Zero Trust
Back to the year 2000?

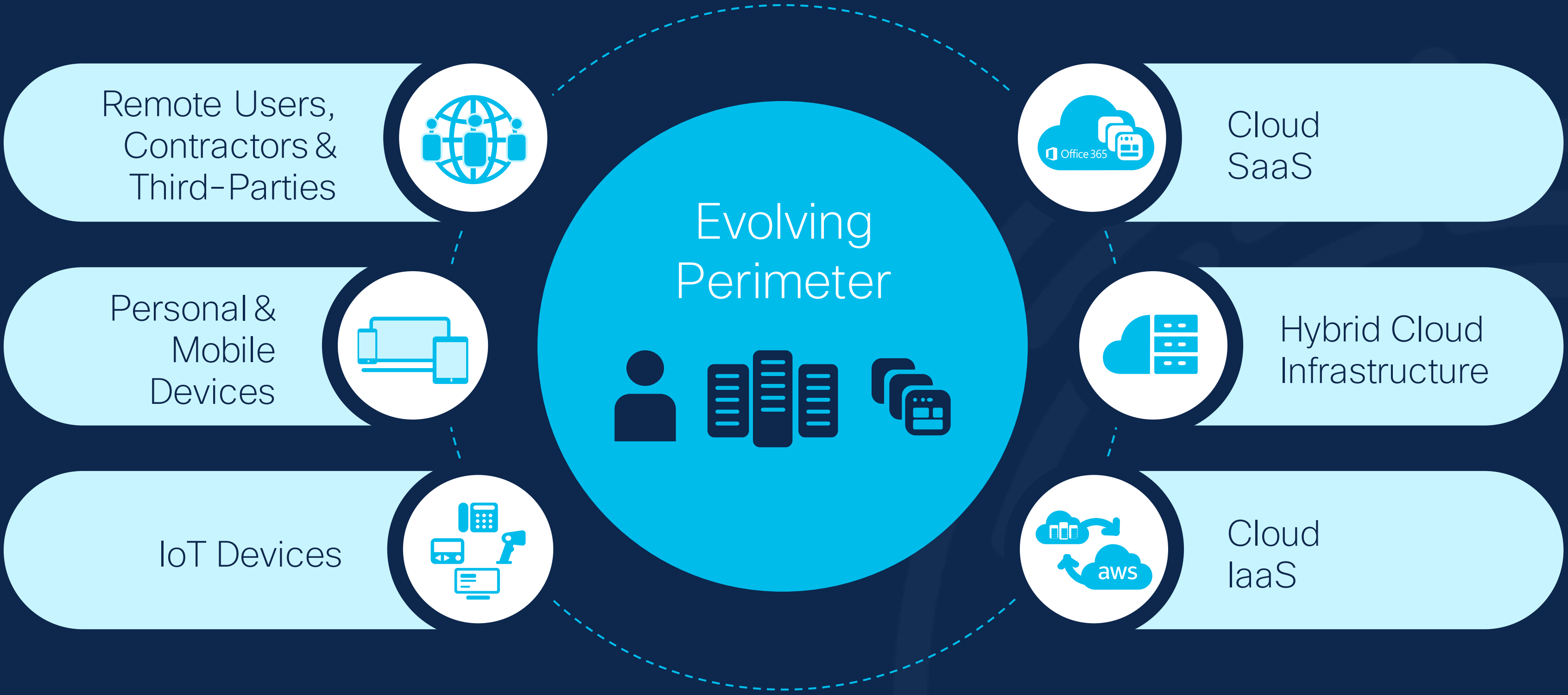
Marko Haarala, Security Lead Finland & Baltic’s

