



# Cisco Community Meet The Author

Meet the Authors Event- CCIE Security and Practical  
Applications in Today's Network: Zero Trust

Vivek Santuka, Mason Harris, Jamie Sanbower and Aaron Woland.  
World-class Security experts.

October 29<sup>th</sup>, 2020



## Welcome to the new “Meet Authors event”

Learn from the IT expert that literally wrote the books & content  
*“Learn more about the latest trends in cybersecurity and the alternatives to enhance your security career”*



Meet  
Author



Learn the  
Story behind



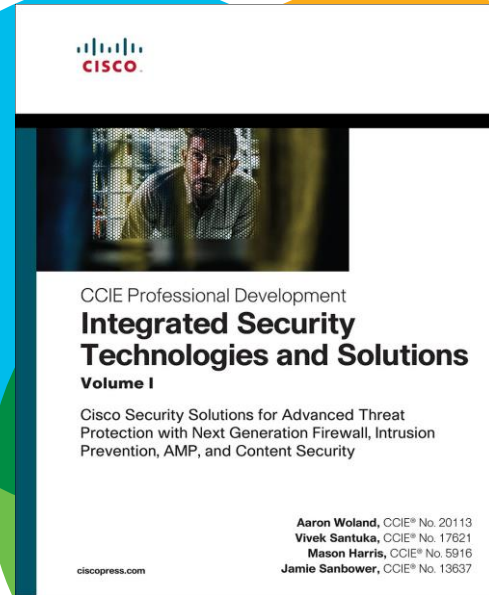
Trends &  
Key Content



Clarify  
Questions

# Win a free signed copy!

Signed by the authors



2 free copies

# Meet the Authors



**Aaron Woland**  
Principal Engineer  
CCIE #20113



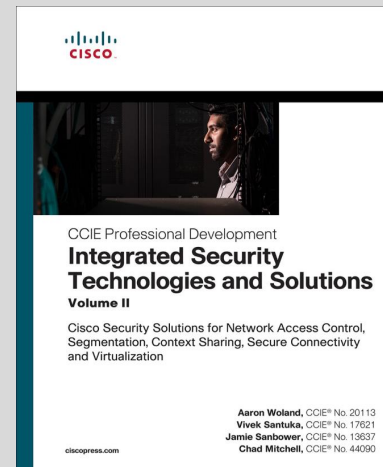
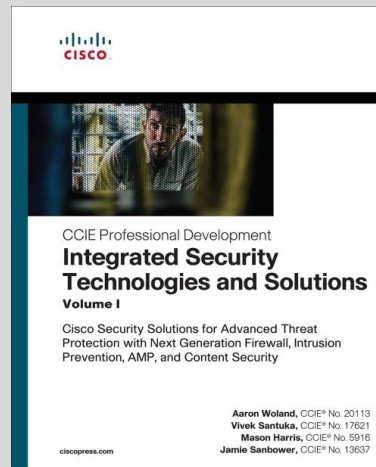
**Vivek Santuka**  
Technical Solutions  
Architect CCIE #17621



