How To Do Segmentation Without Getting Fired

Mark Bernard, Systems Architect, CCIE
Oct 2019

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
- Call to Action

About Me

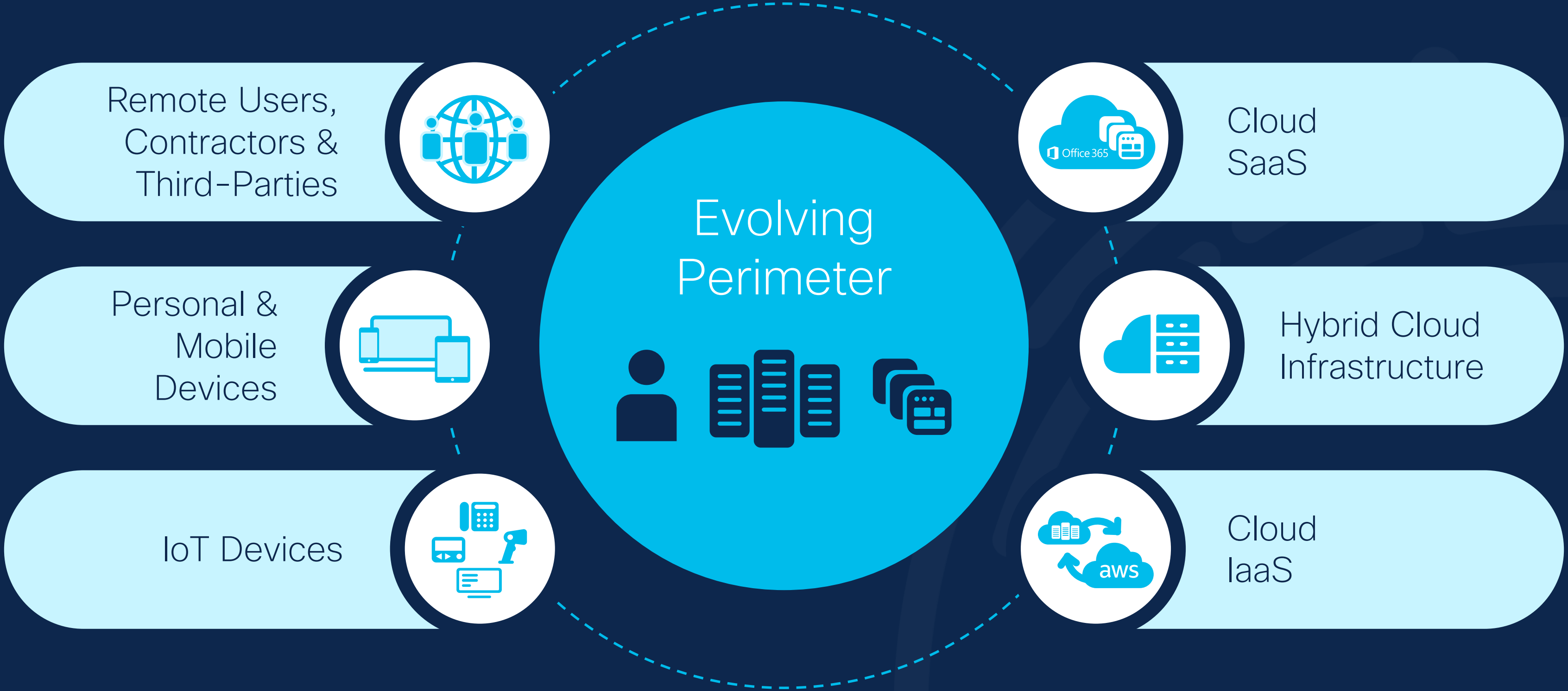
- Systems Architect supporting Commercial South Area
- Joined Cisco in 2005
- Masters Degree (MS) in Cyber Security
- CCIE Mentor for Cisco Employees
- Cisco Live Speaker since 2006
- Cisco Live Distinguished Speaker
- CCIE #23864, CISSP, etc.