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

Evolving Perimeter

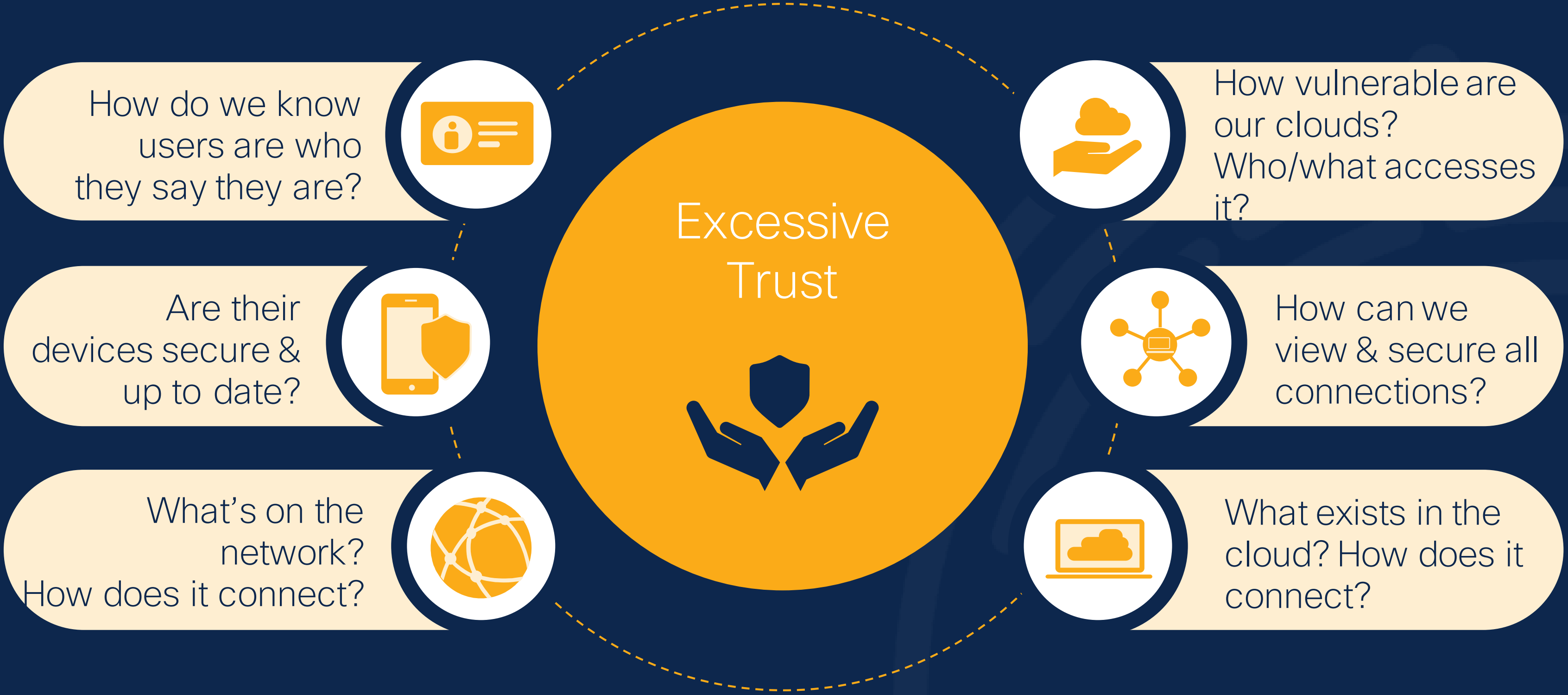
Cloud SaaS

Hybrid Cloud Infrastructure

Cloud IaaS

IT Challenges

Increased diversity in access & gaps in visibility



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?

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!

300% Increase in malware for IoT devices

Business impact of a breach rising

81% of breaches involved weak or stolen passwords

Security tools going blind due to privacy and encryption methods

Zero Trust History

A Little Bit of Zero Trust History

Jericho Forum — 2004

ZT — 2010

BeyondCorp — 2014

ZTX — 2017

ZTA — TODAY

De-perimiterization

An international group of corporate CISOs and vendors (Cisco hosted initial meeting)

Focused on solving "de-perimiterization" 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

