
cisco
You make possible

Build with Duo

Zero Trust for your Workforce

Leya Leydiker, Product Manager, Technology Partnerships
Ruoting Sun, Head of Technology Partnerships and Commercial Expansion

DEVNET-2088

cisco Live!
Barcelona | January 27-31, 2020

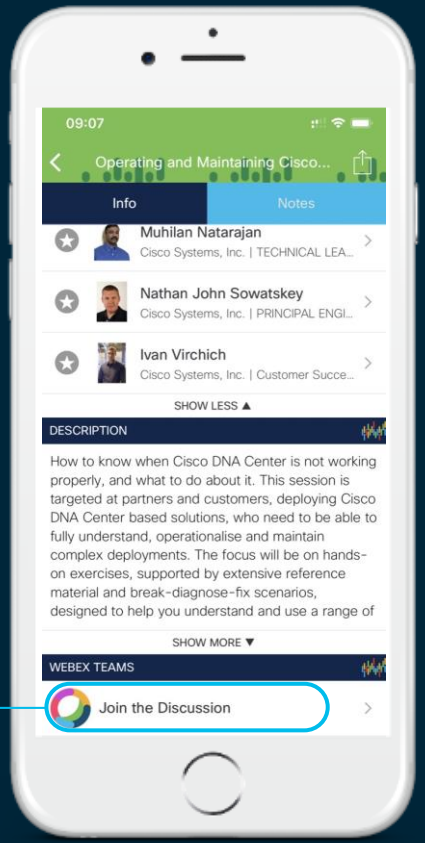
Cisco Webex Teams

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

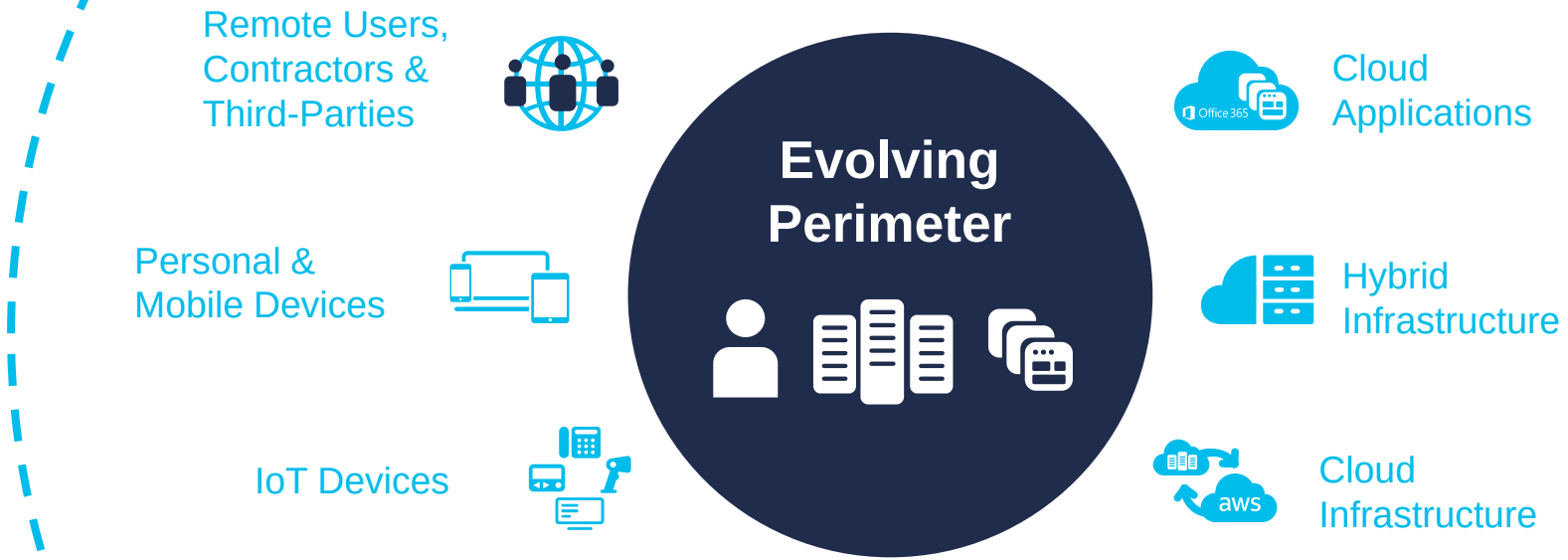


Agenda

- Cisco Approach to Zero Trust with Duo
- The reasons to integrate with Duo
- Who Can Build with Duo
- Benefits of Building with Duo
- Developer Resources