**Jamie Sanbower**  
Principal Architect  
CCIE #13637



**Mason Harris**  
Solutions Architect  
CCIE x5 #5916



Experts who combined have over 70  
years of security experience



# CCIE Security and Practical Applications in Today's Network: Zero Trust

Vivek Santuka, Technical Solutions Architect, CCIE #17621

Mason Harris, Solutions Architect, CCIE #5916

Jamie Sanbower, Principal Architect, CCIE #13637

Aaron Woland, Principal Engineer, CCIE #20113

# Meet the Authors



Aaron Woland, CCIE  
#20113, Principal Architect



Vivek Santuka, CCIE  
#17621,  
Solutions Architect

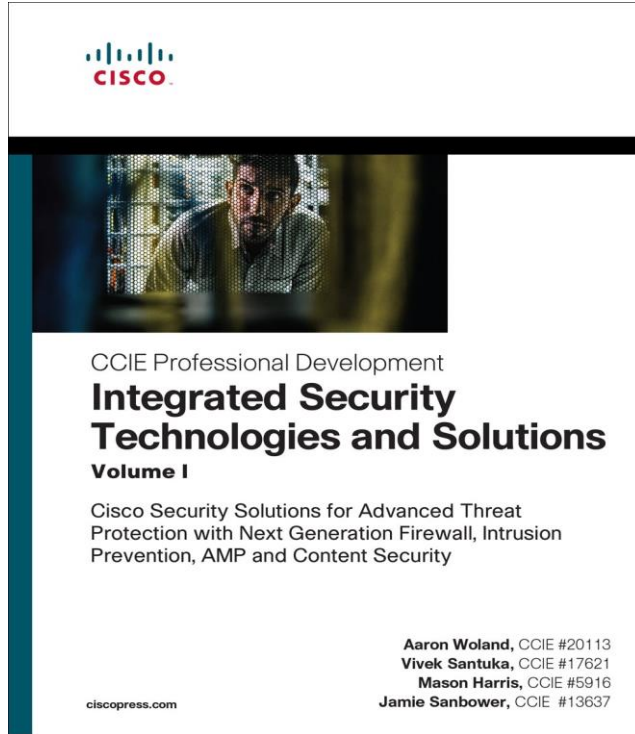


Mason Harris, CCIE #5916,  
Solutions Architect



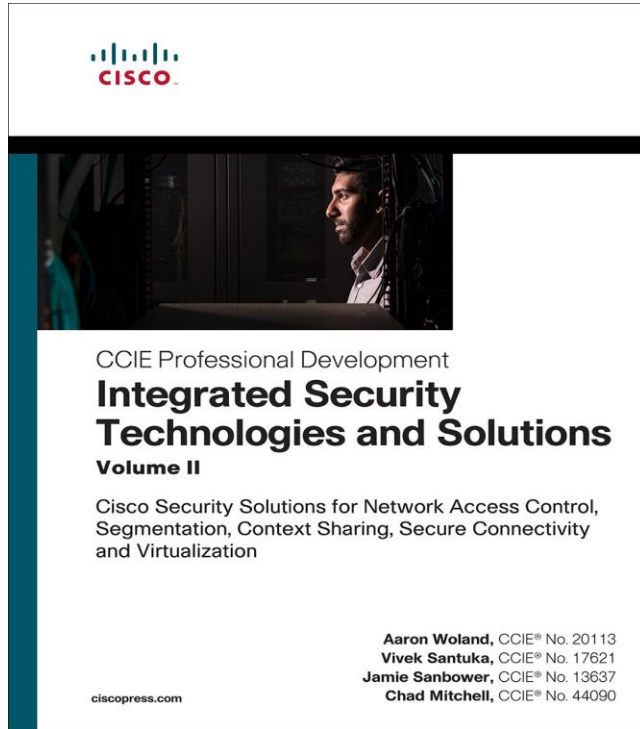
Jamie Sanbower, CCIE #13637,  
Principal Architect

# Integrated Security Technologies and Solutions I



1. Hi There! This is Network Security
  - *Infrastructure Security*
2. Deny IP any any
  - *Firewalls*
  - *IDS/IPS*
3. <HTML> EHLO. You have threat in Content </HTML>
  - *Content Security*
  - *Cisco Umbrella*
  - *Advanced Malware Protection (AMP)*

# Integrated Security Technologies and Solutions II



## 1. Knock, Knock! Who's There?

- *Access Control*
- *Cisco ISE*

## 2. Spread the Love!

- *Context Sharing*
- *PxGrid*

## 3. c2889775343d1ed91b

- *Encryption*
- *VPN*

## 4. The Red Pill

- *Virtualization*



# CCIE Security in real world

- Zero Trust

# Enabling Secure Access

Take a zero-trust approach to secure access across your entire IT environment

## Prevent Risks



## Gain Visibility



## Reduce Attack Surface



## The Zero Trust Approach

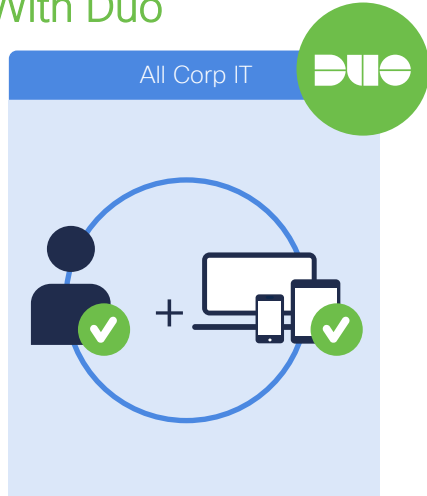
Enable policy-based controls for every access request in a corporate environment

