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

Cisco Zero Trust

Securing the Workforce

Mark Pretty, Technical Solutions Architect

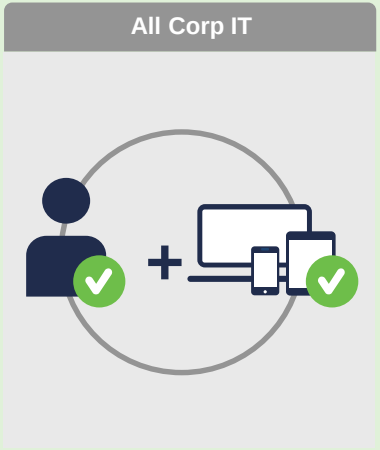
BRKSECv-2718

Virtual Event APJC • 1-2 April 2020

#CiscoLiveAPJC

The Cisco Zero Trust Journey

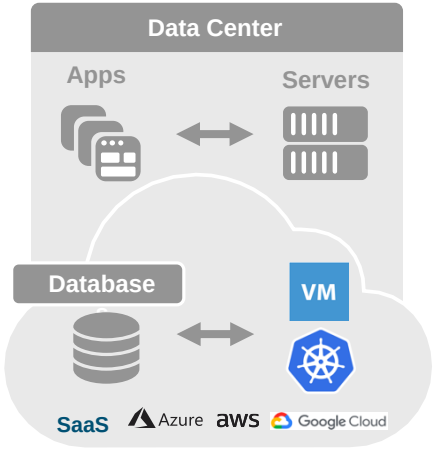
Secure the Workforce
With Duo



User & Device Access

Application Access

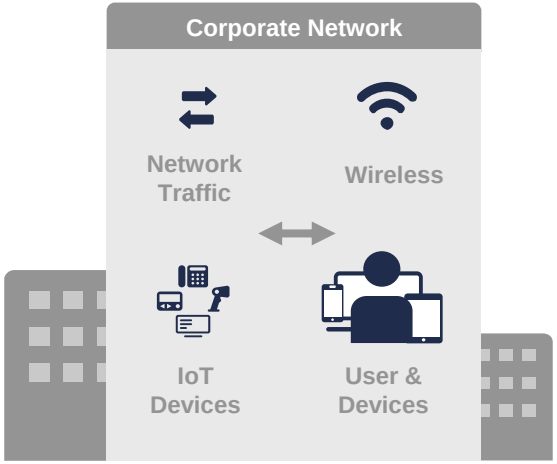
Secure Your Workloads
With Tetration



Workload Access

WAN Routing

Secure the Workplace
With Software-Defined Access



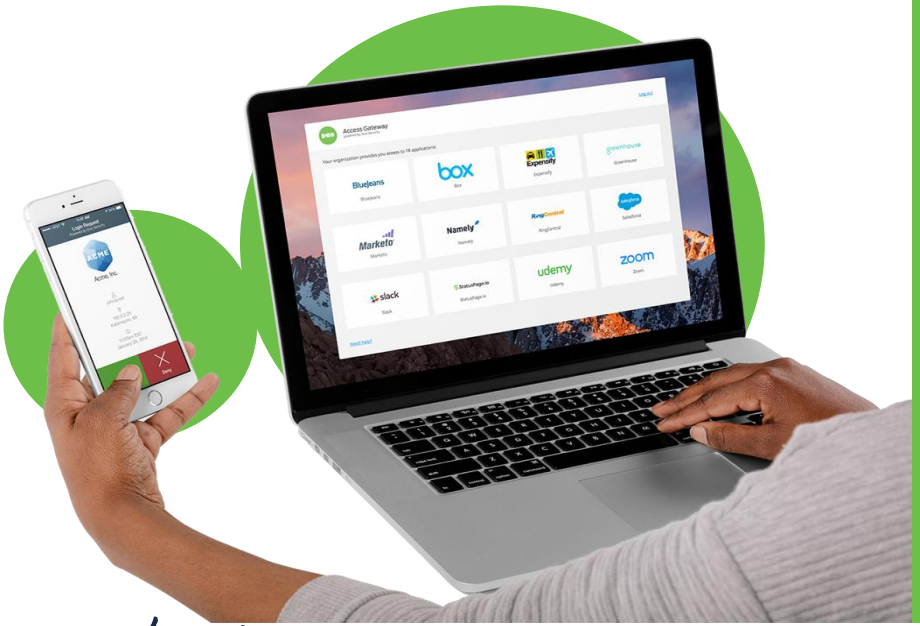
Network Access

MFA + Device Trust | Application Micro-Segmentation | Network Segmentation

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

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

Zero Trust for the Workforce



Pain Points

- Phishing
- Malware
- Credential Theft

Solution: Duo

With Duo Security, ensure only the right users and secure devices can access applications.

