



You make **possible**

CISCO *Live!*

Virtual Event APJC • 1-2 April 2020

#CiscoLiveAPJC

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



Zero Trust Architecture

A Practical Approach

Yazan Mughrabi

Technical Solutions Architect

CISCO *Live!*

Virtual Event APJC • 1-2 April 2020

#CiscoLiveAPJC

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

2



Agenda

- Why Zero Trust?
- What is Zero Trust?
- How to Zero Trust?

Why?



You make security **possible**

Shift in IT Landscape

Users, devices and apps are everywhere

Remote Users,
Contractors &
Third-Parties



Personal &
Mobile Devices



IoT Devices



Evolving
Perimeter



Cloud
Applications



Hybrid
Infrastructure



Cloud
Infrastructure

Business Challenges

Increased access, attack surface & gaps in visibility



How do we know users are who they say they are?



Are their devices secure & up to date?



What's on the network?
How does it connect?



What data's in the cloud?
Who/what accesses it?



How can we view & secure all connections?



What exists in the cloud?
How does it connect?

Threats Today, As a Result

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

Workforce



Targeting Identity

81% of breaches involved
compromised credentials

Workloads



Targeting Apps

54% of web app vulnerabilities
have a public exploit available

Workplace



Targeting Devices

300% increase in IoT malware
variants

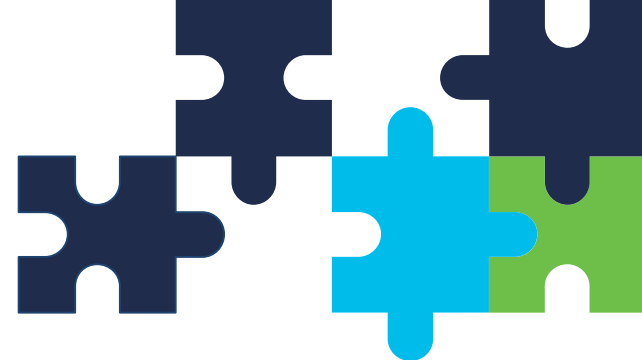
What?



You make security **possible**

The Zero-Trust Approach

Basic Tenet – Ubiquitous Least Privilege Access



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.

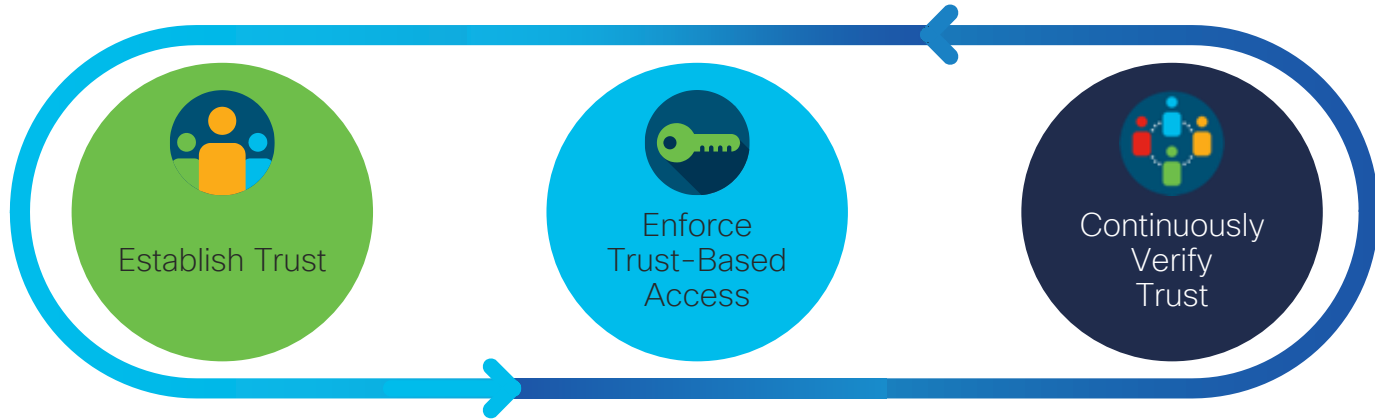
Extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environments & more.