MNB@cisco.com

@bernarmn

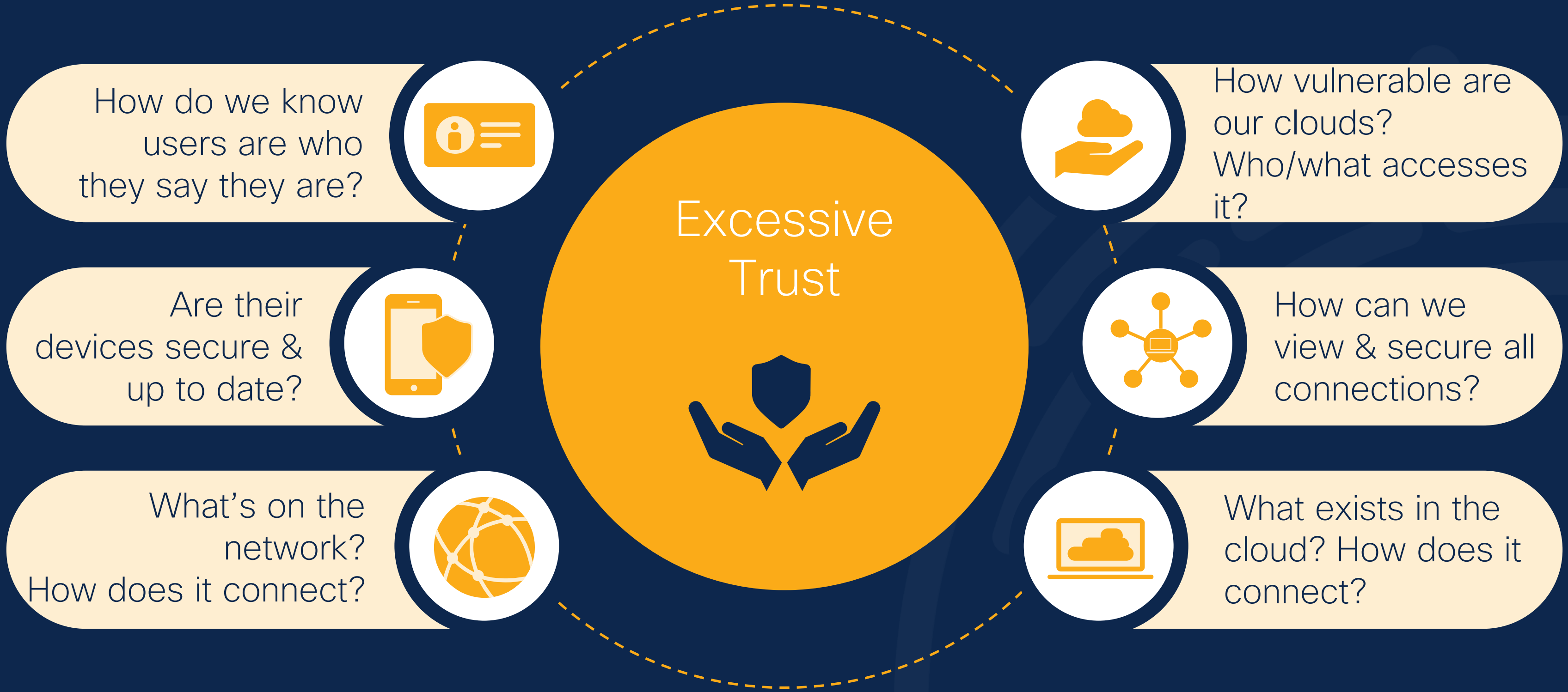
Shift in IT Landscape

Users, devices and apps are everywhere



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

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

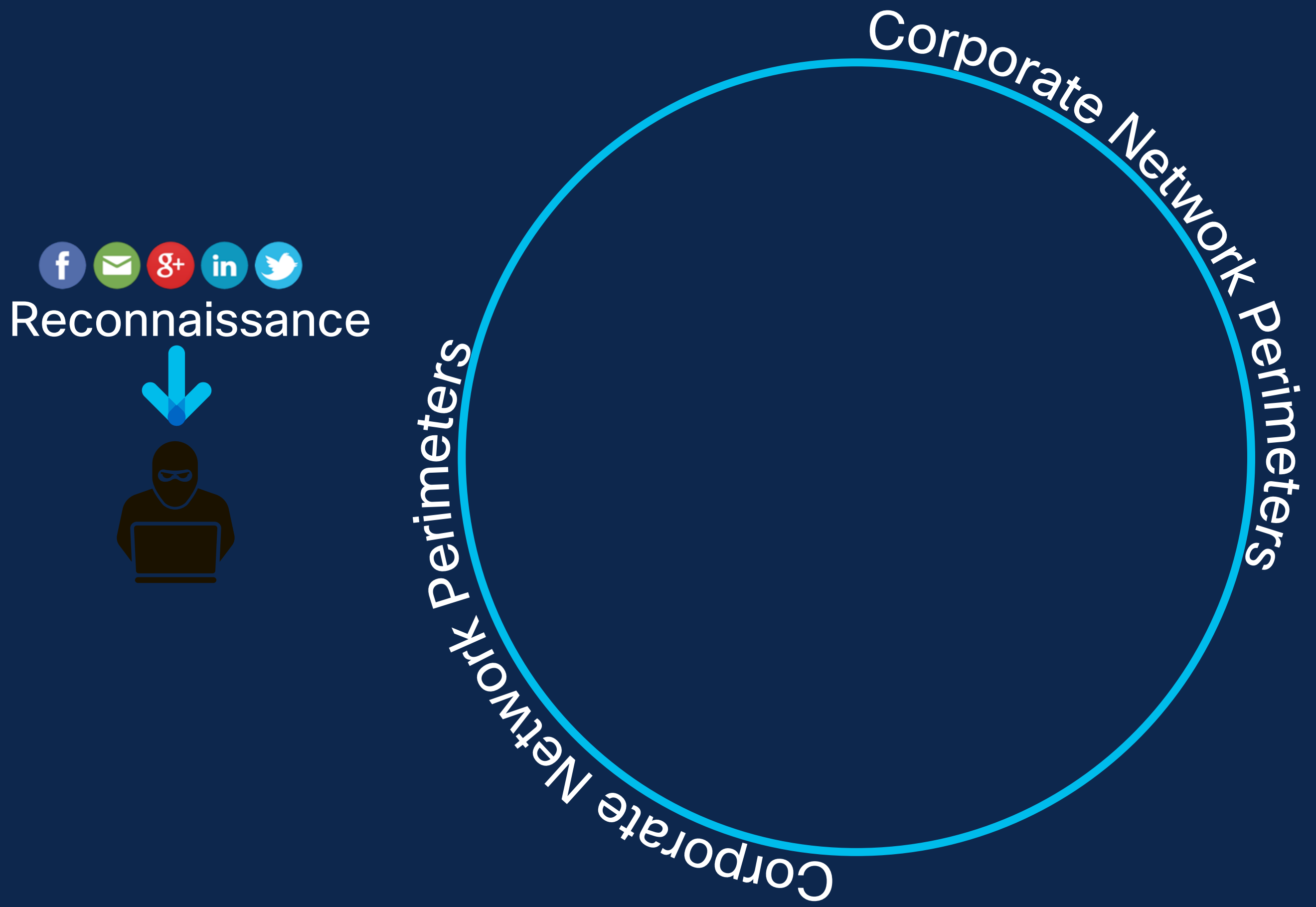
Security tools going blind due to privacy and encryption methods

Zero Trust

Zero Trust

Assume zero trust when someone or something requests access to work assets. You must first verify their trustworthiness before granting access.

When we trust too much…

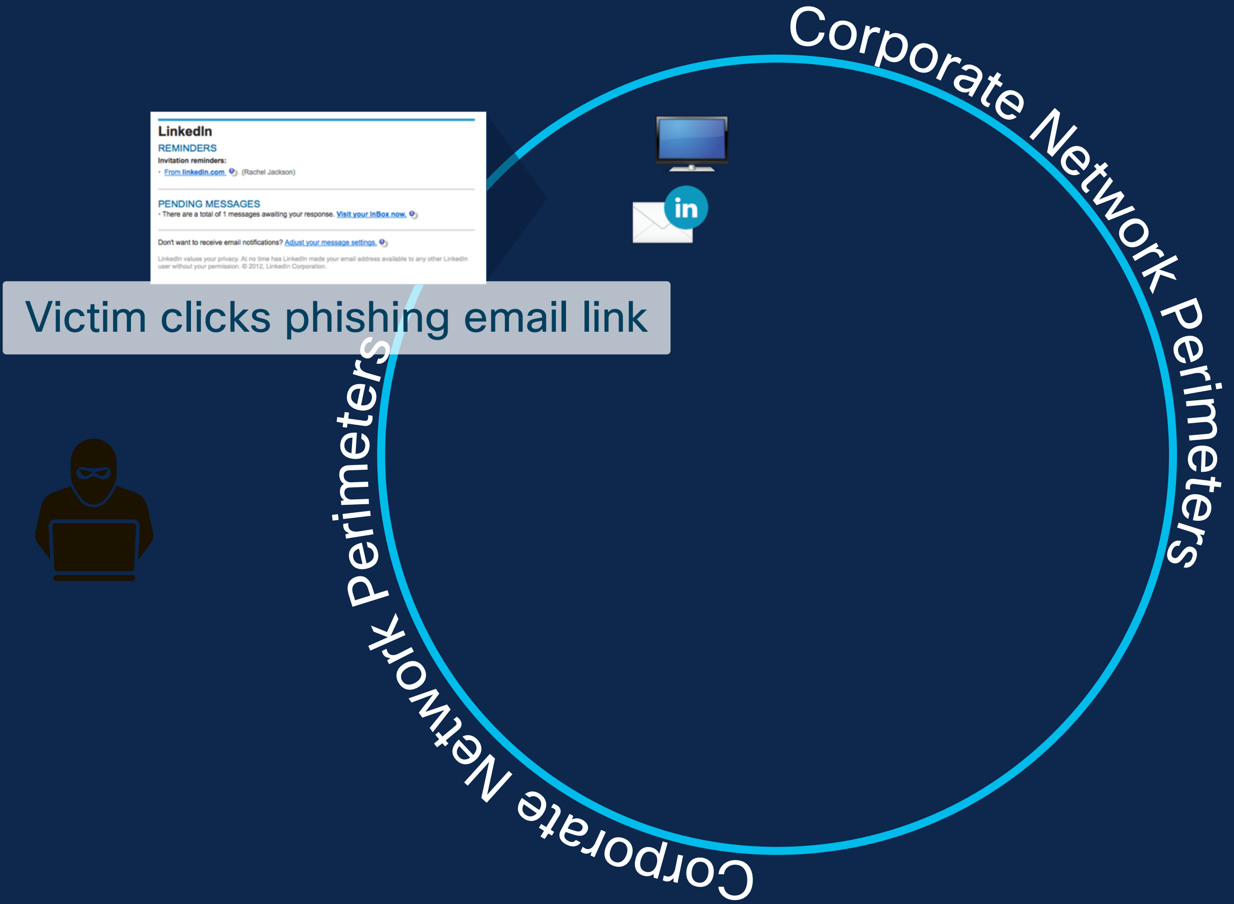


Reconnaissance

Corporate Network Perimeters

Corporate Network Perimeters

When we trust too much…



LinkedIn

REMINDERS

Invitation reminders:

- From linkedin.com (Rachel Jackson)

PENDING MESSAGES

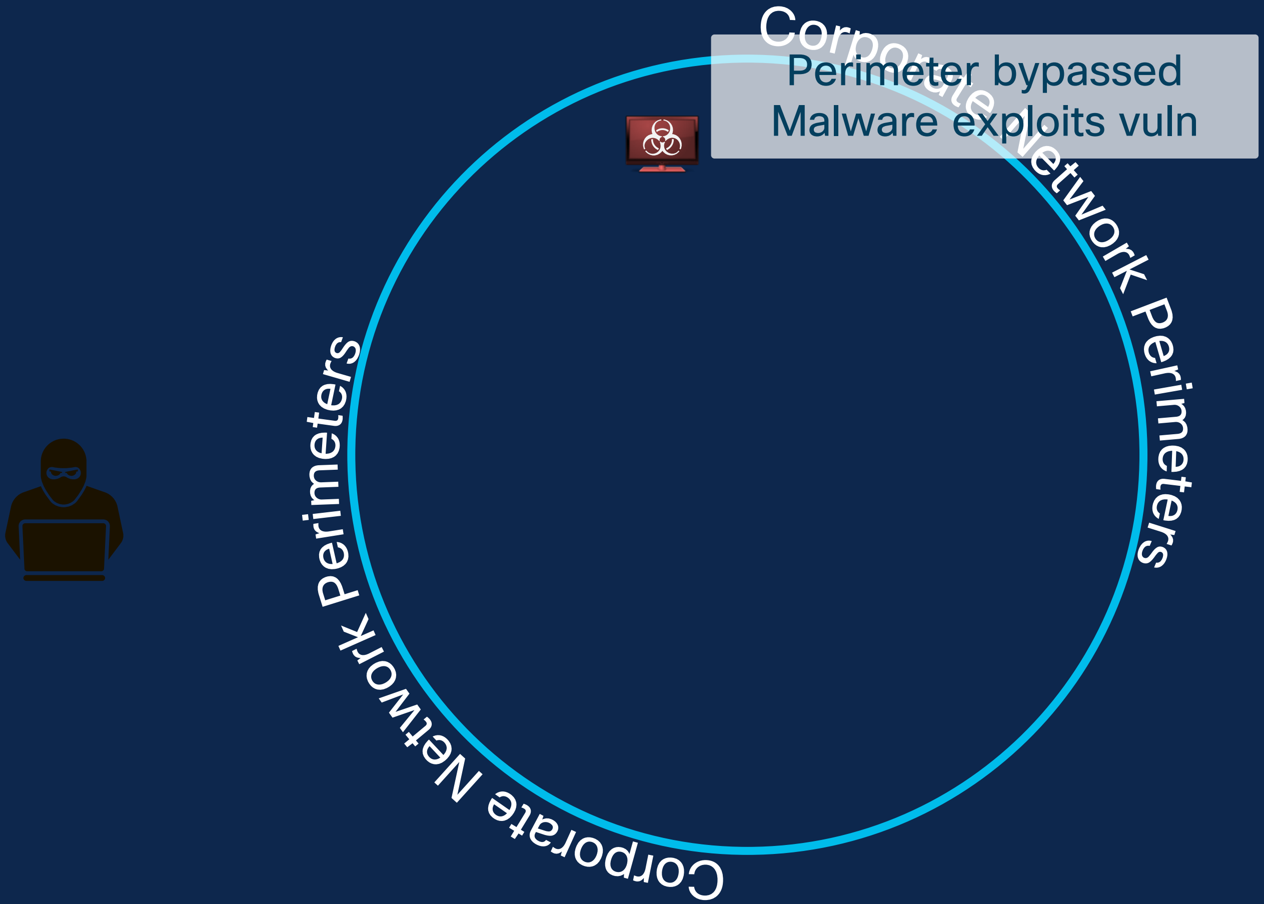
- There are a total of 1 messages awaiting your response. Visit your InBox now.

Don't want to receive email notifications? Adjust your message settings.

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2012, LinkedIn Corporation.