Shift in IT Landscape

Users, devices and apps are everywhere



Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity

81% of breaches involved compromised credentials

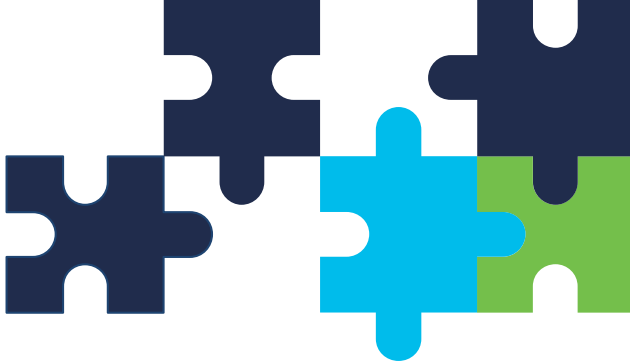
Targeting Apps

54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in IoT malware variants

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: Never implicitly trust, always verify

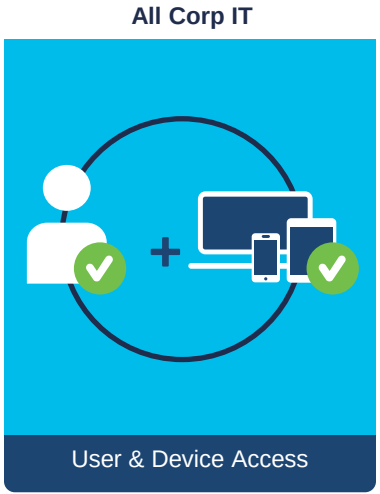
Trust is established for **every access request**, regardless of where the request is coming from. → **Secures access** across your applications and network. Ensures only right users & devices have access. **Extends trust** to support a modern enterprise with BYOD, cloud apps, hybrid environments & more.

Zero Trust
The Cisco Approach

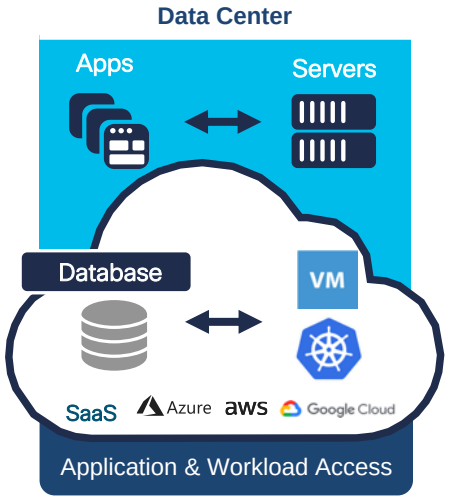
Securing Access

Access happens everywhere – how do you get visibility & ensure secure access?

