Cisco Zero Trust
Secure access for the workforce, workloads and workplace

Andrej Jeleník – Cisco Systems Engineer

November 26th, 2019
Shift in IT Landscape

Users, devices and apps are everywhere

- Remote Users, Contractors & Third-Parties
- Personal & Mobile Devices
- IoT Devices
- Cloud Applications
- Hybrid Infrastructure
- Cloud Infrastructure

Evolving Perimeter
Excessive Trust

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

Workforce

Workload

Workplace

User & Device Access

Data Center

Corporate Network

Application & Workload Access

Network Access

Servers

SaaS

VM

Network Traffic

IoT Devices

User & Devices
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
Enabling Secure Access

Take a zero-trust approach to security to secure access across your entire IT environment.

**Prevent Risks**
Reduce risk of a breach before it happens

**Gain Visibility**
Identify risks and indicators of a breach of trust

**Reduce Attack Surface**
Contain breaches and stop attacker lateral movement

---

**The Zero Trust Approach**

Enable policy-based controls for every access request in a corporate environment

See who and what is accessing applications, workloads & the network

Segment your network & workloads by enforcing granular controls

---

© 2019 Cisco and/or its affiliates. All rights reserved.
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
Cisco Zero Trust
A zero-trust approach to securing access across your applications and environment, from any user, device and location.

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

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

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

Enforce Policy-Based Controls
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

Solution: Duo

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

Verify User & Device Trust

Workforce: Establish Trust
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.
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
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

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

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

Integrates to protect every application
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.

**Location-Based Policy**
Prevent authorized access to your applications from any geographic location.

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

**Network-Based Policy**
Grant or deny access based on a set of IP address ranges or from anonymous networks like Tor.
Simplify With Secure SSO

Pair Duo’s 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

Start Here

```
VPN RA
- cisco
- Juniper Networks
- Citrix
- Palo Alto Networks
- Pulse Secure
- box
- Dropbox
```

```
Multicloud
- Google
- salesforce
- aws
- Microsoft
- Remote Desktop Services
- Box
```

```
Email/MSFT
- Office 365
- Outlook
- Microsoft
- Horizon View
- Windows Server
- RRAS
```

```
On-Prem
- Epic
- Oracle PeopleSoft
- VMware
- >_SSH
- Shibboleth.
```

Then Expand

```
SSO
- Microsoft Azure
- AD FS
- Centrify
- onelogin
- Okta
```

```
Custom
- REST APIs
- WEB SDK
- RADIUS
- SAML
- OIDC
```

Learn more about application integrations

© 2019 Cisco and/or its affiliates. All rights reserved.
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
Workforce: Continuously Verify Trust

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
Device Visibility

- Admins get an easy-to-navigate, search & filter view of user endpoints accessing your organization’s applications.

- Quickly identify out-of-date devices.
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
Detect Device Malware & Respond

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

Prevent compromised devices from accessing Duo-protected applications.

**Trusted Endpoints**

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

- **Allow all endpoints**
  Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

- **Require endpoints to be trusted**
  Only Trusted Endpoints will be able to access browser-based applications.

- **Allow AMP for Endpoints to block compromised endpoints**
  Endpoints that AMP deems to be compromised will be blocked from accessing browser-based applications.
  **Note:** This option only applies to trusted endpoints.

*Currently available to select customers for private beta
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.
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
Duo Architecture Overview

Workforce: Recap

Duo Cloud Platform

Multi-Factor Authentication

User Management

MFA Management

Device Visibility

User Policy

Device Policy Check

Duo Integrated (Azure AD, RDP, SSH, Windows, App, API, etc.)

Web/SSH (Duo Network Gateway)

VPN, Virtual Desktop, etc.

Cloud Apps

Duo Access Gateway [SAML/SSO]

Duo Auth Proxy [Radius/LDAP]

Primary Auth (AD, Azure-AD, LDAP, etc.)
Extend Trust for the Workforce

**Umbrella**
Get visibility & protect internet access for all devices on the network, office locations and roaming users.