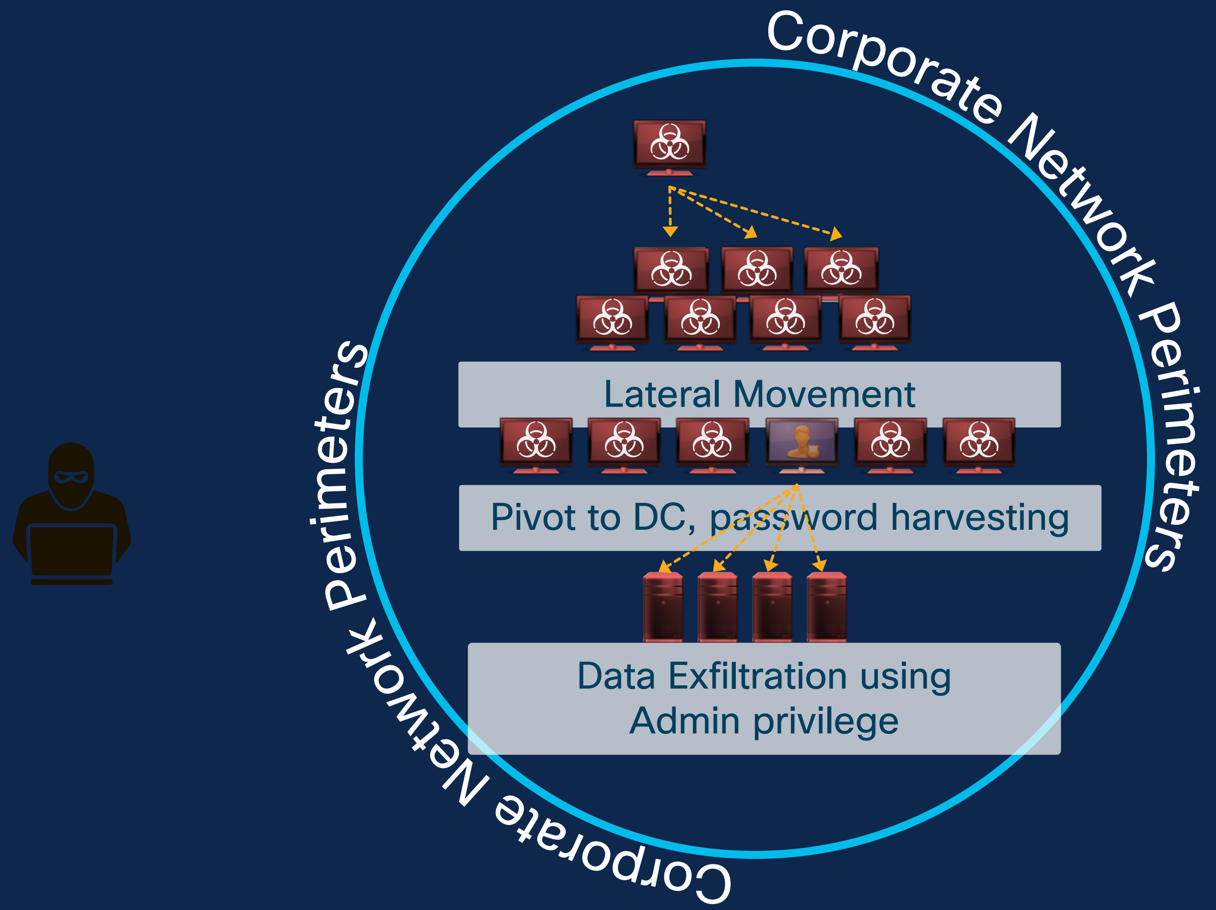
Victim clicks phishing email link

When we trust too much…



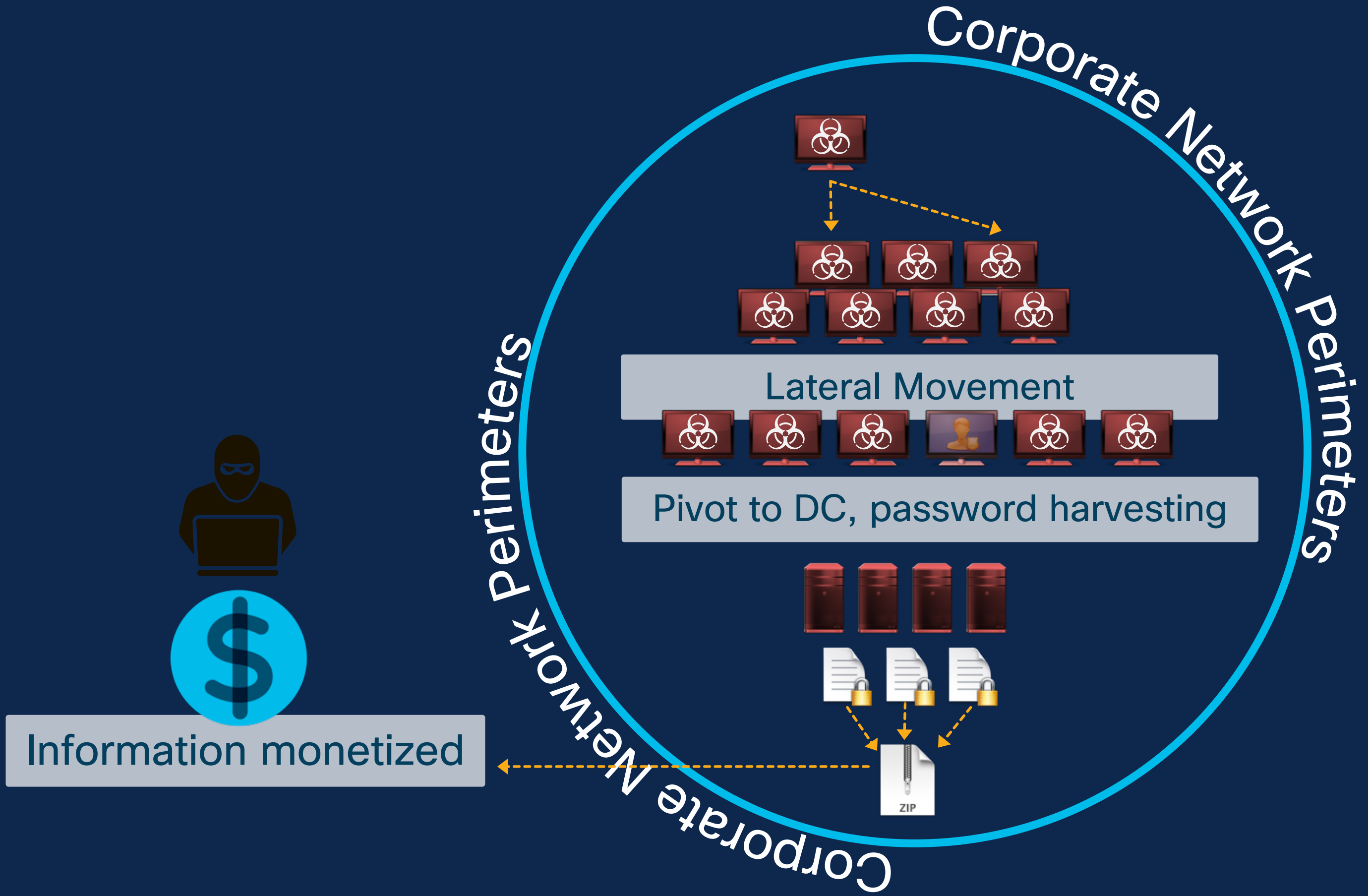
Perimeter bypassed
Malware exploits vuln

When we trust too much…



Corporate Network Perimeters
Lateral Movement
Pivot to DC, password harvesting
Data Exfiltration using Admin privilege
Corporate Network Perimeters

