Hitachi Vantara

RED SIFT

Skyline
Advanced Technology Services

ONSTAK

algosec

AppOmni

AMD

imagicle®

NUTANIX

Megaport

wyebot™

The bridge to possible

Zero Trust Network Segmentation

Bill Clay III, CISSP
Technical Security Architect
Cisco Tech Day Colorado

cisco Engage

#CiscoEngage

Story Time!
Gather Around....

Little Boy Billy vs His First Polymorphic Worm

Once upon a time...

Billy got his first security role!

International Law Firm - IT Service

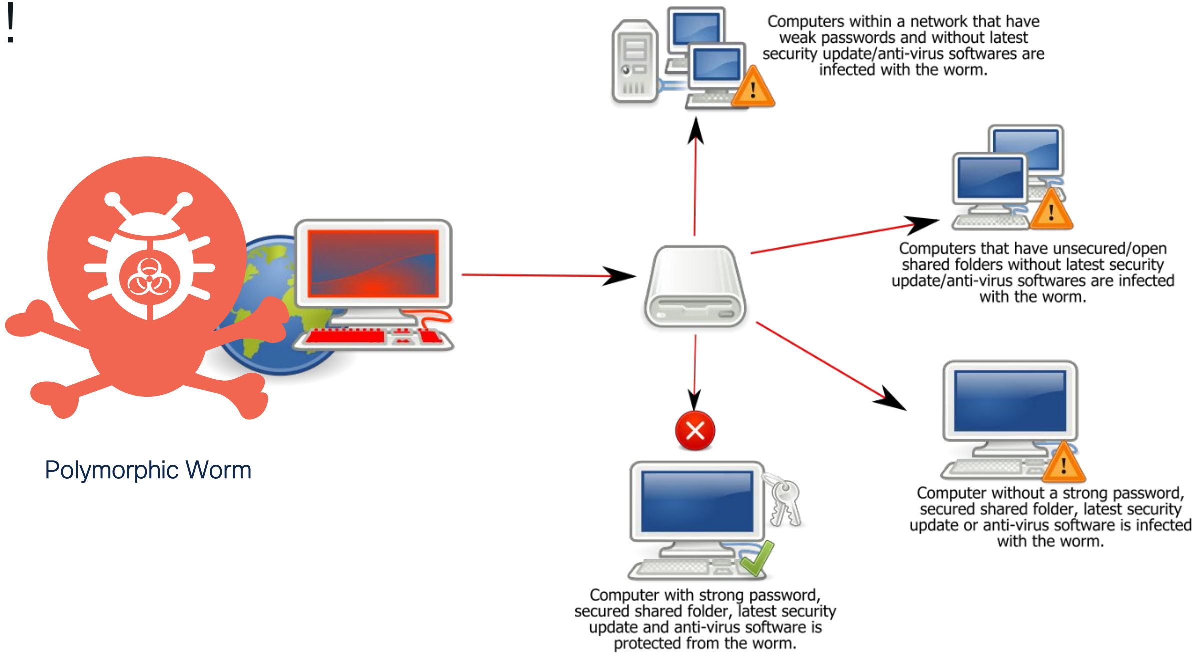
Basic Endpoint Antivirus, Stateful Firewall,
No SIEM... Not much else

2 Person Security Team, Billy as the Analyst!

Little Boy Billy vs His First Polymorphic Worm

Enter... conflict!
Malware!

Worm:Win32 Conficker



Polymorphic Worm

Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.

Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.

Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.

Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

Little Boy Billy vs His First Polymorphic Worm

Let's see if you can guess what happened next!

slido

Please download and install the Slido app on all computers you use

Join at slido.com #3465044

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

How many windows hosts were infected at the time the threat was discovered?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

How much time do you think it took Little Boy Billy and team to eradicate the worm and fully recover?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Has anyone here experienced a business outage that would not have been as bad if network segmentation was better?

ⓘ Start presenting to display the poll results on this slide.

Next time this happens...

how can we save Little Boy Billy and team?

Agenda

- Modern Zero Trust
- Cisco Secure Firewall
- Cisco Identity Services Engine
- Cisco Secure Workload / Hypershield
- Zero Trust Strategy
- Segmentation Strategy & Architectures

Modern Zero Trust

slido

Please download and install the Slido app on all computers you use

What is the first word that comes to mind when thinking about Zero Trust?

ⓘ Start presenting to display the poll results on this slide.

Zero Trust Principles

- Never assume trust
- Always verify
- Enforce least privilege

Zero Trust is maturing

Emergence of regulations and standards

It’s segmentation

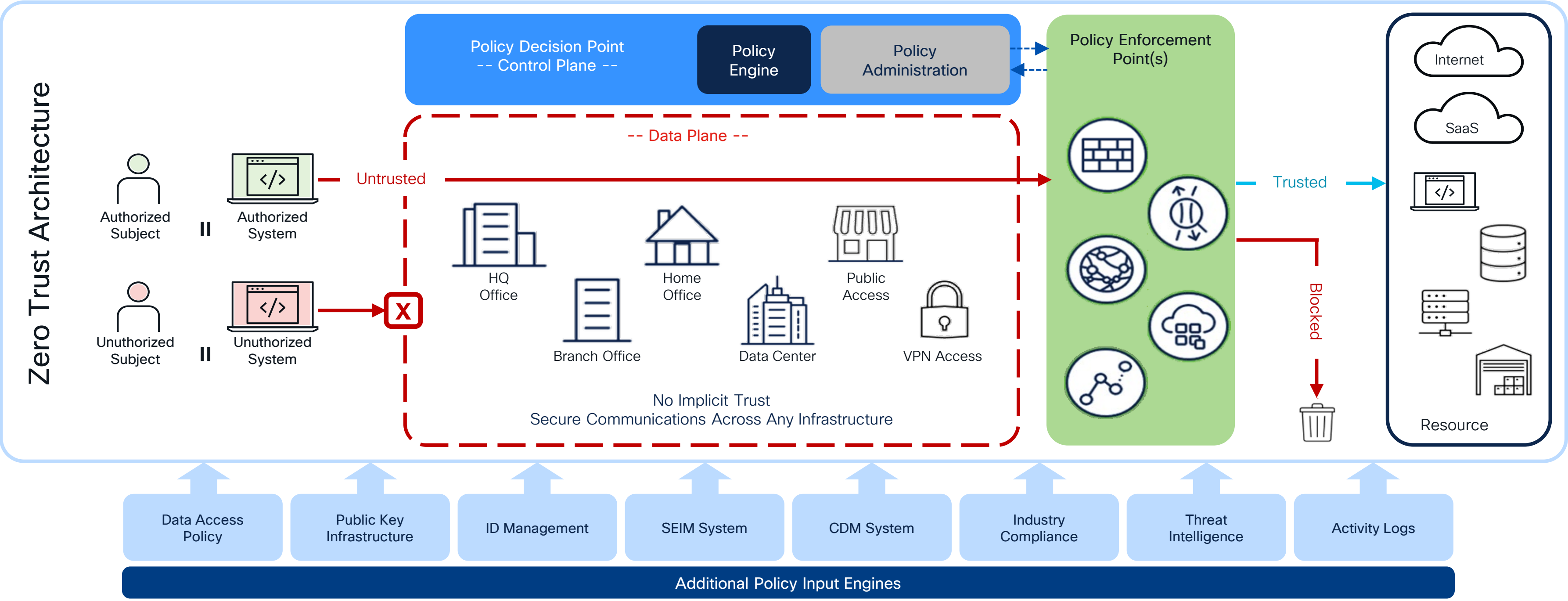
It’s ZTNA

It’s endpoint security

It’s firewall

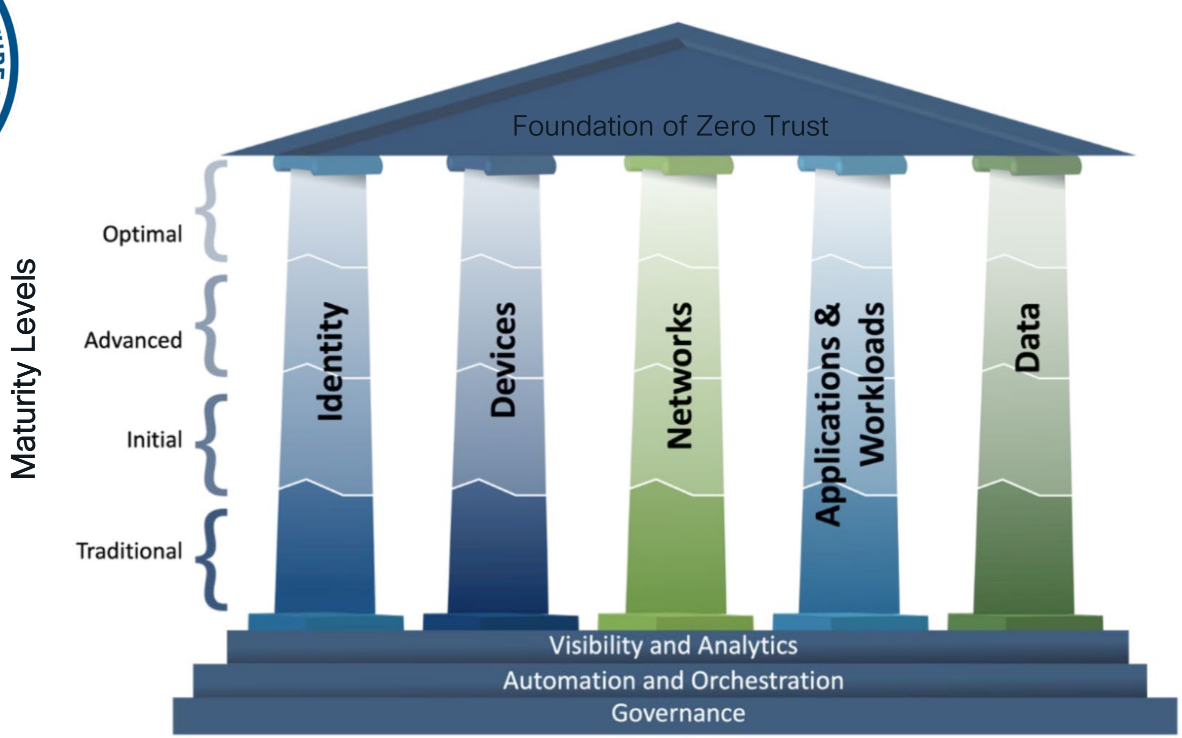
It’s identity

NIST Special Publication 800-207
Zero Trust Architecture



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

CISA Zero Trust Maturity Model



Segmentation spans all pillars!

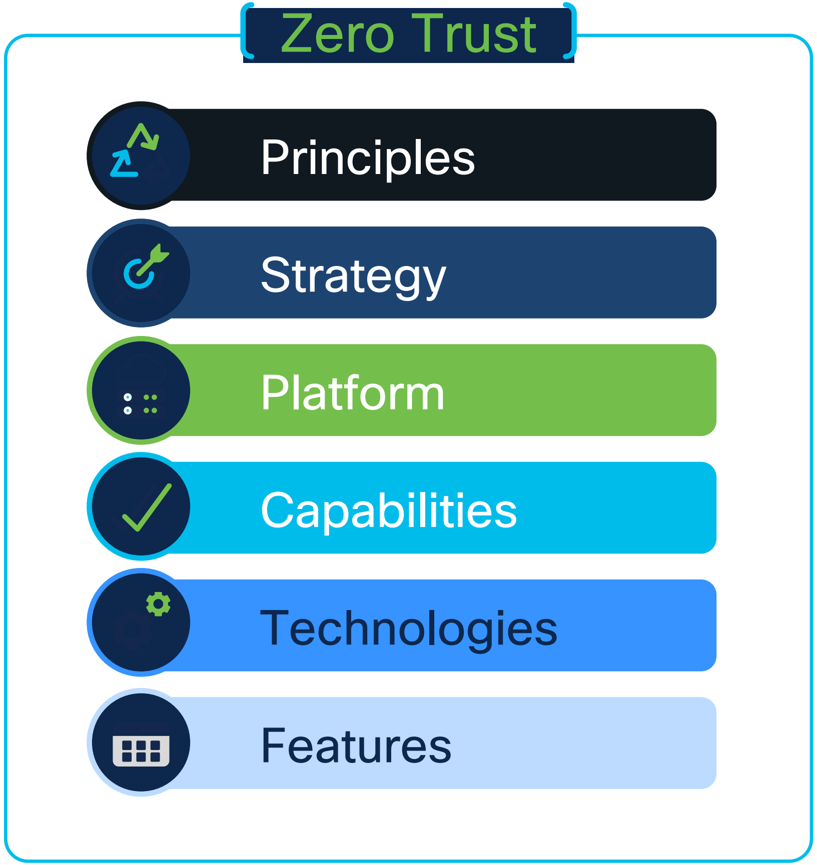
Dynamic – Continuous – Integrated – Optimized – Automated

https://www.cisa.gov/zero-trust-maturity-model

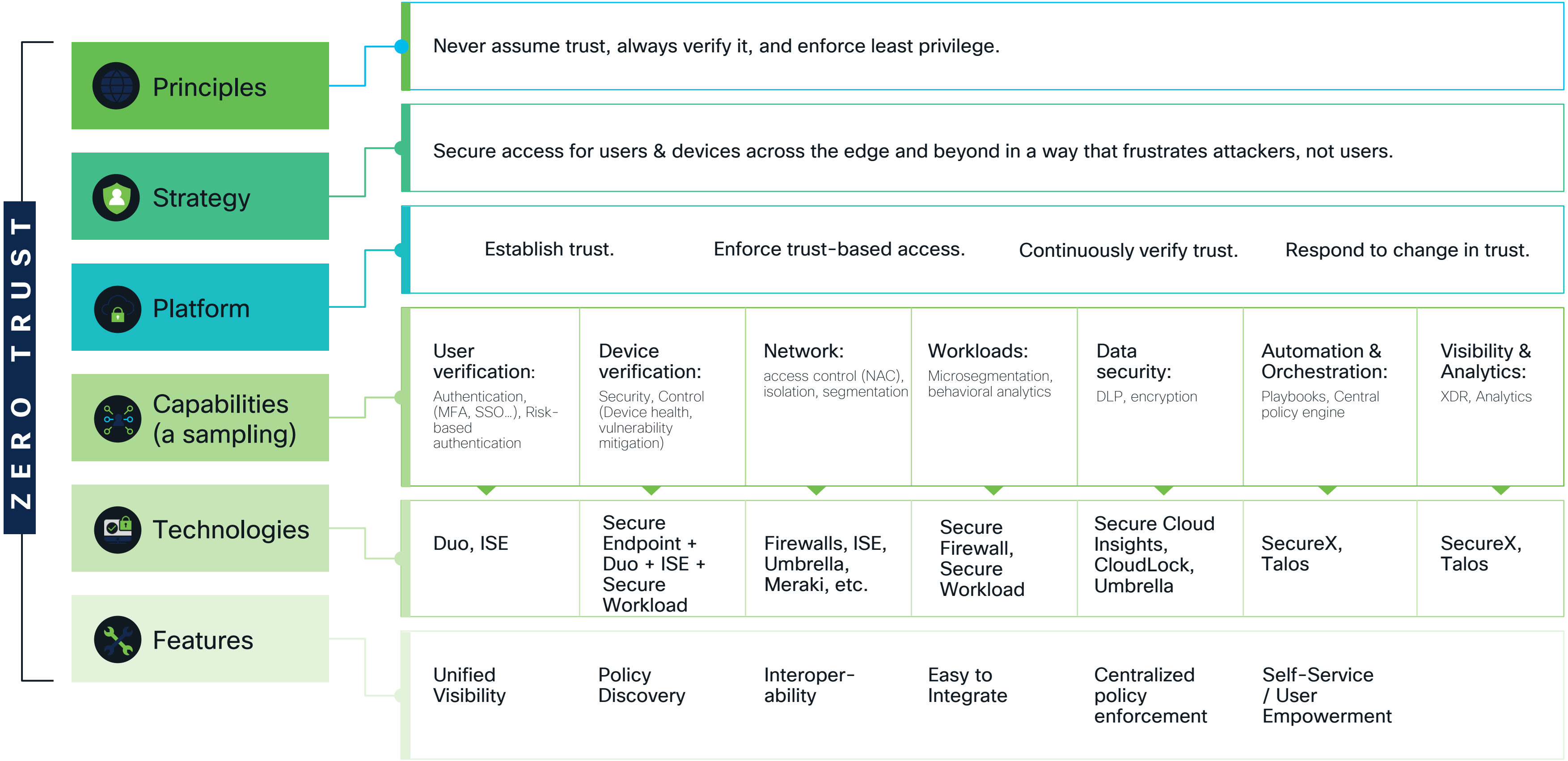
Zero Trust Frameworks

Cisco	NIST 800-207 Zero Trust Architecture	CISA Zero Trust Maturity Model	DISA Zero Trust Framework	Common
User and Device Security	Users and/or Devices	Identity	Users	Visibility & Analytics Automation & Orchestration Governance
		Devices	Devices	
Network and Cloud Security	Policy Decision and Enforcement Points	Networks	Network/ Environment	
Application and Data Security	Enterprise Resources	Applications and Workloads	Workloads	
		Data	Data	

Zero Trust Must Be Driven Top-Down



Zero Trust Top-Down Strategy



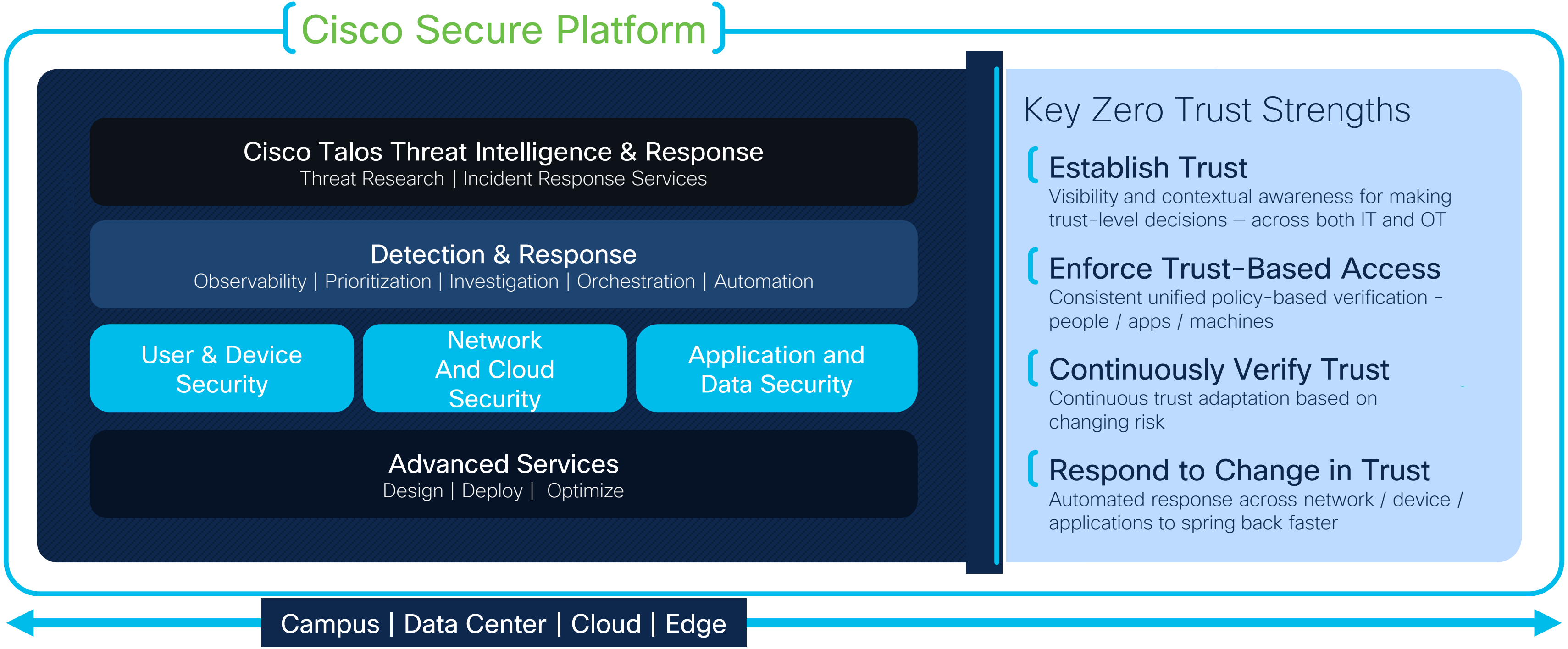
Principles: Never assume trust, always verify it, and enforce least privilege.

Strategy: Secure access for users & devices across the edge and beyond in a way that frustrates attackers, not users.

Platform: Establish trust. Enforce trust-based access. Continuously verify trust. Respond to change in trust.