Learn more about Umbrella

**AMP**
Protect endpoints, network and email and get visibility into network/endpoint threats, while blocking & removing malware.

Learn more about AMP

**Meraki**
Get unified device management and control of mobile/desktop devices. Enable seamless onboarding & automated security policy enforcement.

Learn more about Meraki

**Cloudlock**
Manage risks in the cloud and protect users, data and apps. Monitor cloud environments to detect & secure sensitive data.

Learn more about Cloudlock

**Email Security**
Defend against data loss and encrypt sensitive information. Protect against phishing, business email compromise, and ransomware.

Learn more about Email Security
Duo Resources

**Duo TDM (internal)**
Get more technical detail on each feature, integrations, use cases, etc.

**Duo.com**
Learn more about Duo, the product, industry solutions, case studies, etc.

**Duo Demo**
See Duo in action - easy click-through demos of different user scenarios

**Duo Documentation & Integrations**
See which resources Duo protects, how to set them up, video walkthroughs and more

**Getting Started With Duo**
Practical guide for admins

**Duo Knowledge Base**
Support articles to address every use case and question
Zero Trust for the Workplace

Problems Solved:
• Complete network visibility
• Prevent lateral movement
• Prevent unauthorized access

Solution: SD-Access
With SD-Access, secure all user and device connections across your network, including IoT.
Establish Trust

Discover & classify devices with IoT device profiling, BYOD & user device posture.

Enforce Trust-Based Access

Network access control policies for users & devices with network segmentation.

Continuously Verify Trust

Continuous monitoring with vulnerability assessments & identifying indicators of compromise.
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 Visibility

Gain Insight Into:
• User groups
• Device types
• Location/time
• Posture
• Threats
• Behavior
• Vulnerability

And devices:
• Uses probes in Identity Services Engine (ISE) & network infrastructure
• Profiles and determines device type
• Determines access for IoT devices
Classification

Classify devices by groups based on their specific access needs and function.

After assets are identified, they’re tagged & classified by groups using either dynamic or static classification methods, or by assigning a tag to an IP address.

Clearly identify what needs to be protected. Example: Production servers; employees, guests or contractors; printers, etc.

Examples of Virtual Networks & Groups

Campus Groups:
- Employee
- Contractor

IoT Groups:
- Cameras
- IoT Mgmt
Network Segmentation

SD-Access end-to-end segmentation:

- Identity-based network segmentation
- Keep corporate, facilities/IoT and guest user devices separate & secure
- Without completely redesigning your network
Network Segmentation

With SD-Access, you can:

- Segment network access based on only what the device needs to access, and nothing more
- Partition your network to contain a breach
- Enable dynamic segmentation for growing networks, changing conditions & threats
Network Segmentation: Policy

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 thru policy manager
- Distribute policy dynamically to network devices
- Simplify segmentation with group-based policy
Network Segmentation: Policy

Determine policy compliance:
- Measure network device posture

Posture Flow:
- Authenticate User/Device
- Quarantine or limit access
- Assess Posture
- Remediation
- Change Authorization

- Posture
  - Anti-Malware Condition
  - Anti-Virus Condition
  - Application Condition
  - Disk Encryption Condition
  - File Condition
  - Patch Management Condition
  - Registry Condition

© 2019 Cisco and/or its affiliates. All rights reserved.
IoT Segmentation

Segment & Group IoT Devices
• Define policies for IoT group access & management
• Device profiling with flexible authentication options

Example IoT Device Classes:
• HVAC
• Power & lighting systems
• Healthcare patient monitors
• Medical imaging devices
• Manufacturing controllers
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

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
Continuous Monitoring & Response
Detect indicators of compromise & take action with Stealthwatch + ISE
Recap: Zero Trust for the Workplace

SD-Access secures user and device (IoT) access to your network, while preventing lateral movement and unauthorized access.