How?



You make security **possible**

Cisco's implementation of Zero Trust



We establish trust by verifying:

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise

We enforce least privilege access to:

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins

We continuously verify:

- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

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

Zero Trust for the Workforce



Pain Points

- Phishing
- Malware
- Credential Theft

Primary Solution: Duo

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

Secondary Solutions: Umbrella & AMP

Umbrella & AMP keep roaming users safe & AMP also lets Duo adapt policy to infection

Workforce: Establish Trust

Verify User & Device Trust

Duo's Multi-Factor Authentication (MFA)

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

Device Trust

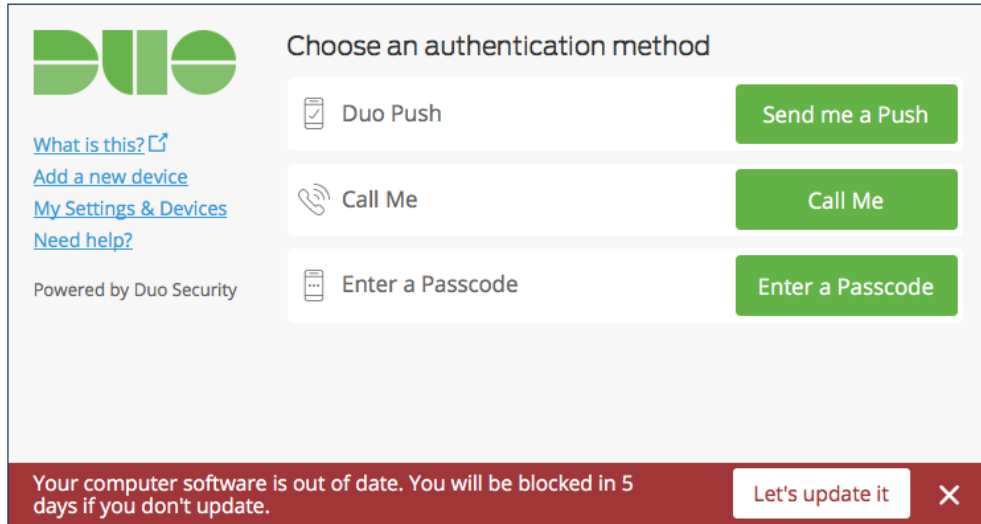
- Check devices for vulnerable software & security features
- Identify managed vs. unmanaged
- Notify users of out-of-date devices



Enforce Adaptive Policies

Duo's Policy Framework

- Create customizable security policies
- Enforce Global, App & Group Level controls
- Establish a level of trust based on users and devices