Capabilities (a sampling)	Technologies	Features
User verification: Authentication, (MFA, SSO…), Risk-based authentication	Duo, ISE	Unified Visibility
Device verification: Security, Control (Device health, vulnerability mitigation)	Secure Endpoint + Duo + ISE + Secure Workload	Policy Discovery
Network: access control (NAC), isolation, segmentation	Firewalls, ISE, Umbrella, Meraki, etc.	Interoper-ability
Workloads: Microsegmentation, behavioral analytics	Secure Firewall, Secure Workload	Easy to Integrate
Data security: DLP, encryption	Secure Cloud Insights, CloudLock, Umbrella	Centralized policy enforcement
Automation & Orchestration: Playbooks, Central policy engine	SecureX, Talos	Self-Service / User Empowerment
Visibility & Analytics: XDR, Analytics	SecureX, Talos	

Delivering Zero Trust to meet you where you are



Cisco Secure Platform

Cisco Talos Threat Intelligence & Response
Threat Research | Incident Response Services

Detection & Response
Observability | Prioritization | Investigation | Orchestration | Automation

User & Device Security

Network And Cloud Security

Application and Data Security

Advanced Services
Design | Deploy | Optimize

Key Zero Trust Strengths

Establish Trust
Visibility and contextual awareness for making trust-level decisions – across both IT and OT

Enforce Trust-Based Access
Consistent unified policy-based verification - people / apps / machines

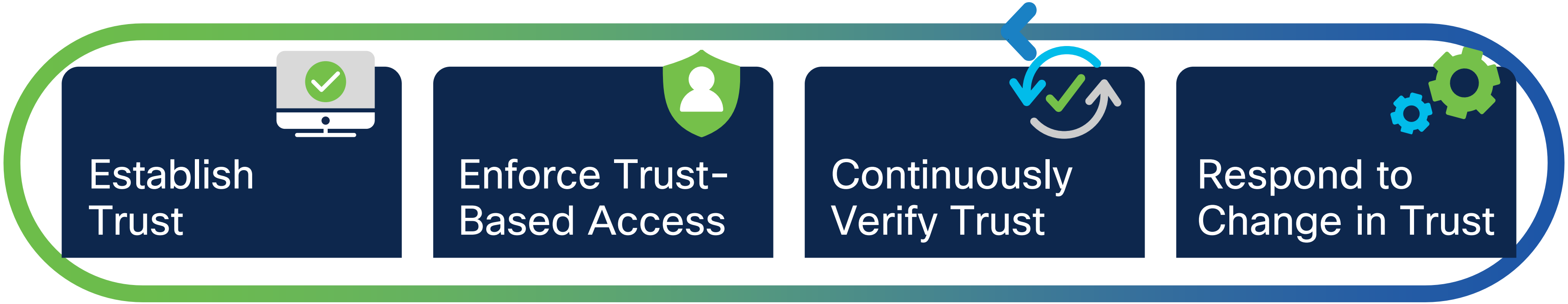
Continuously Verify Trust
Continuous trust adaptation based on changing risk

Respond to Change in Trust
Automated response across network / device / applications to spring back faster

Campus | Data Center | Cloud | Edge

Zero Trust Platform Requirements

What it takes to get Zero Trust right



Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust

Zero Trust Maturity

What it takes to get Zero Trust right

Establish Trust

- User & Device Trust
- Network Profiling & Posture
- Identity Analytics

Enforce Trust-Based Access

- Segmentation
- Microsegmentation
- Network Access Control

Continuously Verify Trust

- Re-assessment of trust
- Shared signals
- Behavior monitoring – threat and non-threat activity
- Vulnerability management
- Indicators of compromise

Respond to Change in Trust

- Trust Response Engine
- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

User & Device Security ← → Network & Cloud Security ← → Application & Data Security

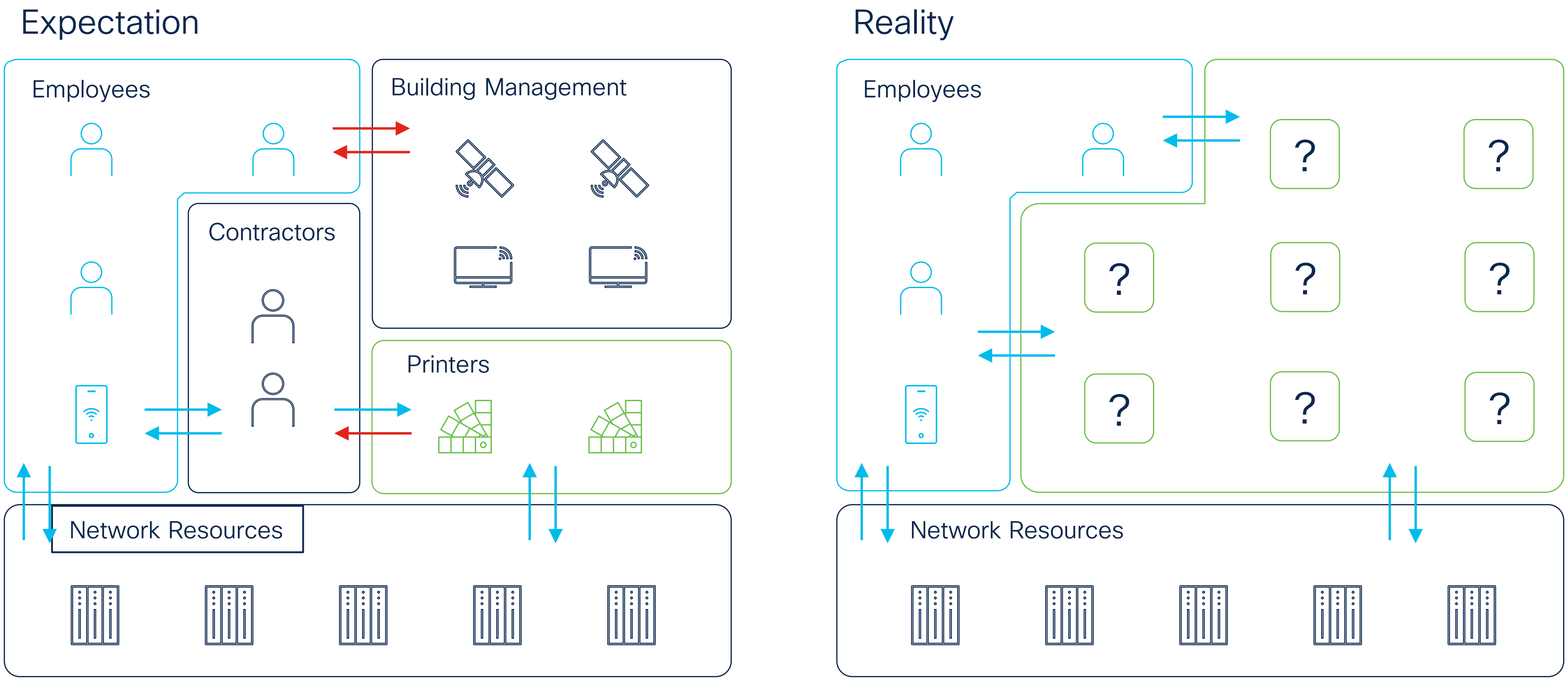
slido

Please download and install the Slido app on all computers you use

What is the first word that comes to mind when thinking about network segmentation?

ⓘ Start presenting to display the poll results on this slide.

Least Privilege Access: Expectation vs. Reality

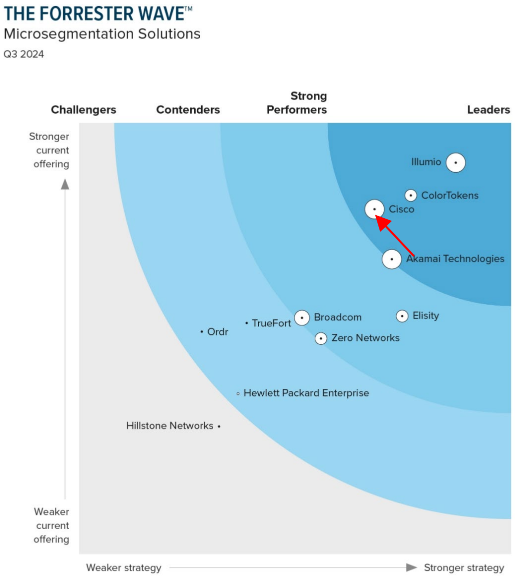


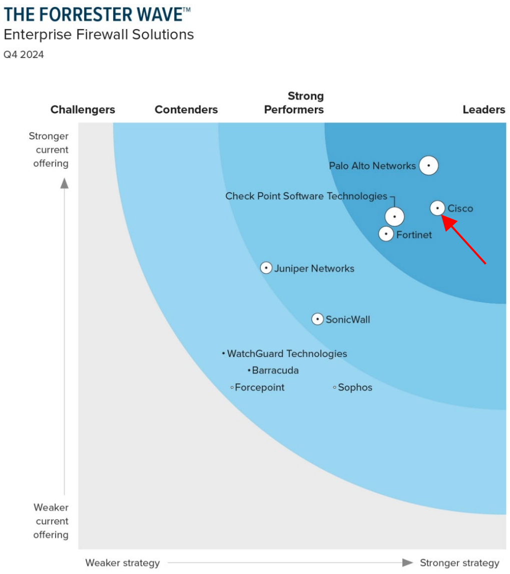
Network Segmentation Benefits

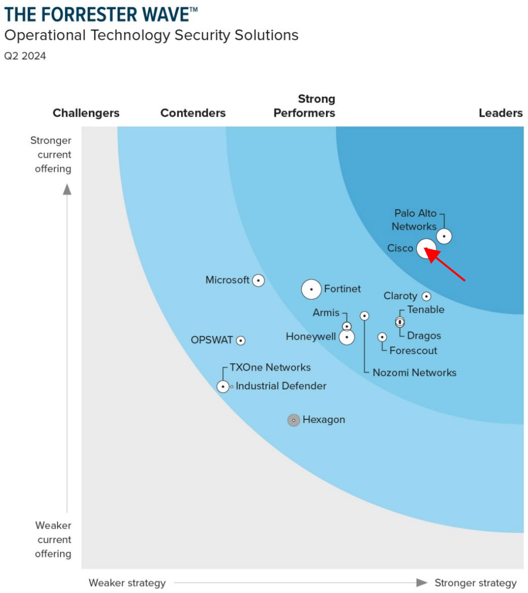
Visibility and control doesn't stop at the end user

Threats	Zero Trust Solution
Unauthorized endpoints or devices with unhygienic posture can disrupt productivity	No network access until endpoint trust is evaluated (authenticate and evaluate system health)
Noncritical assets with unrestricted access can make the entire infrastructure vulnerable	Provide confined access to essential services through macro and micro-segmentation
Compromised endpoints can infect other assets in the network through lateral movements	Continuously evaluate trust and apply adaptive controls to isolate threats in the real-time

Cisco – Market Leader in Segmentation

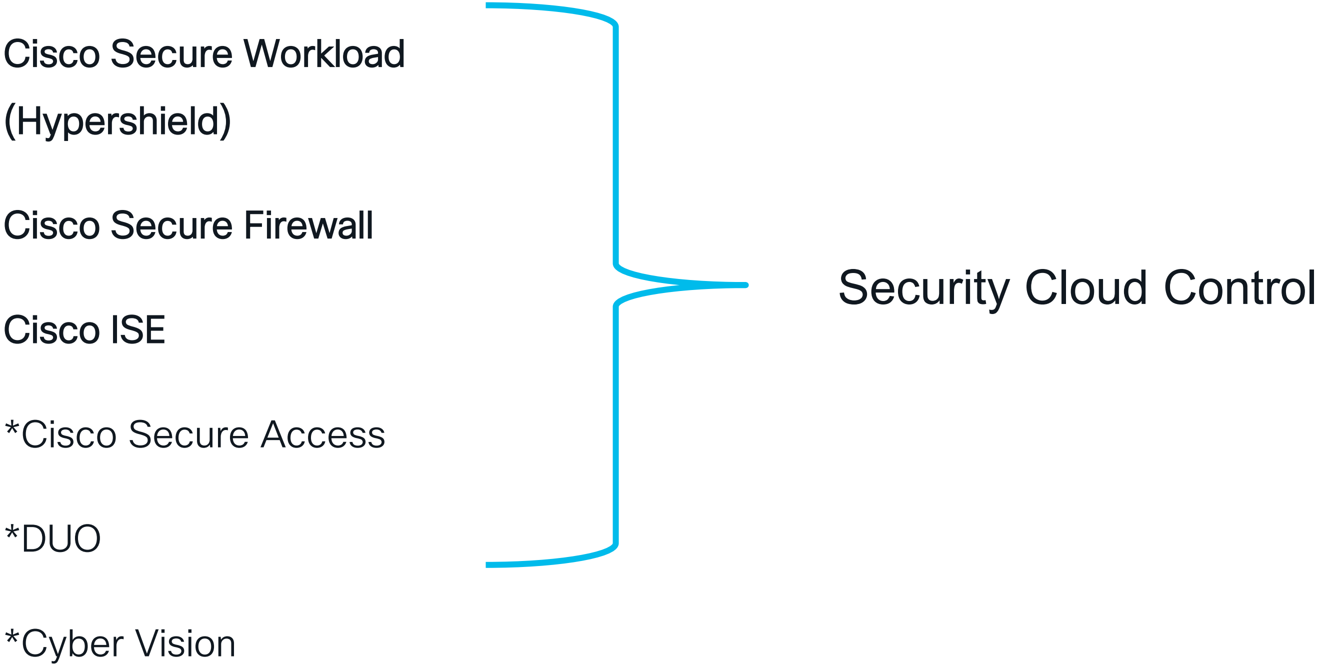






The ONLY cybersecurity company named a Leader in Microsegmentation, Enterprise Firewall, and OT Security

Cisco Network Segmentation Solutions for Zero Trust



Cisco Secure Workload (Hypershield)

Cisco Secure Firewall

Cisco ISE

*Cisco Secure Access

*DUO

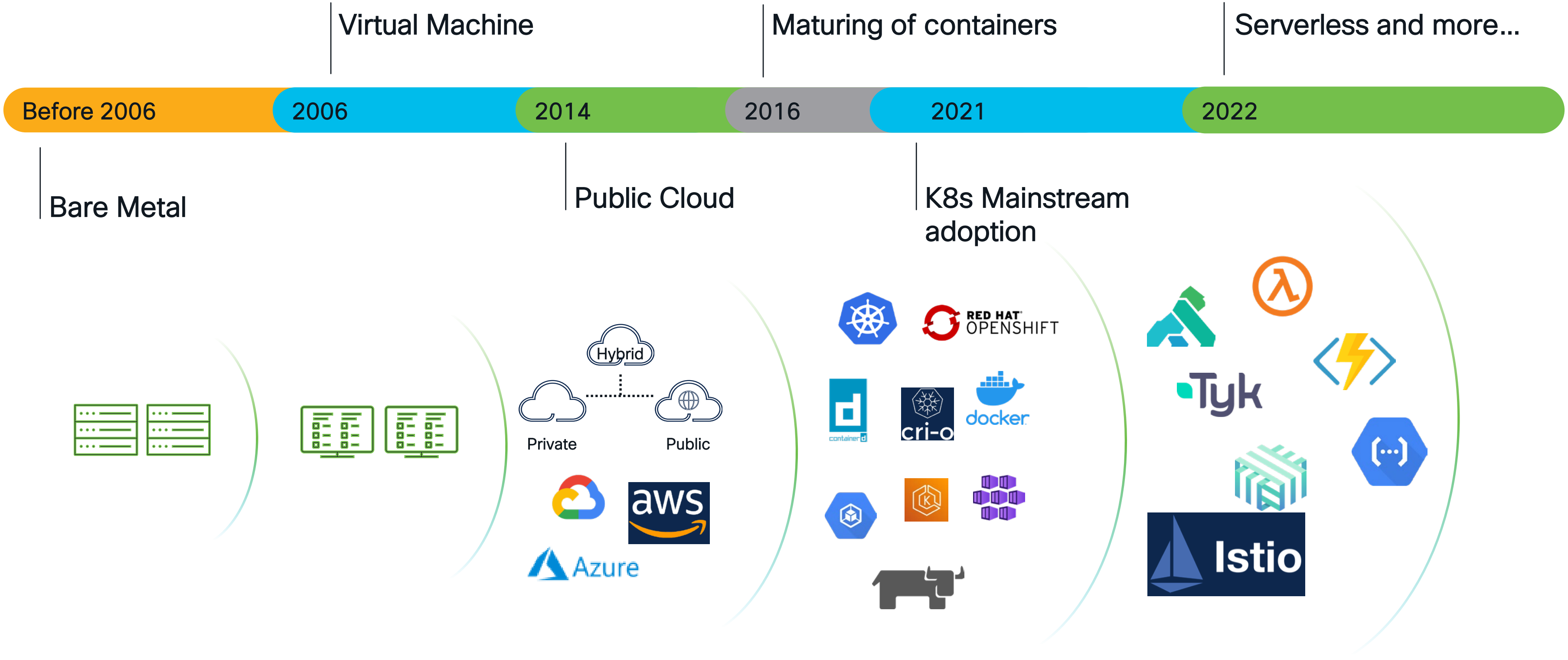
*Cyber Vision

Security Cloud Control

Cisco Secure Workload

Application Workload Evolution

Workload Security is Getting More Complex!



Virtual Machine

Maturing of containers

Serverless and more...

Before 2006

2006

2014

2016

2021

2022

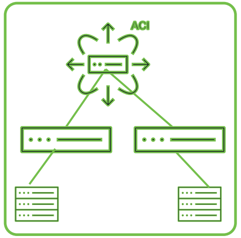
Bare Metal

Public Cloud

K8s Mainstream adoption

But... what is an application workload?