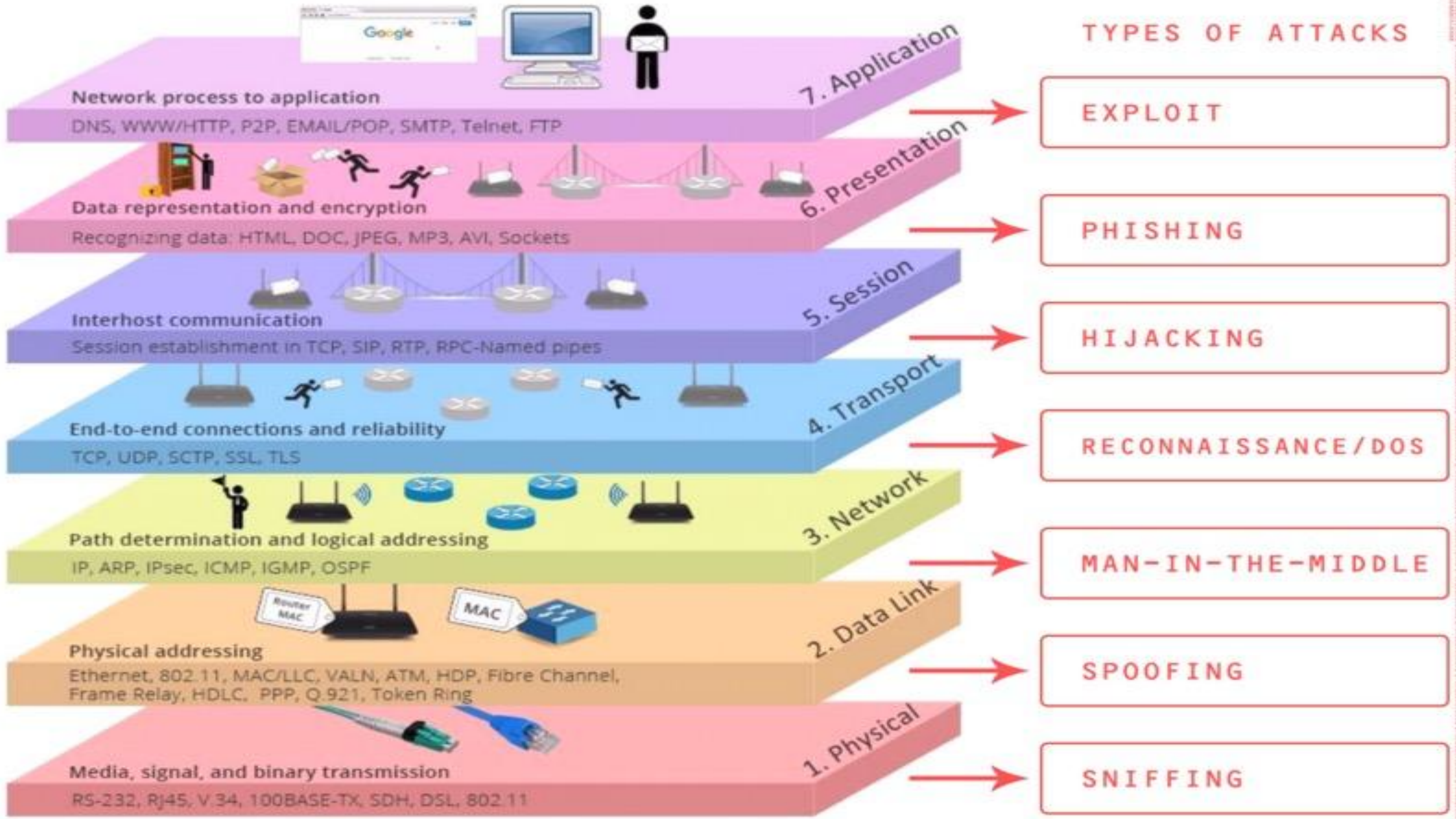
When we trust too much…



Lateral Movement

Pivot to DC, password harvesting

Information monetized



TYPES OF ATTACKS

7. Application

Network process to application

DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

EXPLOIT

6. Presentation

Data representation and encryption

Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

PHISHING

5. Session

Interhost communication

Session establishment in TCP, SIP, RTP, RPC-Named pipes

HIJACKING

4. Transport

End-to-end connections and reliability

TCP, UDP, SCTP, SSL, TLS

RECONNAISSANCE/DOS

3. Network

Path determination and logical addressing

IP, ARP, IPsec, ICMP, IGMP, OSPF

MAN-IN-THE-MIDDLE

2. Data Link

Physical addressing

Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring

SPOOFING

1. Physical

Media, signal, and binary transmission

RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

SNIFFING

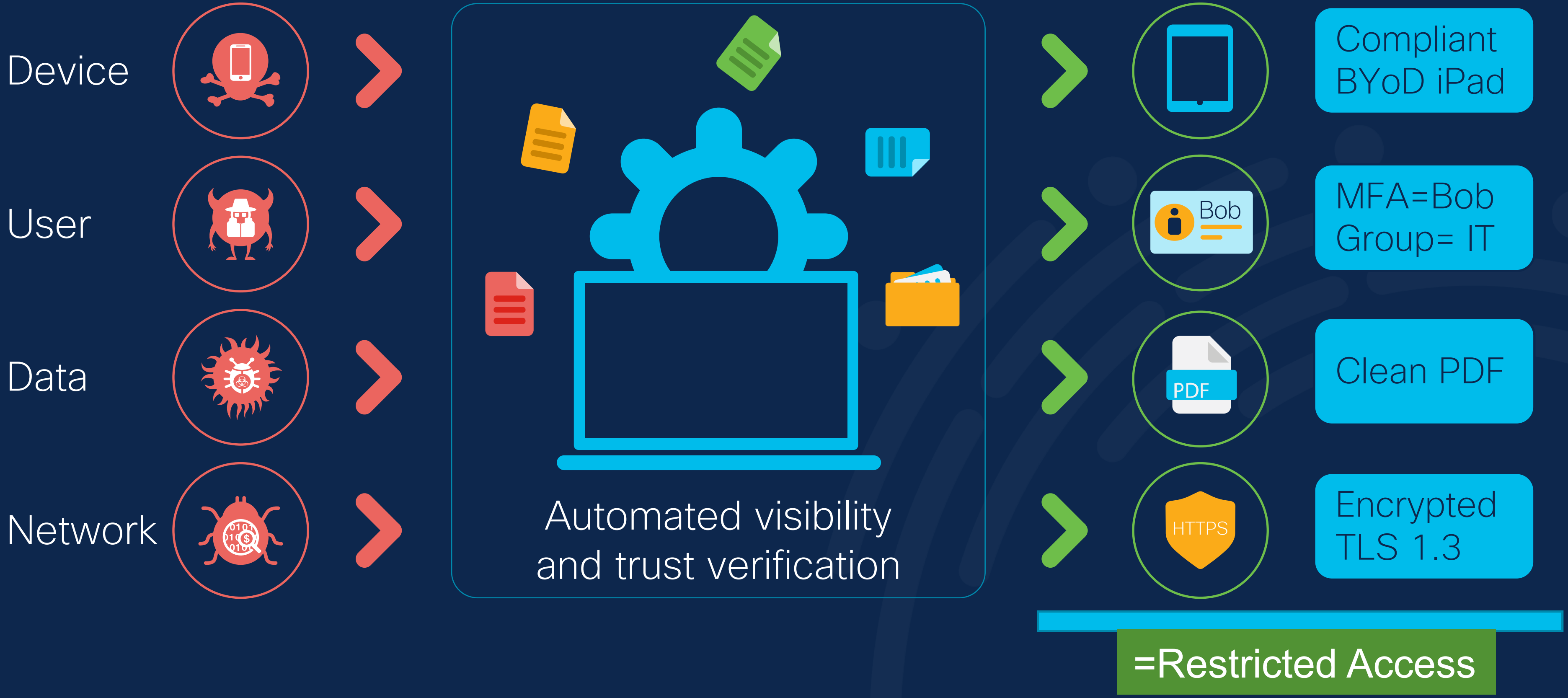
Basic Tenant of Zero Trust

The effect of Zero Trust is

Ubiquitous Least-Privilege Access

(i.e. grant access,
but make it specific!)

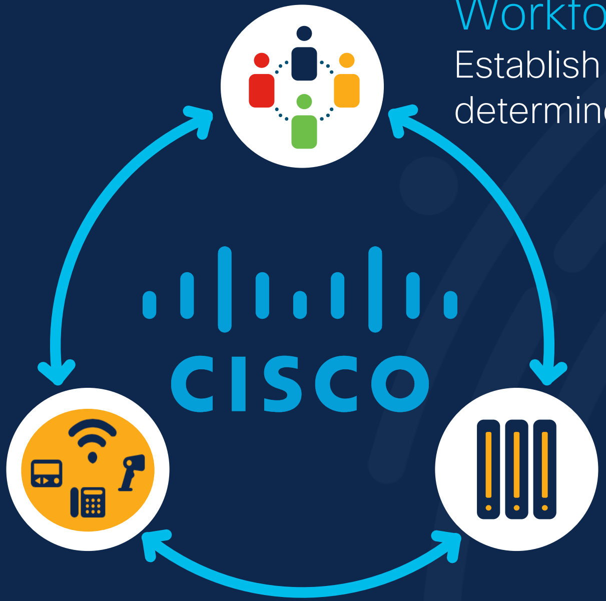
Zero Trust: Assume Malicious Until Proven Otherwise



