Zero Trust
Back to the year 2000?

Marko Haarala, Security Lead Finland & Baltic’s
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
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 vulnerable are our clouds? Who/what accesses it?
- How can we view & secure all connections?
- What exists in the cloud? How does it connect?
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
- Business impact of a breach rising
- 300% Increase in malware for IoT devices
- Security tools going blind due to privacy and encryption methods

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Zero Trust History
A Little Bit of Zero Trust History

**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
Cisco NaaS & NaaE architectures

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

Huge Customer Interest

---

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Zero Trust: Assume Malicious Until Proven Otherwise

Device > Automated visibility and trust verification > Restricted Access

User > Compliant BYoD iPad

Data > MFA=Bob Group=IT

Network > Clean PDF

Encrypted TLS 1.3
Cisco’s Zero Trust Architecture
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
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

How does Cisco Zero Trust work
3 Step Cyclical Process
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.
Cisco Zero Trust Architecture Differentiators

- **Time to Value**
- **Leaders in networking and Access**
- **Unrivaled Integrated Architecture**
- **Usability and Automation**
- **Brodest End-to-End ZT Coverage**
- **Broadest Visibility and control of hosts**

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Workforce
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.
Duo MFA Supports Your Work Applications

Start Here

VPN RA
- Cisco
- Juniper Networks
- Citrix
- Palo Alto Networks
- Pulse Secure
- Google
- Salesforce
- AWS
- Box
- Dropbox
- RRAS

Email/MSFT
- Office 365
- Outlook
- Microsoft Remote Desktop Services
- Windows Server
- Shibboleth

Multicloud
- Google
- AWS
- Box
- Dropbox

On-Prem
- Epic
- Oracle PeopleSoft
- VMware Horizon View
- AD FS
- Okta
- Centrify
- Shibboleth
- OneLogin
- OIDC

SSO
- Microsoft Azure
- Windows Azure
- AD
- SAML
- Radius

Custom
- REST APIs
- WEB SDK
- SAML
- OIDC

Then Expand

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Let’s recap...

• Workforce – Duo – Establish Trust and continuously verify
  • DAG app portal provided MFA, biometric, SSO, device health, device trust
  • Duo endpoint health for firewall, disk encryption, system password
  • Umbrella remote protection: blocked phish, blocked unapproved apps, policy to reduce shadow IT risk with new app discovery
  • Both Duo and Umbrella deployment are super quick and easy for admins and users
Workload
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

Per workload, micro-segmentation policy

WITH
Automated, context-based, segmentation policy
Consistent policy: Any workload, Anywhere

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
Dynamic Policies

<table>
<thead>
<tr>
<th>Priority</th>
<th>Action</th>
<th>Consumer</th>
<th>Provider</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>DENY</td>
<td>client posture=non-compliant</td>
<td>ZTX:ACME:DC:PAYMENT PROCESSOR</td>
<td>Any</td>
</tr>
<tr>
<td>10</td>
<td>DENY</td>
<td>SGIT=Quarantine</td>
<td>ZTX:ACME</td>
<td>Any</td>
</tr>
<tr>
<td>90</td>
<td>ALLOW</td>
<td>LB Internal Interface</td>
<td>ZTX:ACME:DC:PAYMENT PROCESSOR</td>
<td>TCP : 80 (HTTP)</td>
</tr>
<tr>
<td>100</td>
<td>ALLOW</td>
<td>active-directory</td>
<td>ZTX:ACME:DATABASES:ORACLE</td>
<td>TCP : 3306 (MySQL)</td>
</tr>
<tr>
<td>100</td>
<td>ALLOW</td>
<td>card-processing-active</td>
<td>ZTX:ACME:DATABASES:POSTGRES</td>
<td>TCP : 3306 (MySQL)</td>
</tr>
</tbody>
</table>
Let’s recap...

- Workload – Tetration – Application level segmentation
  - Security dashboard provided an overall health score
  - Vulnerability dashboard showed what was most critical to patch
  - Detailed forensics with new Att&ck tactics rules
  - And much more
Workplace
Zero Trust for the Workplace
How to Establish Trust with SD-Access & ISE

- Establish Trust
- 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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
What's is SD-Access?
Networking at the Speed of Software!

DNA Center
- Policy
- Automation
- Analytics

Automated Network Fabric
- Single Fabric for Wired & Wireless with workflow Automation

Identity-Based Policy & Segmentation
- Decoupled security policy from VLAN and IP Address

Insights & Telemetry
- Analytics and Insights into User and Application behavior

IoT Network
- User Mobility
- Policy stays with user

Employee Network
Let’s recap: 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
In Summary...
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.
Did we go back to 2000?
Thank You!