Network Engineer



- Vlans/VRF
- Subnets
- Contracts

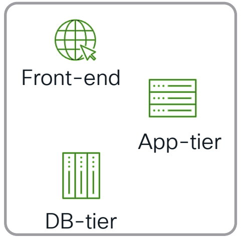
Firewall Engineer

- Zones
- Subnets
- ACLs

Cloud Engineer

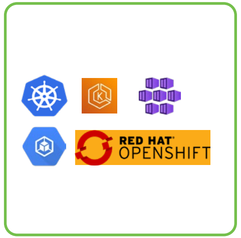
- VPC
- Subnets
- Security Groups

Application Owners



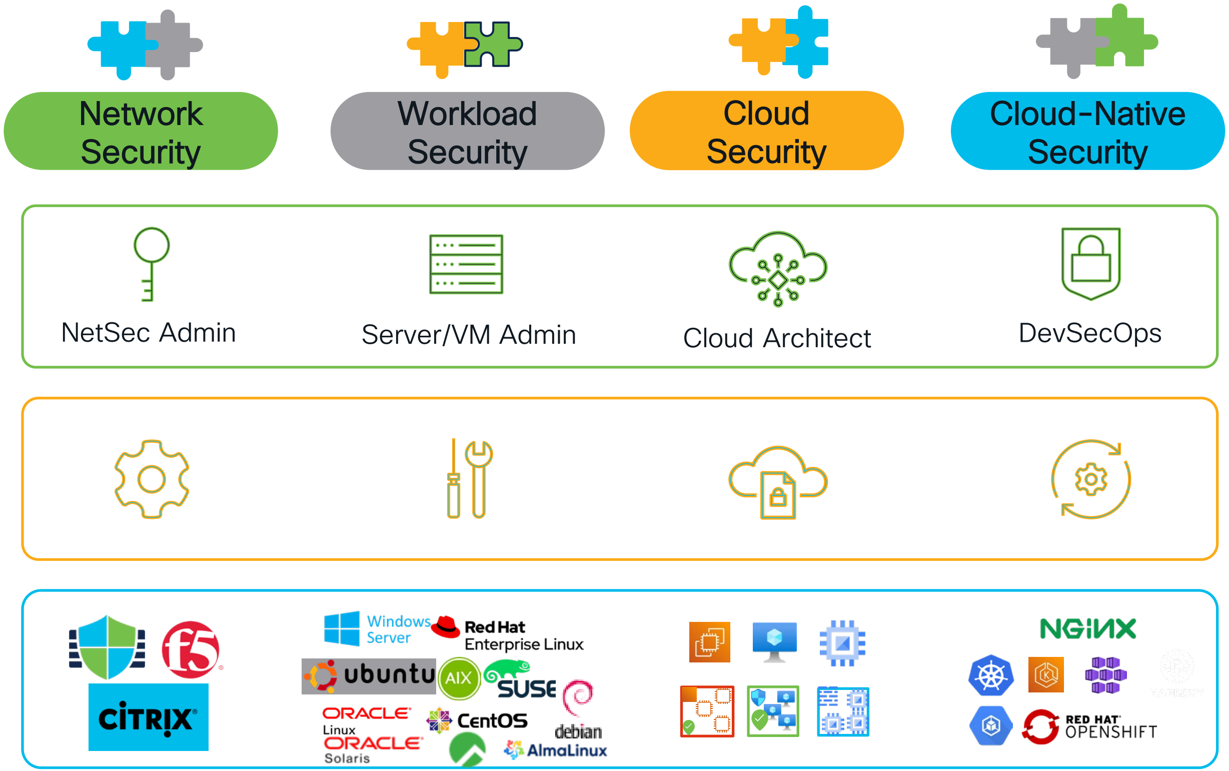
- Service
- Application
- Workload

Cloud-Native Engineer



- Namespace
- Service
- CNI

Segmentation and Policy Control Challenges



Network Security

Workload Security

Cloud Security

Cloud-Native Security

NetSec Admin

Server/VM Admin

Cloud Architect

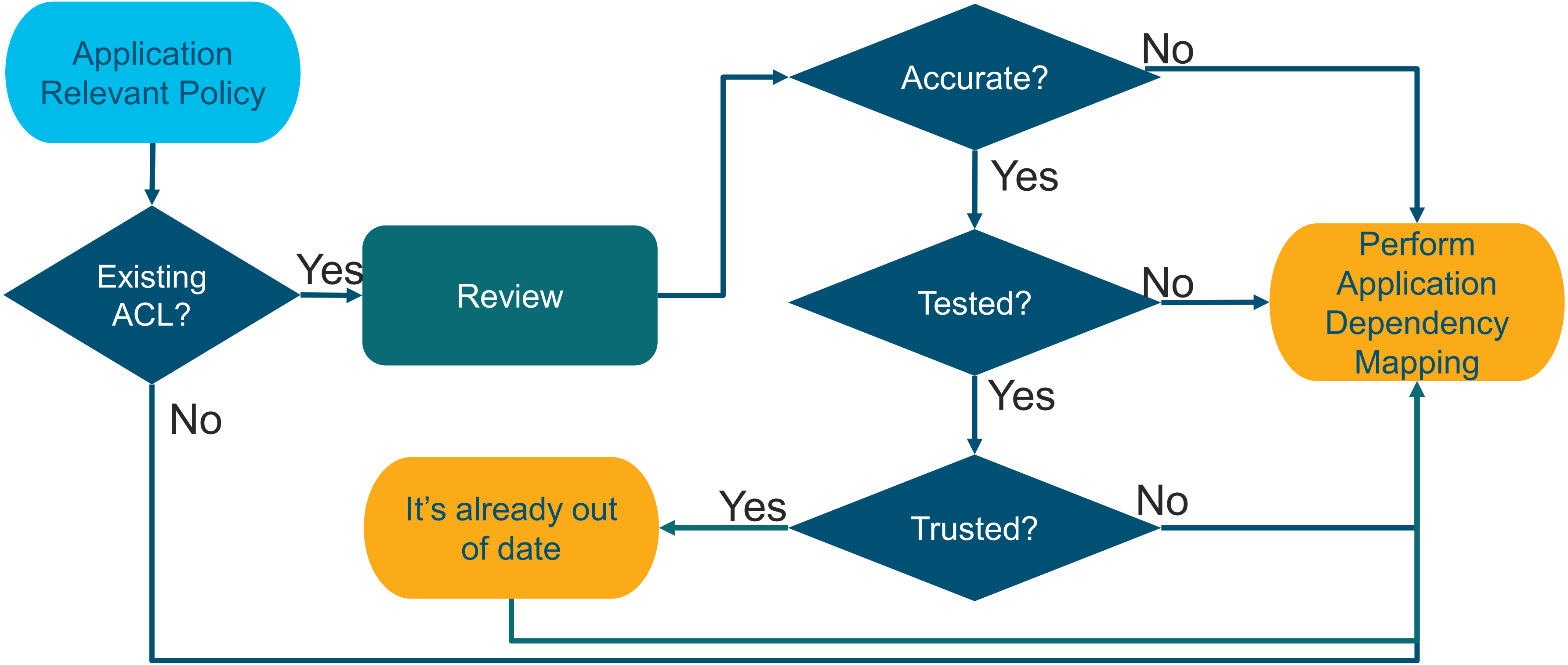
DevSecOps

Organizational Challenges

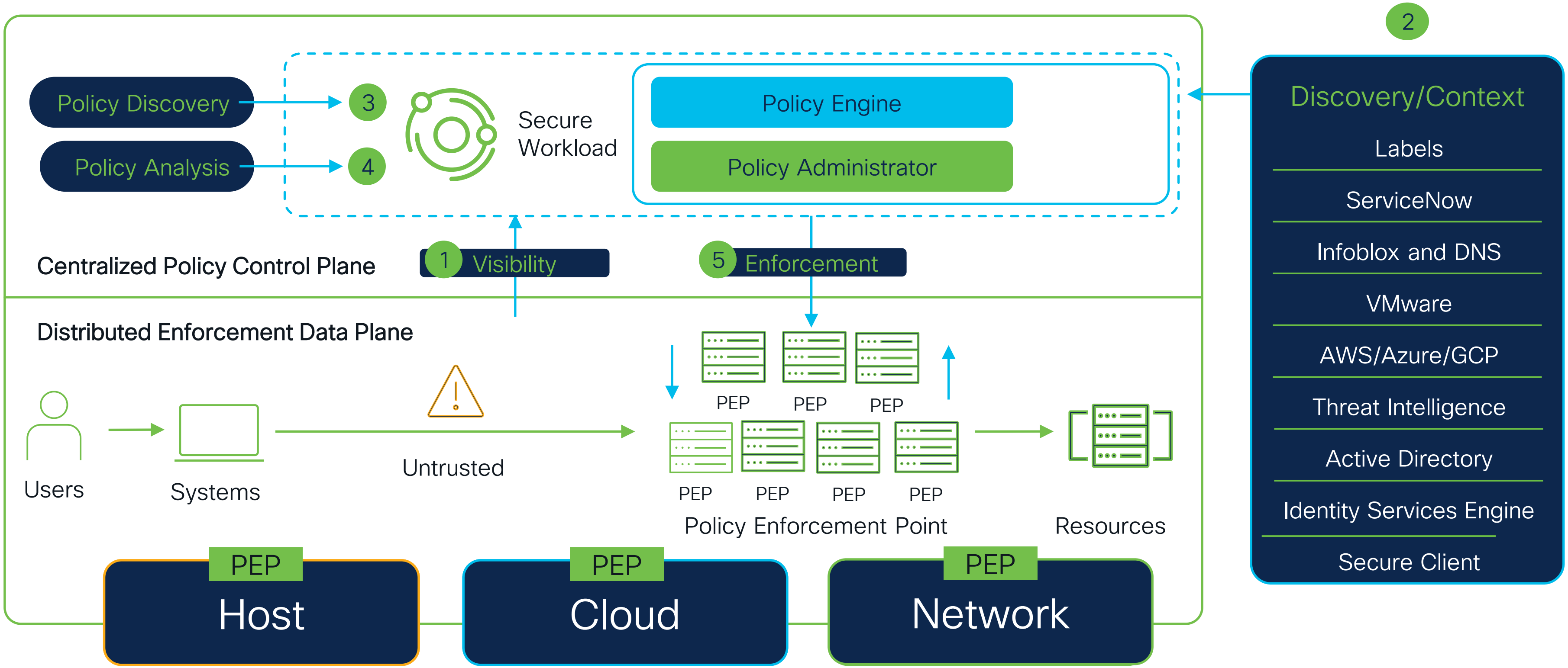
Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

How well do you understand your applications?



Secure Workload – Zero Trust Segmentation



Secure Workload Use-Cases

Microsegmentation

Behavioral detection and protection

Vulnerability detection and protection

Microsegmentation Approach Evaluation

	Agent	Agentless
Pros	• Network Abstraction • In-depth visibility and protection • Flexible segmentation	• Less organizational dependencies • Leverage existing infrastructure • Faster time to deploy
Cons	• Organizational dependencies • OS dependency (legacy) • Agent fatigue	• Network/CSP infrastructure dependency • Segmentation granularity/scalability • Only network-flows visibility

Cisco Secure Workload Offerings

On-Prem

- Turnkey Hadoop Appliances
- SW & HW Sensors
- Highest Performance
- $500K to $20M+

SaaS *NEW*

- Secure Workload As A Service
- Cisco Hosted & Managed
- Cloud First Customers
- $42K to $20M+

1K to 25K+ Workloads

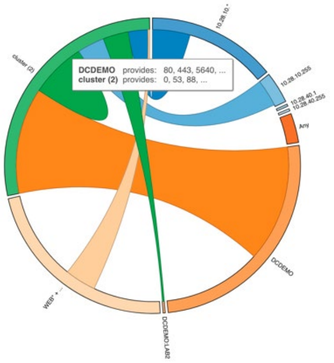
Software Only *NEW*

- VM Virtual Appliance
- DC, Amazon or Azure
- 3 Server Platform
- $24K+

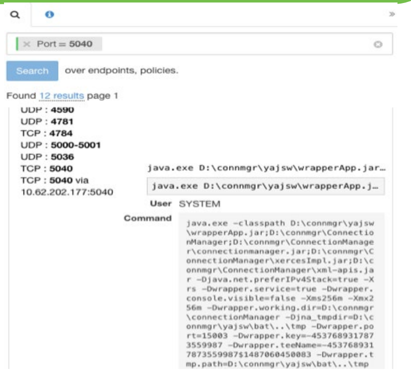
100 to 1000 Workloads

Cisco Secure Workload Zero Trust Automation
Automated Security Policy Recommendation

Step1: Behavior Analysis



Application conversations



Port = 5040

Search over endpoints, policies.

Found 12 results page 1

```
UDP : 4590
UDP : 4781
TCP : 4784
UDP : 5000-5001
UDP : 5036
TCP : 5040
TCP : 5040 via
10.62.202.177:5040
```

java.exe D:\connmgr\yajsw\wrapperApp.jar…

java.exe D:\connmgr\yajsw\wrapperApp.j…

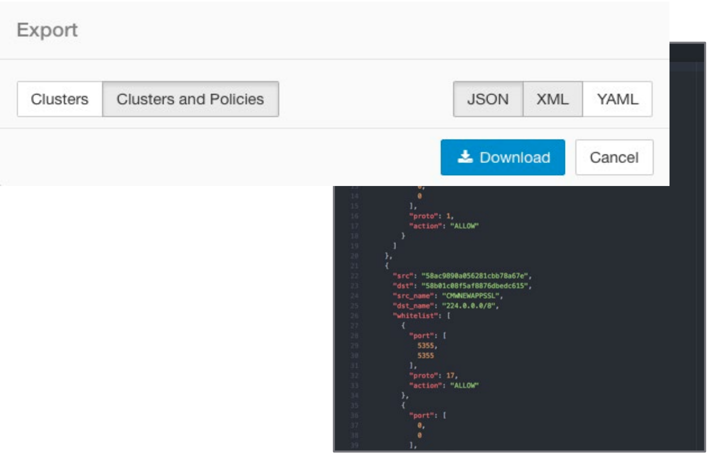
User SYSTEM

Command

```
java.exe -classpath D:\connmgr\yajsw
\wrapperApp.jar;D:\connmgr\Connectio
nManager;D:\connmgr\ConnectionManage
r\connectionmanager.jar;D:\connmgr\C
onnectionManager\xercesImpl.jar;D:\c
onnmgr\ConnectionManager\xml-apis.ja
r -Djava.net.preferIPv4Stack=true -X
rs -Dwrapper.service=true -Dwrapper.
console.visible=false -Xms256m -Xmx2
56m -Dwrapper.working.dir=D:\connmgr
\connectionManager -Djna_tmpdir=D:\c
onnmgr\yajsw\bat\..\tmp -Dwrapper.po
rt=15003 -Dwrapper.key=-453768931787
3559987 -Dwrapper.teeName=-453768931
7873559987$1487060450083 -Dwrapper.t
mp.path=D:\connmgr\yajsw\bat\..\tmp
```

Conversation details/ process bindings

Step2: Auto-Enforcement of Whitelist Policies



```
            0
          ],
          "proto": 1,
          "action": "ALLOW"
        }
      ]
    },
    {
      "src": "58ac9890a056281cbb78a67e",
      "dst": "58b01c08f5af8876dbedc615",
      "src_name": "CMWNEWAPPSSL",
      "dst_name": "224.0.0.0/8",
      "whitelist": [
        {
          "port": [
            5355,
            5355
          ],
          "proto": 17,
          "action": "ALLOW"
        },
        {
          "port": [
            0,
            0
          ],
```

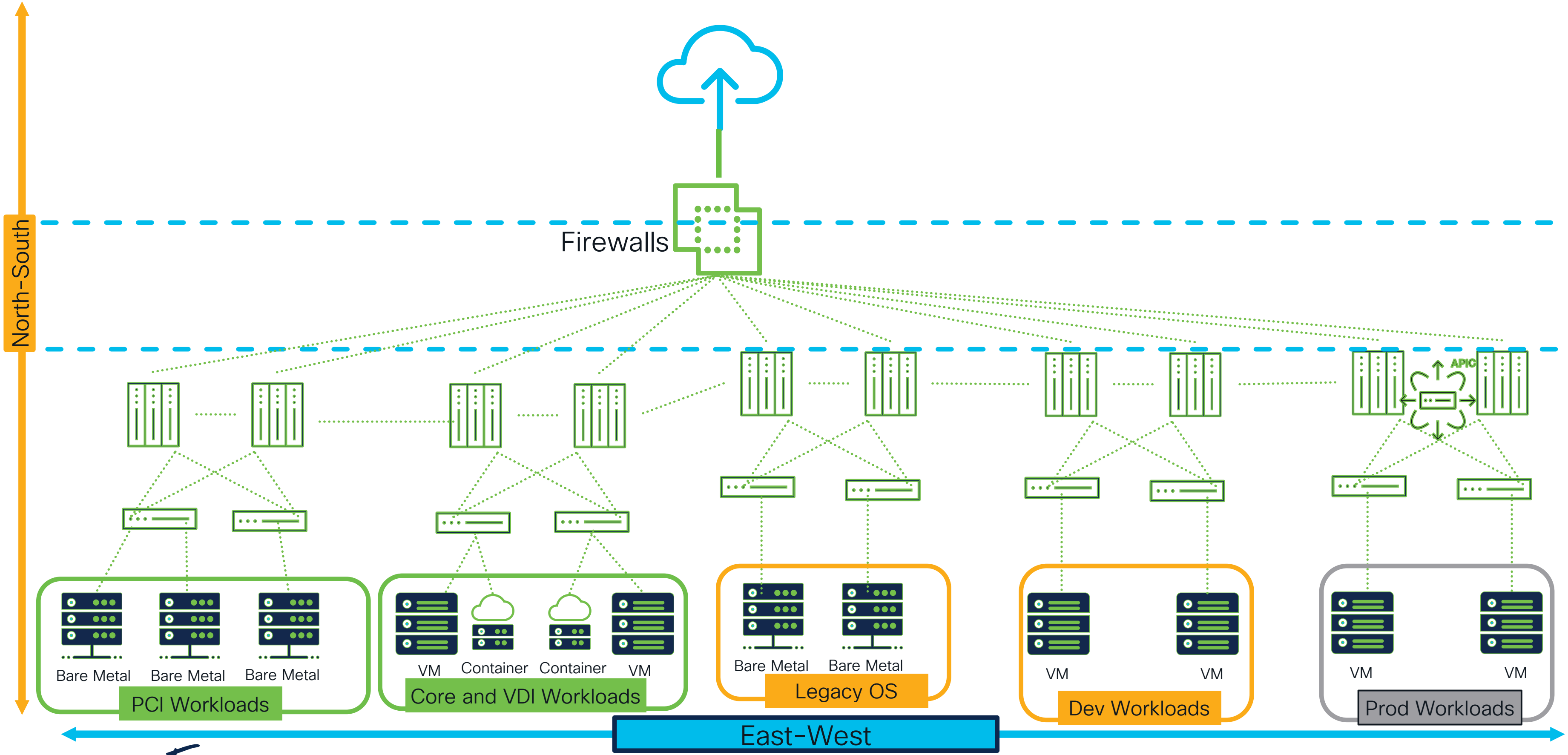
Whitelist policy recommendation

- Identifies application intent
- Generates 4 tuple policies

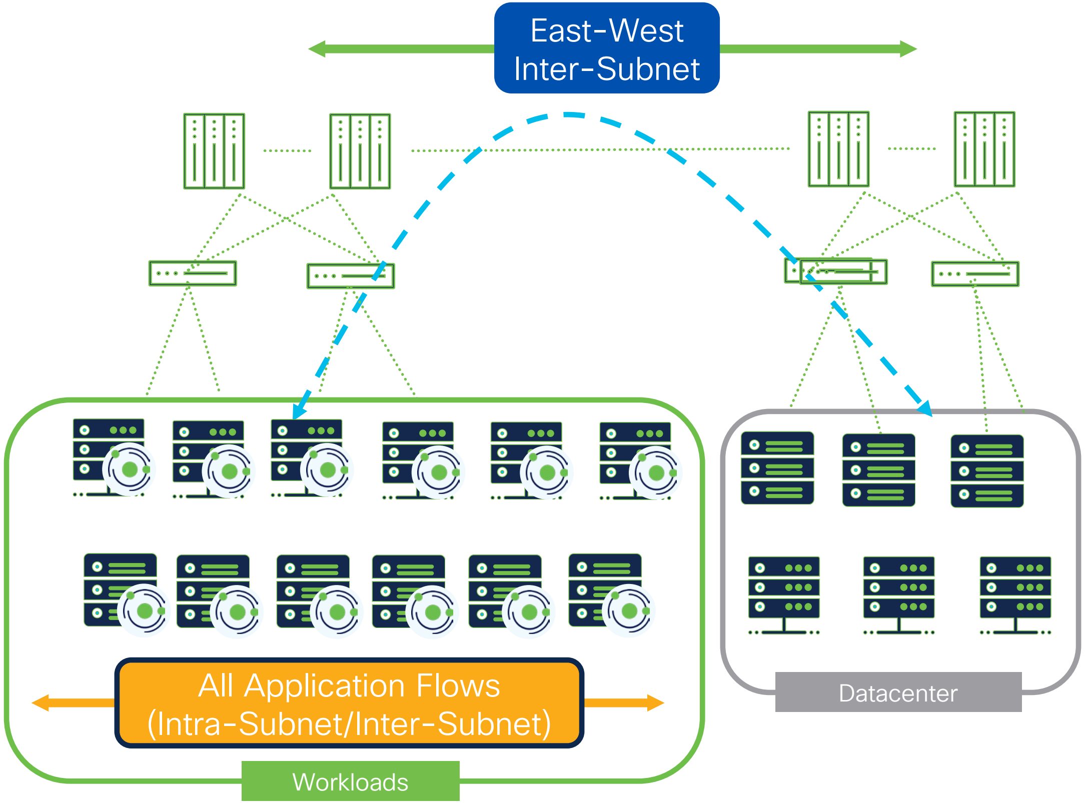
Export into Cisco solutions

- Export in JSON, XML and YAML
- Import into ACI, Secure Firewall

On–Prem (DC) Microsegmentation



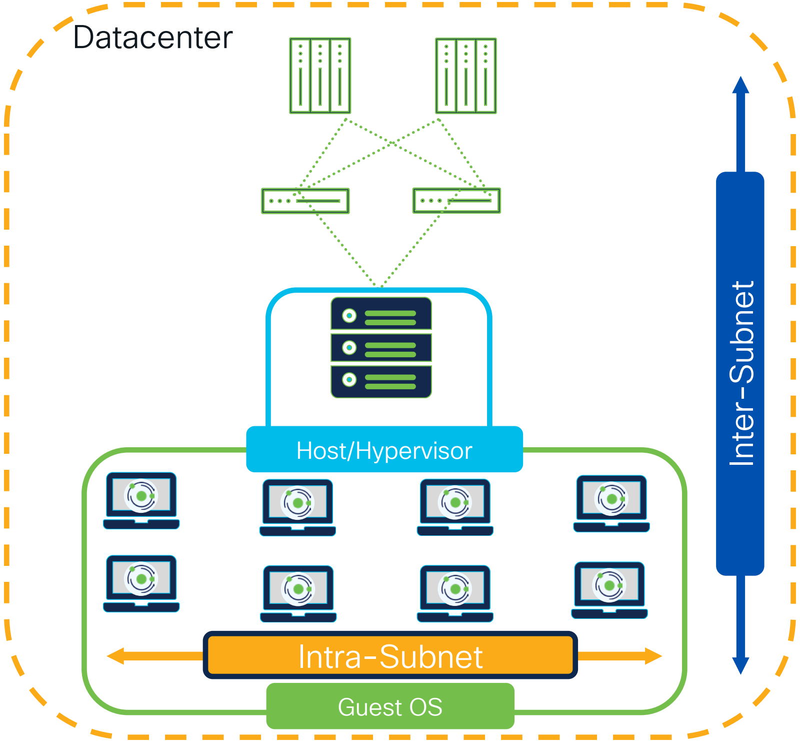
Workload Microsegmentation – Agent-Based



Host–Based Agent Workload Protection

- **Ideal** for fine-grained segmentation
  - In-depth workload visibility
  - Protection at the workload level
- Suitable for <u>all personas</u>
  - Enables delegation of policy controls to <u>application owners</u>

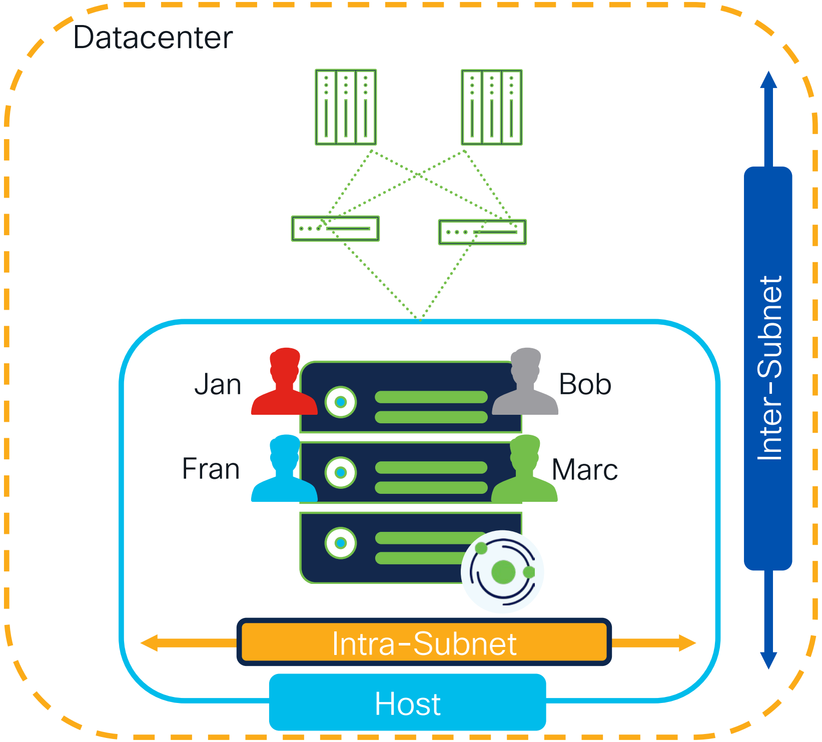
Virtual Desktop Infrastructure Microsegmentation



Host-Based Agent VDI Microsegmentation

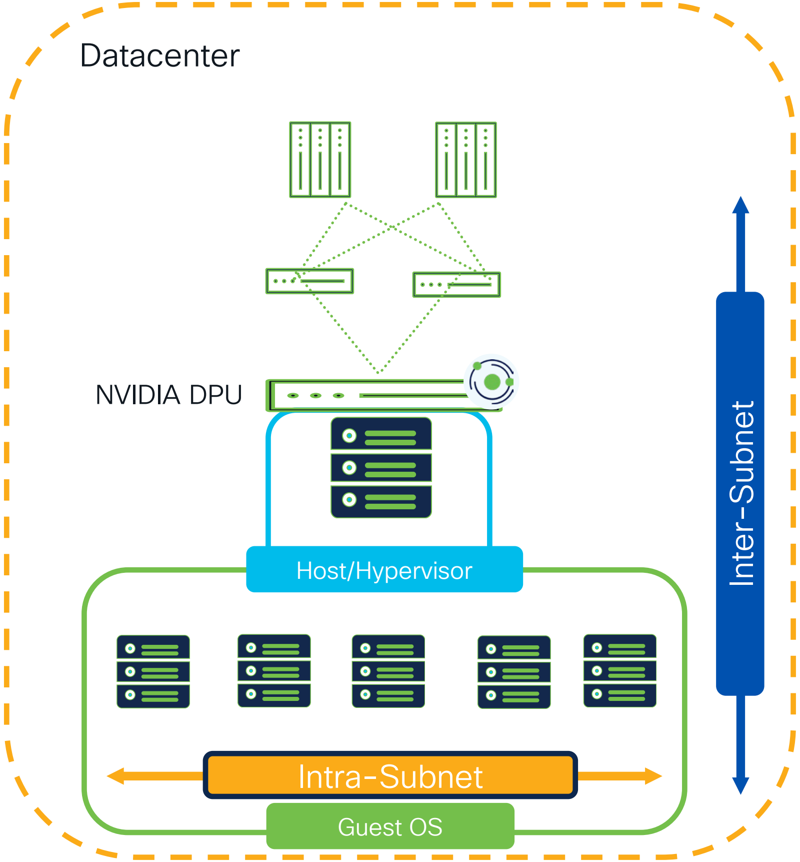
- Same agent as for workloads
- Ideal for fine-grained segmentation
  - In-depth endpoint visibility
  - Protection at the VDI user/desktop level
- Suitable for <u>all personas</u>

Terminal Services Microsegmentation



- Same agent as for workloads
- Ideal for fine-grained segmentation
    - In-depth endpoint visibility
    - Protection for multi-user sessions at workload level
- Suitable for all personas