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

Workforce

Zero-Trust Security

Verify user & device trust with multi-factor authentication (MFA)

Enforce access policies for every app with adaptive & role-based access controls

Continuously monitor risky devices with endpoint health & management status

© 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

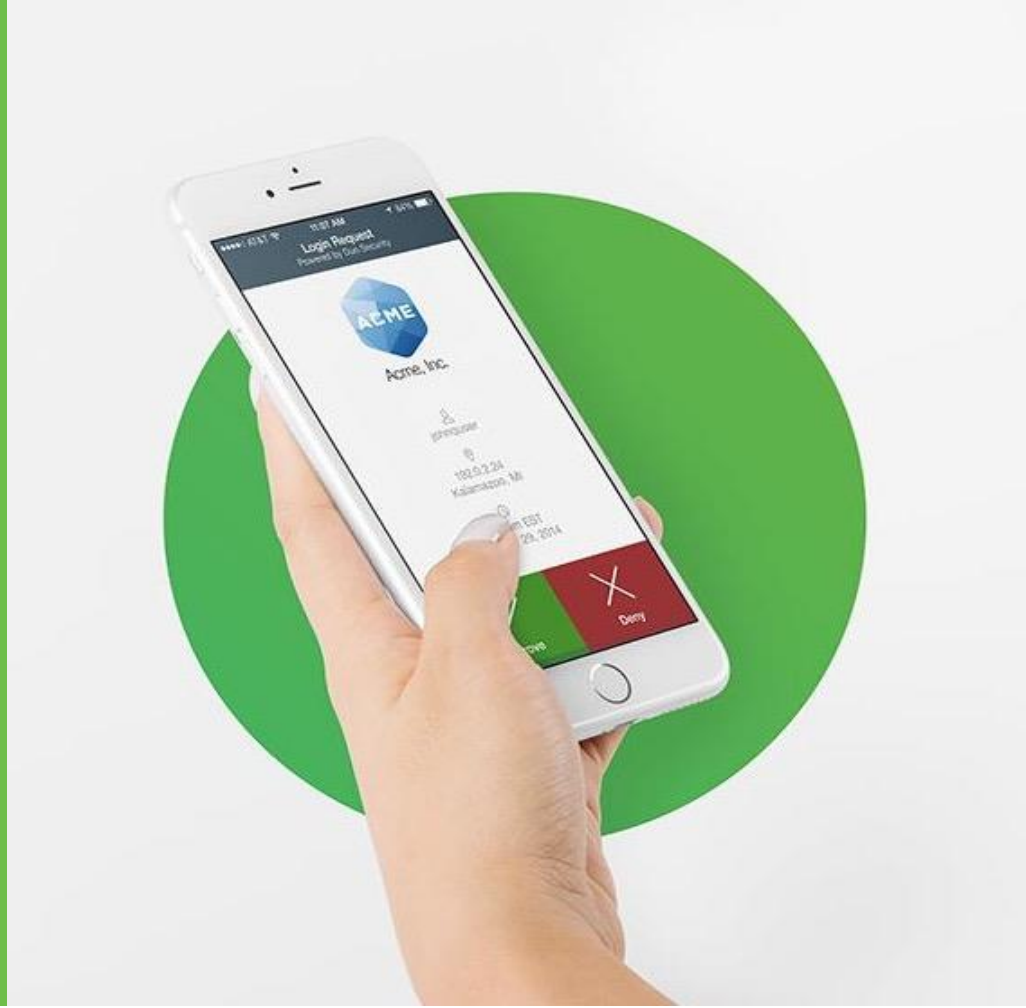
Verify User & Device Trust

Duo's Multi-Factor Authentication (MFA)

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

Device Trust

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



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

Multi-Factor Authentication (MFA)

