How to approach a Zero Trust security model

Jamey Heary
Cisco Distinguished Systems Architect, CCIE #7680
Global Security Architecture Team
Agenda

• Intro to Zero Trust
• Cisco’s Zero Trust Architecture
• Where to start
Shift in IT Landscape
Users, devices and apps are everywhere

Remote Users, Contractors & Third-Parties

Personal & Mobile Devices

IoT Devices

Cloud SaaS

Hybrid Cloud Infrastructure

Cloud IaaS
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?
How can we view & secure all connections?
What exists in the cloud? How does it connect?

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

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

- Incident response way too slow: 10K devices encrypted in <10mins!
- 81% of breaches involved weak or stolen passwords
- 300% Increase in malware for IoT devices
- Security tools going blind due to privacy and encryption methods

Business impact of a breach rising
Zero Trust
When we trust too much...

Reconnaissance
Victim clicks phishing email link

Perimeter bypassed
Malware exploits vuln

Lateral Movement
Pivot to DC, password harvesting

Data Exfiltration using Admin privilege

Information monetized
1. Monkey Island Server

Congrats! You have successfully set up the Monkey Island server.

The Infection Monkey is an open source security tool for testing a data center’s resiliency to perimeter breaches and internal server infections. The Monkey uses various methods to propagate across a data center and reports to this Monkey Island Command and Control server.

To read more about the Monkey, visit infectionmonkey.com

Go ahead and run the monkey.
De-perimeterization

An international group of corporate CISOs and vendors (Cisco hosted initial meeting)
Focused on solving “de-perimeterization” problem
Early output calling for “the need for trust”

Multiple models emerge

Forrester coined Zero Trust. NGFW biased
Google cloud first ZT arch, BeyondCorp
Forrester then expands to Zero Trust eXtended

Generalized

The industry has largely accepted Zero Trust Architecture as the general term

Customer Interest
Basic Tenet of Zero Trust

The effect of Zero Trust is **Ubiquitous Least-Privilege Access**
(i.e. grant access, but make it specific!)
Zero Trust: Assume Malicious Until Proven Otherwise

Device ➞ Compliant BYoD iPad
User ➞ MFA=Bob Group= IT
Data ➞ Clean PDF
Network ➞ Encrypted TLS 1.3

Automated visibility and trust verification

=Restricted Access
Cisco’s Zero Trust Architecture
Securing Access

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

**Workforce**

- All Corp IT
- User & Device Access

**Workload**

- Data Center
- Apps
- Servers
- Database
- SaaS
- Application & Workload Access

**Workplace**

- Corporate Network
- Network Traffic
- Wireless
- IoT Devices
- User & Devices

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

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

Simplifying the Journey: Cisco Zero Trust architecture in 3 critical areas

Workplace
On networks you control, establish trust-based access control for users/devices and including IoT.

Workforce
Establish trust of users and devices to determine their application access privileges

Workload
Minimizing the attack surface while enforcing least privilege access to/from our workloads

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
How does Cisco Zero Trust work?
3 Step Cyclical Process

- **Establish Trust**
  - We establish trust by verifying:
    - Multi-factors of User Identity
    - Device context and Identity
    - Device posture & health
    - Location
    - Relevant attributes and context

- **Enforce Trust-Based Access**
  - We enforce least privilege access to:
    - Networks
    - Applications
    - Resources
    - Users & Things

- **Continuous Trust Verification**
  - 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

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

<table>
<thead>
<tr>
<th>Microsoft</th>
<th>Google</th>
<th>kubernetes</th>
<th>AWS</th>
<th>UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>vmware</td>
<td>IBM</td>
<td>vmware [api]</td>
<td>ORACLE</td>
</tr>
<tr>
<td>Symantec</td>
<td>MobileIron</td>
<td>Azure</td>
<td>Ping</td>
<td>SDK</td>
</tr>
<tr>
<td>Okta</td>
<td>Forgerock</td>
<td>Splunk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cisco Zero Trust Portfolio Depth