See who and what is accessing applications, workloads and the network

Segment your network and workloads by enforcing granular controls

# Cisco Secure Zero Trust

## Secure the Workforce With Duo



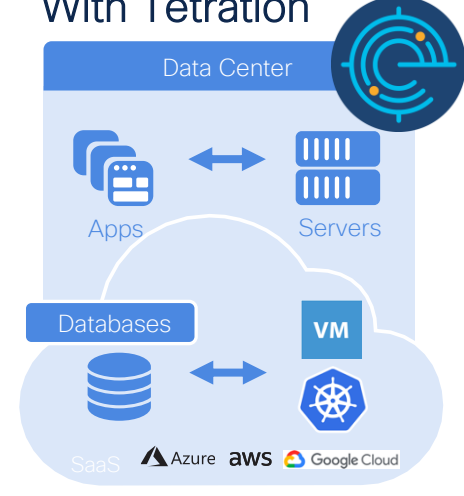
User-bound Device Access

## Secure the Workplace With SD-Access



Network Access

## Secure Your Workloads With Tetration



Workload Access

# Cisco Zero Trust Tenants



## Establish Trust

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise



## Enforce Trust-Based Access

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins



## Continuously Verify Trust

- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

# Trusted Endpoint Example

## Trusted Device Standards

Device Registration

Anti-malware

Minimum OS

Software Patching

Encryption

Rooted Device Detection (mobile only)