Workload Microsegmentation – DPU

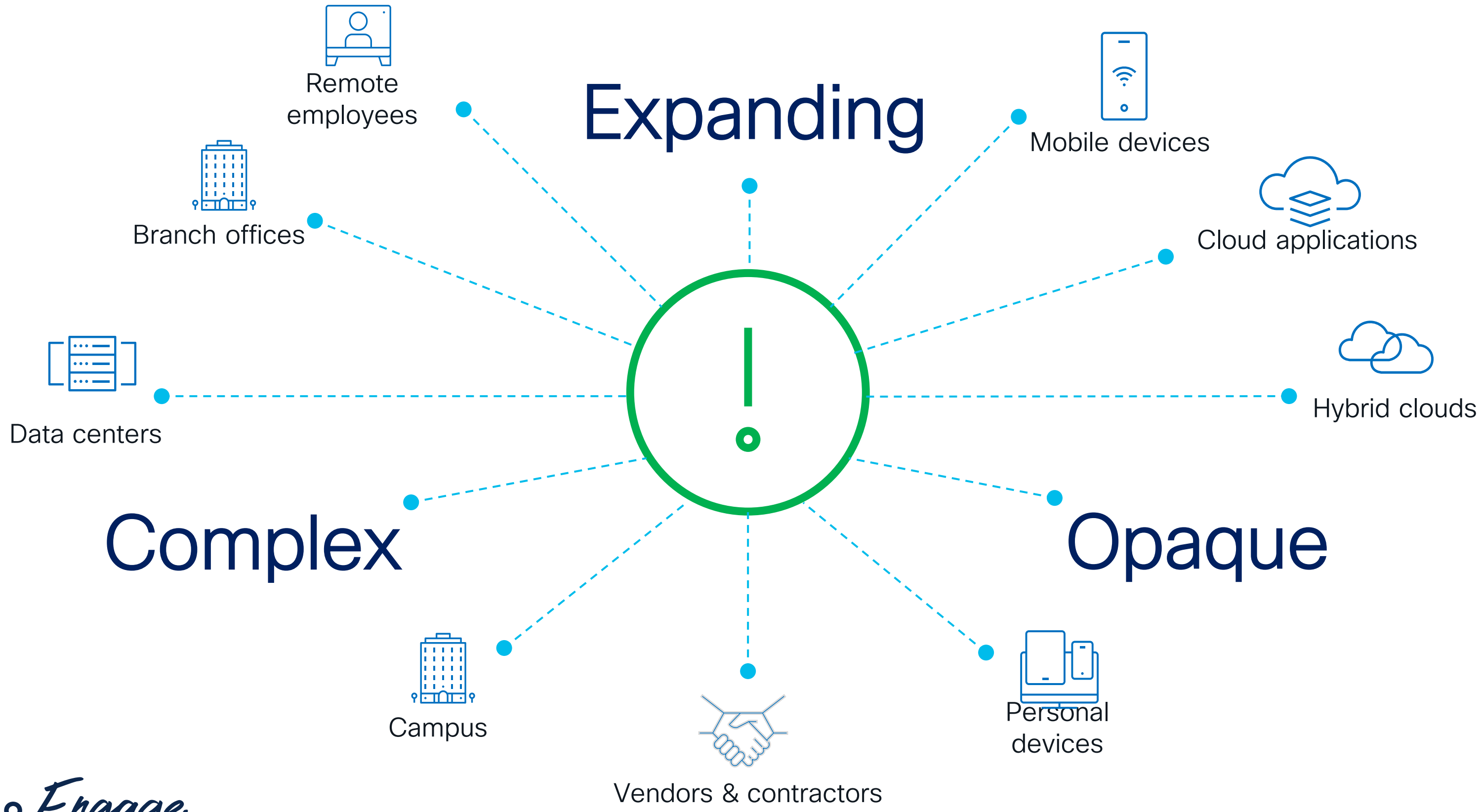


Host-Based DPU Microsegmentation

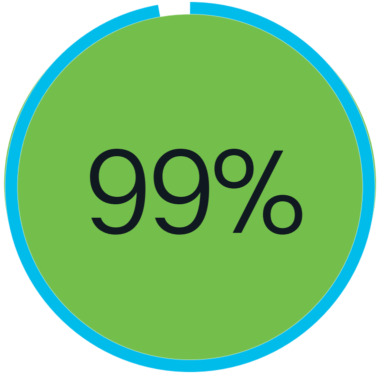
- **Acceptable** for fine-grained segmentation
- Visibility of workload flows
- Protection at the workload level (network)
- Suitable for **all personas**
  - Enables delegation of policy controls to **application owners**

Cisco Secure Firewall

Network attack surfaces are increasingly...

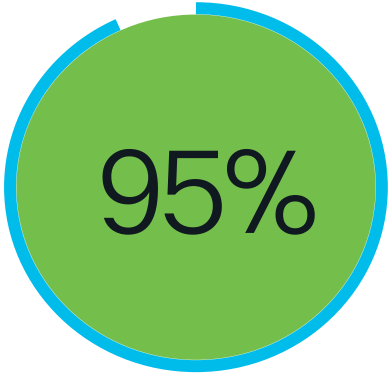


And attackers leverage the gaps



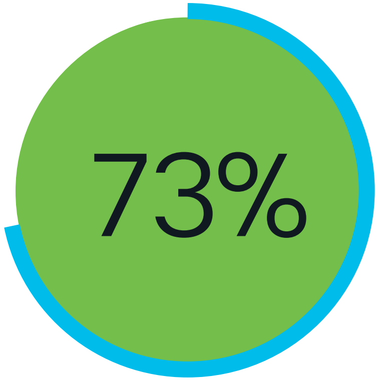
99%

of firewall breaches will be caused by firewall misconfigurations[1]



95%

of web traffic is encrypted[2]



73%

of organizations lack sufficient visibility into threats and are struggling to implement zero trust[3]

[1] Gartner Technology Insight for Network Security Policy Management; [2]Google Transparency Report; [3]Cybersecurity Insiders, 2022 Application Security Report;

slido

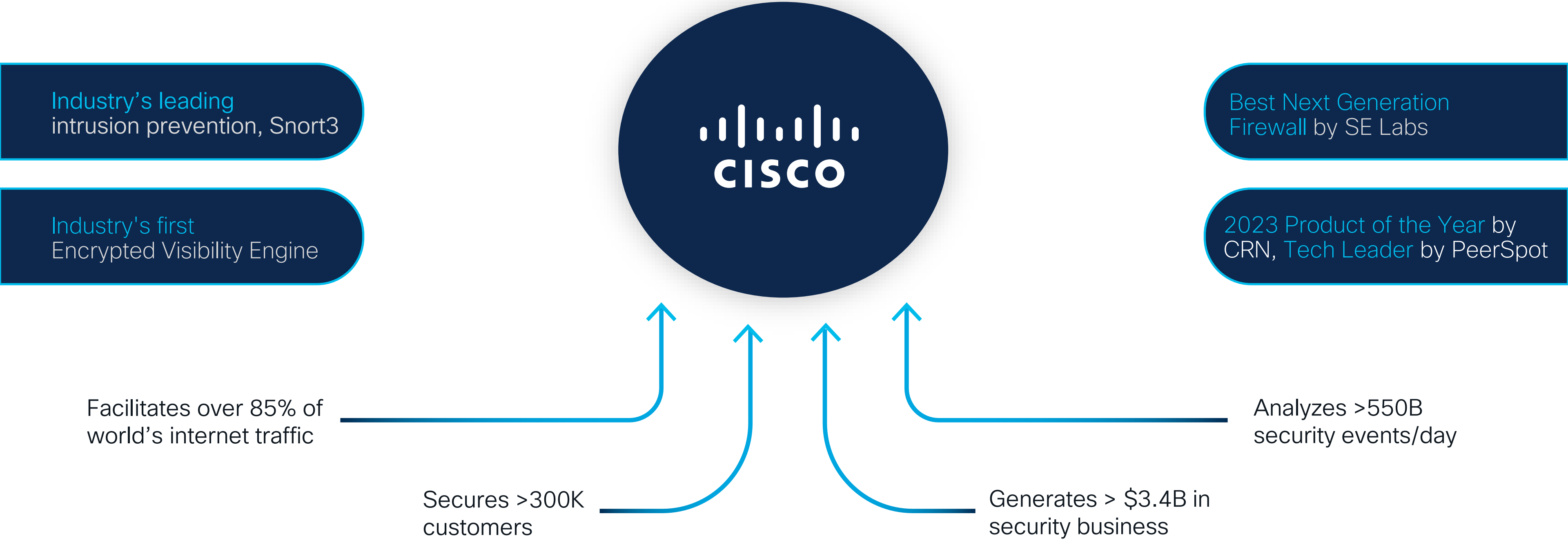
Please download and install the Slido app on all computers you use

What percent of network traffic does your organization decrypt?

ⓘ Start presenting to display the poll results on this slide.

Cisco Secure Firewall

By the company that builds **the most** networks across the globe



Industry’s leading intrusion prevention, Snort3

Industry's first Encrypted Visibility Engine

Best Next Generation Firewall by SE Labs

2023 Product of the Year by CRN, Tech Leader by PeerSpot

Facilitates over 85% of world’s internet traffic

Secures >300K customers

Generates > $3.4B in security business

Analyzes >550B security events/day

Secure Firewall Industry Differentiation

AI Assistant

Simplify operations and achieve granular visibility and control of traffic to bolster security and performance

Zero Trust Application Access

Move beyond traditional “authorize then ignore” ZTNA models by adding complete threat inspection and policy for each individual application

Encrypted Visibility Engine

Gain control over encrypted traffic, while eliminating performance bottlenecks and ensuring privacy compliance

Microsegmentation Policy Integration

Ease policy lifecycle management by integrating Microsegmentation solutions

Encrypted Visibility Engine (EVE)

Enhanced Visibility and Detection Efficacy of Encrypted Traffic

Inferenced Based Identification without Decryption in TLS & QUIC of:

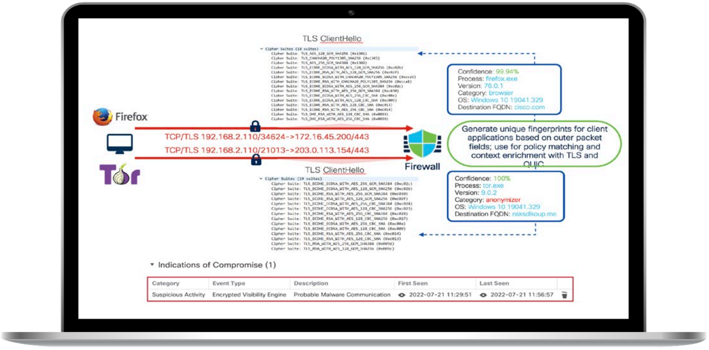
- Client Applications
- Operating Systems
- Compromised Hosts

Machine Learning Generated Fingerprints with data from:

- Computer Security Incident Response Team (CSIRT)
- Network Visibility Module (NVM)
- Secure Malware Analytics (ThreatGrid)

AI @ Speed of the Network:

- Network Protocol Fingerprinting (NPF) selects classifier
- Weighted Naïve Bayes classifier with sparse updates
- Best Threat Detection efficacy in recent internal testing



TLS ClientHello

```
˅ Cipher Suites (18 suites)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Confidence: 99.94%
Process: firefox.exe
Version: 76.0.1
Category: browser
OS: Windows 10 19041.329
Destination FQDN: cisco.com

TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

Generate unique fingerprints for client applications based on outer packet fields; use for policy matching and context enrichment with TLS and QUIC

TLS ClientHello

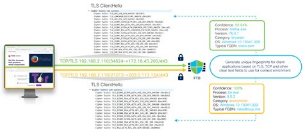
```
˅ Cipher Suites (19 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
```

Confidence: 100%
Process: tor.exe
Version: 9.0.2
Category: anonymizer
OS: Windows 10 19041.329
Destination FQDN: nsksdlkoup.me

▾ Indications of Compromise (1)

Category	Event Type	Description	First Seen	Last Seen
Suspicious Activity	Encrypted Visibility Engine	Probable Malware Communication	2022-07-21 11:29:51	2022-07-21 11:56:57

Encrypted Visibility Engine Benefits

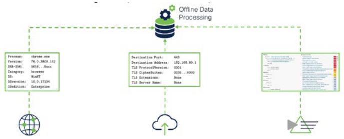

TLS ClientHello
TCP/TLS 192.168.2.110/34624->172.16.45.200/443
TCP/TLS 192.168.2.110/21013->203.0.113.154/443
FTD
TLS ClientHello

Confidence: 99.94%
Process: firefox.exe
Version: 76.0.1
Category: browser
OS: Windows 10 19041.329
Typical FQDN: cisco.com

Generate unique fingerprints for client applications based on TLS, TCP and other clear text fields to use for context enrichment

Confidence: 100%
Process: tor.exe
Version: 9.0.2
Category: anonymizer
OS: Windows 10 19041.329
Typical FQDN: naksdkoup.me

Encrypted Visibility Engine