Sample Zero Trust Architecture

Zero Trust Architecture

Simplifying the Journey: Zero Trust architecture in 3 critical areas



Workforce

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

Workplace

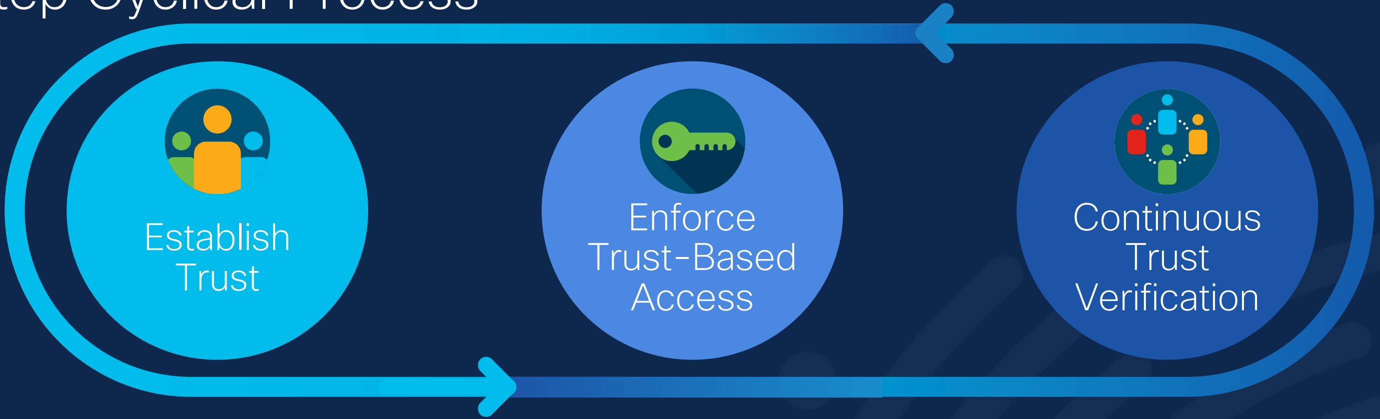
On networks you control, establish trust-based access control for users/devices and including IoT.

Workload

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

How does 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

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 (ISE) for Workplace

Establish least privilege access control for all users and devices, including IoT, accessing your networks.

How does compare?

Sample Zero Trust Portfolio

+ Enhance & Extend Trust

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

+ Detect & Respond

- Cisco Threat Response (CTR)
- Stealthwatch

Use Case: End-to-End Zero Trust Architecture

What’s the customer problem?	What solution helps:
I need to discover and classify my devices and application everywhere	ISE & SDA, Tetration, Duo
I need zero trust access control policy everywhere	ISE & SDA, Tetration, Duo
I need constant verification my users, devices and applications are trustworthy	ISE & SDA, Tetration, Duo

Let’s recap…

Customer problems: Solved!

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

Workforce

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

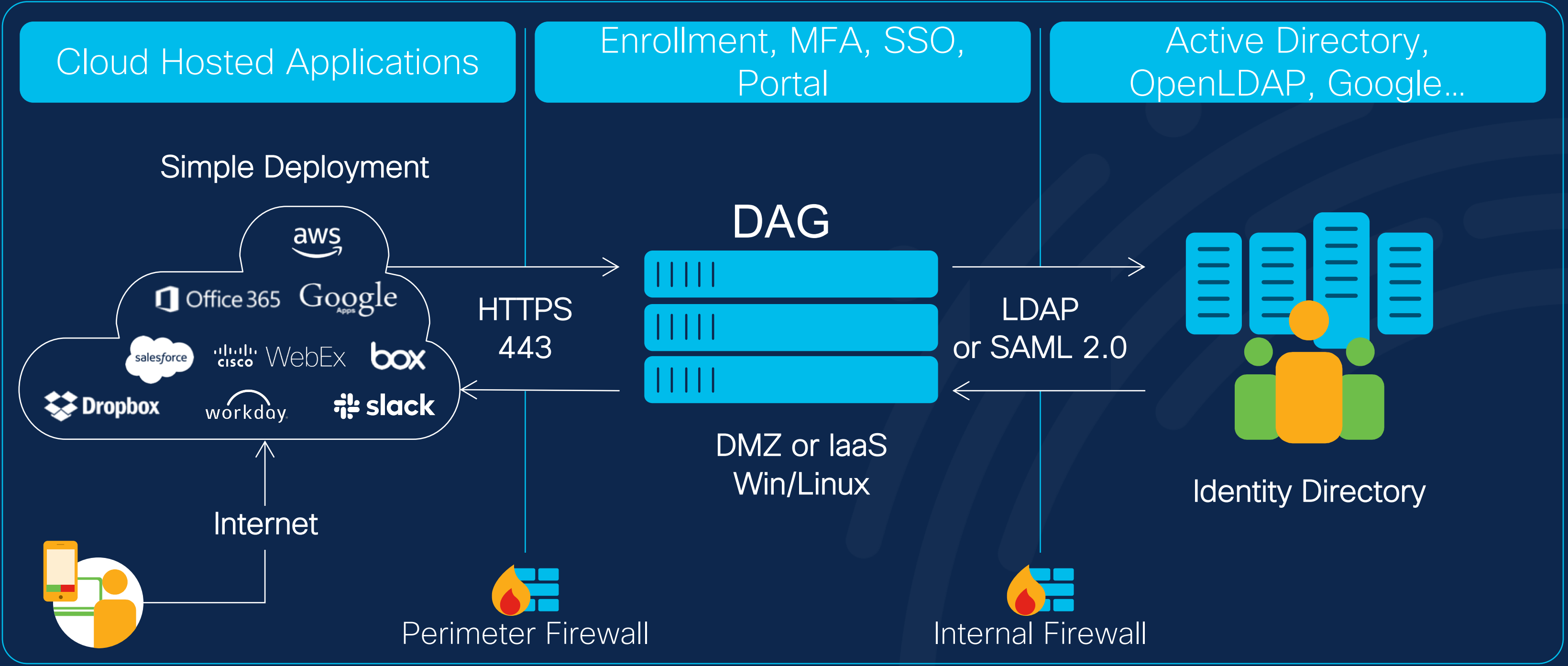
Enforce risk-based and adaptive access policies

WITH

Per application access policies that vary based on risk tolerance levels

Easily Secure Cloud Application Access

Duo Access Gateway (DAG)



Demo: Workforce- Employee Off-Prem to SaaS

What’s the customer problem?	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

Customer problems: Solved!