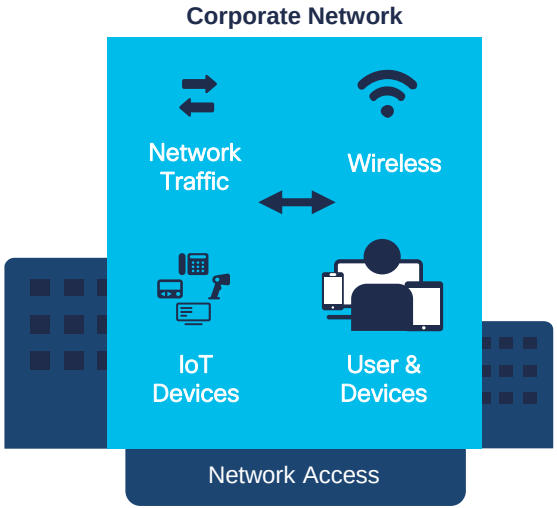
Workforce



Workload



Workplace

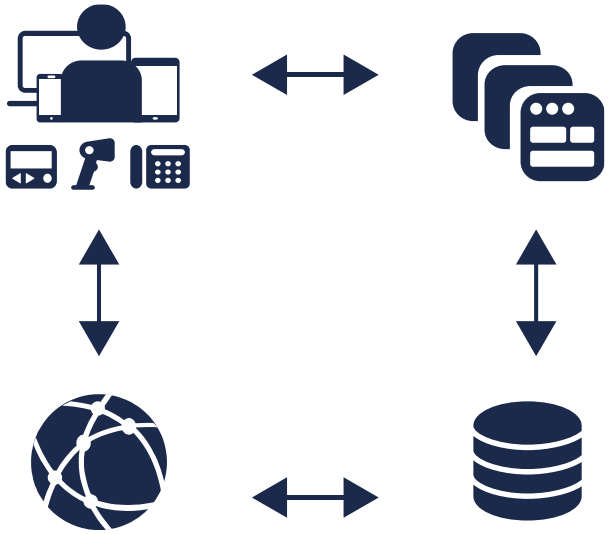


Cisco Zero Trust

Secure access for your workforce, workloads and workplace.

Duo for Workforce

Ensure only the right users and secure devices can access applications.



SD-Access for Workplace

Secure all user and device connections across your network, including IoT.

Tetration for Workload

Secure all connections within your apps, across multi-cloud.

Enforce Policy-Based Controls

Workforce

Zero-Trust Security

Establish Trust

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

Enforce Trust-Based Access

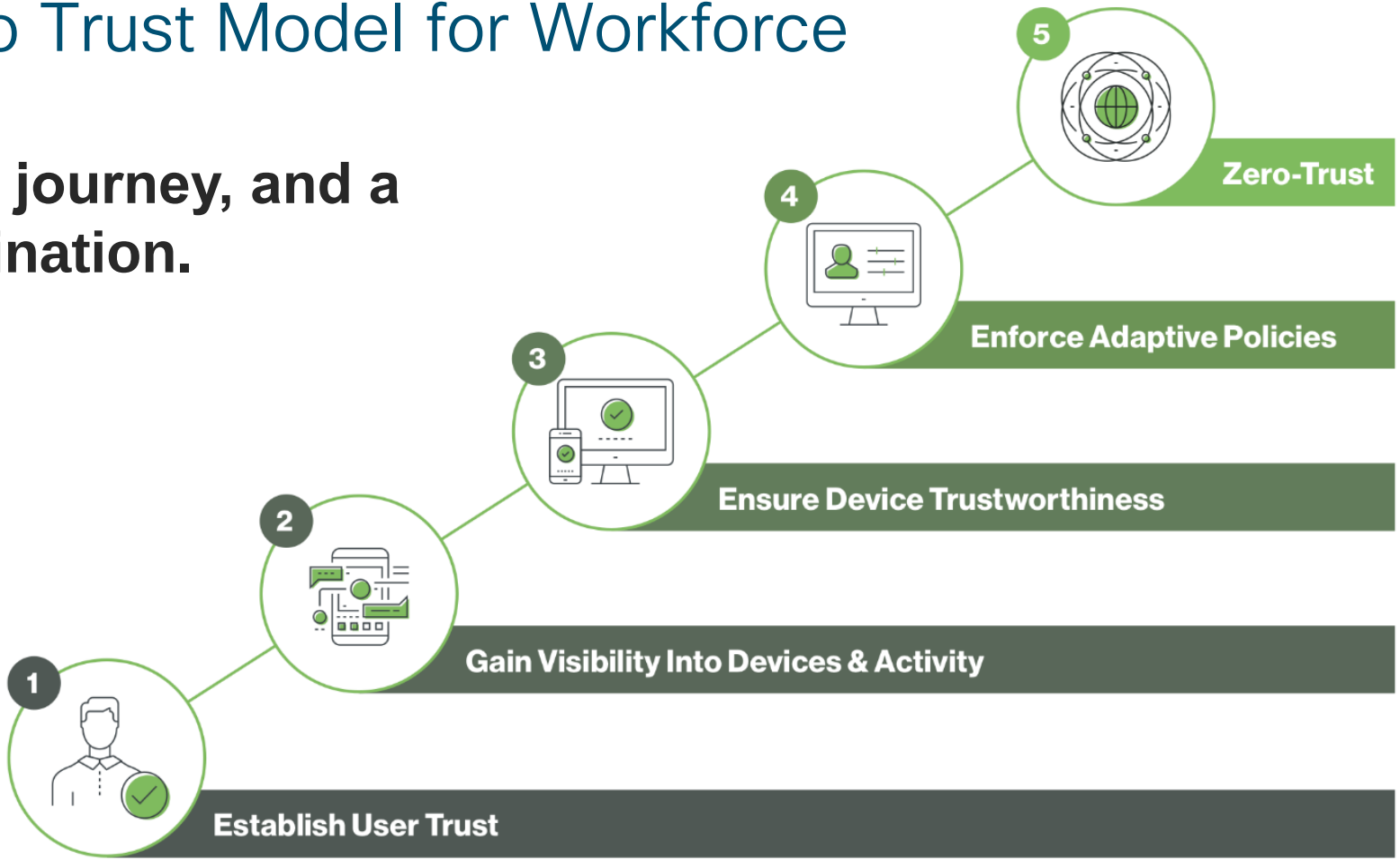
Enforce access policies for every app with adaptive & role-based access controls