```
Process:     chrome.exe
Version:     76.0.3809.132
SHA-256:     5616...9acc
Category:    browser
OS:          WinNT
OSversion:   10.0.17134
OSedition:   Enterprise
```

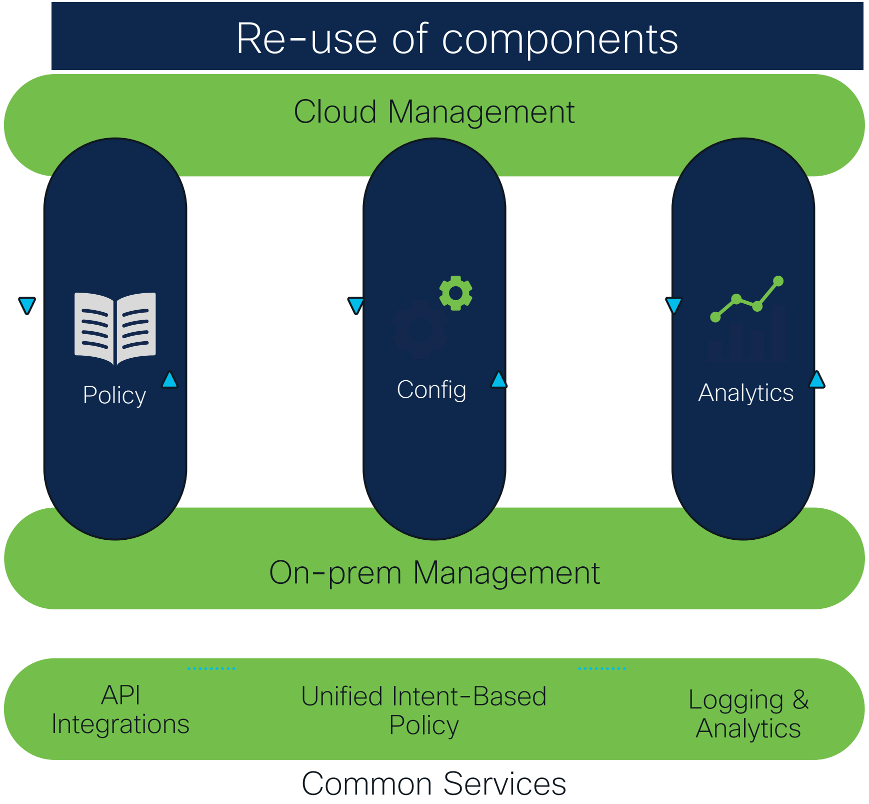
```
Destination Port:      443
Destination Address:   192.168.60.1
TLS ProtocolVersion:   0301
TLS CipherSuites:      0035...0003
TLS Extensions:        None
TLS Server Name:       None
```

- Detects and blocks malware in encrypted flows
- Can be used for APP control in the firewall policy
- Triggers Indications of Compromise
- Minimal performance impact
- Enriches Endpoint DB with Application and OS

Unifying Cloud and On-Prem Management

New Cloud-Delivered FMC

- Simple and consistent UX
- Easy migration from on-prem to cloud
- Shared components for consistency
- Common services for unified policy, XDR and logging



Cisco Security Cloud Control

Simplify operations

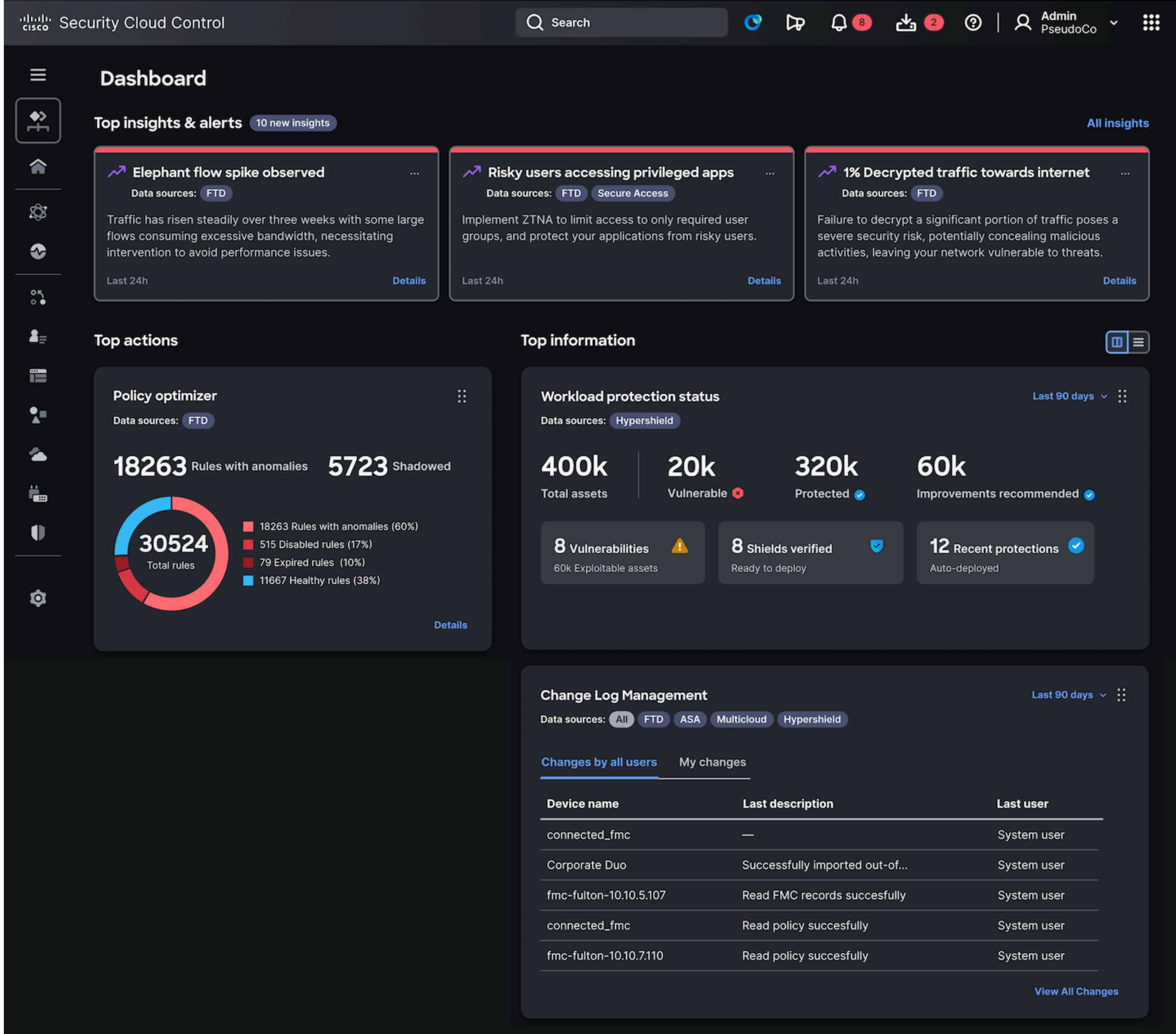
Centralize control of devices and policies

Enhance security

Leverage AI to strengthen protection and prevent downtime

Increase efficiency

Reduce time spent on manual tasks up to 90%



Security Cloud Control

Search

Admin
PseudoCo

Dashboard

Top insights & alerts 10 new insights

All insights

Elephant flow spike observed
Data sources: FTD
Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues.
Last 24h Details

Risky users accessing privileged apps
Data sources: FTD Secure Access
Implement ZTNA to limit access to only required user groups, and protect your applications from risky users.
Last 24h Details

1% Decrypted traffic towards internet
Data sources: FTD
Failure to decrypt a significant portion of traffic poses a severe security risk, potentially concealing malicious activities, leaving your network vulnerable to threats.
Last 24h Details

Top actions

Policy optimizer
Data sources: FTD

18263 Rules with anomalies 5723 Shadowed

30524 Total rules

- 🟥 18263 Rules with anomalies (60%)
- 🟥 515 Disabled rules (17%)
- 🟥 79 Expired rules (10%)
- 🟦 11667 Healthy rules (38%)

Details

Top information

Workload protection status Last 90 days
Data sources: Hypershield

400k Total assets
20k Vulnerable
320k Protected
60k Improvements recommended

8 Vulnerabilities — 60k Exploitable assets
8 Shields verified — Ready to deploy
12 Recent protections — Auto-deployed

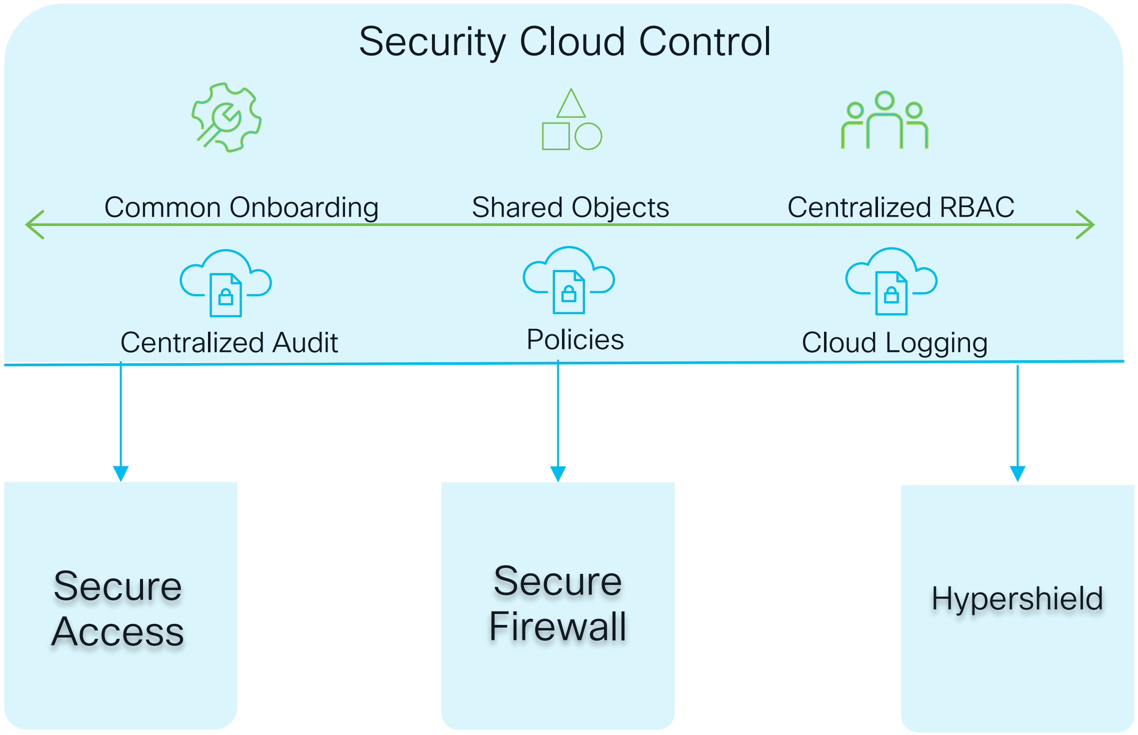
Change Log Management Last 90 days
Data sources: All FTD ASA Multicloud Hypershield

Changes by all users My changes

Device name	Last description	Last user
connected_fmc	—	System user
Corporate Duo	Successfully imported out-of...	System user
fmc-fulton-10.10.5.107	Read FMC records succesfully	System user
connected_fmc	Read policy succesfully	System user
fmc-fulton-10.10.7.110	Read policy succesfully	System user

View All Changes

Cisco Security Cloud Control (SCC) Overview



Security Cloud Control

Common Onboarding

Shared Objects

Centralized RBAC

Centralized Audit

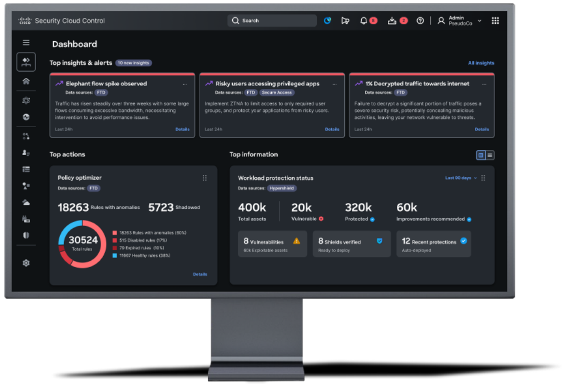
Policies

Cloud Logging

Secure Access

Secure Firewall

Hypershield



Security Cloud Control

Search

Admin
PseudoCo

Dashboard

Top insights & alerts 10 new insights

All insights

Elephant flow spike observed
Data sources: FTD
Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues.
Last 24h Details

Risky users accessing privileged apps
Data sources: FTD Secure Access
Implement ZTNA to limit access to only required user groups, and protect your applications from risky users.
Last 24h Details

1% Decrypted traffic towards internet
Data sources: FTD
Failure to decrypt a significant portion of traffic poses a severe security risk, potentially concealing malicious activities, leaving your network vulnerable to threats.
Last 24h Details

Top actions

Policy optimizer
Data sources: FTD
18263 Rules with anomalies 5723 Shadowed
30524 Total rules
- 18263 Rules with anomalies (60%)
- 515 Disabled rules (17%)
- 79 Expired rules (10%)
- 11667 Healthy rules (38%)

Details

Top information

Workload protection status
Last 90 days
Data sources: Hypershield
400k Total assets
20k Vulnerable
320k Protected
60k Improvements recommended
8 Vulnerabilities
60k Exploitable assets
8 Shields verified
Ready to deploy
12 Recent protections
Auto-deployed

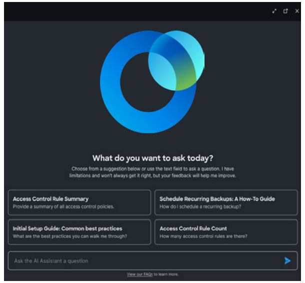
Consolidate firewall management

Ensure consistent security policies and compliance

Automate and optimize policy management

AI Assistant in Firewall

Accelerate policy queries, troubleshooting, and rule management



What do you want to ask today?

Choose from a suggestion below or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

Access Control Rule Summary
Provide a summary of all access control policies.

Schedule Recurring Backups: A How-To Guide
How do I schedule a recurring backup?

Initial Setup Guide: Common best practices
What are the best practices you can walk me through?

Access Control Rule Count
How many access control rules are there?

Ask the AI Assistant a question

View our FAQs to learn more.

Policy identification & reporting

Configuration information in one click

Troubleshooting & threat defense

Correlate documentation and insights at machine-speed

Policy lifecycle management

Take actions to create new rules or block existing ones

Simplifying firewall policy management

cisco.com/go/firewall

Zero Trust Firewall Integrations

Secure Workload and Secure Firewall Use-Cases

North-South Security with Cisco Secure Firewall

Broad Visibility

- Threat Inspection at data center edge or cloud edge
- Visibility into Internet, branch, campus
- Virtual patch with Secure Workload

East-West Security with Cisco Secure Firewall or Catalyst Center

Coarse Control

- Segment within your data centers and cloud
- Protect workloads without agents
- Single/multi site public cloud
- Physical/virtual form factors

Microsegmentation with Cisco Secure Workload

Fine-Grained Control

- Zero trust microsegmentation enforcement at workload level
- Automated policy discovery

→ Closer to application

Secure Firewall & Secure Workload Integration

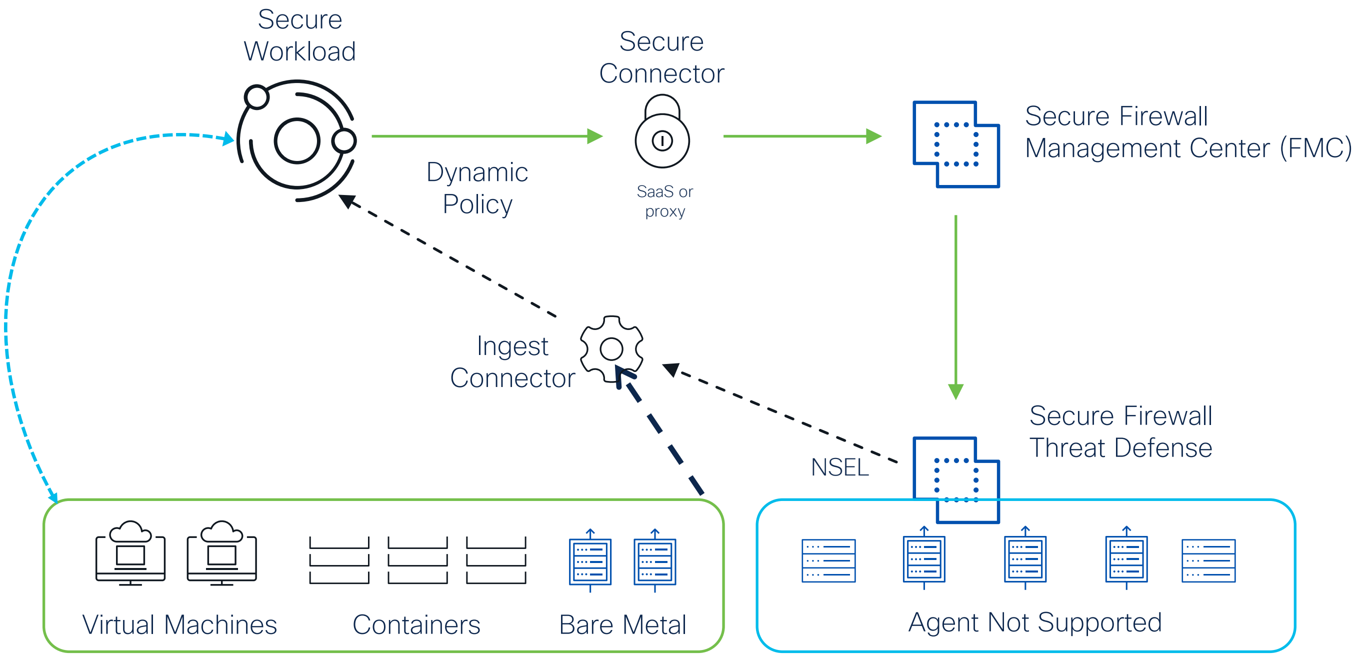
Use-Cases

- East-West microsegmentation for agentless workloads
- North-South virtual patch on Secure Firewall

Key Capabilities

- Real time updates on rules using Dynamic objects without policy deployment
- Fine grained policies from Secure Workload to implement contextual access-rules on firewall
- Automated policy lifecycle
- Dual firewall rules management (FMC and Secure Workload)
- Export of CVE information from agent-based workloads

Secure Firewall – High Level Architecture

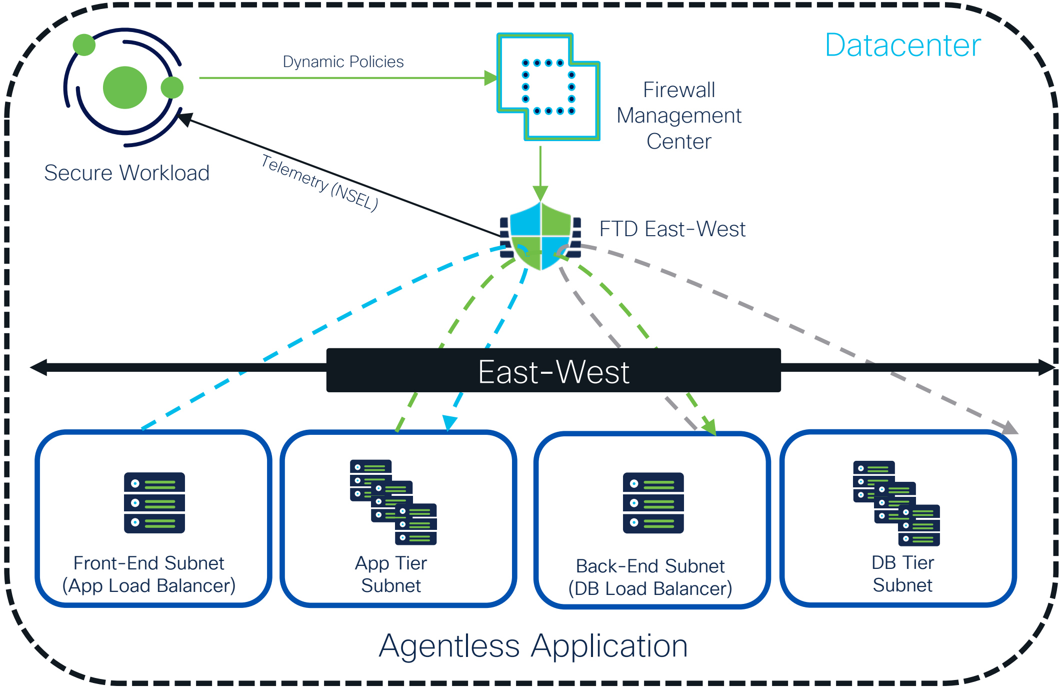


East-West Segmentation policies enforcement at workloads

East-West segmentation policies enforcement at firewall

East-West Microsegmentation

Traditional Networking Insertion



Layer 2 Firewall (Transparent)

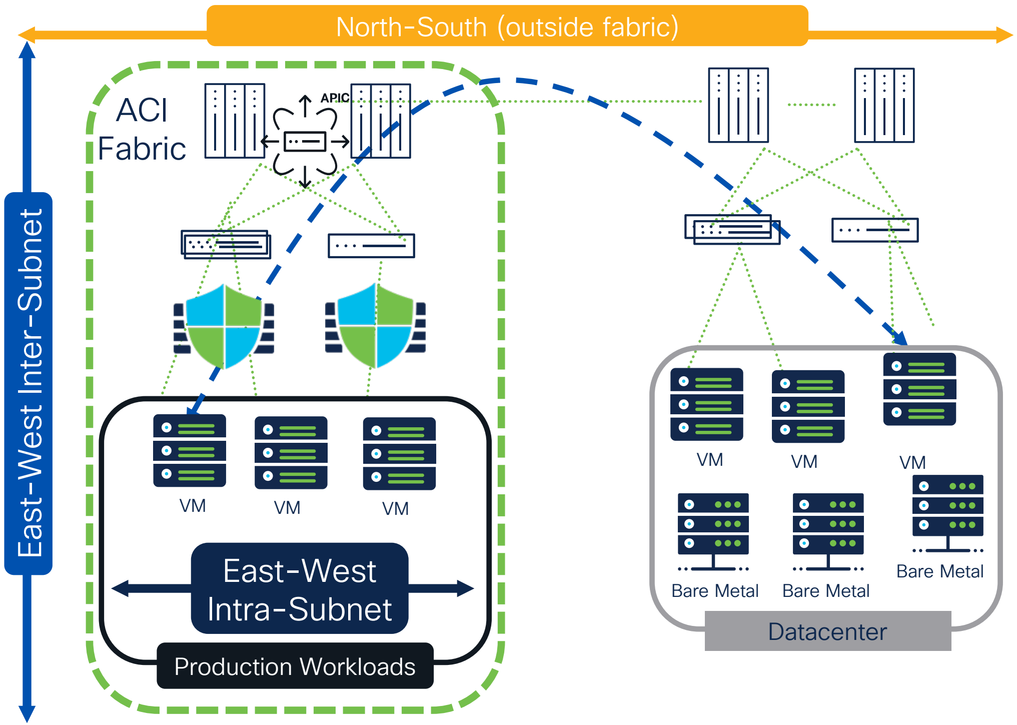
- Acceptable for fine-grained segmentation
- Full visibility of flows
  - Bump-in-Wire on the datapath
  - Intra and Inter-subnet flows
- Protection at the network level
  - Intra-Subnet (App-App)
  - Inter-Subnet (App-App and External-App)
- Best fit for localized workloads
- Allows policy dual-management
- Convenient for network and firewall engineers

Layer 3 Firewall (Routed)

- Reasonable segmentation for workloads
- Partial visibility of flows
  - Firewall as GW
  - Inter-subnet flows only
- Protection at the network level
  - Inter-Subnet (App-App and External-App)
- Excellent fit for distributed workloads
- Allows policy dual-management
- Convenient for network and firewall engineers

East-West Microsegmentation

SDN Controller (ACI) Insertion



Service Graph with Policy Based Routing

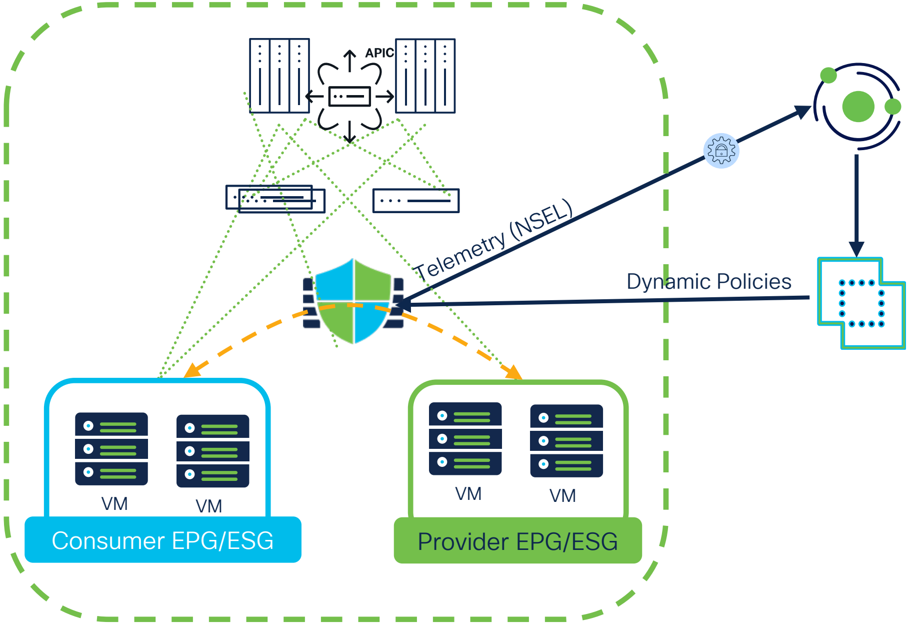
- No re-architecture
  - Flexible and easy to configure
  - FW is selectively inserted in the path
- Supports both L3 and L2 FW modes
  - Intra and inter-subnet flow visibility (both)
  - Intra and Inter-subnet protection (both)
- Preferred L3 mode
- Can do intra-ESG redirection

Service Graph Go-To-Go-Through Mode

- FW is in-path (Security over Connectivity)
  - Not very flexible and more complex
  - Typically used for North-South traffic
- Go-To
  - Inter-subnet visibility and protection
- Go-Through
  - Intra and Inter-subnet visibility protection

East-West Microsegmentation

SDN Controller (ACI) Insertion

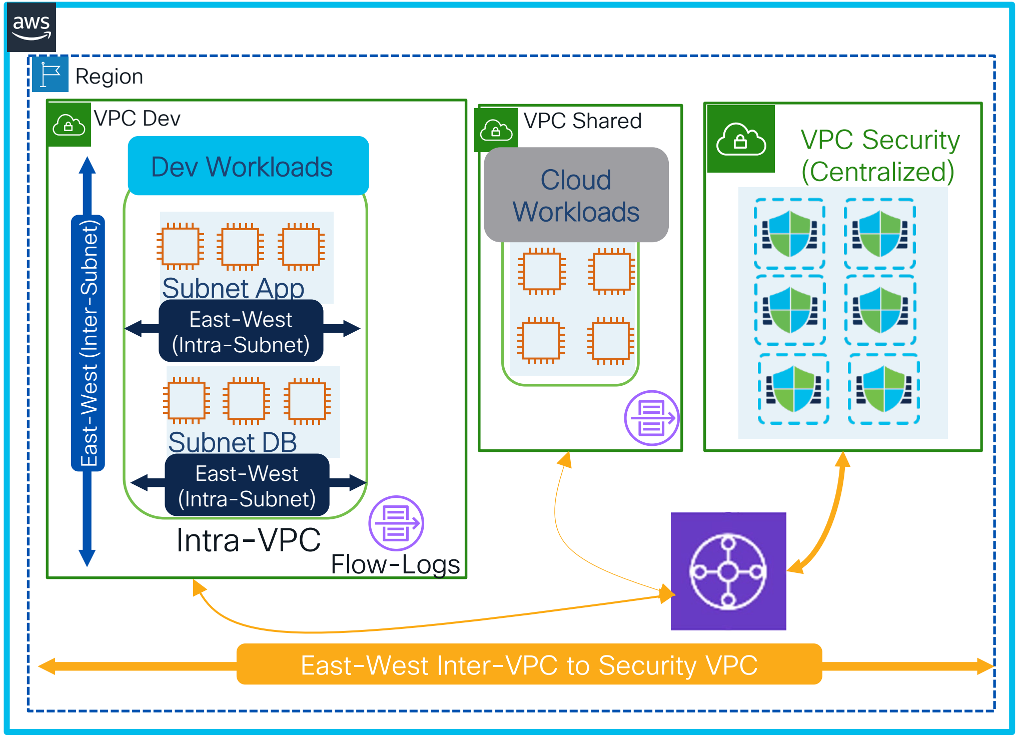


Service Graph PBR and Firewall Insertion Protection

- Full visibility of flows
  - FW inserted in datapath with service graph
  - Intra and inter EPG/ESG
- Flexible level of workload protection
  - Intra EPG/ESG (fine-grained intra-app)
  - Inter EPG/ESG (reasonable inter-app)
- Allows policy triple-management
  - CSW owned-policies
  - FMC owned-policies
  - ACI owned-policies
- Convenient for network (ACI) and firewall engineers

East-West Microsegmentation

Centralized VPC Insertion with AWS

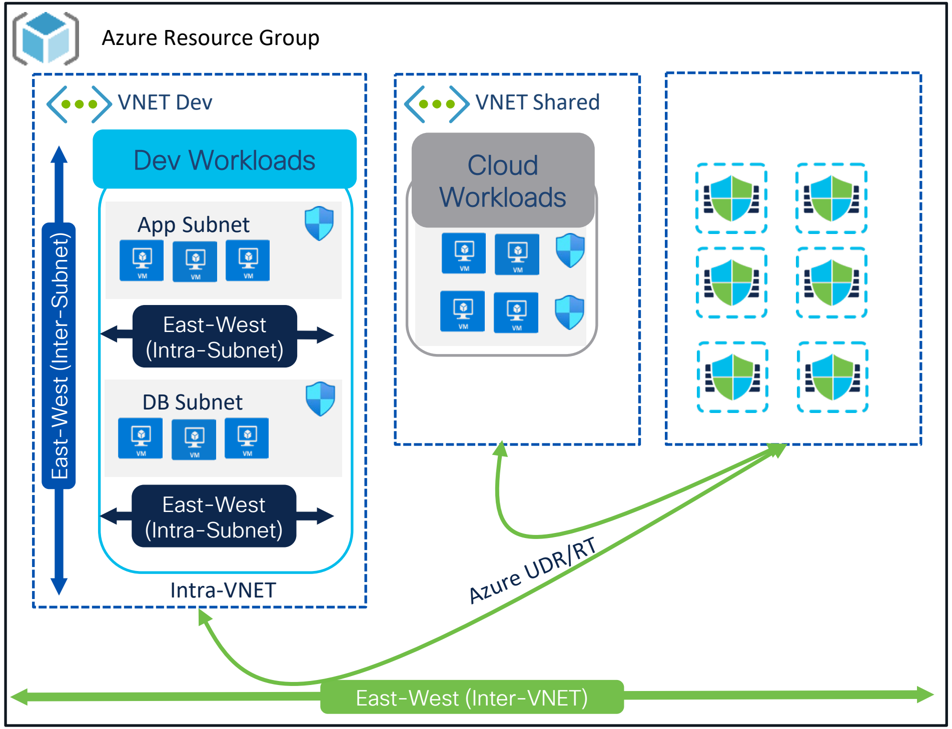


Centralized East-West VPC Inspection

- Reasonable segmentation
- Full visibility of flows
  - Ingestion of flow-logs and NSEL
  - Intra and Inter-subnet flows
- Cloud context
  - Labels
    - Instances and NICs
    - Autoscaling
    - Region/Account
  - Template/Golden Image
- Protection at the network level
  - Inter-Subnet (App-App and External-App)
  - Inter-VPC (App-App and External-App)
- Suitable for network/firewall engineers

East-West Microsegmentation

Centralized VNET Insertion with Azure

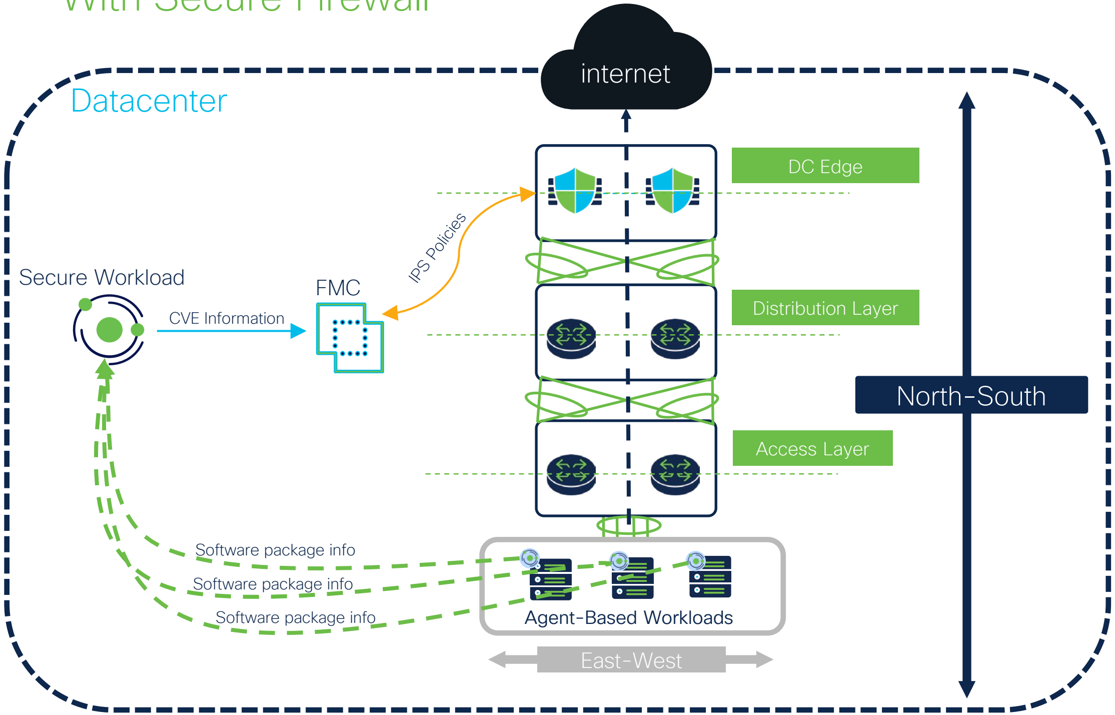


Centralized East-West VNet Inspection

- Acceptable for fine-grained segmentation
- Full visibility of flows
  - NSG flow-logs and NSEL
  - Intra and Inter-subnet flows
- Cloud context
    - Labels
    - VMs and NICs
    - Scale-Sets
    - Subscriptions
  - Template/Golden Image
- Protection at the network level
  - Intra-subnet (App-App)
  - Inter-subnet (App-App and External-App)
  - Inter-VNET(App-App and External-App)
- Suitable for network/firewall engineers

North-South Virtual Patch

With Secure Firewall



L7 Virtual Patch Inspection

- Quickly identify vulnerable workloads
- Vulnerability information export done by Secure Workload to FMC
- Run Firepower Recommendations to get IPS signature
- Apply IPS policy to interested traffic flows
- Configure the compensating control to mitigate risk while patching schedule is done
- De-risk end-of-life applications without patching support

Cisco ISE

ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

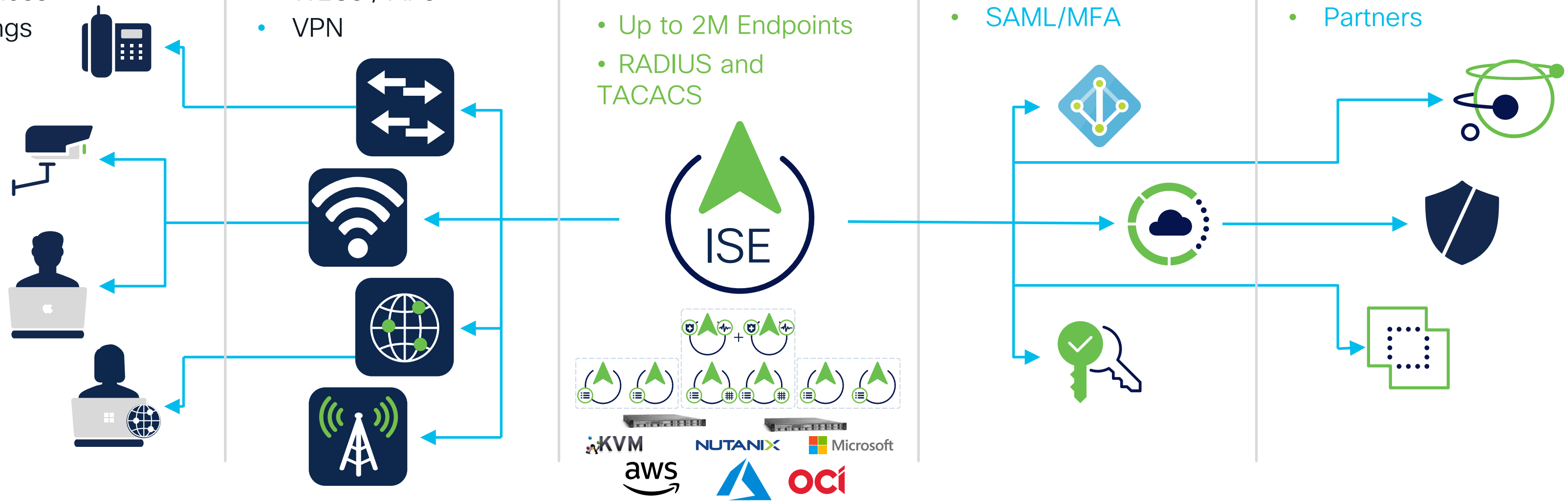
- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS

Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
- Secure Firewall
- Partners



See It | Secure It | Share It

How Identity Services Engine enforces Zero Trust

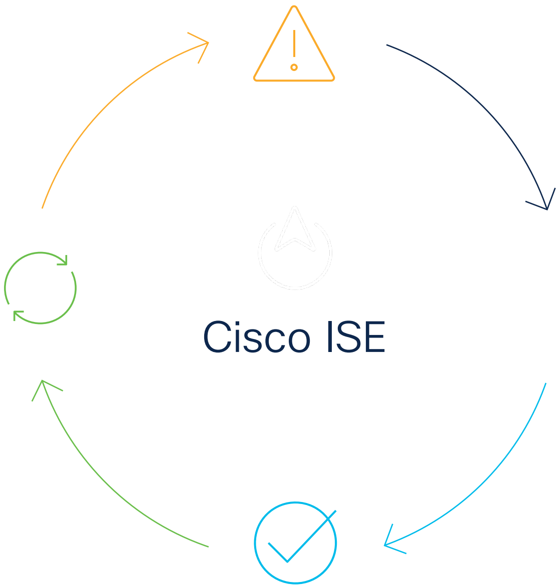
- Connecting trusted users and endpoints with trusted resources

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy



Cisco ISE

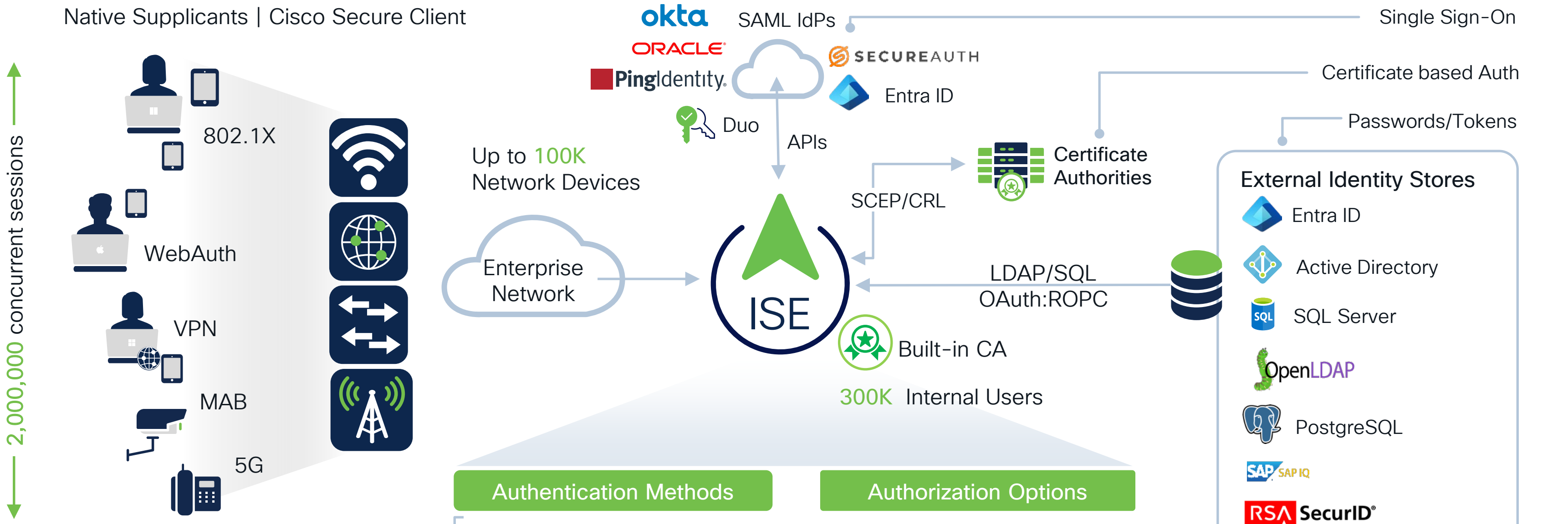
Endpoint classified, and profiled into groups

- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

ISE Secure Access Control Options



Native Supplicants | Cisco Secure Client

2,000,000 concurrent sessions

802.1X

WebAuth

VPN

MAB

5G

Up to 100K Network Devices

Enterprise Network

ISE

SAML IdPs

Single Sign-On

APIs

Duo

Certificate based Auth

Passwords/Tokens

Certificate Authorities

SCEP/CRL

LDAP/SQL
OAuth:ROPC

Built-in CA

300K Internal Users

External Identity Stores

- Entra ID
- Active Directory
- SQL Server
- OpenLDAP
- PostgreSQL
- SAP IQ
- RSA SecurID

Authentication Methods

Passive Identity
- MAC Authentication Bypass
- Easy Connect ®

Active Identity
- IEEE 802.1X
- Web Authentication
  - Central WebAuth
  - Local WebAuth

Authorization Options

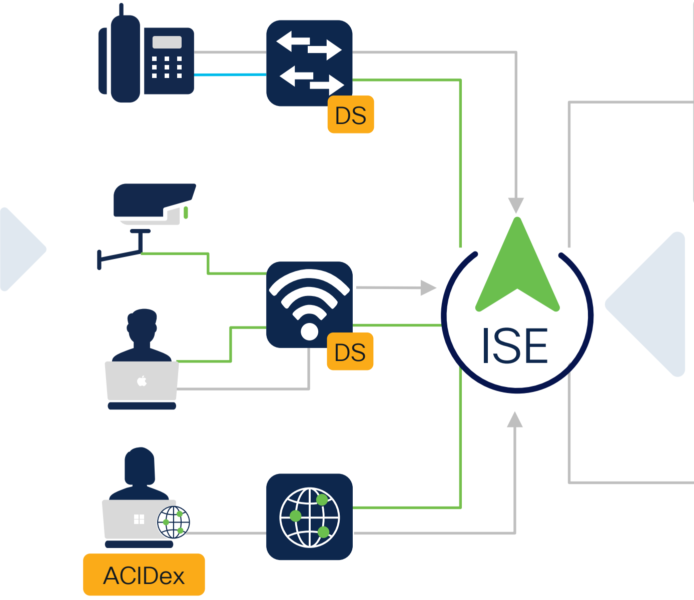
- Downloadable / Named ACL
- Air Space ACL
- VLAN Assignment
- Security Group Tags
- URL-Redirection
- Port Configuration :
  ASP Macro / Interface-Template

Up to 50 distinct AD domain support

Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data, that reveal their device type



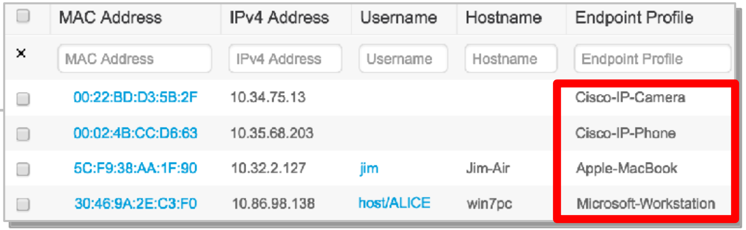
ISE Data Collection Methods for Device Profiling

Active Probes: Netflow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

Cisco Secure Client (formerly AnyConnect): ACIDex

Feed Service (Online/Offline)



□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

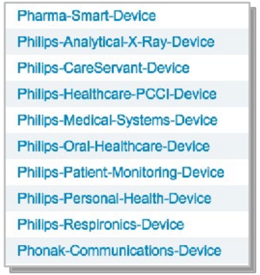
Cisco Secure Client Identity Extensions (ACIDex) | Device Sensor (DS)

Profiling Packages and Integrations

Medical Devices

Hospital

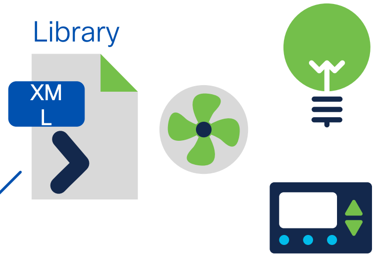
250+ Medical device profiles

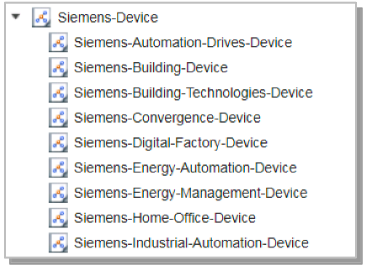


Pharma-Smart-Device
Philips-Analytical-X-Ray-Device
Philips-CareServant-Device
Philips-Healthcare-PCCI-Device
Philips-Medical-Systems-Device
Philips-Oral-Healthcare-Device
Philips-Patient-Monitoring-Device
Philips-Personal-Health-Device
Philips-Respironics-Device
Phonak-Communications-Device

IOT Building & Automation

Library

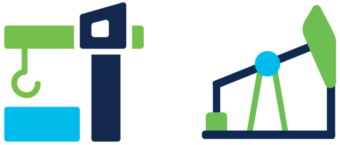




Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device

pxGrid

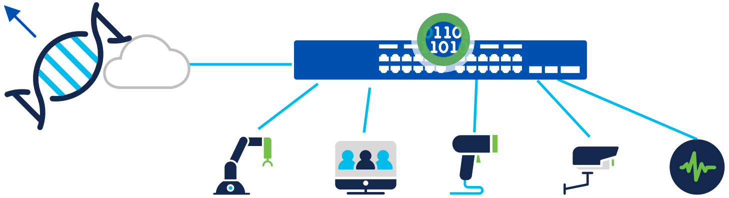
pxGrid



Factory

Industrial Devices

Cisco CyberVision

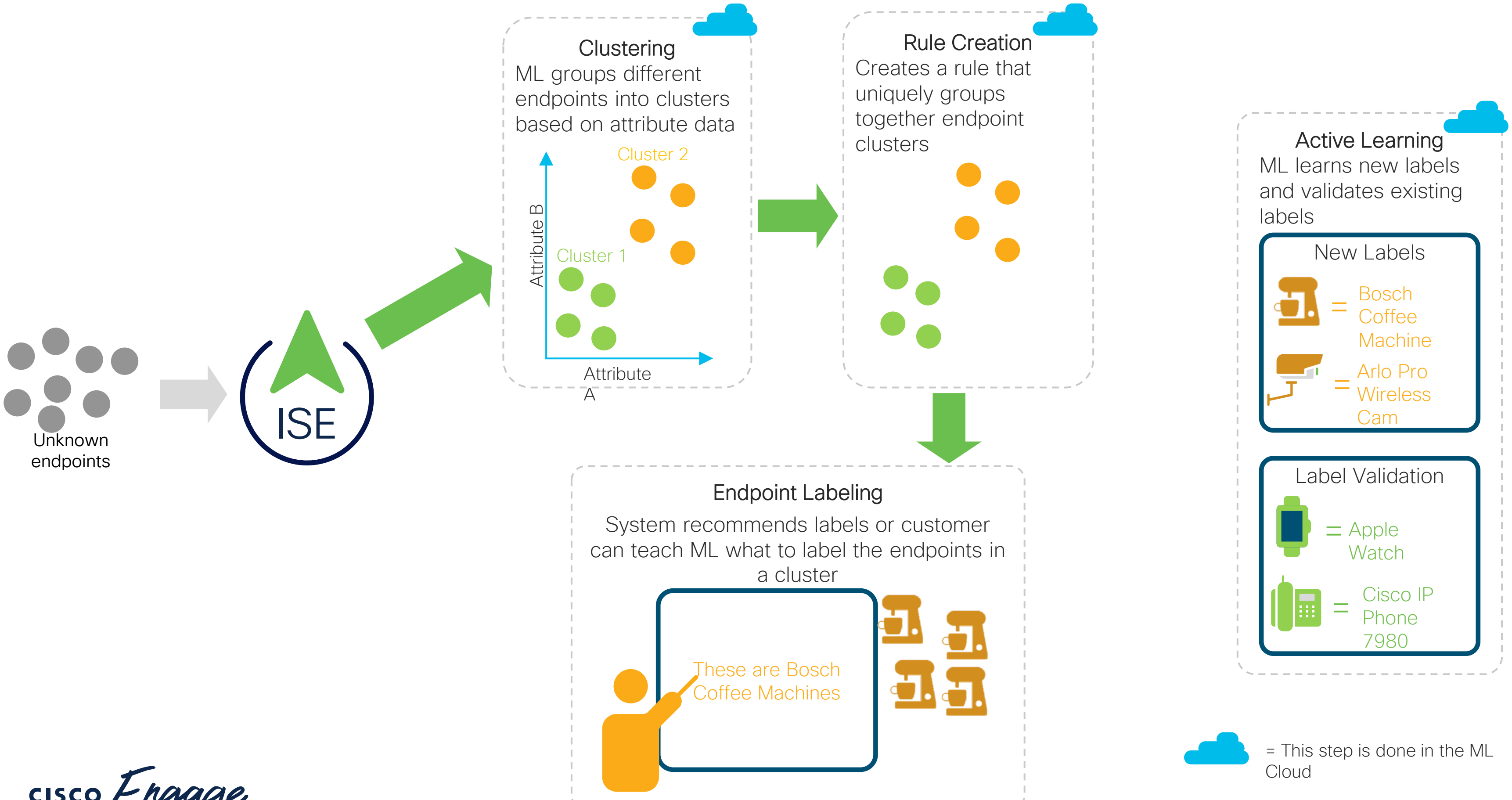


Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security

Cisco AI Machine Learning Profiling



Clustering
ML groups different endpoints into clusters based on attribute data

Rule Creation
Creates a rule that uniquely groups together endpoint clusters

Endpoint Labeling
System recommends labels or customer can teach ML what to label the endpoints in a cluster

These are Bosch Coffee Machines

Active Learning
ML learns new labels and validates existing labels

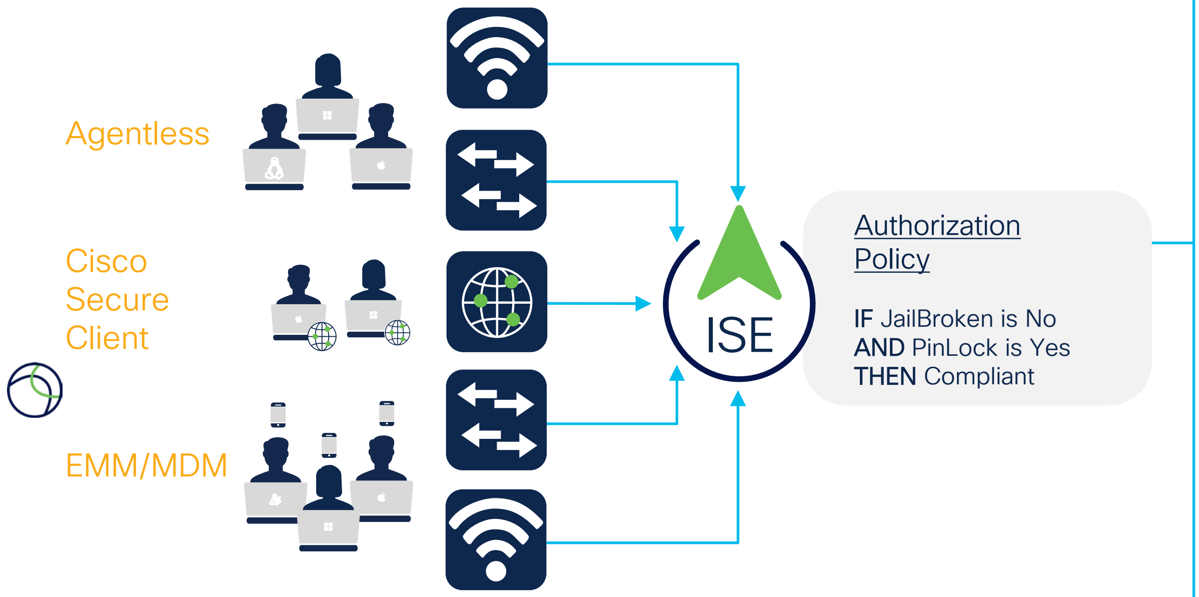
New Labels
= Bosch Coffee Machine
= Arlo Pro Wireless Cam

Label Validation
= Apple Watch
= Cisco IP Phone 7980

= This step is done in the ML Cloud

Posture & Compliance

cisco.com/go/csta



Authorization Policy

IF JailBroken is No
AND PinLock is Yes
THEN Compliant

AbsoluteSoftware
SOPHOS
GLOBO
IBM Security
Microsoft
SOTI
tangoe
cisco Meraki
citrix XenMobile
jamf
SAP
MobileIron
Symantec.
airwatch by vmware

MDM Attributes
ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName
MEID
Model
OperatingSystem
PhoneNumber
PinLock
PolicyMatched
RegisterStatus
SerialNumber
ServerType
SessionId
UDID
UserName
UserNotified

ISE Capabilities for Zero Trust from Workplace

Establish Trust

- User/Device Authentication
- MFA thru Integrations
- Profiling
- Posture + Context
- Guest
- BYOD Onboarding

Enforce Trust-Based Access

- Network based Authorization Policies
- Microsegmentation
- Compliance-based CoA
- Device Administration with TACACS+

Continuously Verify Trust

Integrations :

- Threat Detection
- Behavior Analysis
- Vulnerability Assessment

Respond to Change in Trust

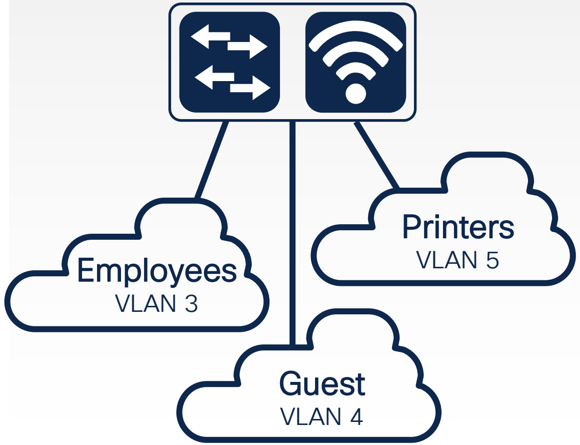
- RADIUS Change of Authorization (CoA)
- Adaptive Network Control (ANC)

ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

Dynamic VLAN Assignments



Employees
VLAN 3

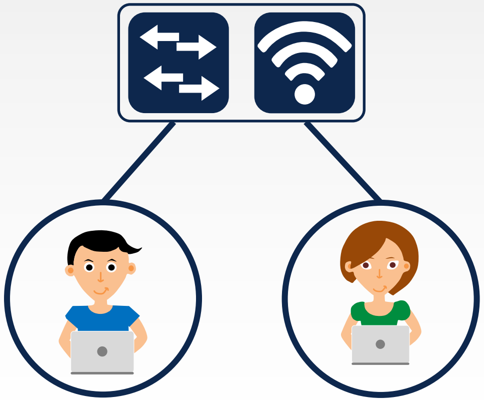
Printers
VLAN 5

Guest
VLAN 4

Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee

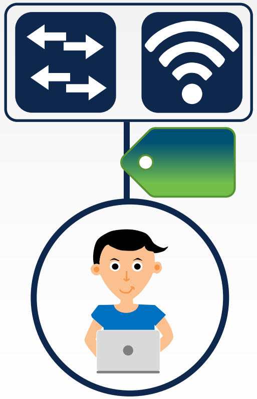
```
permit ip any any
```

Contractor