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

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

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

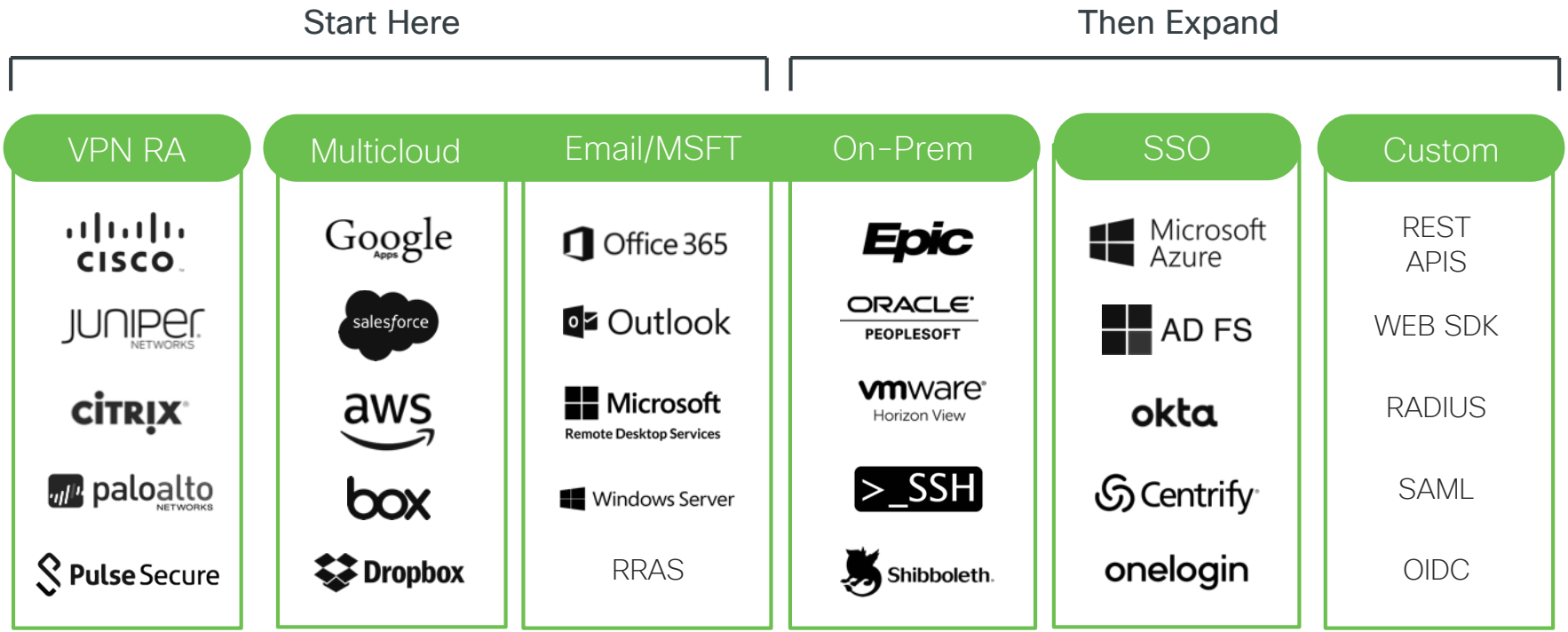
Import Users

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

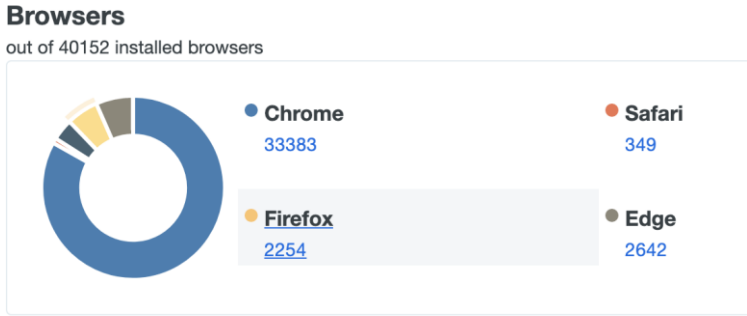
Protect Every Application – External and Internal



Learn more about application integrations

© 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?

Attackers exploit known vulnerabilities

Patching devices (especially user-owned) is complex

Accessing critical data from vulnerable devices can be risky

Compromised devices can

How Duo Establishes Device Trust

Device Insight

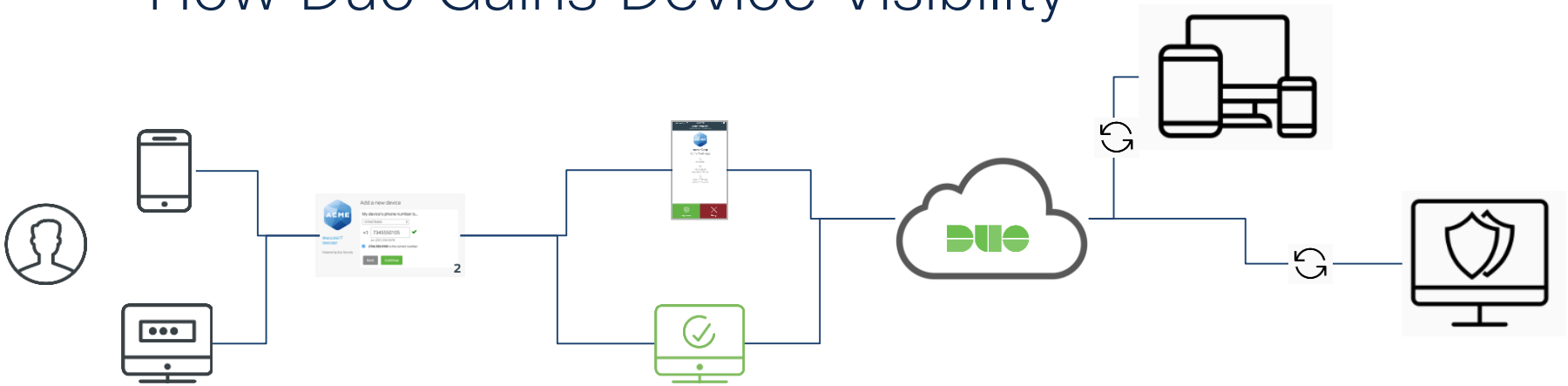
Duo's Unified Endpoint Visibility inspects users' devices at login -- without installing any endpoint agents.

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

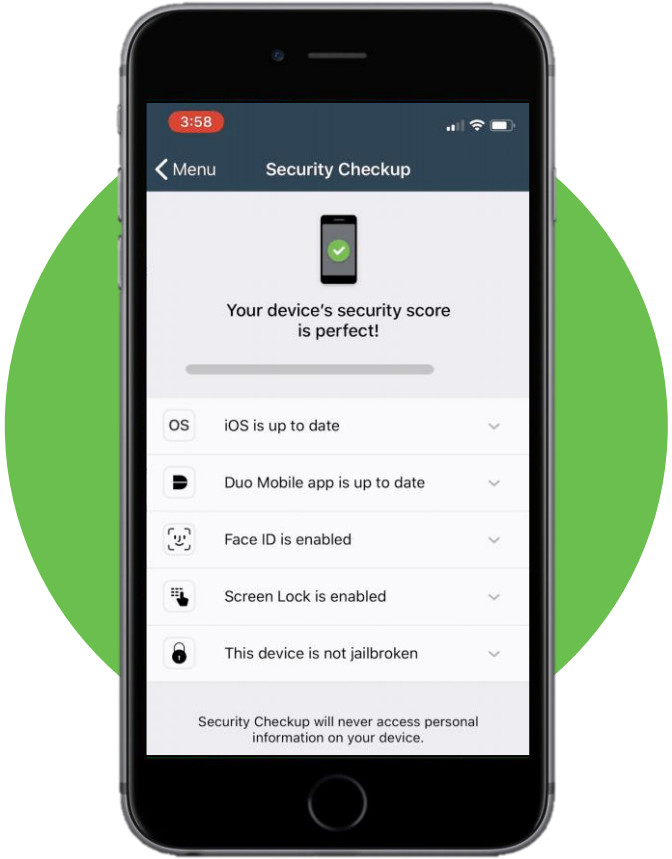


Visibility Source	Duo prompt in Web Browser	Duo mobile app Duo Device Health app	Device Manager (MDM/UEM)	EDR / EPP Agents+Services
Information Collected	Browser, OS, Plugins	Password, Disk Encryption, OS, Browser, (Mobile only: Jailbroken) (Desktop only:Firewall)	Device mgmt. Status (Managed/BYO)	Compromises,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