Continuously Verify Trust

Continuously monitor risky devices with endpoint health & management status

Zero Trust Model for Workforce

It's a journey, and a destination.



The reasons to integrate with Duo

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.

Broad 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 user and flexibility
- Push notification
- Mobile passcode
- Phone
- SMS
- HOTP token
- U2F/WebAuthn

Ease of 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

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

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.

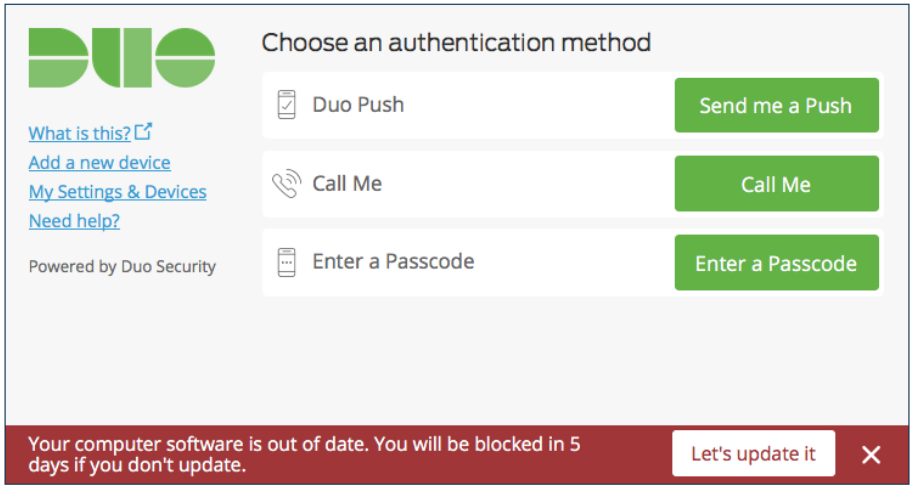
Inform Users

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.