```
deny ip host <critical>
permit ip any any
```

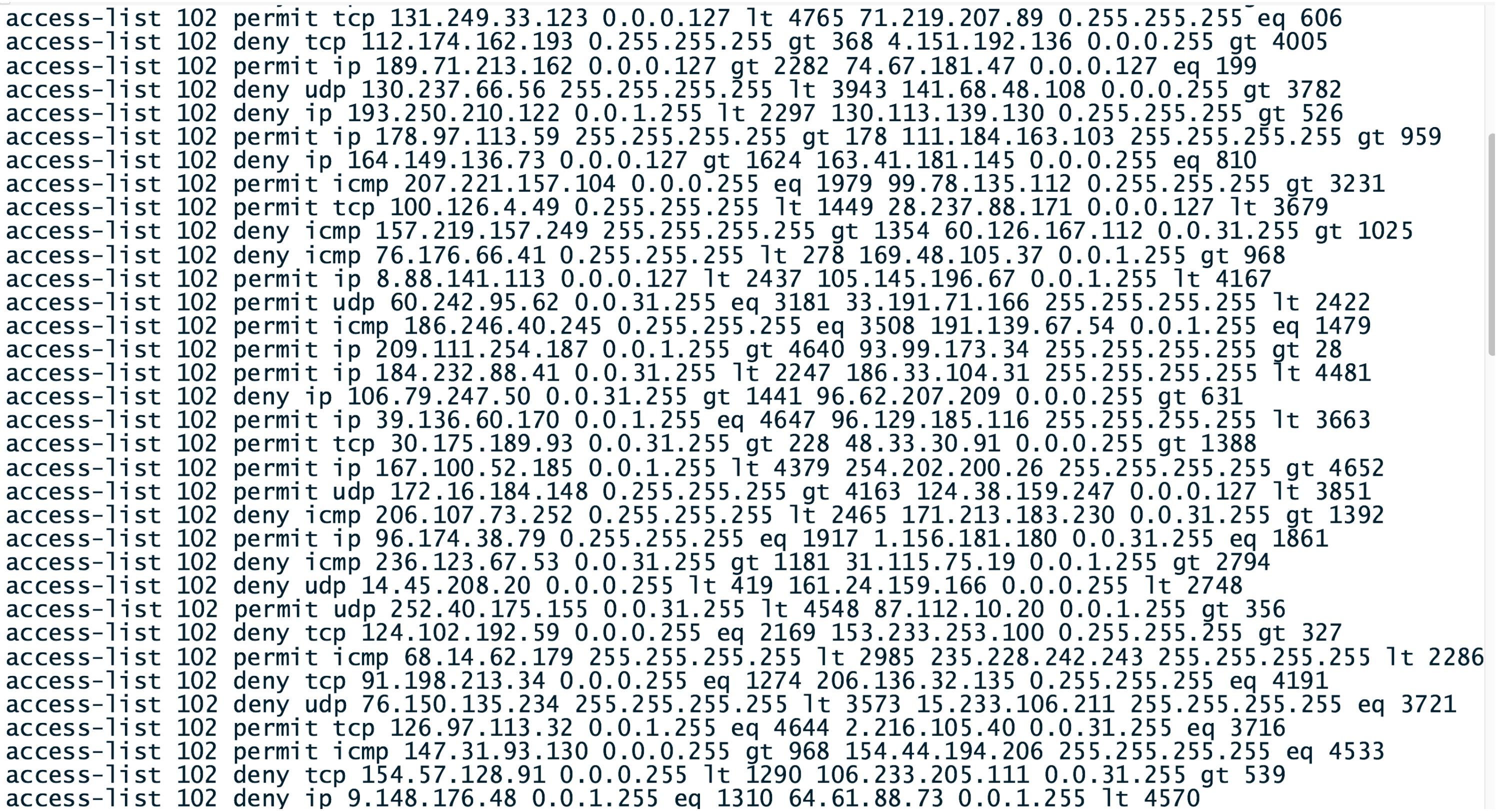
Security Group Tags

Cisco Group-Based Policy



16-bit SGT assignment and
SGT based Access Control

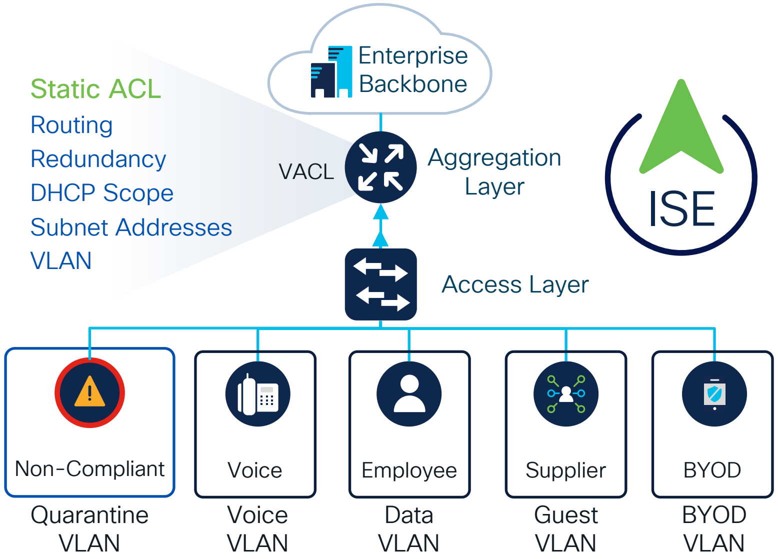
Can You See the Business Intent Here?