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

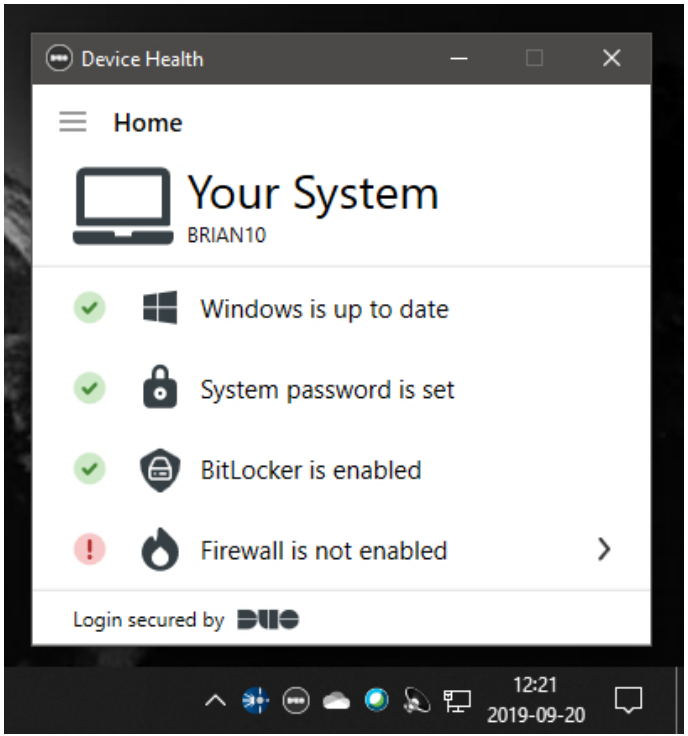
Assess Mobile Device Posture without MDM

- 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



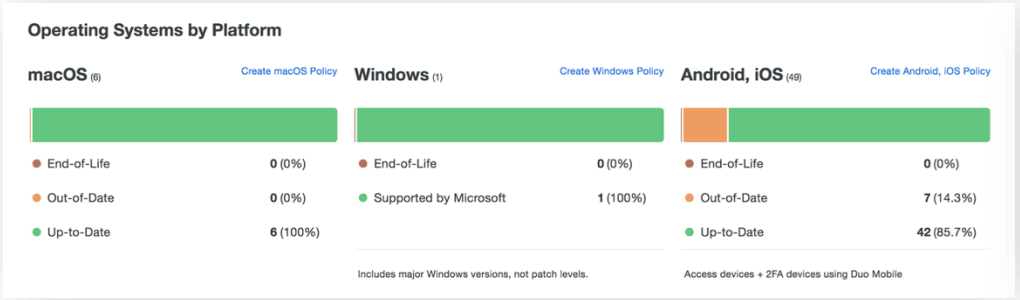
Duo Device Health Application:

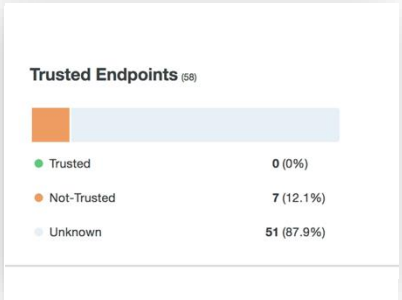
- New functionality
- Laptop / desktop security health
- Check devices before they login
- Corporate managed and BYO devices
- Supports web-based applications
- Windows 10 and macOS
- Launches On-Demand
- Inspects for third party AV clients including AMP for endpoints*

*Public beta

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

Unified Device Visibility





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 Adaptive 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

Require devices that access applications to be:

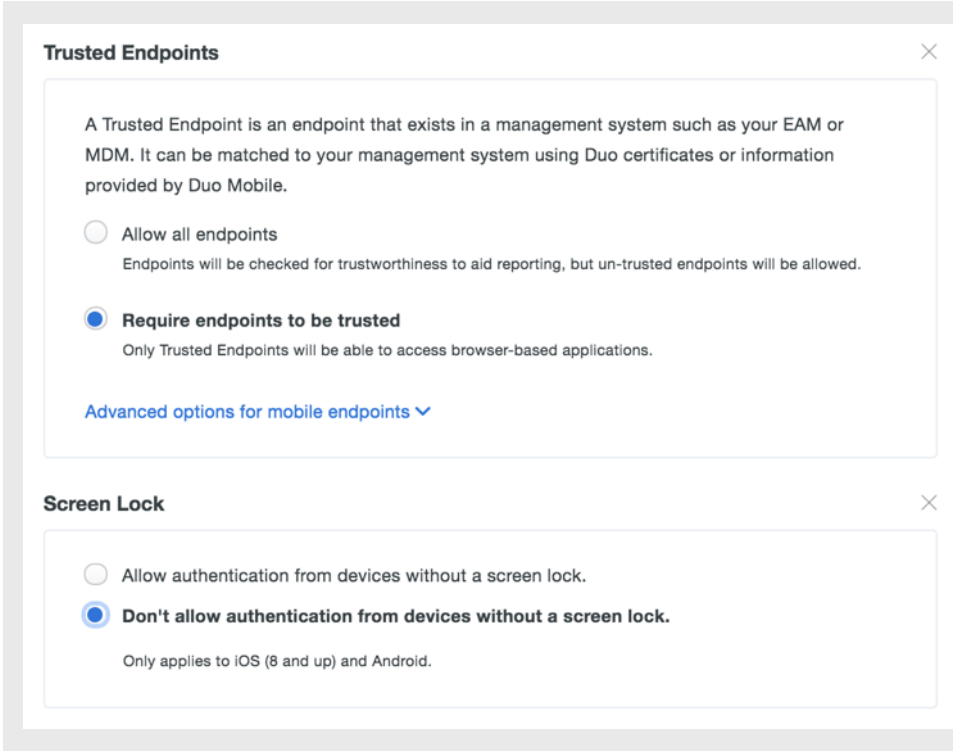
- Corporate-owned
- Up-to-date OS, browsers, Flash/Java