+ Enhance & Extend Trust
- Umbrella
- AMP
- Meraki
- AnyConnect
- SD-WAN
- Email Security
- Next-Generation Firewall
- ACI

+ Detect & Respond
- Cisco Threat Response (CTR)
- Stealthwatch

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cisco is the leader in ZT

- Q4 2019
- “Deployment and ease of use are strengths across the portfolio.”
- “Cisco excels in Zero Trust, with a renewed and targeted focus.”
**Demo: End-to-End Cisco Zero Trust Architecture**

<table>
<thead>
<tr>
<th>What’s the customer problem?</th>
<th>How Cisco helps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I need to discover and classify my devices and application everywhere</td>
<td>Cisco SDA, Tetration, Duo</td>
</tr>
<tr>
<td>I need zero trust access control policy everywhere</td>
<td>Cisco SDA, Tetration, Duo</td>
</tr>
<tr>
<td>I need constant verification my users, devices and applications are trustworthy</td>
<td>Cisco SDA, Tetration, Duo</td>
</tr>
</tbody>
</table>
Fabric Domains and Transits

Choose a Fabric Domain or Transit below to manage, or add a new item by clicking "Add Fabric Domain or Transit".

**Fabric Domains**

- Default LAN Fabric
- Campus Fabric

**Transits**

- No Transits Created
Let’s recap...

1. Workplace - SD-Access
   • DNAC and ISE really streamlines deployment,
   • New ML profiling
   • Dynamic SGT-based access rules, integrated NGFW.

2. Workload – Tetration
   • Auto-Clustered apps together including ISE context
   • Dynamic, least-privilege application policy with one-click
   • Continuous trust with dashboard attack surface report

3. Workforce – Duo
   • Simple, powerful setup
   • Built-in integrations with tons of applications
   • One-click app enforcement: MFA, Biometric, device health, device trust
Establishing Trust
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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Zero Trust for the Workplace
How to Establish Trust with SD-Access & ISE

Discover and classify devices

Context-based network access control policy for users and things

Continuous security health monitoring of devices

WITH

IoT device profiling
BYOD lifecycle management
User Device Posture

WITH

Dynamic precise policies
Group-based (SGT)

BY
Continuous Posture
Vulnerability assessments
Indications of compromise

Establish Trust

Enforce Trust-Based Access

Continuous Trust Verification
Cisco Zero Trust for Workload
How to Establish Trust with Tetration

Establish Trust
Application discovery and dependency maps
All Processes, cmds, files, users and network comms

Enforce Trust-Based Access
Automated, context-based, segmentation policy
Consistent policy: Any workload, Anywhere

Continuous Trust Verification
Security visibility and health score
Vulnerability, anomaly, forensic and threat data

SaaS entry ~$35 Per workload/month!
$40K to start for 100 workloads
One license for workloads, all-in

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public
Demo: Workload – Continuous Trust Verification

What’s the customer problem?

What is the real-time security health of my workload environments?

How Cisco helps:

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
Welcome!

The Struts Showcase demonstrates a variety of use cases and tag usages. Essentially, the application exercises various framework features in isolation. The Showcase is not meant as a "best practices" example.

For more "by example" solutions, see the Struts Cookbook pages.

Copyright © 2003-2019 The Apache Software Foundation.
Let’s recap...

- 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
Cisco Zero Trust - Summary

Secure the Workforce
With Duo

Secure Your Workloads
With Tetration

Secure the Workplace
With Software-Defined Access

User & Device Access

All Corp IT

Application Access

Data Center

WAN Routing

Corporate Network

Visibility

Policy

Enforce

Report

MFA + Device Trust

Application Micro-Segmentation

Secure Network Access Control

User & Devices

IoT Devices

Network Traffic

Wireless

All Corp IT

Application

Servers

VM

Database

SaaS

Amazon Web Services

Google Cloud

WAN

Routing

User & Device Access

Workload Access

All Corp IT

Cisco Zero Trust
Thank you
You make possible