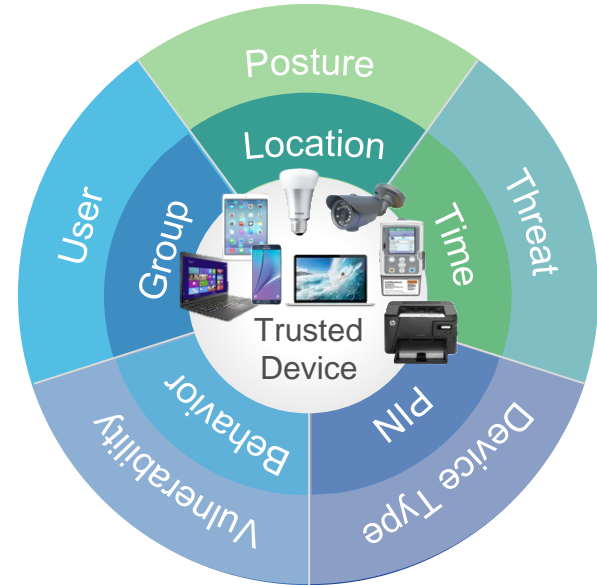
Password/Screen-lock Enforcement

Remote Wipe

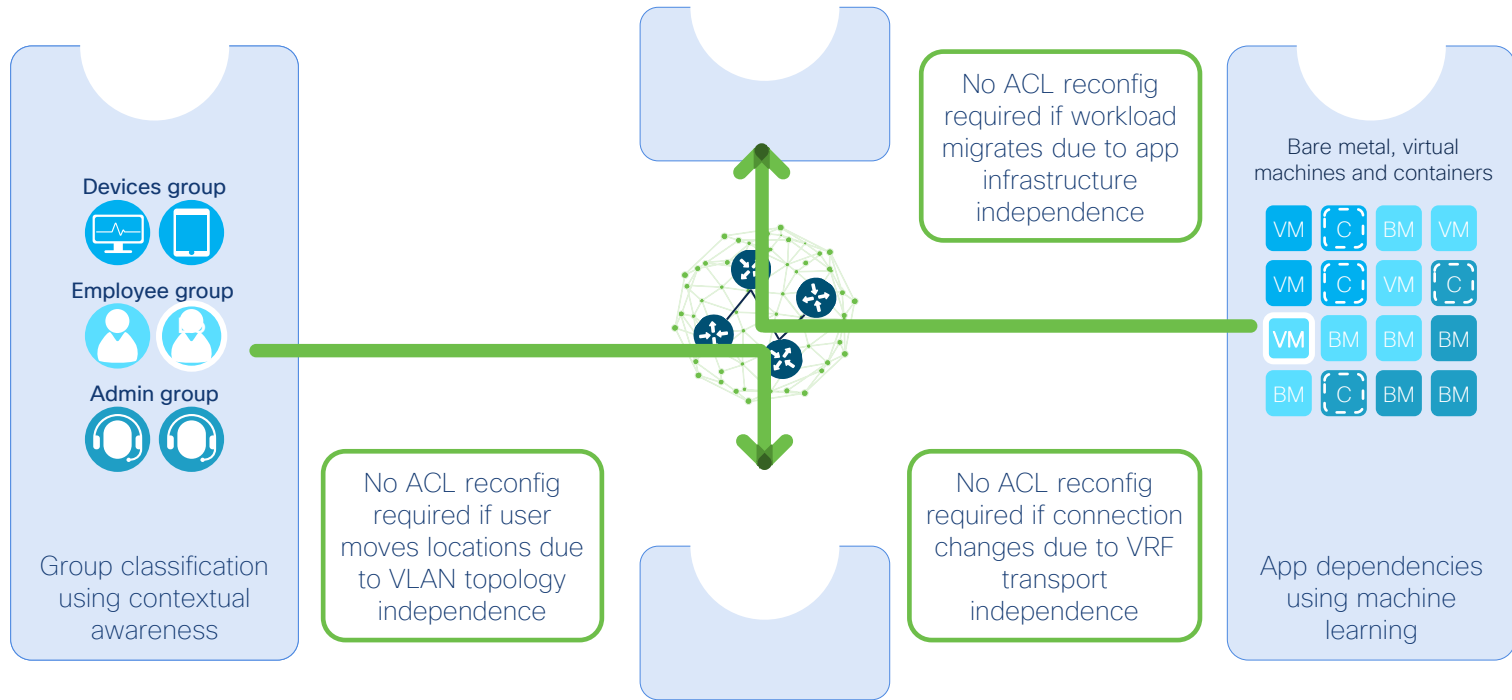
Device Management

Hardware and Software Inventory

Security Agents



# Zero-trust access follows user & app anywhere



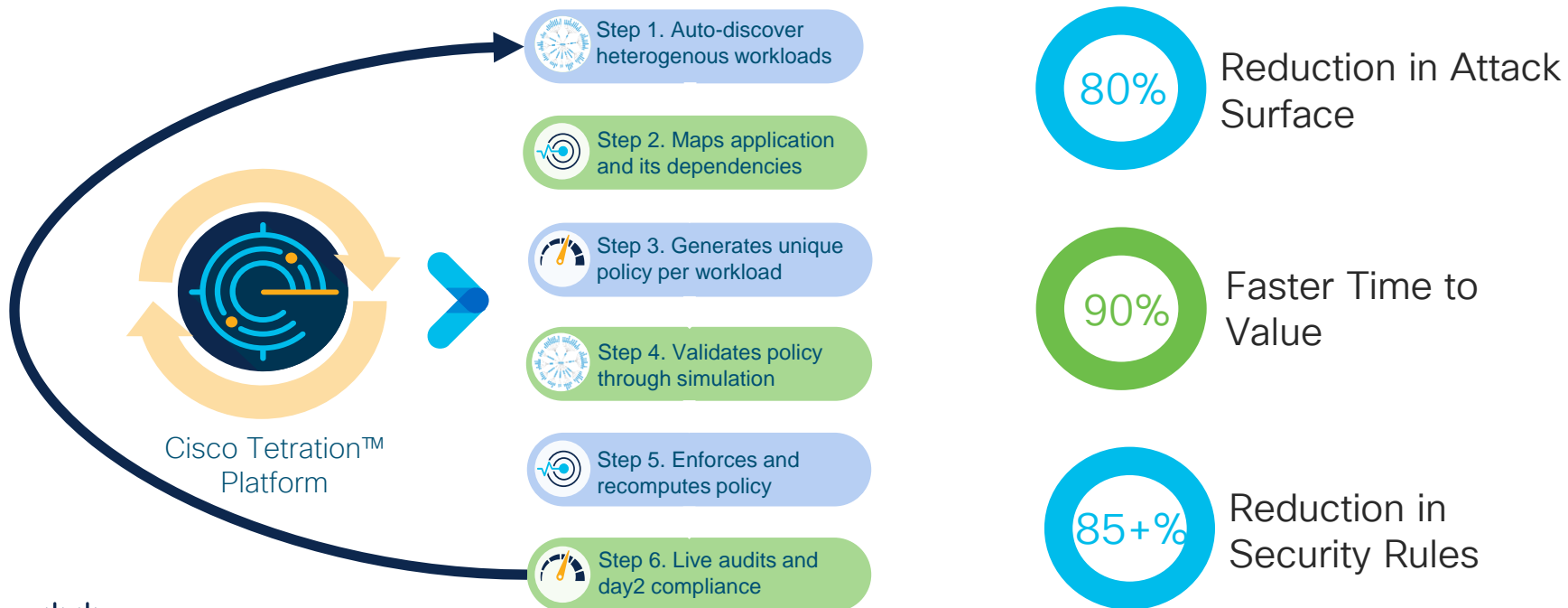
# How Cisco Duo delivers Zero Trust for your Workforce