Require mobile devices to have:

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

Remembered devices

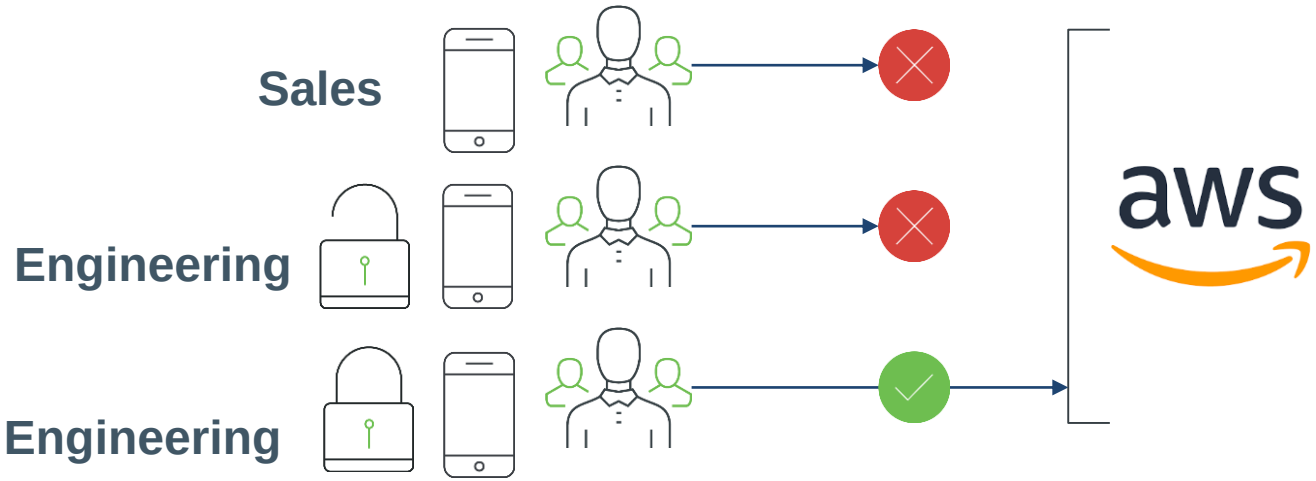
- Allow trusted and known devices to automatically authenticate



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

Role/Trusted Endpoint Policy Example

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

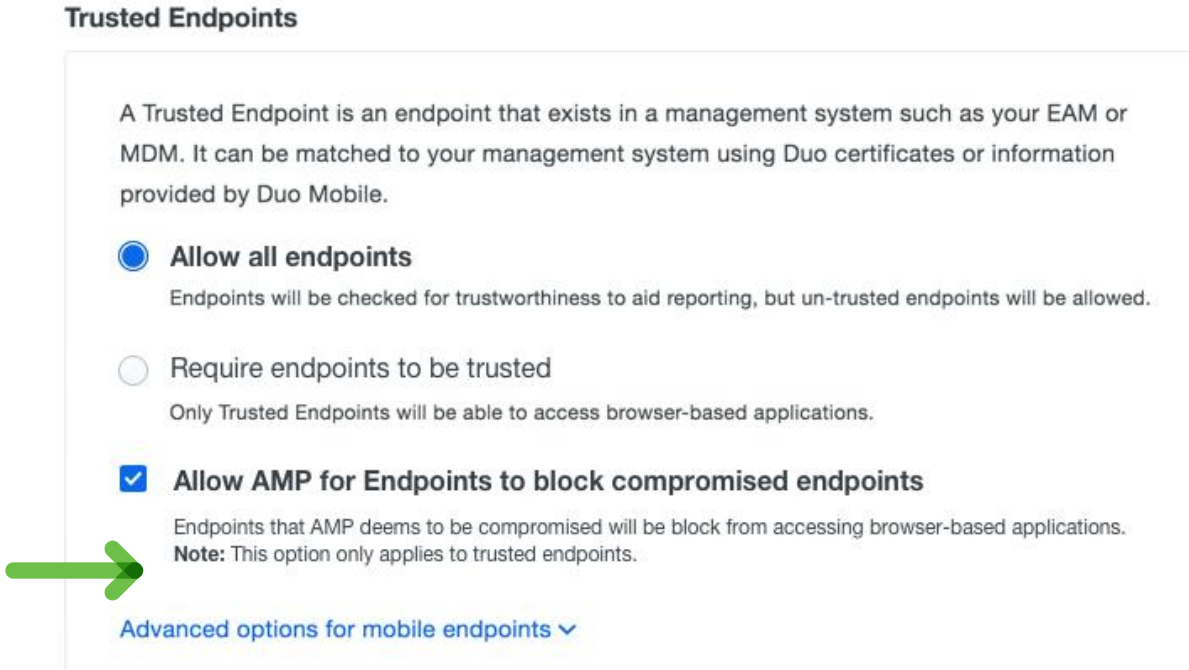


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detect Device Malware & Respond

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

Prevent compromised devices from accessing Duo-protected applications.