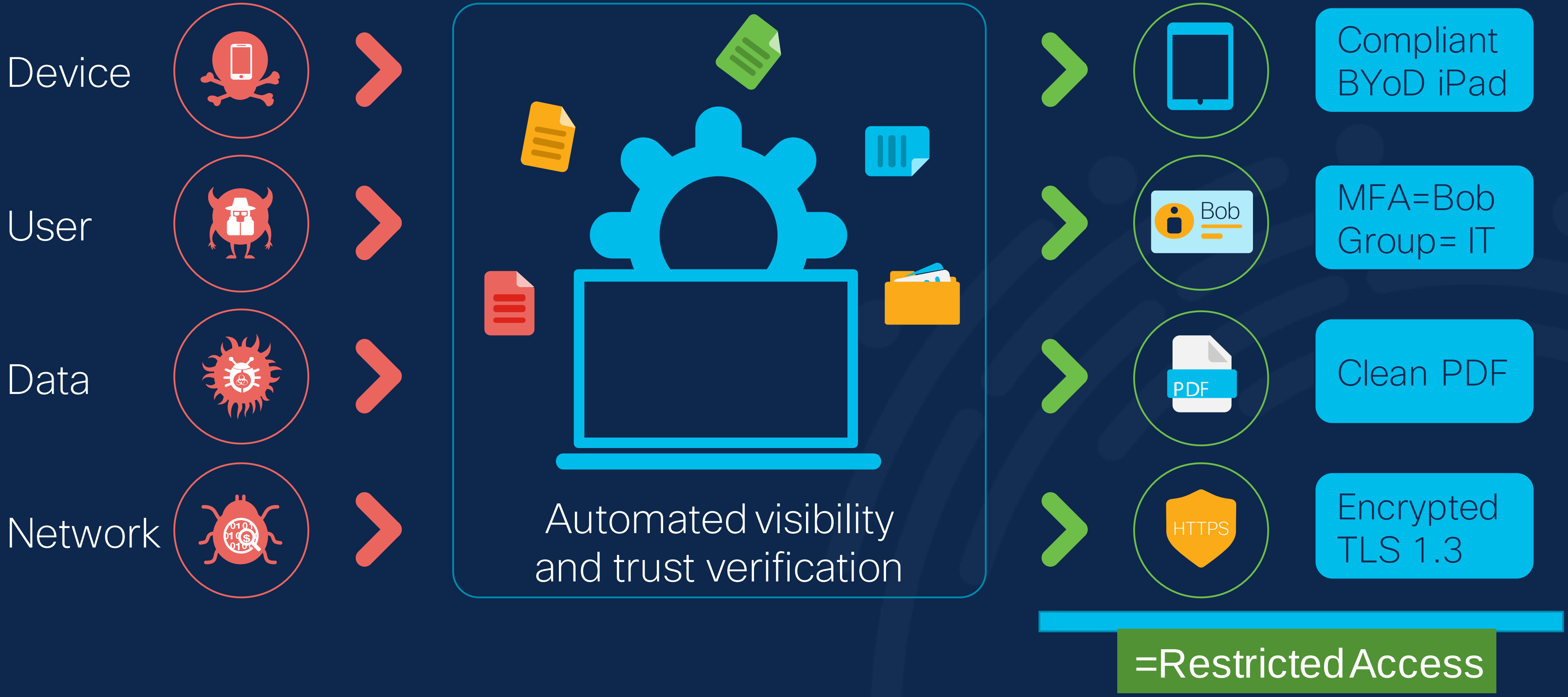
Cisco NaaS & NaaE architectures

Generalized

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

Huge Customer Interest

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

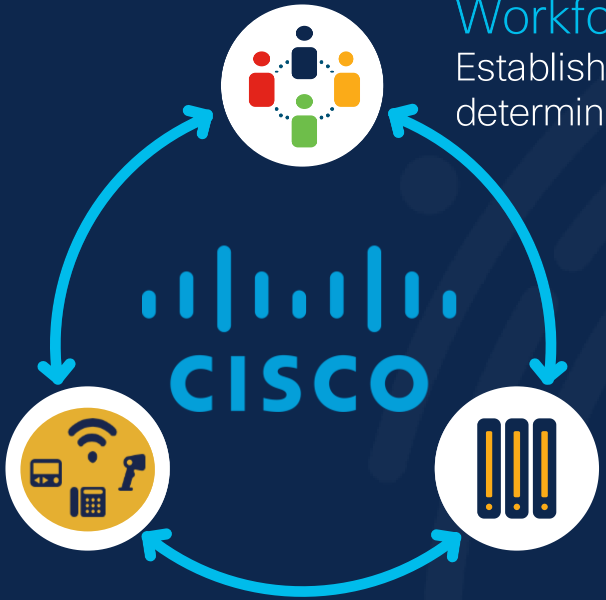
Encrypted TLS 1.3

=Restricted Access

Cisco’s Zero Trust Architecture

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

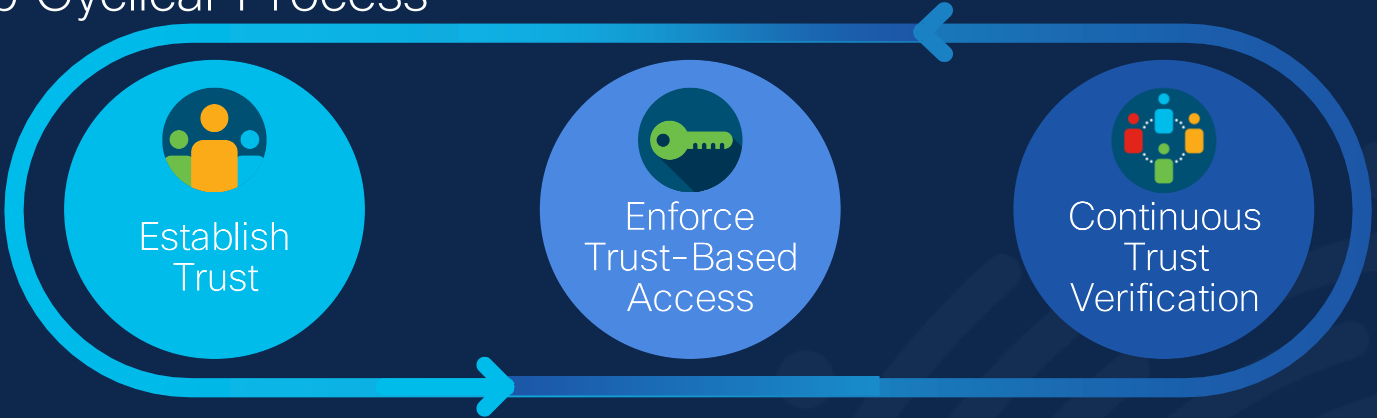
On networks you control, establish trust-based access control for users/devices and including IoT.

Workload

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

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:

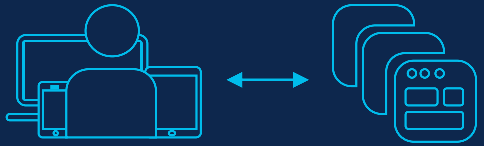
- Original tenets used to establish trust are still true
- Traffic is not threat traffic
- Behavior for any risky, anomalous or malicious actions
- If compromised, then the trust is broken

Cisco Zero Trust Journey

Primary Solutions

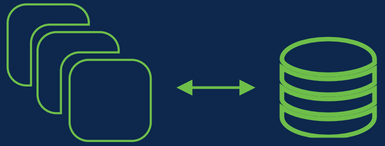
Duo for Workforce

Establish trust level for users and their devices accessing applications and resources



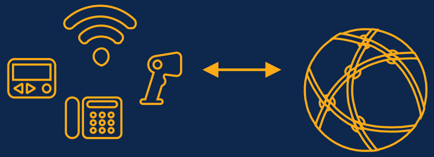
Tetration for Workload

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
- ✓ Broadest End-to-End ZT Coverage
- ✓ Broadest Visibility and control of hosts