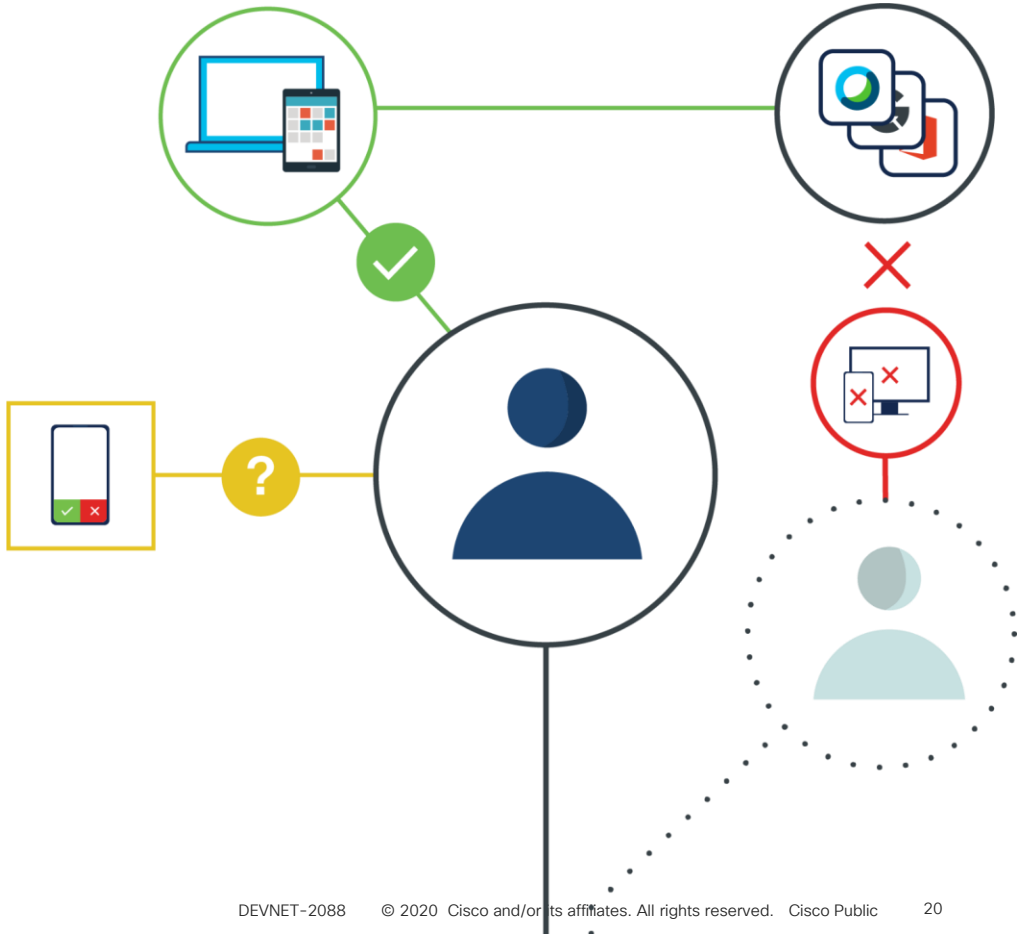
Quickly improve security without support desk help