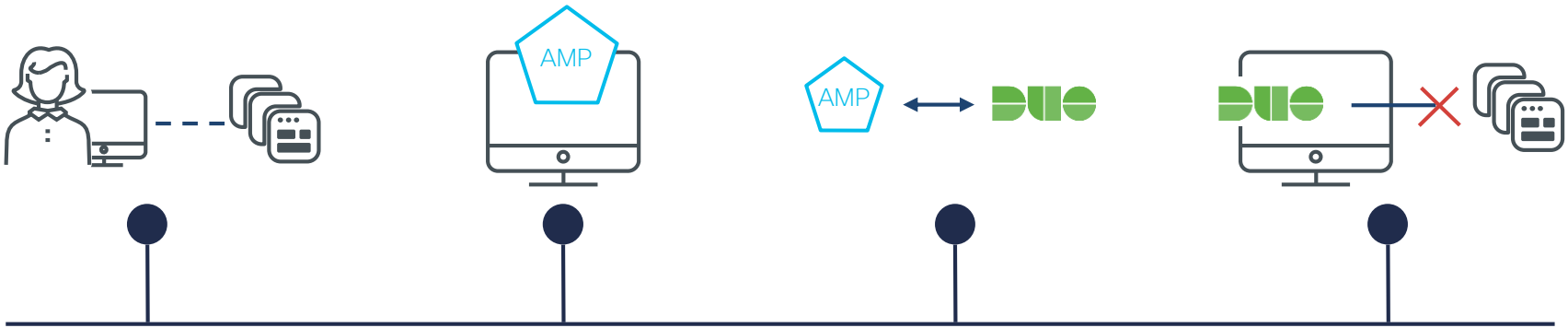
*Currently available to select customers for private beta

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

Detect Device Malware & Respond

How It Works:

Block malicious devices from accessing applications with Duo and AMP.



Users use their devices to access application.

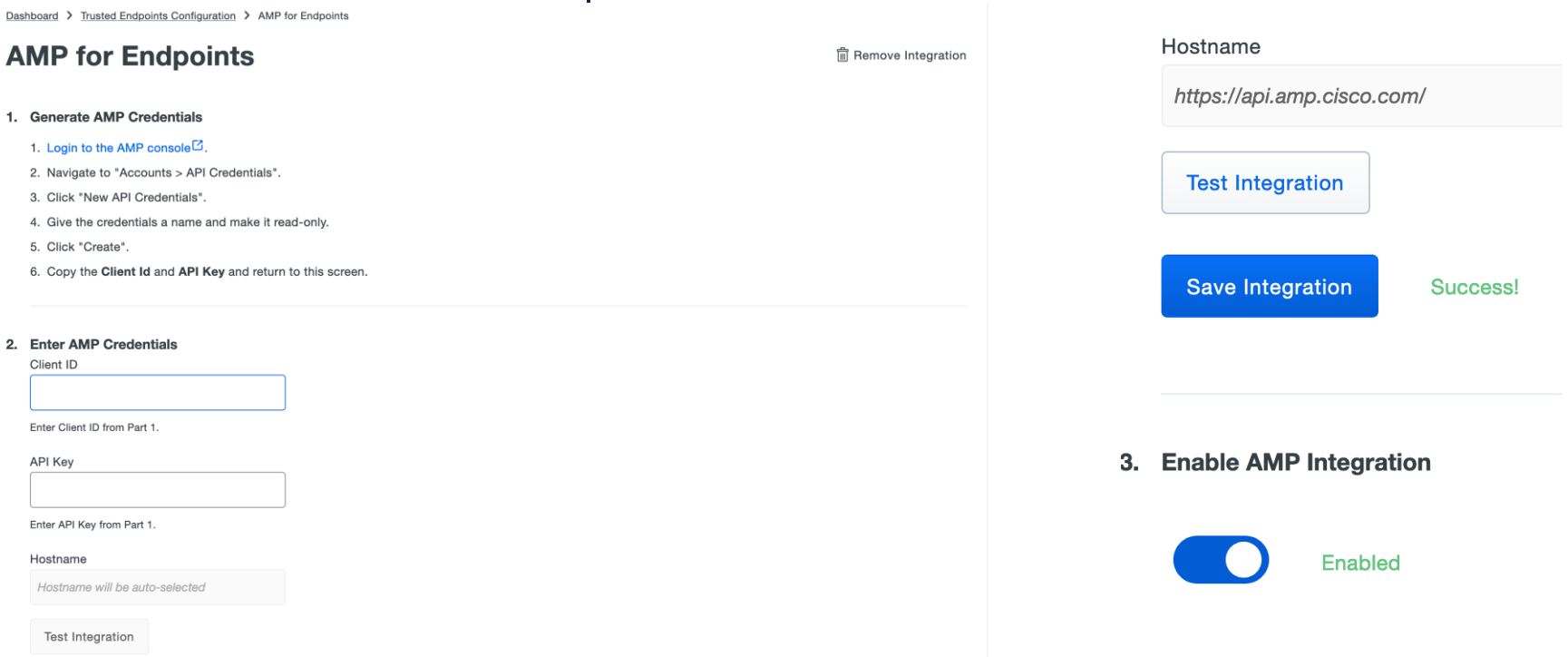
Cisco AMP running on the device detected malware.