Discover & classify devices:
- IoT device profiling
- BYOD & user device posture

Enforce network access policies:
- For users & devices
- With network segmentation

Continually monitor trust:
- Vulnerability assessments
- Identify indicators of compromise
- Respond by revoking network access
SD-Access Integrations

ISE + Meraki
Quarantine any devices on your network that do not comply with your policies

ISE + Stealthwatch
Provides policy analytics tool that feeds into tagging policies for device groups
Cisco DNA Center (DNAC)

Automated deployment of zero-trust capabilities - making zero trust practical in the workplace.

DNAC is the network management & command center for Cisco DNA, the intent-based network for the enterprise.

DNAC allows you to provision and configure all of your network devices in minutes

It allows for:
Simple SDA fabric creation - VLANs, VXLANs, lisp, routing, BGP, ECMP & VRFs

Learn more about DNAC

Easy set up of access control:
- 802.1x configuration
- ISE integration and policies
- SGT TrustSec
- Switch device sensor
- Profiling configuration
- AAA and device administration
SD-Access Architecture Overview

Next-Gen FW
Inter-VN, Perimeter
Rapid threat containment & groups (tags)

Macro-segmentation

Campus VN
Groups:
Employee
Contractor
Campus-Quar

IoT VN
Groups:
Cameras
IoT-mgmt,
IoT-Quar

Guest VN
Groups:
Guest
Guest-Quar

Infra VN
Groups:
Net Services
Net Devices
Infra-Quar

Micro-segmentation

DNAC

Micro-segmentation

802.1x
dACL Blacklists

SDA Fabric

Identity Services Engine (ISE)

pxGrid

Tetration

© 2019 Cisco and/or its affiliates. All rights reserved.
Extend Trust for the Workplace

Next Gen Firewall
With deep network and security visibility, you can detect and stop threats fast before they reach your workforce, workloads, and workplace.

Learn more about NGFW

SD-WAN
Software-defined WAN securely connects any user to any app, from the WAN to cloud edge, providing a consistent user experience.

Learn more about SD-WAN

AnyConnect
Provide secure access to the workforce and workplace, as well as more insight into user and endpoint behavior across your entire enterprise.

Learn more about AnyConnect

Web Security Appliance
Automatically block access to risky sites and test unknown sites before allowing users to link to them; detect zero-day attacks quickly; and create and enforce granular policies for sites with embedded applications.

Learn more about WSA
Workplace

SD-Access Resources

**Cisco Software-Defined Access (SD-Access) Product Page**
Learn more about Software-Defined Access

**ISE TDM (internal)**
Get more in-depth technical detail on the features of ISE

**Cisco ISE Product Page**
Learn more about the features and benefits of ISE

**ISE + Stealthwatch for Continuous Monitoring & Response**
Learn about how Stealthwatch enables threat detection and ISE allows you to respond

**Top 10 Benefits of Stealthwatch & ISE**
Learn about why integrating the two products automates threat detection & response
Cisco Zero Trust
Secure access for your workforce, workloads and workplace.

SD-Access for Workplace
Secure all user and device connections across your network, including IoT.

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

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

Enforce Policy-Based Controls
Extended Protection
Complementary products to extend trust for any app, any workload & any network.

+ **Extend Trust**
  - Umbrella
  - AMP
  - Next-Generation Firewall
  - AnyConnect
  - WSA
  - SD-WAN
  - CloudLock
  - Meraki
  - ACI
  - Email Security

+ **Detect & Respond**
  - Cisco Threat Response (CTR)
  - Stealthwatch
Extend to Any Integration
Our technical partnerships make it easy to integrate security with your existing platforms.

Any Endpoint Platform
INTEGRATE WITH
Microsoft
Symantec
vmware
MobileIron

Any Infrastructure
INTEGRATE WITH
Google
kubernetes
Azure
amazon web services
vmware
UNIX

Any Third-Party (ID, SIEM)
INTEGRATE WITH
okta
splunk
IBM
Google
FORGEROCK
Dell
CA
Ping
ORACLE

Learn more about Duo partners
Learn more about Cisco partners

© 2019 Cisco and/or its affiliates. All rights reserved.
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