Microsoft Google kubernetes aws UNIX

vmware IBM vmware {api} ORACLE

Symantec. MobileIron Azure Ping Identity SDK

okta FORGEROCK splunk>

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

Duo MFA Supports Your Work Applications

Start Here			Then Expand		
VPN RA	**Multicloud**	**Email/MSFT**	**On-Prem**	**SSO**	**Custom**
cisco	Google Apps	Office 365	Epic	Microsoft Azure	REST APIS
juniper NETWORKS	salesforce	Outlook	ORACLE PEOPLESOFT	AD FS	WEB SDK
citrix	aws	Microsoft Remote Desktop Services	vmware Horizon View	okta	RADIUS
paloalto NETWORKS	box	Windows Server	>_SSH	Centrify	SAML
Pulse Secure	Dropbox	RRAS	Shibboleth	onelogin	OIDC

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

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

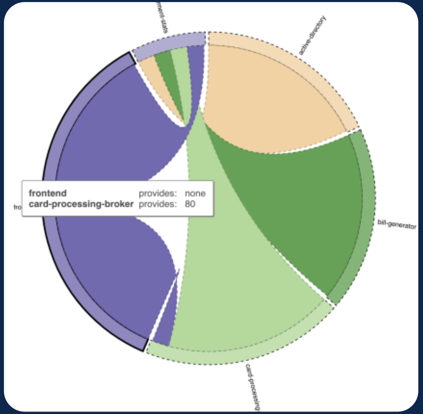
BY

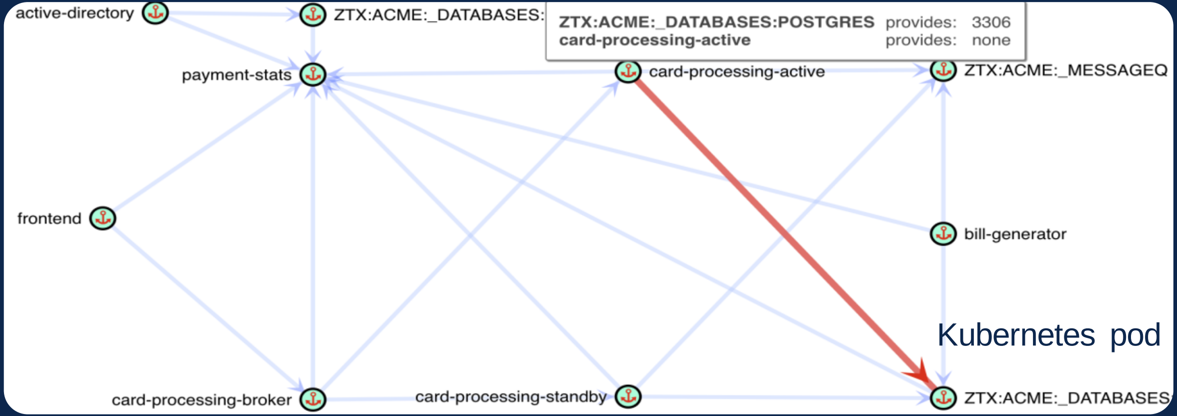
Security visibility and health score

Vulnerability, anomaly, forensic and threat data