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



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

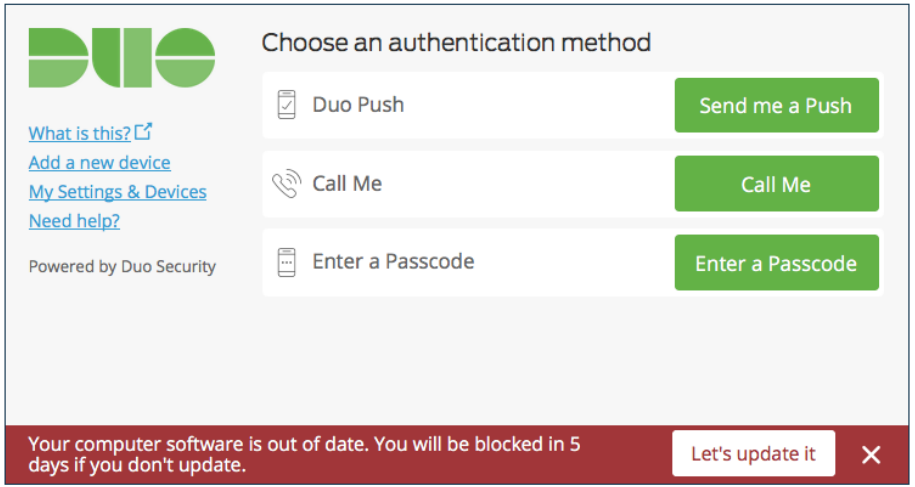
Inform Users

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

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

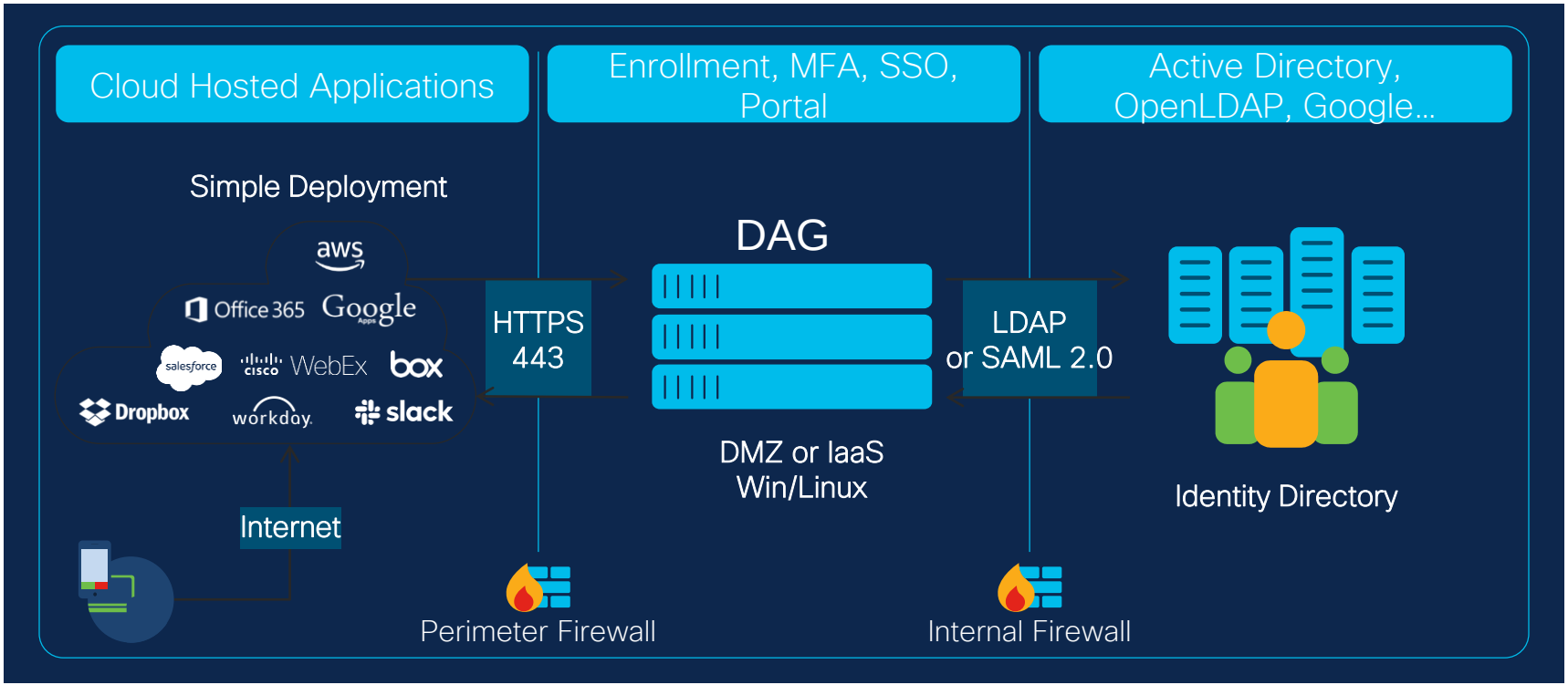
End users get notified about out-of-date OS, browsers, Flash and Java.