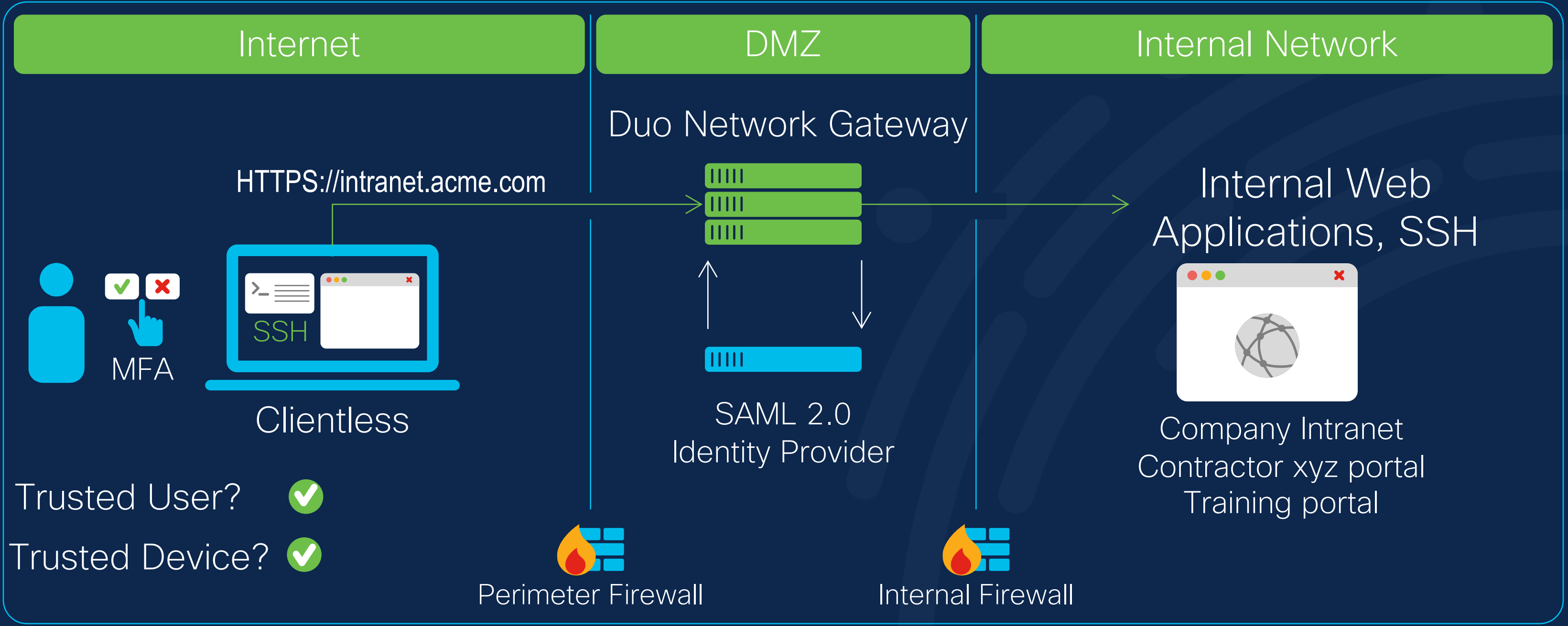
Let’s recap…

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
- Umbrella remote protection: blocked phish, blocked unapproved apps, policy to reduce shadow IT risk with new app discovery
- Both Duo and Umbrella deployment was super quick and easy for admins and users

Duo Network Gateway: Application remote access

Simple and secure remote access to specific Internal Apps



Customer problems: Solved!

Let’s recap…

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

Workload

Cisco Zero Trust for Workload

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

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

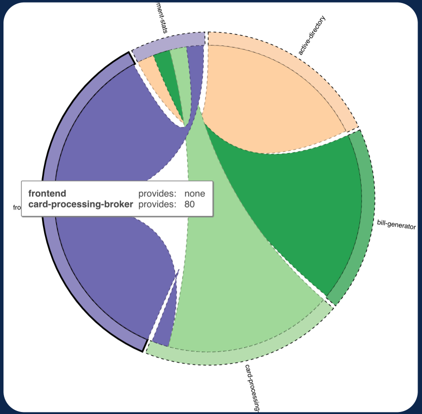
BY

Security visibility and health score

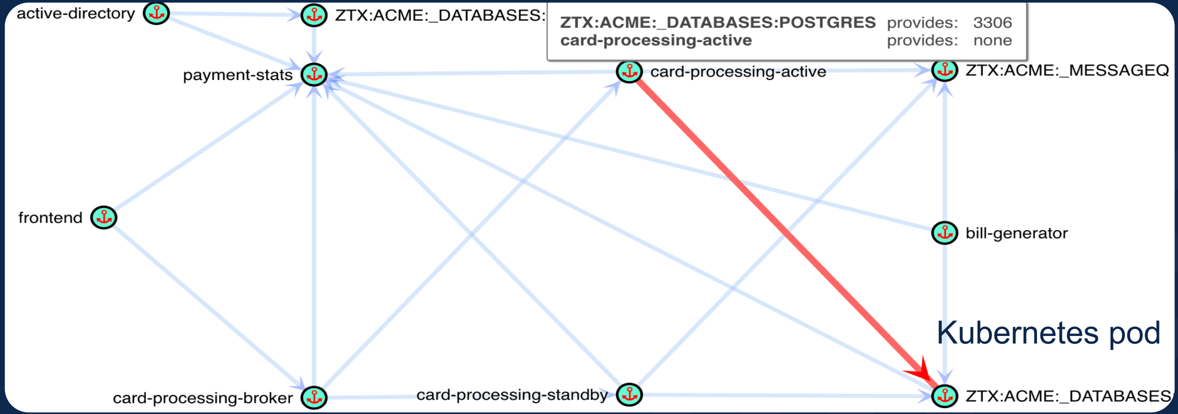
Vulnerability, anomaly, forensic and threat data

Understand your workloads

Automated discovery, clustering and policy generation



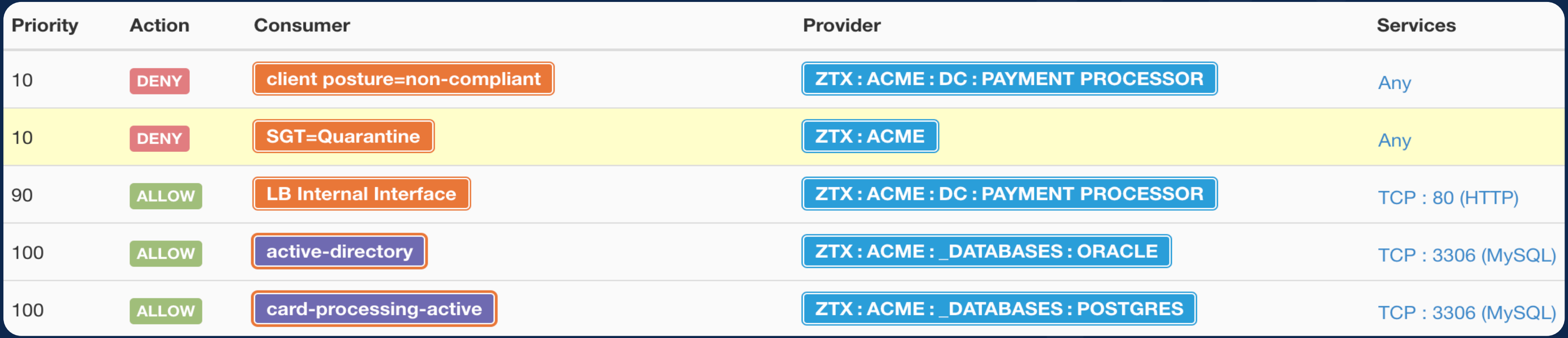
frontend	provides:	none
card-processing-broker	provides:	80



ZTX:ACME:_DATABASES:POSTGRES	provides:	3306
card-processing-active	provides:	none

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

Demo: Workload – Hybrid Cloud Segmentation

What's the customer problem?	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

Customer problems: Solved!

Let’s recap…

- Workload – Tetration – Hybrid-DC multi-tier invoicing application
  - Started with flat network, clean slate in tetration
  - 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

Demo: Workload – Continuous Trust Verification

What's the customer problem?	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.