```
access-list 102 permit tcp 131.249.33.123 0.0.0.127 lt 4765 71.219.207.89 0.255.255.255 eq 606
access-list 102 deny tcp 112.174.162.193 0.255.255.255 gt 368 4.151.192.136 0.0.0.255 gt 4005
access-list 102 permit ip 189.71.213.162 0.0.0.127 gt 2282 74.67.181.47 0.0.0.127 eq 199
access-list 102 deny udp 130.237.66.56 255.255.255.255 lt 3943 141.68.48.108 0.0.0.255 gt 3782
access-list 102 deny ip 193.250.210.122 0.0.1.255 lt 2297 130.113.139.130 0.255.255.255 gt 526
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
```

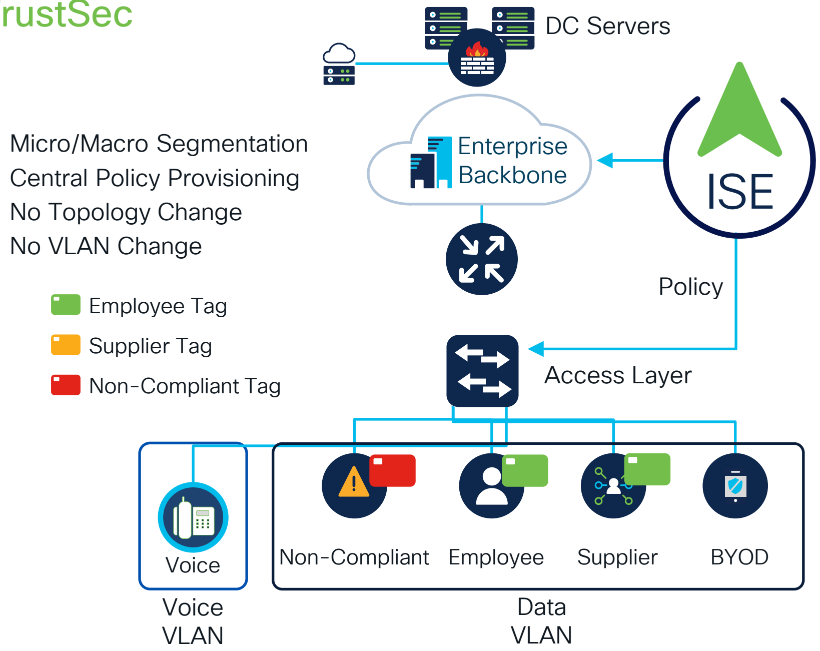
Group Based Policy Simplifies Segmentation

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

TrustSec



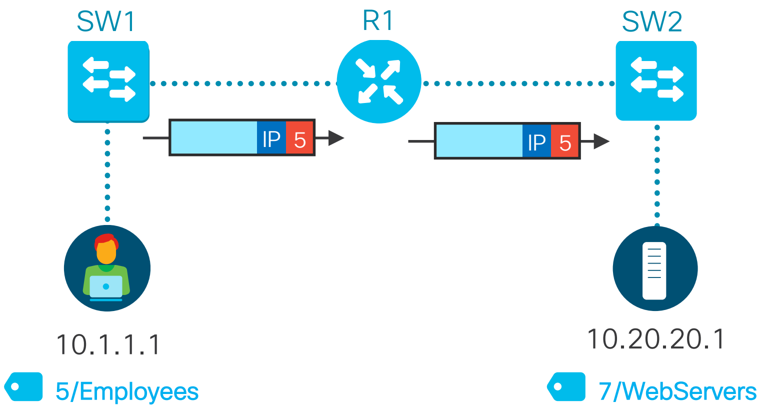
Micro/Macro Segmentation
Central Policy Provisioning
No Topology Change
No VLAN Change

🟩 Employee Tag
🟧 Supplier Tag
🟥 Non-Compliant Tag

Use existing topology and automate security policy to reduce OpEx

TrustSec Propagation

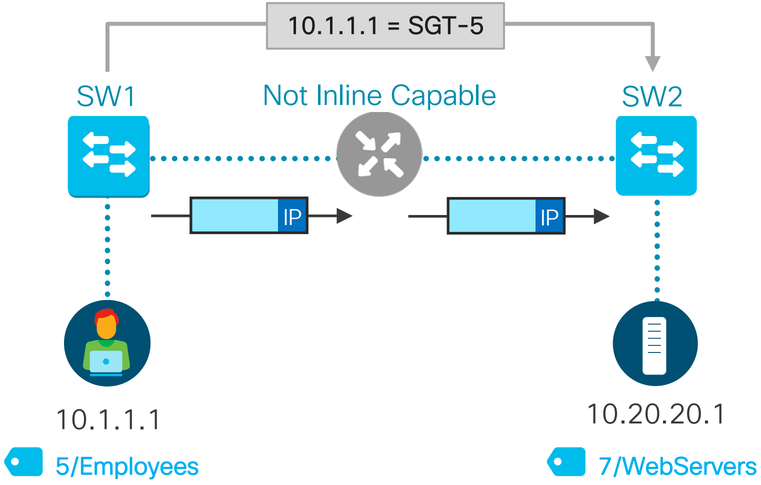
DATA PLANE PROPAGATION (INLINE TAGGING)



SGT carried inline in the data traffic. Methods include, SGT over:

- Ethernet
- MACSec
- LISP/VxLAN
- IPSec
- DMVPN
- GETVPN

CONTROL PLANE PROPAGATION (SXP)

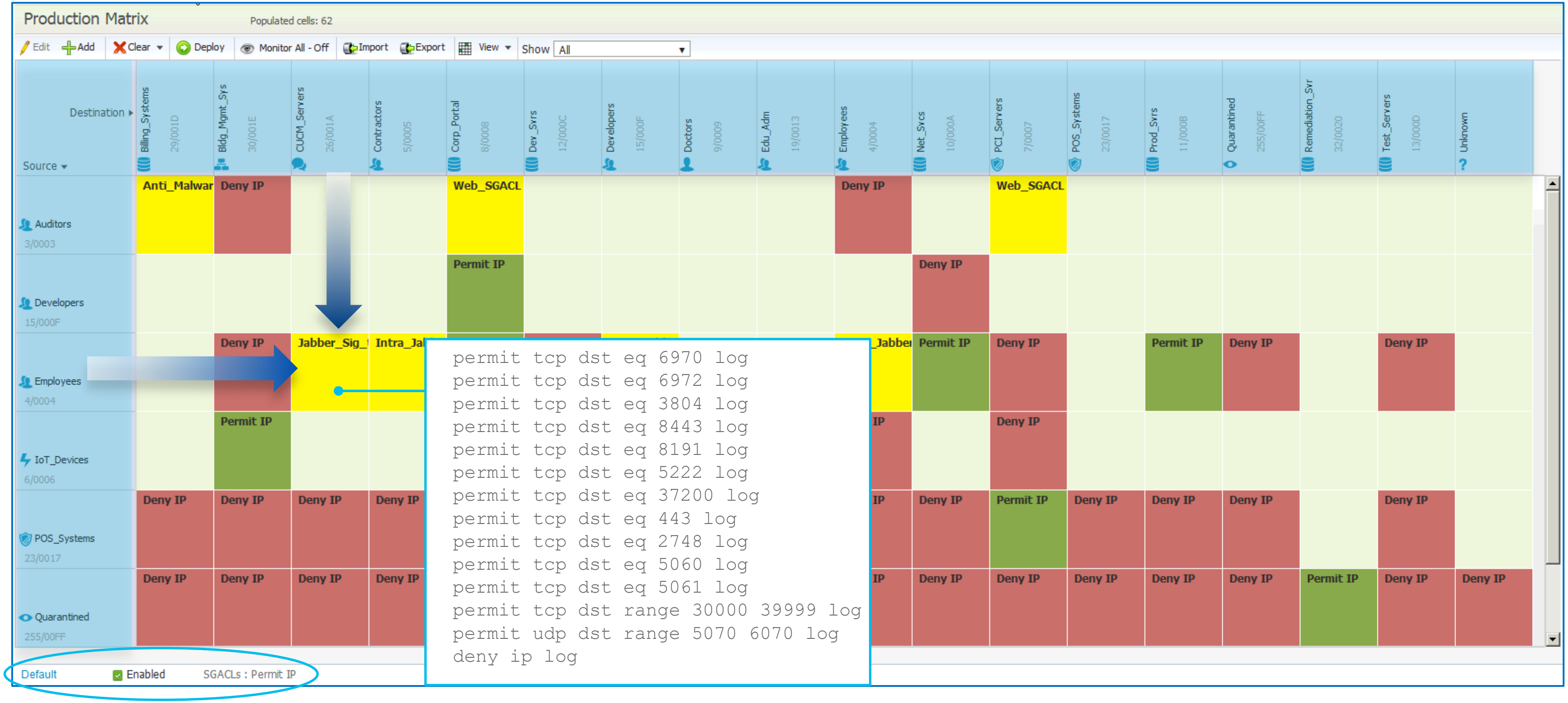


IP-to-SGT data shared over control protocol. No SGT in the data plane. Methods include, IP-to-SGT exchange over:

- SXP
- pxGrid

ISE Policy Matrix (SGACL)

- Centralized policy for switches, routers, WLCs and APs



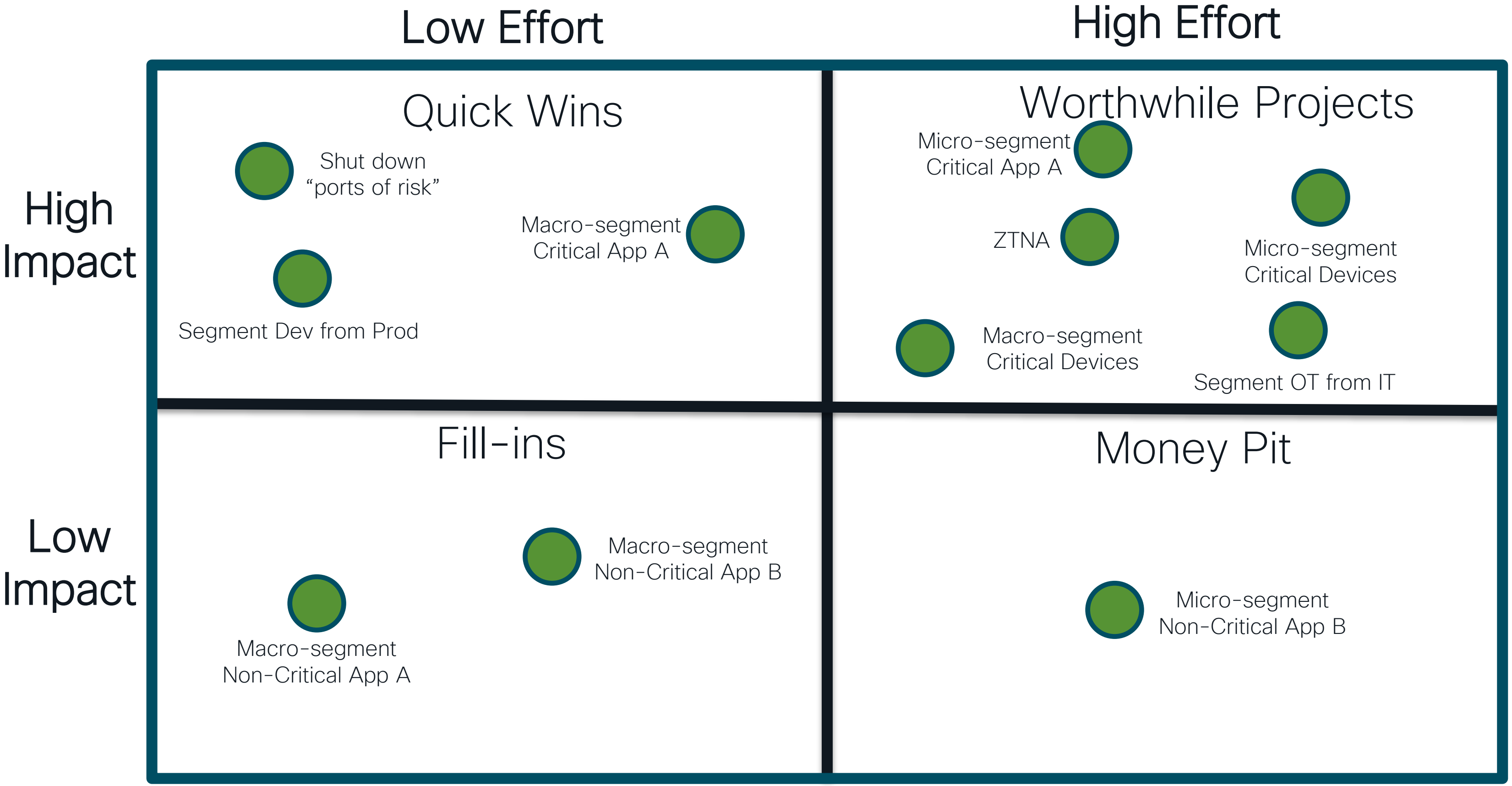
Destination ▸ Source ▾	Billing_Systems 29/001D	Bldg_Mgmt_Sys 30/001E	CUCM_Servers 26/001A	Contractors 5/0005	Corp_Portal 8/0008	Dev_Svrs 12/000C	Developers 15/000F	Doctors 9/0009	Edu_Adm 19/0013	Employees 4/0004	Net_Svcs 10/000A	PCI_Servers 7/0007	POS_Systems 23/0017	Prod_Svrs 11/000B	Quarantined 255/00FF	Remediation_Svr 32/0020	Test_Servers 13/000D	Unknown
Auditors 3/0003	Anti_Malwar	Deny IP			Web_SGACL					Deny IP		Web_SGACL						
Developers 15/000F					Permit IP						Deny IP							
Employees 4/0004		Deny IP	Jabber_Sig_	Intra_Jal						_Jabber	Permit IP	Deny IP		Permit IP	Deny IP		Deny IP	
IoT_Devices 6/0006		Permit IP								IP		Deny IP						
POS_Systems 23/0017	Deny IP	Deny IP	Deny IP	Deny IP						IP	Deny IP	Permit IP	Deny IP	Deny IP	Deny IP		Deny IP	
Quarantined 255/00FF	Deny IP	Deny IP	Deny IP	Deny IP						IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP

Default ☑ Enabled SGACLs : Permit IP

