cisco Connect Vancouver

You make **possible**

cisco Connect Vancouver

Cisco Zero Trust Architecture

Cisco Connect Vancouver 2019

Jason Maynard
Senior Technical Architect Security

Rob Bleeker
Technical Solution Architect Security

Agenda

- Intro to Zero Trust
- Cisco's Zero Trust Architecture
- Zero Trust for the Workforce
- Zero Trust for the Workload
- Zero Trust for the Workplace
- More information

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

Shift in IT Landscape

Users, devices and apps are everywhere

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

IT Challenges

Increased diversity in access & 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?

Excessive Trust

How vulnerable are our clouds? Who/what accesses it?

How can we view & secure all connections?

What exists in the cloud? How does it connect?

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

Security Challenges

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

Business impact of a breach rising

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

300% Increase in malware for IoT devices

81% of breaches involved weak or stolen passwords

Security tools going blind due to privacy and encryption methods

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

Let’s look at a IT infrastructure with no zero trust architecture in place

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

When we trust too much…

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

The Zero Trust approach

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

Zero Trust: Assume Malicious Until Proven Otherwise

Device

User

Data

Network

Automated visibility and trust verification

Compliant BYoD iPad

MFA=Bob
Group= IT

Clean PDF

Encrypted
TLS 1.3

=Restricted Access

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

Cisco’s Zero Trust Architecture

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

cisco Connect

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

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

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

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

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.

How does Cisco compare?

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

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

Cisco Zero Trust Portfolio Depth

+ Enhance & Extend Trust

- Umbrella
- AMP
- ISE
- AnyConnect
- SD-WAN
- Email Security
- Next-Generation Firewall
- ACI

+ Detect & Respond

- Cisco Threat Response (CTR)
- Stealthwatch

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

Workforce

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

CISCO Connect

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

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

Easily Secure Cloud Application Access

Duo Access Gateway (DAG)

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

Demo: Workforce- Employee Off-Prem to SaaS

Use Cases	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

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

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

Let’s recap…

Use Cases: Solved!

- 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

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

Duo Network Gateway: Application remote access

Simple and secure remote access to specific Internal Apps

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

Search for users, groups, applications, or devices

Sanbower | ID: 1496-3762-75 Jamie Sanbower

- Dashboard
- Device Insight
- Policies
- **Applications**
  - Protect an Application
- Users
- Endpoints
- 2FA Devices
- Groups
- Administrators
- Trusted Endpoints Configuration
- Reports

Dashboard > Applications > Contractor Power Management Access

Contractor Power Management Access

Authentication Log | Remove Application

See the Duo Network Gateway documentation to integrate Duo into your Duo Network Gateway deployment.

Details

Reset Secret Key

Integration key	DI8HNQVSJMSM0OT1AKY3	select
Secret key	Click to view.	select
	Don't write down your secret key or share it with anyone.	
API hostname	api-5930e3d3.duosecurity.com	select

nticate when accessing this application. Your Global Policy always applies, but you can override its rules with

Duo Admin Console

Let’s recap…

Uses Cases: Solved!

- Workforce – Duo – Remote contractor, personal client to internal apps
  - DNG Deployment and Policy was simple and 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

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

Workload

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

Cisco Zero Trust for Workload

How to Establish Trust with Tetration

Establish Trust

Visibility and behavior modeling

WITH

Application discovery and dependency maps

All Processes, cmds, files, users and network comms

Enforce Trust-Based Access

Per workload, micro-segmentation policy

WITH

Automated, context-based, segmentation policy

Consistent policy: Any workload, Anywhere

Continuous Trust Verification

Real-time security health of workloads

BY

Security visibility and health score

Vulnerability, anomaly, forensic and threat data

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

Understand your workloads

Automated discovery, clustering and policy generation

App View

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)

Dynamic Policies

sco Connect

Demo: Workload – Hybrid Cloud Segmentation

Use Cases	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

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

Cisco Tetration APPLICATIONS

Monitoring

Payment Processor App

PRIMARY

ZTX : ACME : DC : PAYMENT PROCESSOR | DYNAMIC | Version: v4 | Endpoints: 7

Last Run: May 29, 6:57 PM

Switch Application

Start ADM Run

Conversations 36 | Clusters 8 | Policies 22 | Provided Services | App View 3 | Policy Analysis | Enforcement

Clusters

Filters | Filter Clusters ...

Create Cluster

Displaying **8** of 8 clusters

Cluster	Endpoints	Confidence	Dynamic	Approved
active-directory	1	Approved	✔	👍
bill-generator	1	Approved	✔	👍
card-processing-active	1	Approved	✔	👍
card-processing-broker	1	Approved	✔	👍
card-processing-standby	0	Approved	✔	👍
frontend	1	Approved	✔	👍
payment-stats	0	Approved	✔	👍
user-defined-cluster	0	N/A		

https://ztx.tetrationpreview.com/#/adm/datasets/5cee3b45755f0203480224da/v4/edit

Let’s recap…

Use cases: Solved!

- Workload – Tetration – Hybrid-DC multi-tier invoicing application
  - 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

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

Demo: Workload – Continuous Trust Verification

Use Cases	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

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

Applications
Places
Terminal
Fri 15:10
Struts2 Showcase - Mozilla Firefox
Terminal
File Edit View Search Terminal Help
RX packets 73026 bytes 4813068 (4.5 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 541477 bytes 101506647 (96.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 2051 bytes 89748 (87.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2051 bytes 89748 (87.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
yum install nmap -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: repos.dfw.quadranet.com
* epel: mirror.compevo.com
* extras: repos.dfw.quadranet.com
* updates: repos.dfw.quadranet.com
Package 2:nmap-6.40-16.el7.x86_64 already installed and latest version
Nothing to do
Powered by
Struts

Let’s recap…

Use cases: Solved!

- 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 Att&ck tactics rules

Workplace

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

CISCO Connect

Zero Trust for the Workplace

How to Establish Trust with SD-Access & ISE

Establish Trust

Discover and classify devices

WITH

IoT device profiling
BYOD lifecycle management
User device Posture

Enforce Trust-Based Access

Context-based network access control policy for users and things

WITH

Dynamic precise policies
Group-based (SGT)

Continuous Trust Verification

Continuous security health monitoring of devices

BY

Continuous Posture
Vulnerability assessments
Indications of compromise

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

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

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

SDA Journey for ZTA

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

Demo: Workplace - SDA for Wired, wireless

Use Cases?	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

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

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…

Use cases: Solved!

- Workspace – SD-Access – Retail payment on iPad and printer
  - ISE integrated Meraki MDM so it was able to quarantine non-compliant iPad
  - ISE profiled and categorized every device

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

In Summary…

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

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.

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

www.cisco.com/go/zerotrust

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

cisco Connect

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

Be the Bridge

Thank You!

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

cisco Connect