Understand your workloads

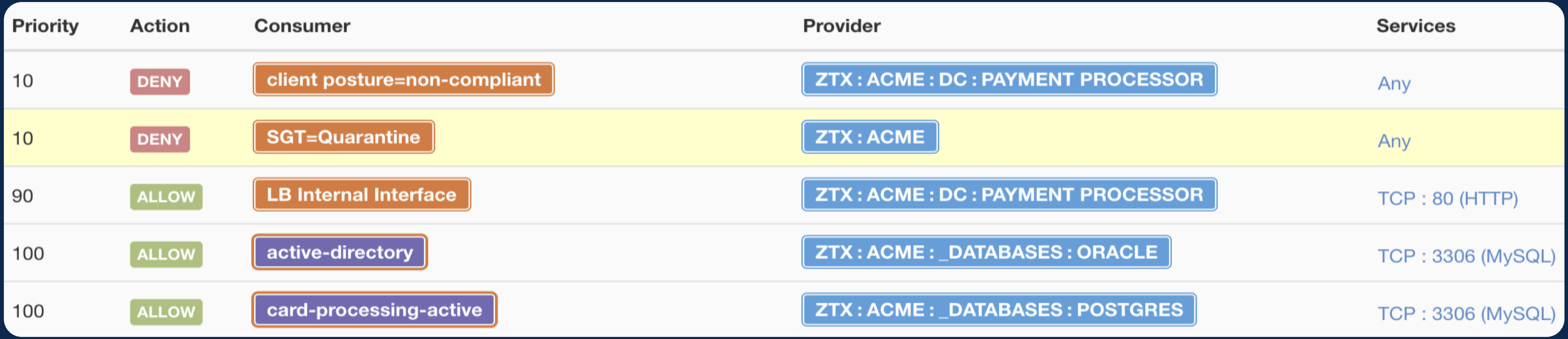
Automated discovery, clustering and policy generation





Kubernetes pod

App View

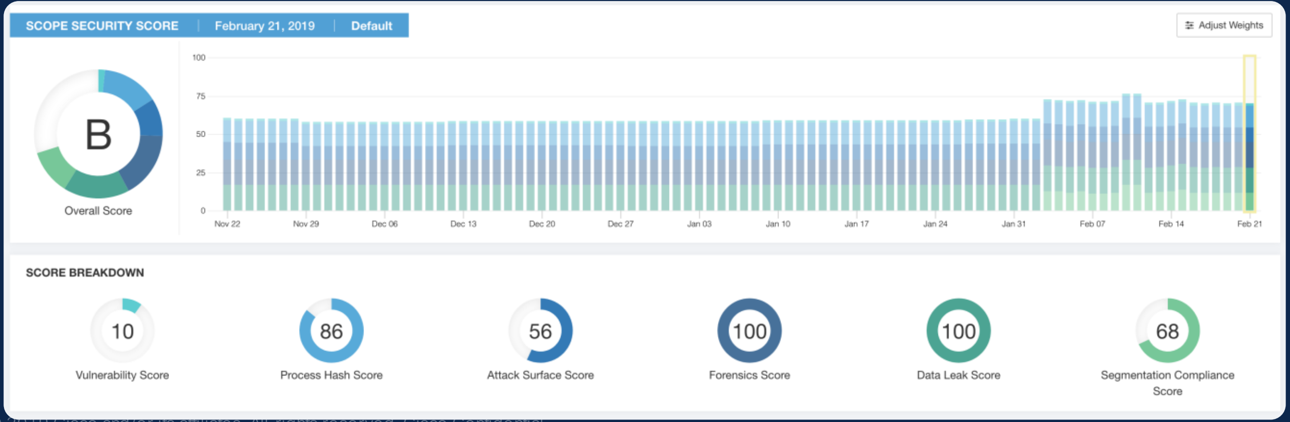


Priority	Action	Consumer	Provider	Services
10	DENY	client posture=non-compliant	ZTX : ACME : DC : PAYMENT PROCESSOR	Any
10	DENY	SGT=Quarantine	ZTX : ACME	Any
90	ALLOW	LB Internal Interface	ZTX : ACME : DC : PAYMENT PROCESSOR	TCP : 80 (HTTP)
100	ALLOW	active-directory	ZTX : ACME : _DATABASES : ORACLE	TCP : 3306 (MySQL)
100	ALLOW	card-processing-active	ZTX : ACME : _DATABASES : POSTGRES	TCP : 3306 (MySQL)

Dynamic Policies

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



SCOPE SECURITY SCORE | February 21, 2019 | Default

SCORE BREAKDOWN

Vulnerability Score	Process Hash Score	Attack Surface Score	Forensics Score	Data Leak Score	Segmentation Compliance Score
10	86	56	100	100	68