Enforce Adaptive Policies

How Adaptive Access Policies Should Work

- Role Based
- Device Based
- Location Based
- Network Based

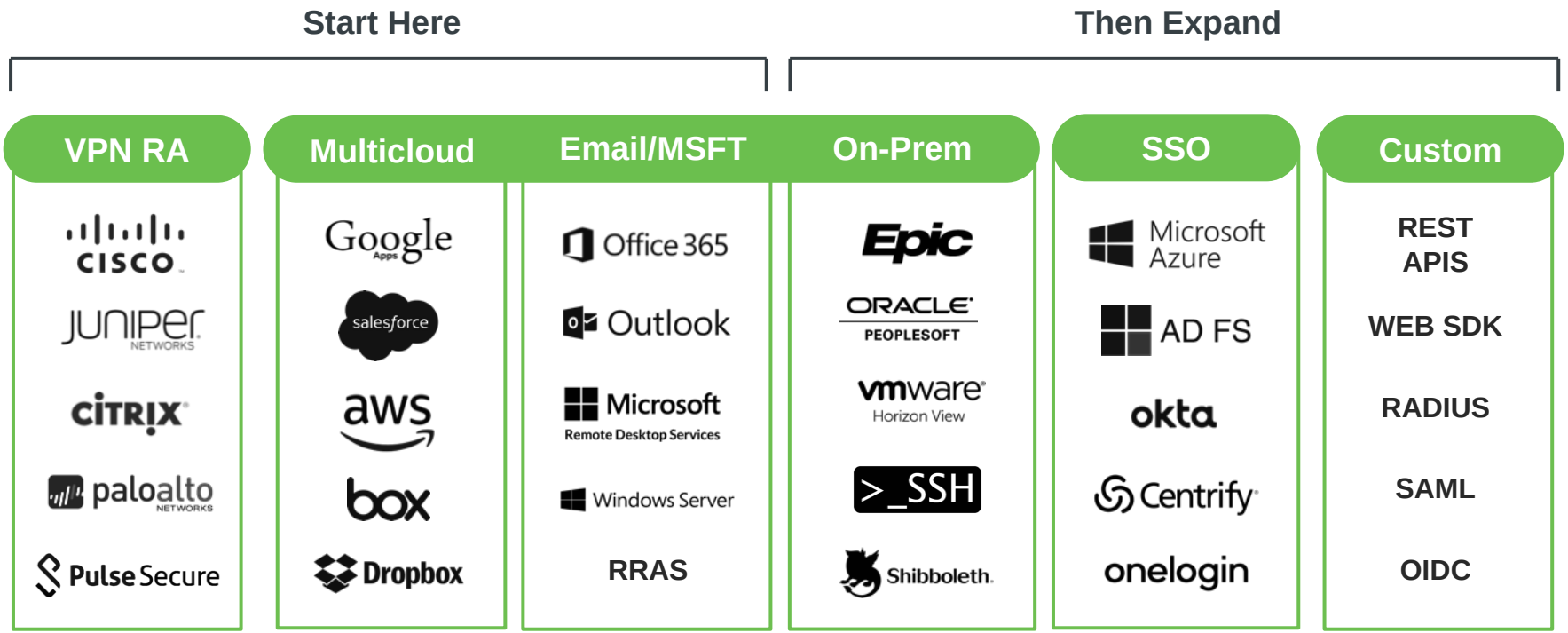


Simplify With Secure SSO

Pair single sign-on with user & device trust:

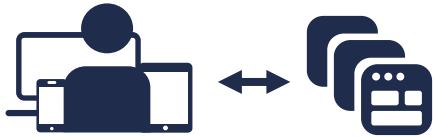
- Easily access all cloud applications from a single dashboard
- Enforce consistent security controls across cloud applications
- Secure every cloud application

Protect Every Application



Learn more about application integrations

Duo for
Workforce



Customer Story: University of Louisville Hospital

Challenge
- Protect against phishing attacks & block malicious attempts to access their applications
- Comply with HIPAA & PCI DSS

Solution
- Consolidated MFA, single sign-on (SSO) & mobile device management (MDM)
- Reduced their overall total cost of ownership by more than 50%

Business Outcomes
- Secure & convenient remote access for every user
- A zero-trust approach to workforce security, plus a single view into mobile devices & risk