Cisco Duo protects organizations by verifying the identity of users and the health of their devices before connecting to the applications they need.



# How Tetration delivers Zero Trust for your Workloads

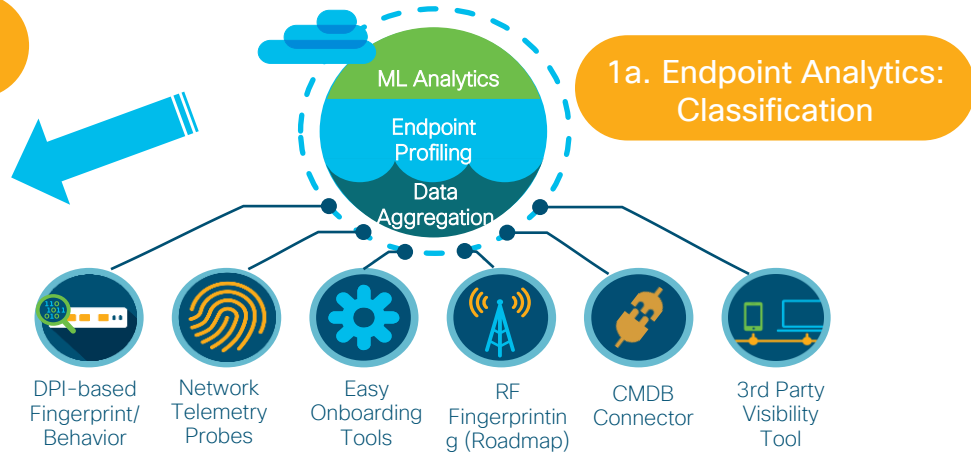
Full Life cycle policy Discovery, Management and Enforcement





# Visibility Driven Workplace Segmentation

## 1b. User Classifications

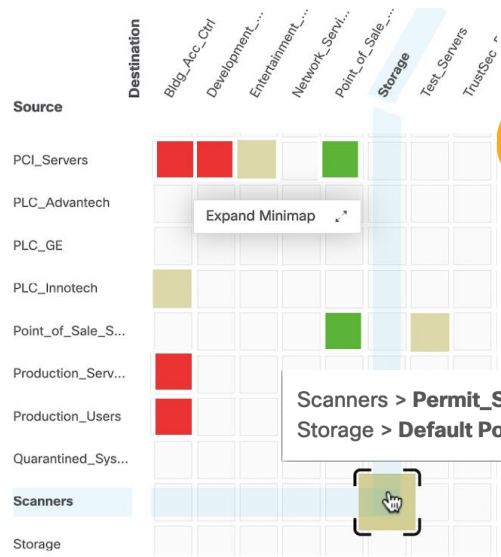


CT-Scanner → Storage

## 2. Group-Based Policy Analytics: Visibility

Filter | Create Report | Download Report | Find

Direction	Service Name	Protocol	Port
→	3m-image-lm	TCP	1550
→	acr-nema	TCP	104
→	dicom	TCP	11112