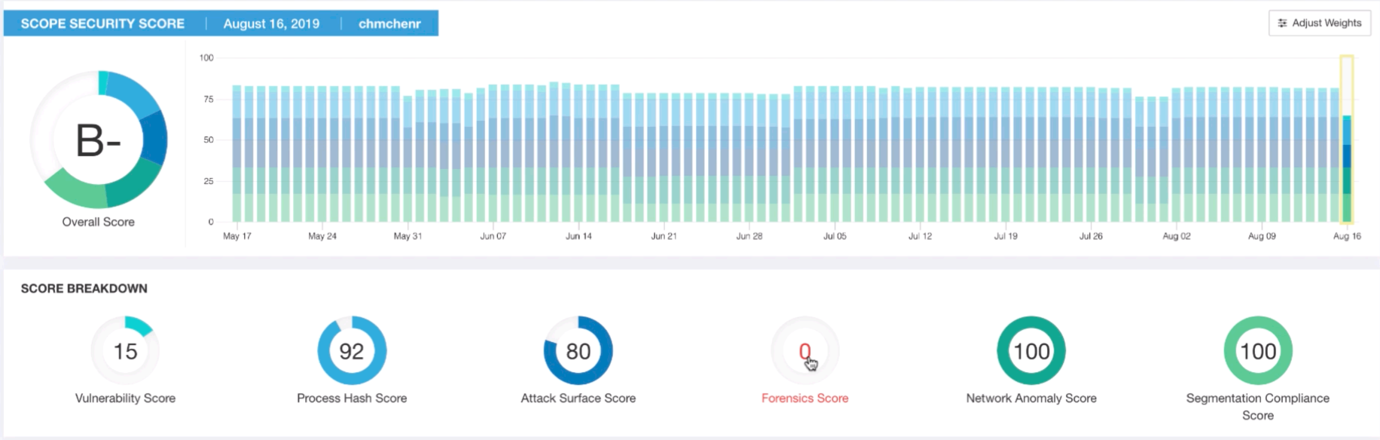
Log and Audit Everything

Customer problems: Solved!

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



SCOPE SECURITY SCORE | August 16, 2019 | chmchenr

SCORE BREAKDOWN

15	92	80	0	100	100
Vulnerability Score	Process Hash Score	Attack Surface Score	Forensics Score	Network Anomaly Score	Segmentation Compliance Score

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

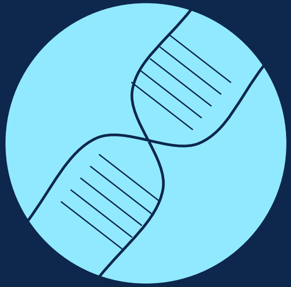
Continuous security health monitoring of devices

BY

Continuous Posture
Vulnerability assessments
Indications of compromise

DNAC: Making ZT practical in the workplace

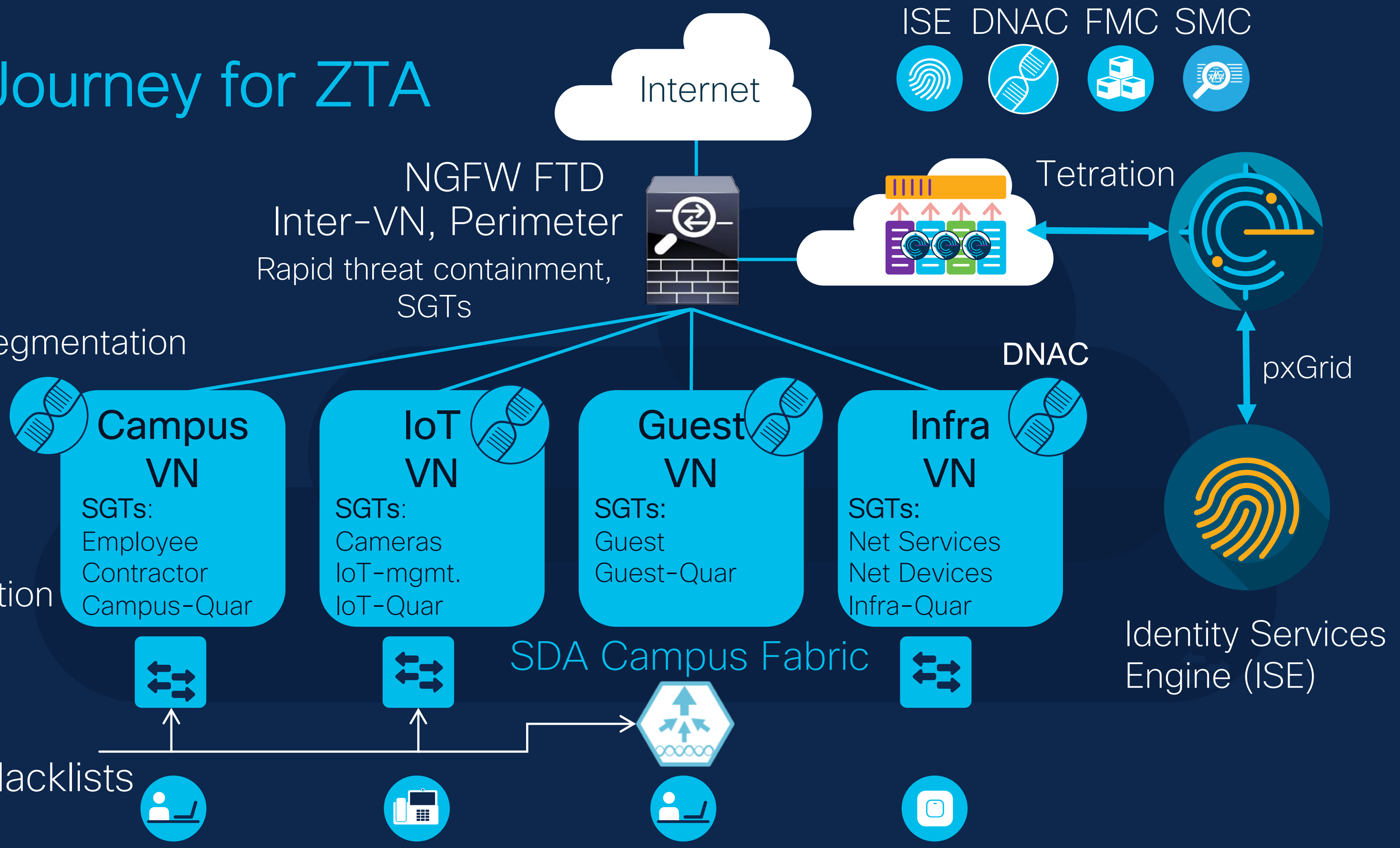
Automated, best practice grounded, deployment of Zero Trust capabilities.



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

SDA Journey for ZTA



Macro-segmentation

Virtual Networks

Micro-segmentation

802.1x
dACL Blacklists

Demo: Workplace - SDA for Wired, wireless

What’s the customer problem?	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

Customer problems: Solved!

Let’s recap…

Workspace – SD-Access – Retail payment on iPad and printer

- ISE integrated Meraki so it was able to quarantine non-compliant iPad
- ISE profiled and categorized every device, like the receipt printer
- Stealthwatch with new DNAC policy analytics tool for SGT policy

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.

Be the Bridge