UofL Hospital

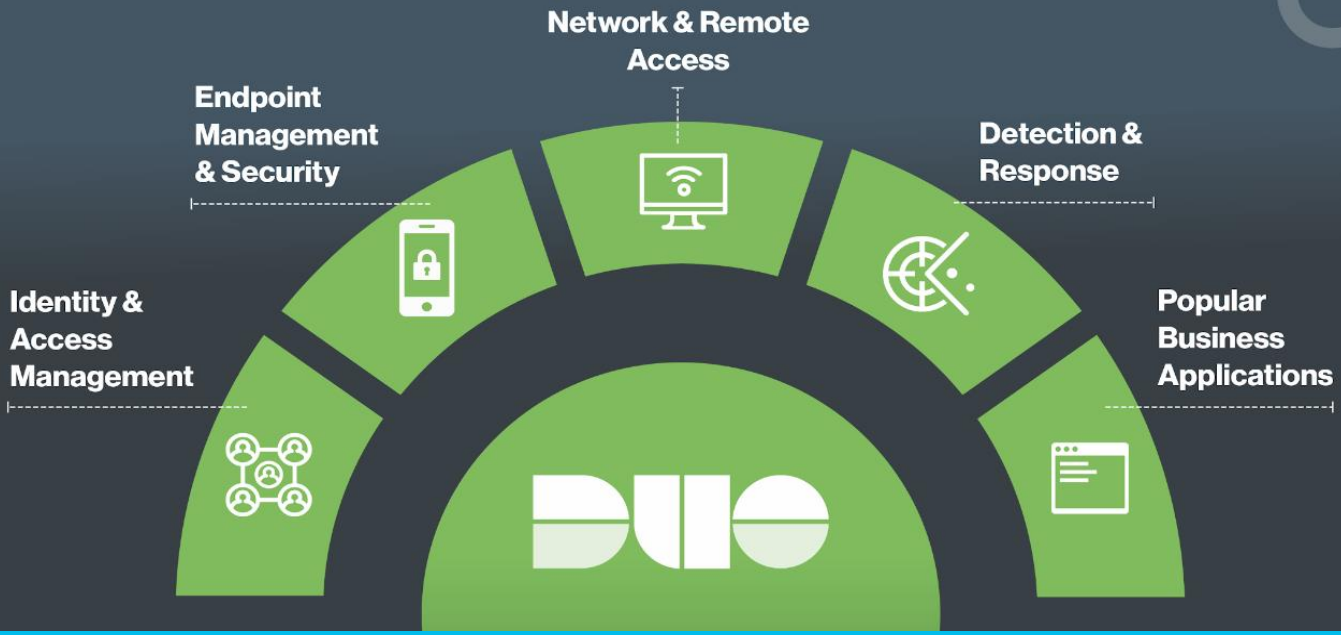
“We are adopting a zero-trust security framework, and we know we needed MFA to start with, and multiple clinician leaders recommended Duo. It was an easy choice for us. It was the first ever security solution recommended by the users and by clinicians. This never happens in healthcare.”

