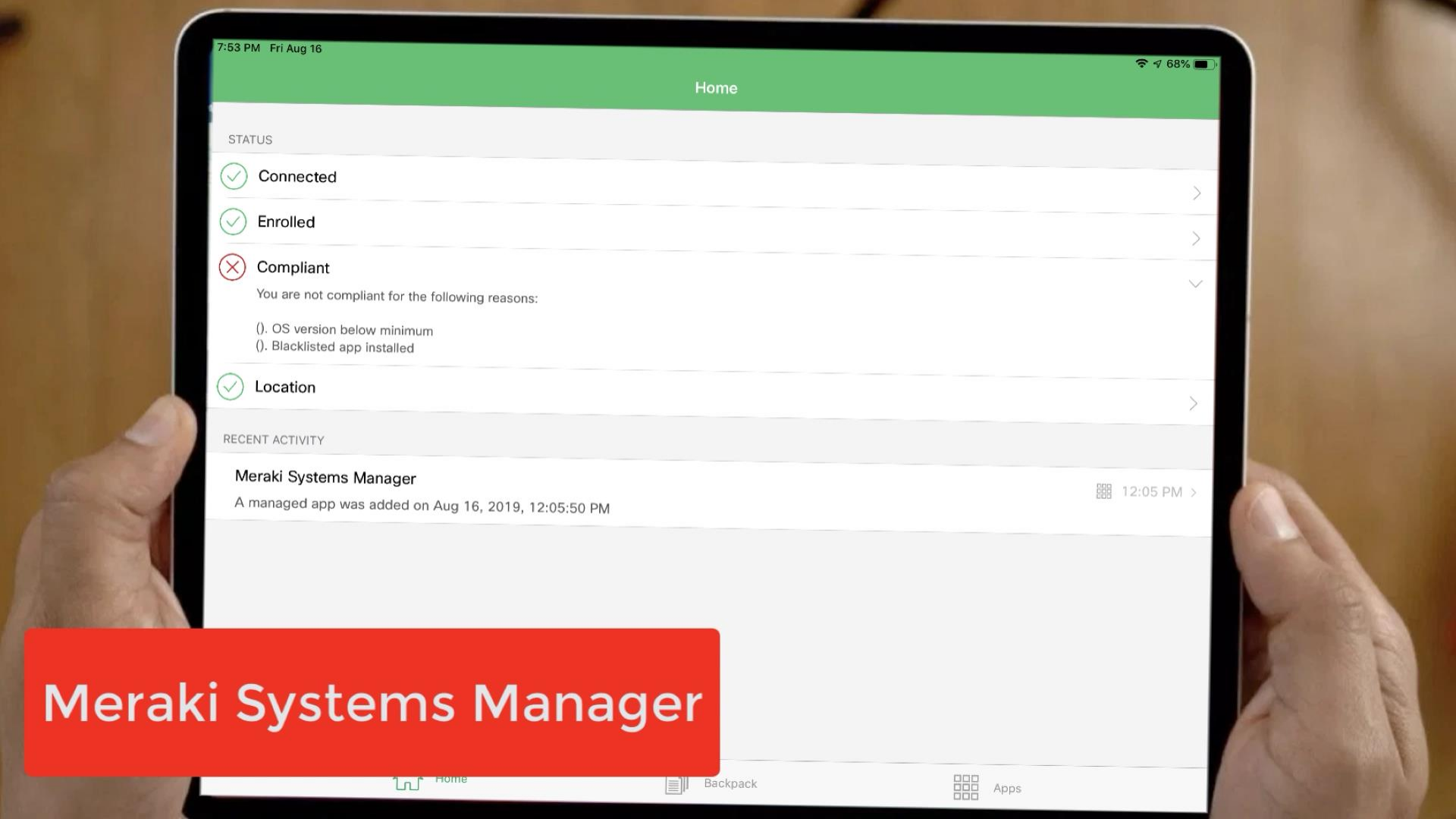
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo: Workplace – SDA for Wired, wireless

What's the problem?	How Cisco helps:
What is, and has been, on my network?	SDA, ISE, DNAC, AAA, Profiling, Context visibility
How do I establish trust for users and things	Threat-Centric NAC, MDM for posture
I need to easily apply group-based access control to every user and device on my network	Network Analytics and Contextual Group-Based Policy

Log and audit everything

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public


7:53 PM Fri Aug 16
68%
Home
STATUS
Connected
Enrolled
Compliant
You are not compliant for the following reasons:
(). OS version below minimum
(). Blacklisted app installed
Location
RECENT ACTIVITY
Meraki Systems Manager
A managed app was added on Aug 16, 2019, 12:05:50 PM
12:05 PM
Home
Backpack
Apps
Meraki Systems Manager

Let’s recap…

- Workspace: SD-Access – Retail payment on iPad and printer
  - ISE integrated Meraki so it was able to quarantine non-compliant iPad
  - ISE profiled and categorized every device, like the receipt printer
  - Stealthwatch with new DNAC policy analytics tool for SGT policy

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

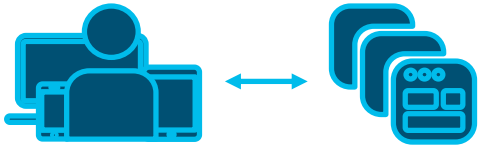
Conclusion

Cisco Zero Trust Architecture

Protecting the most critical areas

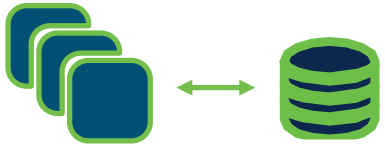
Duo for Workforce

Establish trust level for users and their devices accessing applications and resources



Tetration for Workload

Restrict access to workloads based on risk, contextual policy and verified business need



SD-Access for Workplace

Establish least privilege access control for all users and devices, including IoT, accessing your networks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Start Your Zero-Trust Journey

Start with Duo to protect the workforce.
Sign up for a free trial

Protect workloads with Tetration.
Demo Tetration

Protect the workplace with SD-Access.
Learn about SD-Access

cisco.com/go/zero-trust

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

CISCO

You make **possible**