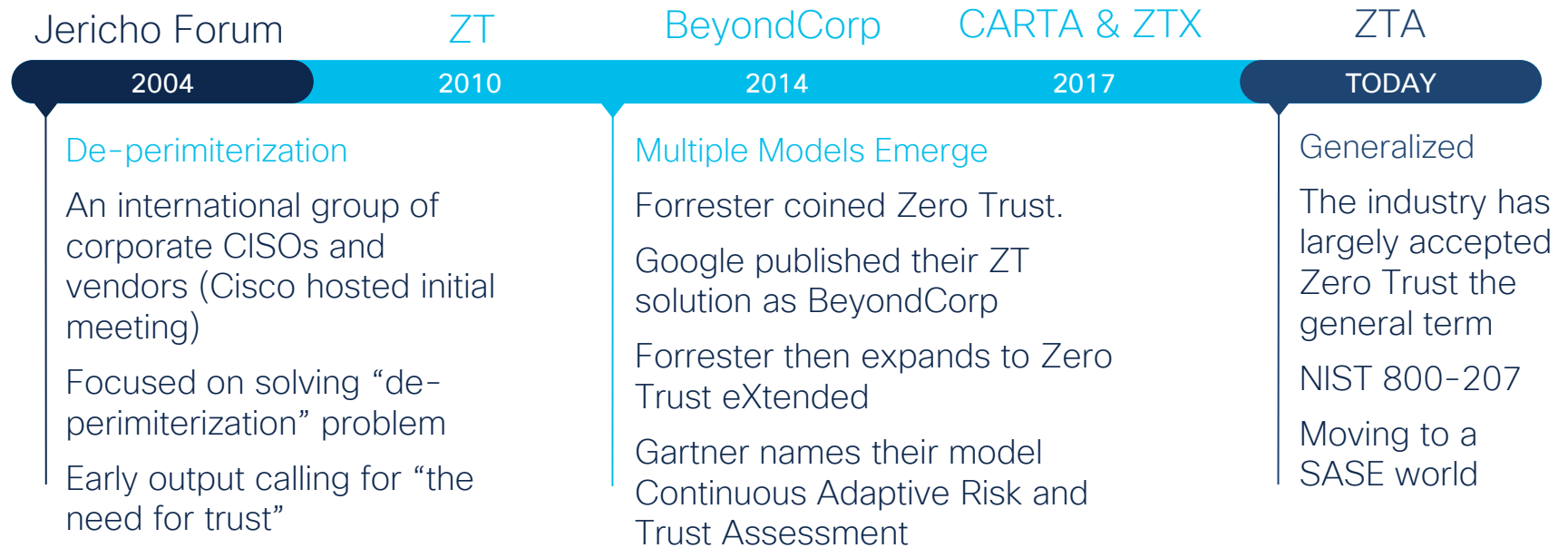
## 3. Policy Enforcement

Scanners > Permit\_Scanner2PACS\_DICOM > Storage  
Storage > Default Policy > Scanners