- John Zuziak, CISO

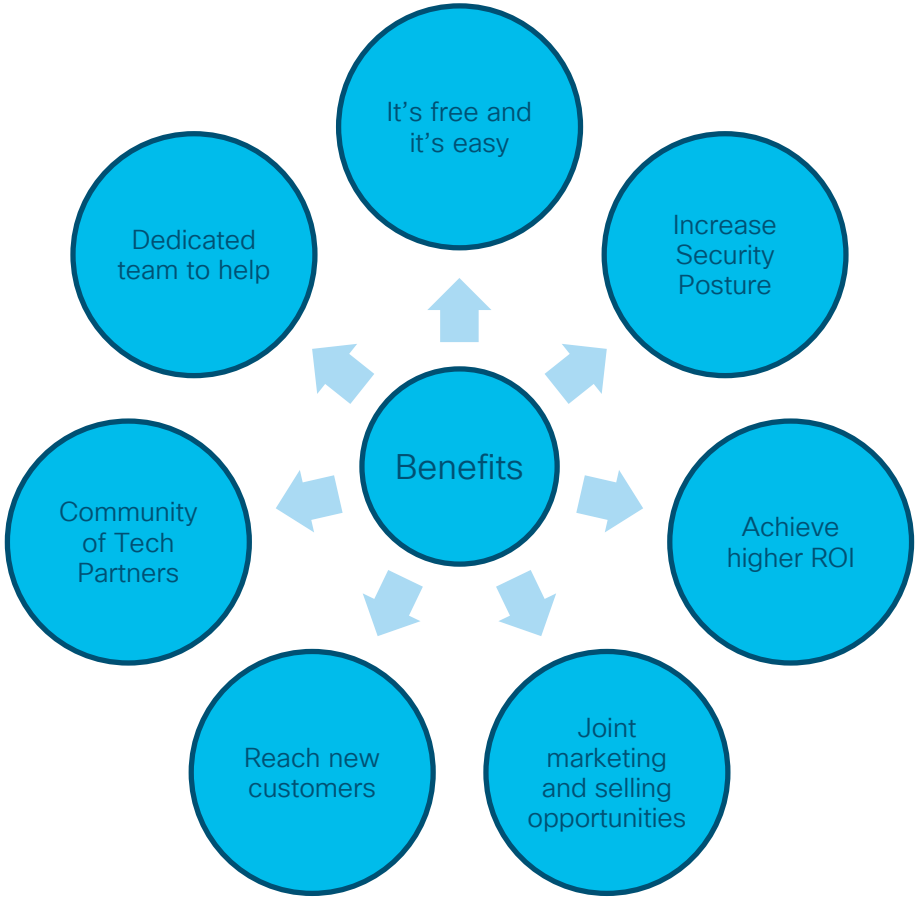
Learn more

Integration partners

Duo's Tech Partnership Ecosystem

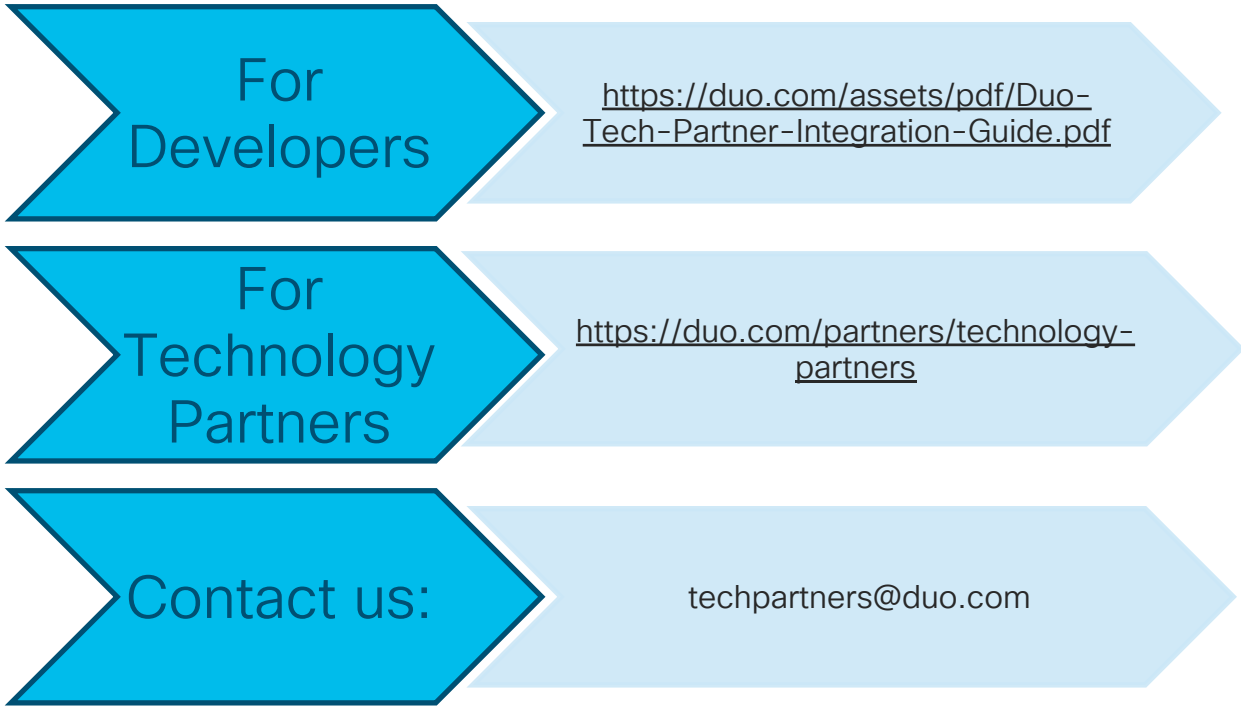


Benefits of partnering with Duo



Developer resources

Get Started



Learn More

Attend another Duo session..	Sign-up:
• Tuesday 28 January 16:40 – 17:00 – “Making Security Easier: Refine the Grind” presented by Ash Devata • Wednesday 29 January 14:00 – 14:30 – “Adopting a Zero Trust architecture with Cisco Zero Trust” presented by Amanda Rogerson & Jeff Groesbeck	• https://duo.com/trial

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.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**