Workplace

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

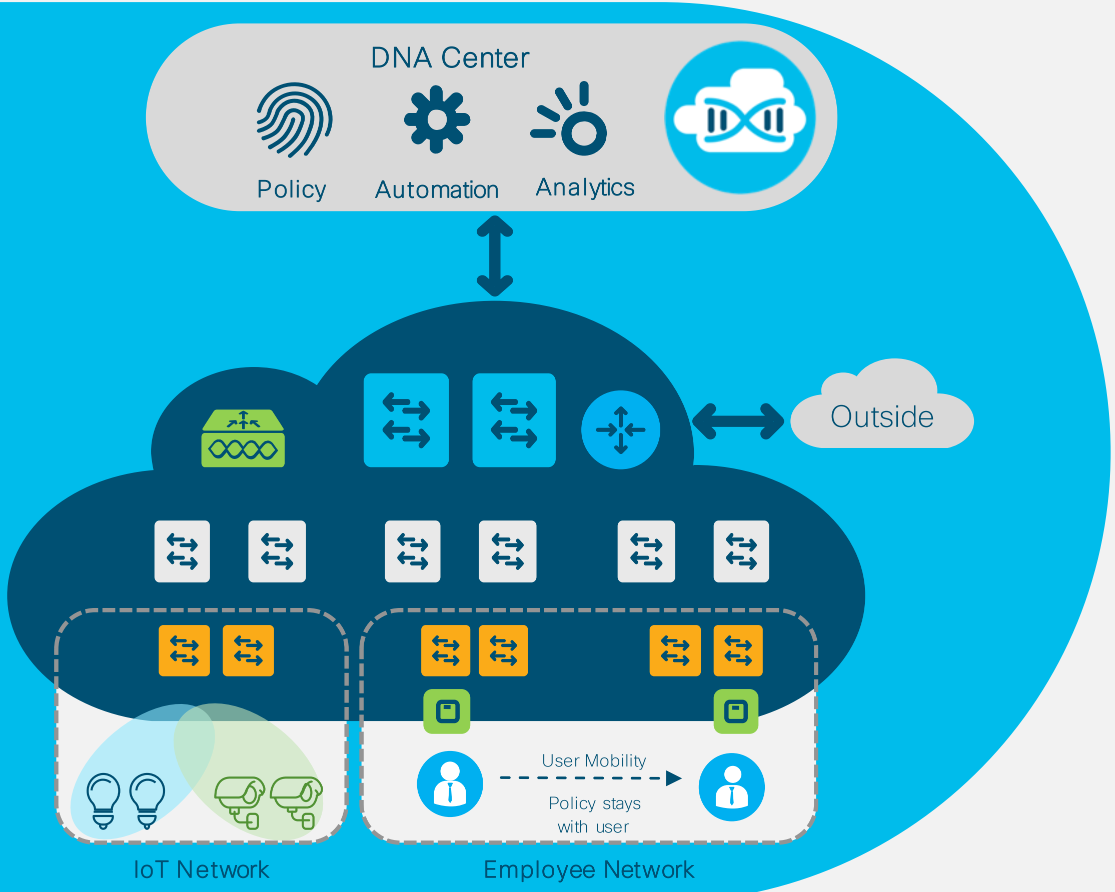
Continuous security health monitoring of devices

BY

Continuous Posture
Vulnerability assessments
Indications of compromise

What’s is SD-Access?

Networking at the Speed of Software!



Automated Network Fabric

Single Fabric for Wired & Wireless with workflow Automation

Identity-Based Policy & Segmentation

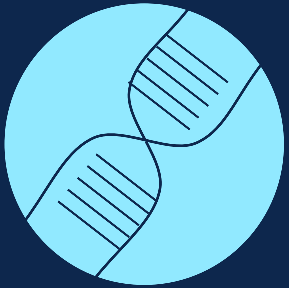
Decoupled security policy from VLAN and IP Address

Insights & Telemetry

Analytics and Insights into User and Application behavior

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!