# Aaron want to rant about Marketing?



# A little bit of Zero Trust history



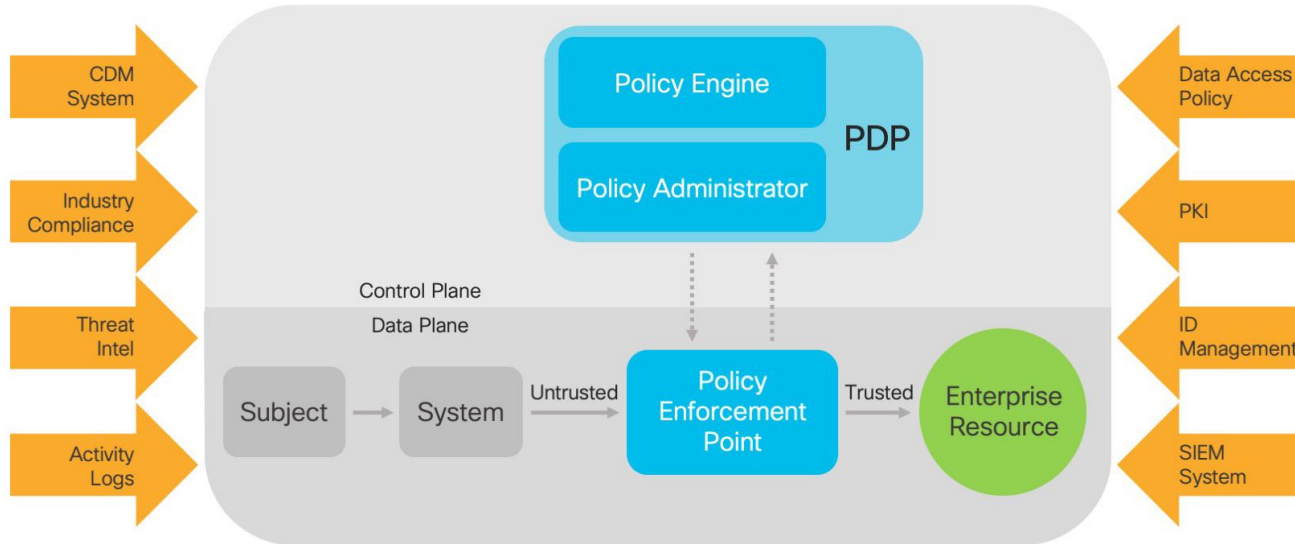


...and many more

Everyone who  
had a security  
product  
magically solves  
Zero Trust now.

# NIST 800-207: Zero Trust Architecture

## Zero Trust Architecture



Scott Rose  
 Oliver Borchert  
*Advanced Network Technologies Division  
 Information Technology Laboratory*

Stu Mitchell  
*Stu2Labs  
 Stafford, VA*

Sean Connelly  
*Cybersecurity & Infrastructure Security Agency  
 Department of Homeland Security*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-207>

August 2020



# NIST 800-207: Zero Trust Architecture

Duo | Tetration | SDA

IDP Int  
Encryptio  
n  
SWC  
Umbrella  
NGFW  
3XWs

ISE  
Tetration  
Vuln  
Partners

CDM  
System

ISE  
Duo

Industry  
Compliance

Talos  
SecureX

Threat  
Intel

Secure  
X

Activity  
Logs

Policy Engine

PDP

Policy Administrator

Control Plane  
Data Plane

Subject

System

Untrusted

Policy  
Enforcement  
Point

Trusted

Enterprise  
Resource

Data Access  
Policy

PKI

ISE

ID  
Management

Duo

SIEM  
System

SecureX

Network, Endpoint,  
Cloud, Application



Submit Your  
Questions Now!



Use the Q&A panel to submit your  
questions, our expert will respond.



# Extra Resources and References

## Volume II

Integrated Security Technologies and Solutions – Volume II: Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization [[Learn more](#)]

Other useful resources:

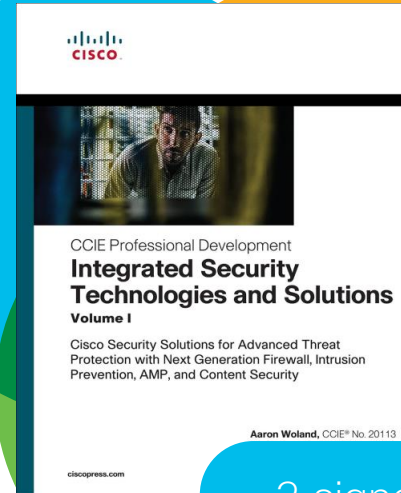
CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

<https://www.ciscopress.com/store/ccnp-and-ccie-security-core-scor-350-701-official-cert-9780135971970>

CCNP and CCIE Security Core SCOR 350-701 Complete Video Course (Video Training)

<https://www.ciscopress.com/store/ccnp-and-ccie-security-core-scor-350-701-complete-video-9780136583363>

Congratulations  
winners!



2 signed books

We'll contact you via email

# Thank you for Your Time!

Please help to complete the survey

Your opinion is important and help us to improve



*Thanks For Joining today!*