Quickly improve security without support desk help



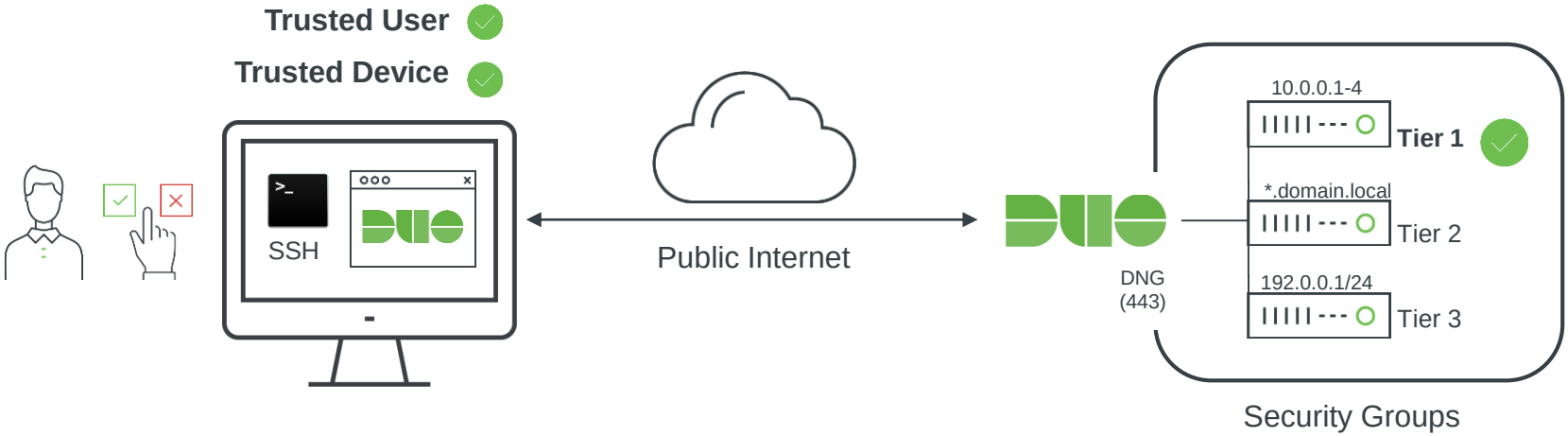
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Easily Secure Cloud Application Access



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

Duo Network Gateway



© 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

Demo

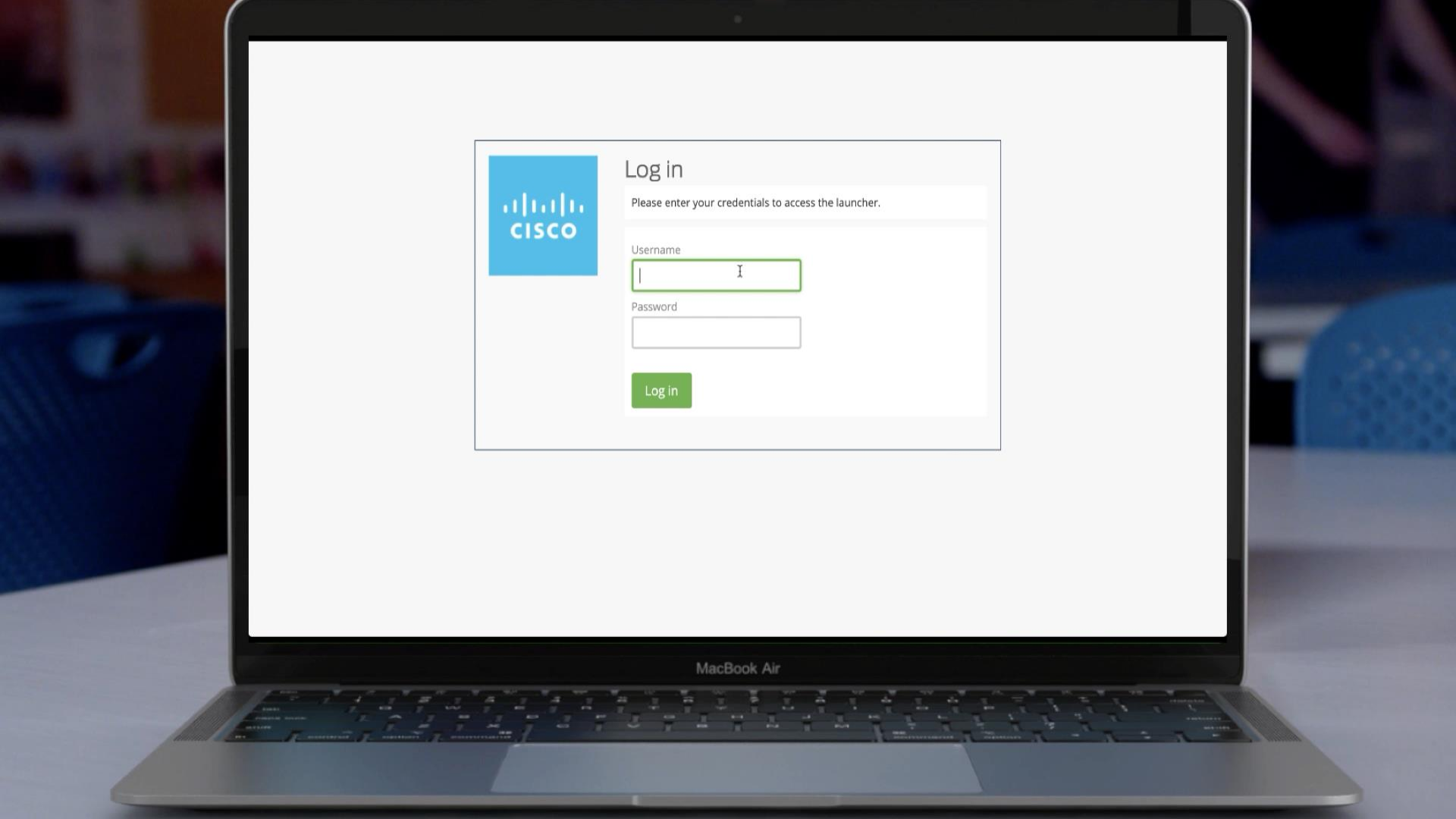
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

You make **possible**

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


CISCO