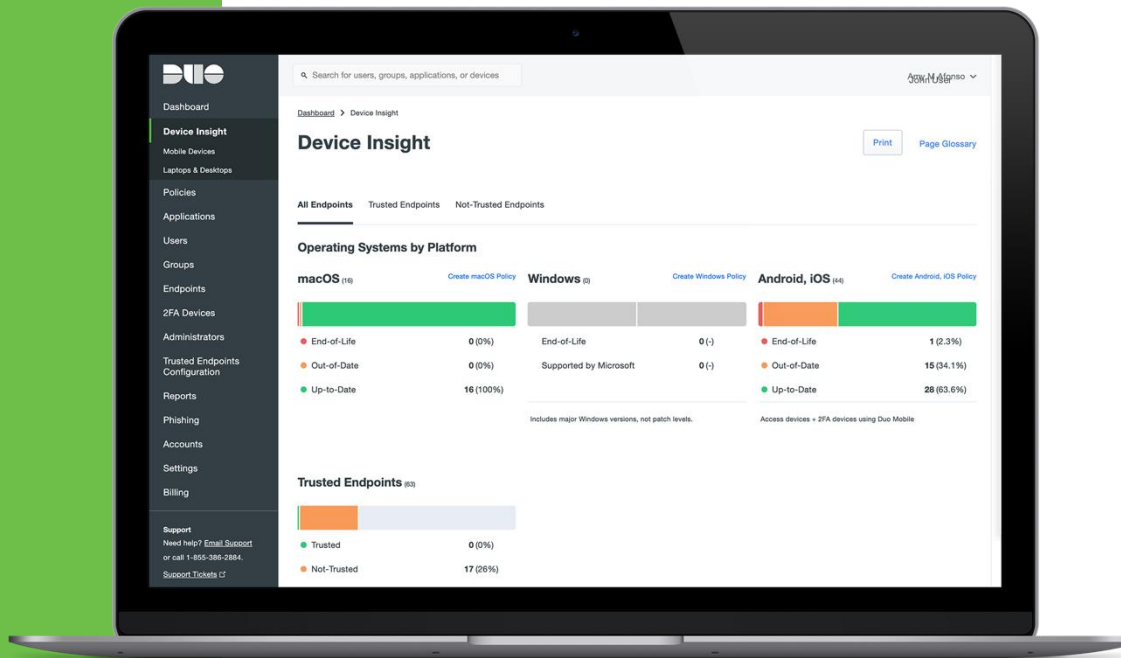
The screenshot displays the Duo authentication interface. At the top left is the Duo logo. Below it are links for "What is this?", "Add a new device", "My Settings & Devices", and "Need help?". The text "Powered by Duo Security" is located below the links. The main heading is "Choose an authentication method". There are three options, each with a corresponding button: "Duo Push" with a "Send me a Push" button, "Call Me" with a "Call Me" button, and "Enter a Passcode" with an "Enter a Passcode" button. At the bottom, a red banner contains a warning: "Your computer software is out of date. You will be blocked in 5 days if you don't update." with a "Let's update it" button and a close icon.

Workforce: Continuously Verify Trust

Monitor Risky Devices

Duo's Device Trust:

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





Zero Trust for Workloads

Problems Solved:

- Complete Application Visibility
- Contain Breaches
- Prevent Lateral Movement

Primary Solution: Tetration

With Tetration, secure all connections within your apps, across multi-cloud.

Secondary Solution: Stealthwatch Cloud

Monitor workloads, containers and serverless functions in public cloud and on-prem

Workload: Establish Trust

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: 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



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





Zero Trust for the Workplace

Problems Solved:

- Complete network visibility
- Prevent lateral movement
- Prevent unauthorized access

Primary Solution: SD- Access & ISE

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

Secondary Solutions: Stealthwatch & Umbrella

Monitor for anomalies and malicious behaviors and respond to incidents with SDA/ISE integrations

Network Visibility

SD-Access's identity context

Visibility into:

- Users and devices (IoT) on the network

Provide identity context for users & devices, including:

- Authentication
- Posture validation
- Device profiling



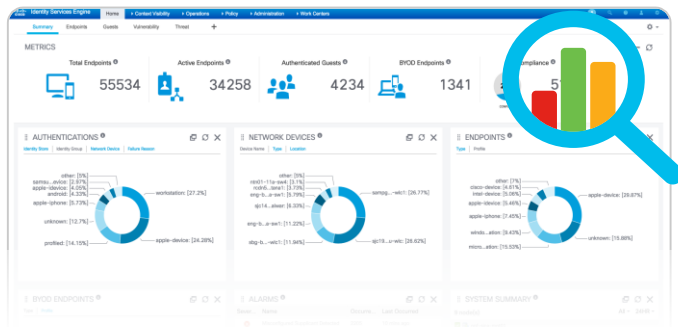
Network Segmentation: Policy

With ISE Segmentation policy enforced the way you actually intended through dynamic Group-Based Policy.	Segmentation Policy	Internet	ERM	Ordering	DevOps
	Visitor	Permit	Deny	Deny	Deny
	Human Resources	Permit	Permit	Deny	Deny
	Sales	Permit	Deny	Permit	Deny
	R&D	Permit	Deny	Deny	Permit

With Trust-Based Access, you can:

- Enforce network authorization policies based on device classification & access needs
- Enforce segmentation policy across wireless, wired and VPN connections
- Manage segmentation via ISE through policy manager
- Distribute policy dynamically to network devices
- Simplify segmentation with group-based policy

Continuous Monitoring & Response



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

Summary



You make security **possible**

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



Thank you





You make **possible**