```
permit tcp dst eq 6970 log
permit tcp dst eq 6972 log
permit tcp dst eq 3804 log
permit tcp dst eq 8443 log
permit tcp dst eq 8191 log
permit tcp dst eq 5222 log
permit tcp dst eq 37200 log
permit tcp dst eq 443 log
permit tcp dst eq 2748 log
permit tcp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst range 30000 39999 log
permit udp dst range 5070 6070 log
deny ip log
```

Segmentation Strategy and Architectures

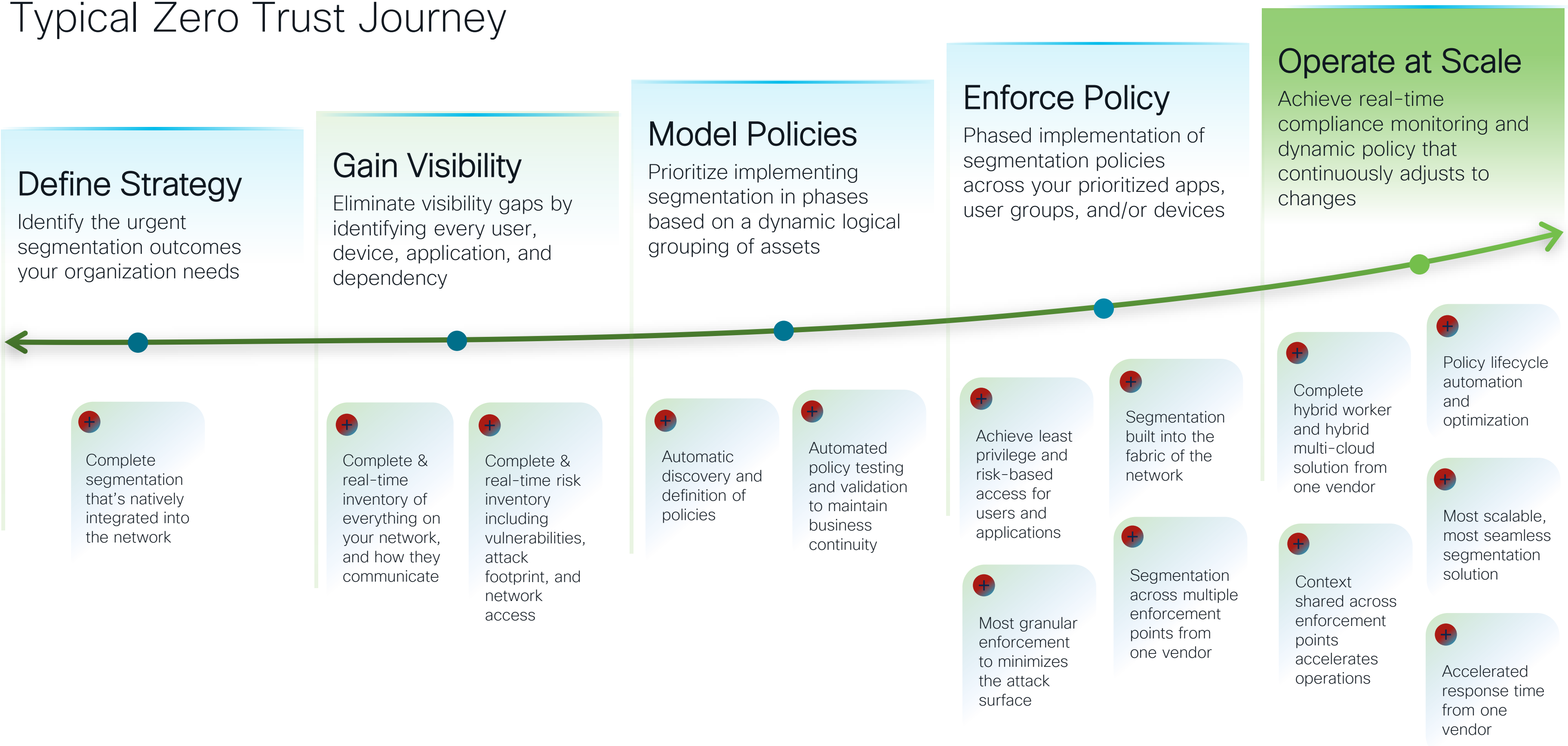
Network Segmentation Project Prioritization



	Low Effort	High Effort
High Impact	Quick Wins Shut down “ports of risk” Macro-segment Critical App A Segment Dev from Prod	Worthwhile Projects Micro-segment Critical App A ZTNA Micro-segment Critical Devices Macro-segment Critical Devices Segment OT from IT
Low Impact	Fill-ins Macro-segment Non-Critical App B Macro-segment Non-Critical App A	Money Pit Micro-segment Non-Critical App B

Segmentation is a Continuous Process

Typical Zero Trust Journey



Define Strategy

Identify the urgent segmentation outcomes your organization needs

- Complete segmentation that's natively integrated into the network

Gain Visibility

Eliminate visibility gaps by identifying every user, device, application, and dependency

- Complete & real-time inventory of everything on your network, and how they communicate
- Complete & real-time risk inventory including vulnerabilities, attack footprint, and network access

Model Policies

Prioritize implementing segmentation in phases based on a dynamic logical grouping of assets

- Automatic discovery and definition of policies
- Automated policy testing and validation to maintain business continuity

Enforce Policy

Phased implementation of segmentation policies across your prioritized apps, user groups, and/or devices

- Achieve least privilege and risk-based access for users and applications
- Most granular enforcement to minimizes the attack surface
- Segmentation built into the fabric of the network
- Segmentation across multiple enforcement points from one vendor

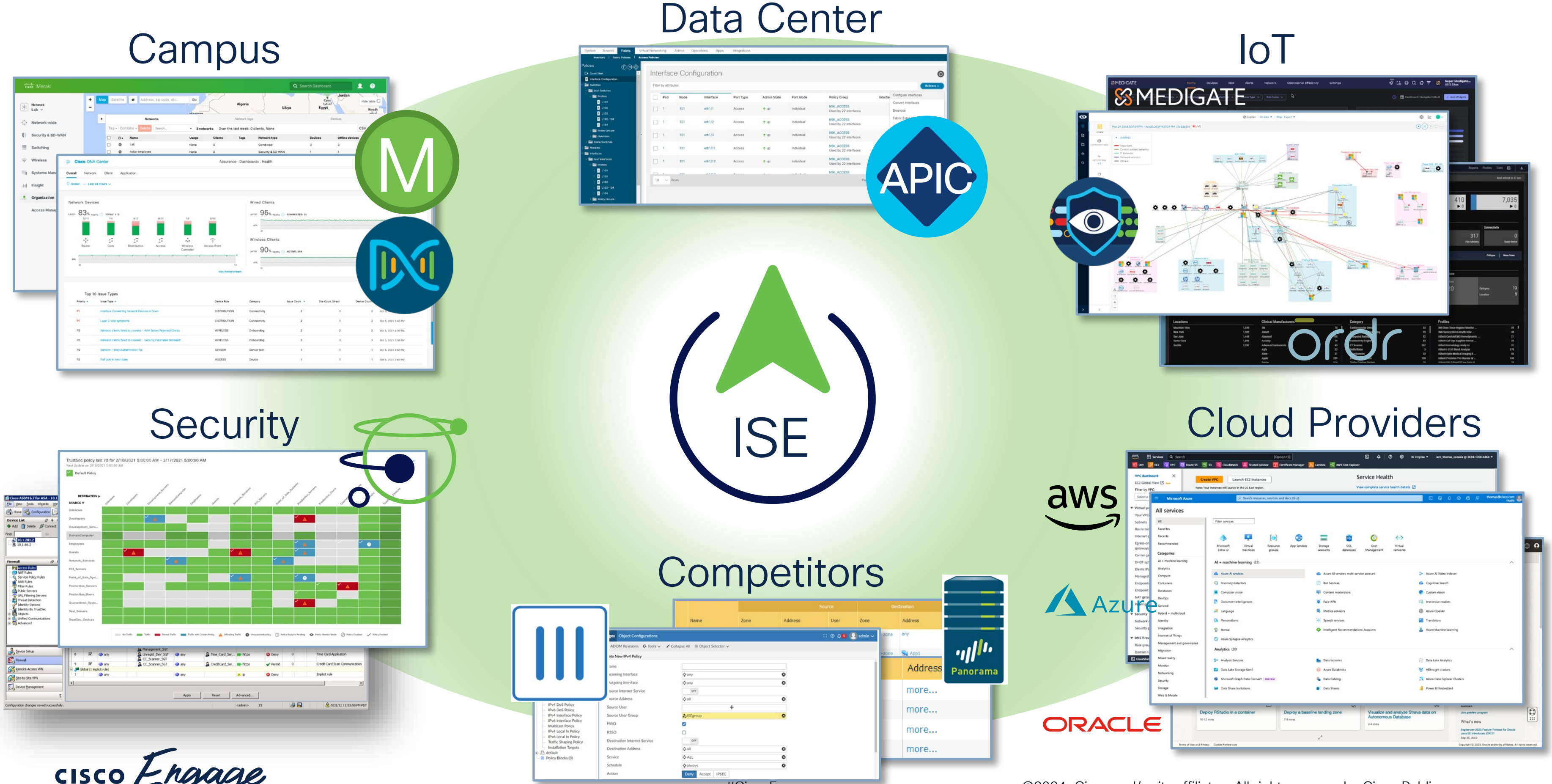
Operate at Scale

Achieve real-time compliance monitoring and dynamic policy that continuously adjusts to changes

- Complete hybrid worker and hybrid multi-cloud solution from one vendor
- Context shared across enforcement points accelerates operations
- Policy lifecycle automation and optimization
- Most scalable, most seamless segmentation solution
- Accelerated response time from one vendor

How Can We Ease Segmentation Policy Lifecycle Management?

ISE is the Core of Cisco’s Cross-Domain Policy



Data Center

Campus

IoT

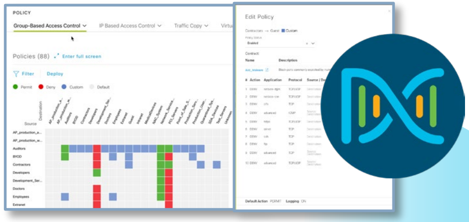
Security

Cloud Providers

Competitors

ISE Unifies the Cisco Segmentation Strategy

cisco Catalyst



POLICY

Group-Based Access Control | IP Based Access Control | Traffic Copy | Virtu

Policies (88) Enter full screen

Filter | Deploy

● Permit ● Deny ● Custom ● Default

Destination / Source

AP_production_a...
AP_production_w...
Auditors
BYOD
Contractors
Developers
Development_Ser...
Doctors
Employees
Extranet

Edit Policy

Contractors → Guest ■ Custom

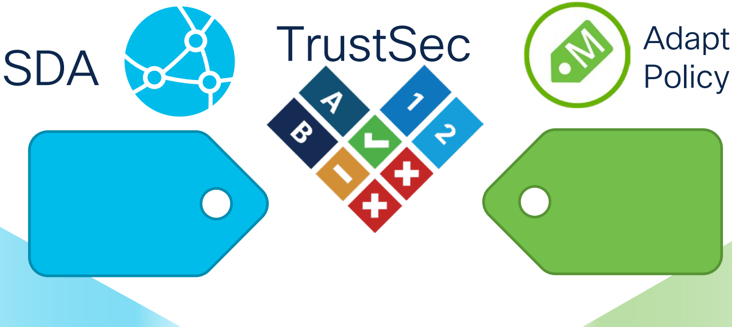
Policy Status: Enabled

Contract

Name	Description
Anti_Malware	Block ports commonly exploited by ma

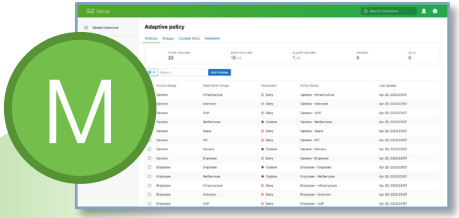
#	Action	Application	Protocol	Source / De
1	DENY	netbios-dgm	TCP/UDP	[illegible]
2	DENY	netbios-ssn	TCP/UDP	[illegible]
3	DENY	nfs	TCP	[illegible]
4	DENY	advanced	ICMP	[illegible]
5	DENY	https	TCP/UDP	[illegible]
6	DENY	telnet	TCP	[illegible]
7	DENY	ssh	TCP	[illegible]
8	DENY	ftp	TCP	[illegible]
9	DENY	advanced	TCP	[illegible]
10	DENY	advanced	TCP/UDP	[illegible]

Default Action PERMIT   Logging ON



Adaptive Policy

cisco Meraki



Meraki | Search Dashboard

Global Overview

Adaptive policy

Policies | Groups | Custom ACLs | Networks

TOTAL POLICIES 25 | DENY POLICIES 19/25 | ALLOW POLICIES 1/25 | GROUPS 8 | ACLS 6

Search... | Add Policies

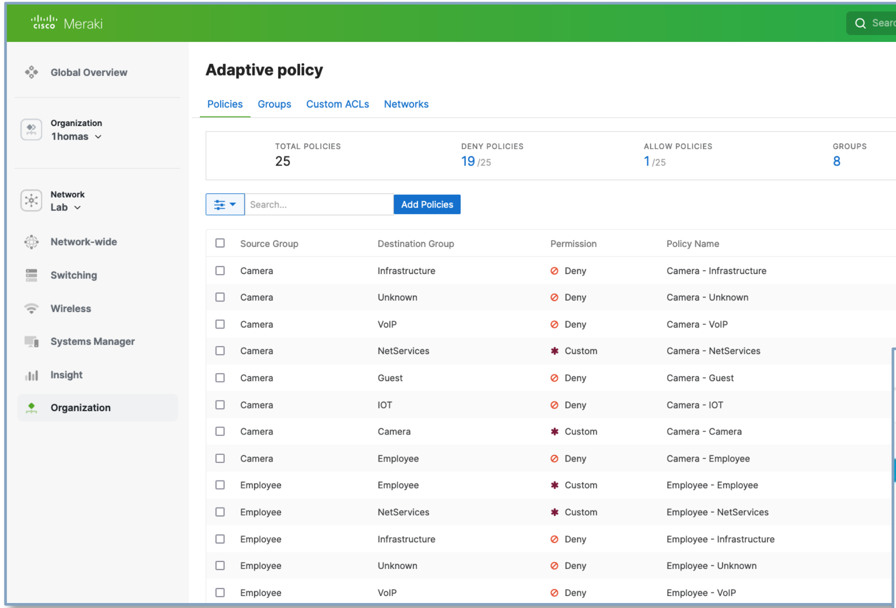
Source Group	Destination Group	Permission	Policy Name	Last update
Camera	Infrastructure	Deny	Camera - Infrastructure	Apr 20, 2023 23:57
Camera	Unknown	Deny	Camera - Unknown	Apr 20, 2023 23:57
Camera	VoIP	Deny	Camera - VoIP	Apr 20, 2023 23:57
Camera	NetServices	Custom	Camera - NetServices	Apr 20, 2023 23:57
Camera	Guest	Deny	Camera - Guest	Apr 20, 2023 23:57
Camera	IOT	Deny	Camera - IOT	Apr 20, 2023 23:57
Camera	Camera	Custom	Camera - Camera	Apr 20, 2023 23:57
Camera	Employee	Deny	Camera - Employee	Apr 20, 2023 23:57
Employee	Employee	Custom	Employee - Employee	Apr 20, 2023 23:57
Employee	NetServices	Custom	Employee - NetServices	Apr 20, 2023 23:57
Employee	Infrastructure	Deny	Employee - Infrastructure	Apr 20, 2023 23:57
Employee	Unknown	Deny	Employee - Unknown	Apr 20, 2023 23:57
Employee	VoIP	Deny	Employee - VoIP	Apr 20, 2023 23:57

Group-based Policy Sync with Meraki dashboard

ISE 3.2p1+

Adaptive Policy

ISE SGT



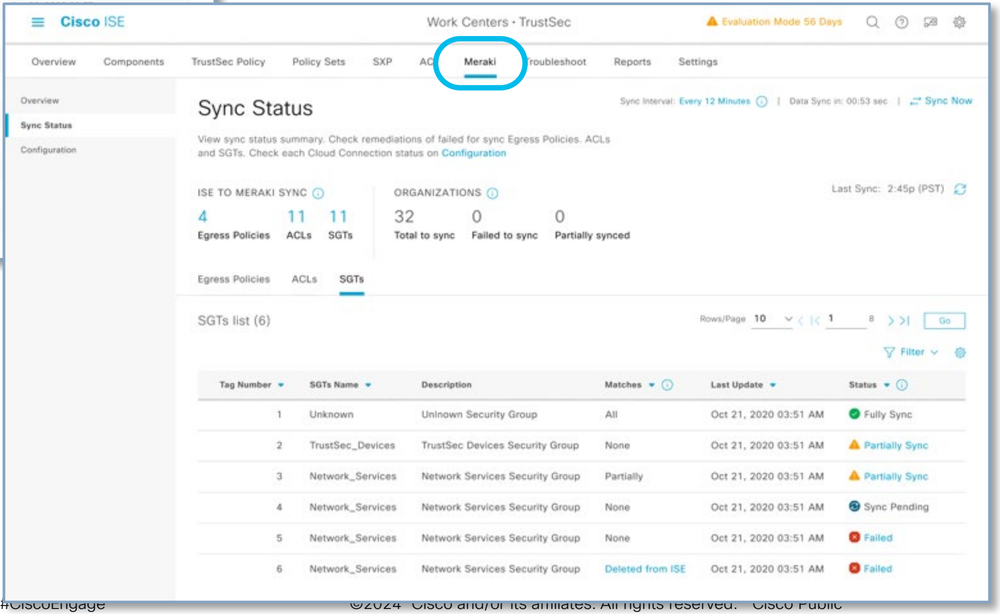
Adaptive policy

Policies | Groups | Custom ACLs | Networks

TOTAL POLICIES	DENY POLICIES	ALLOW POLICIES	GROUPS	ACLS
25	19 /25	1 /25	8	6

Search... | Add Policies

	Source Group	Destination Group	Permission	Policy Name	Last update
□	Camera	Infrastructure	⊘ Deny	Camera - Infrastructure	Apr 20, 2023 23:57
□	Camera	Unknown	⊘ Deny	Camera - Unknown	Apr 20, 2023 23:57
□	Camera	VoIP	⊘ Deny	Camera - VoIP	Apr 20, 2023 23:57
□	Camera	NetServices	✱ Custom	Camera - NetServices	
□	Camera	Guest	⊘ Deny	Camera - Guest	
□	Camera	IOT	⊘ Deny	Camera - IOT	
□	Camera	Camera	✱ Custom	Camera - Camera	
□	Camera	Employee	⊘ Deny	Camera - Employee	
□	Employee	Employee	✱ Custom	Employee - Employee	
□	Employee	NetServices	✱ Custom	Employee - NetServices	
□	Employee	Infrastructure	⊘ Deny	Employee - Infrastructure	
□	Employee	Unknown	⊘ Deny	Employee - Unknown	
□	Employee	VoIP	⊘ Deny	Employee - VoIP	



Sync Status

Sync Interval: Every 12 Minutes | Data Sync in: 00:53 sec | Sync Now

View sync status summary. Check remediations of failed for sync Egress Policies. ACLs and SGTs. Check each Cloud Connection status on Configuration

ISE TO MERAKI SYNC: 4 Egress Policies, 11 ACLs, 11 SGTs

ORGANIZATIONS: 32 Total to sync, 0 Failed to sync, 0 Partially synced

Last Sync: 2:45p (PST)

Egress Policies | ACLs | SGTs

SGTs list (6)

Rows/Page 10 | 1 | 8 | Go

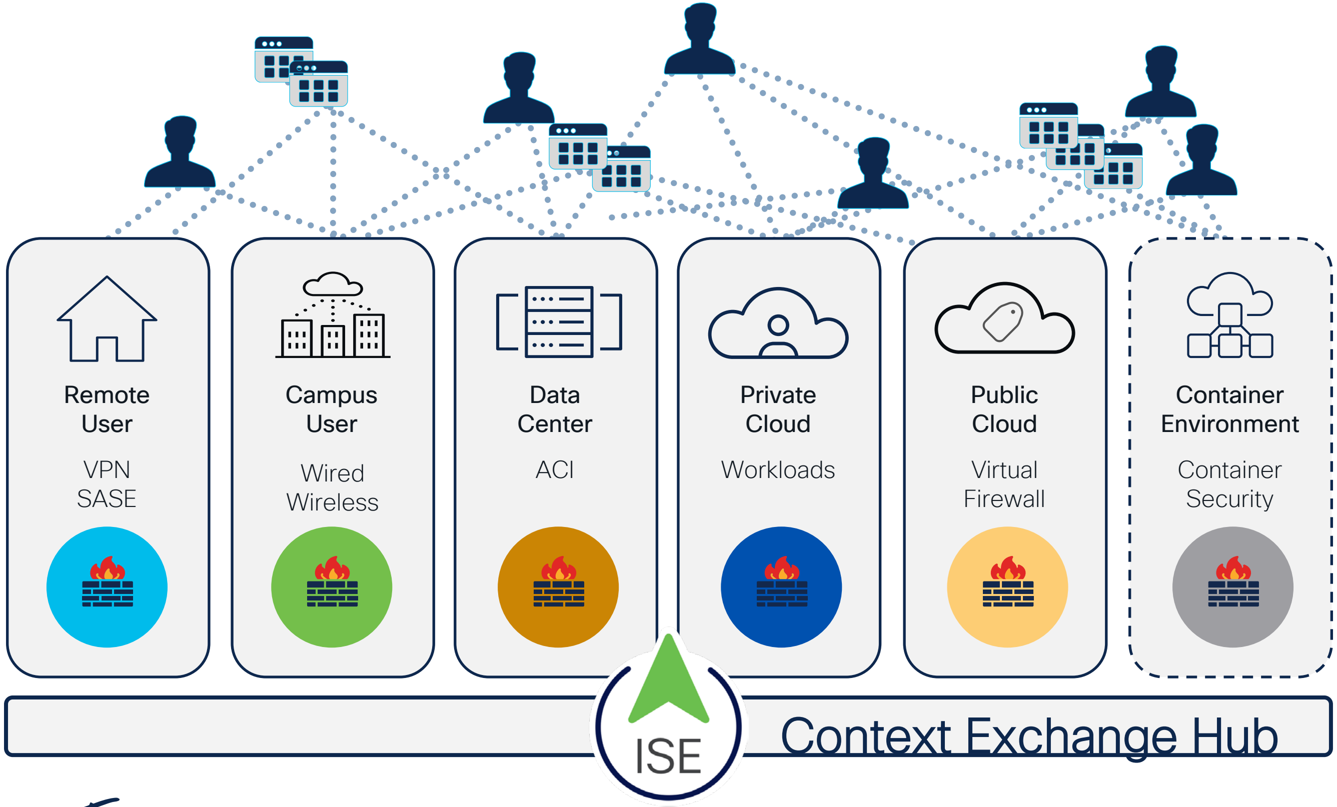
Filter

Tag Number	SGTs Name	Description	Matches	Last Update	Status
1	Unknown	Uninown Security Group	All	Oct 21, 2020 03:51 AM	Fully Sync
2	TrustSec_Devices	TrustSec Devices Security Group	None	Oct 21, 2020 03:51 AM	Partially Sync
3	Network_Services	Network Services Security Group	Partially	Oct 21, 2020 03:51 AM	Partially Sync
4	Network_Services	Network Services Security Group	None	Oct 21, 2020 03:51 AM	Sync Pending
5	Network_Services	Network Services Security Group	None	Oct 21, 2020 03:51 AM	Failed
6	Network_Services	Network Services Security Group	Deleted from ISE	Oct 21, 2020 03:51 AM	Failed

Sync limited to 60 SGTs per org (based on Meraki constraints)

Common Policy with Security Group Tags (SGTs)

The common language across network industry products



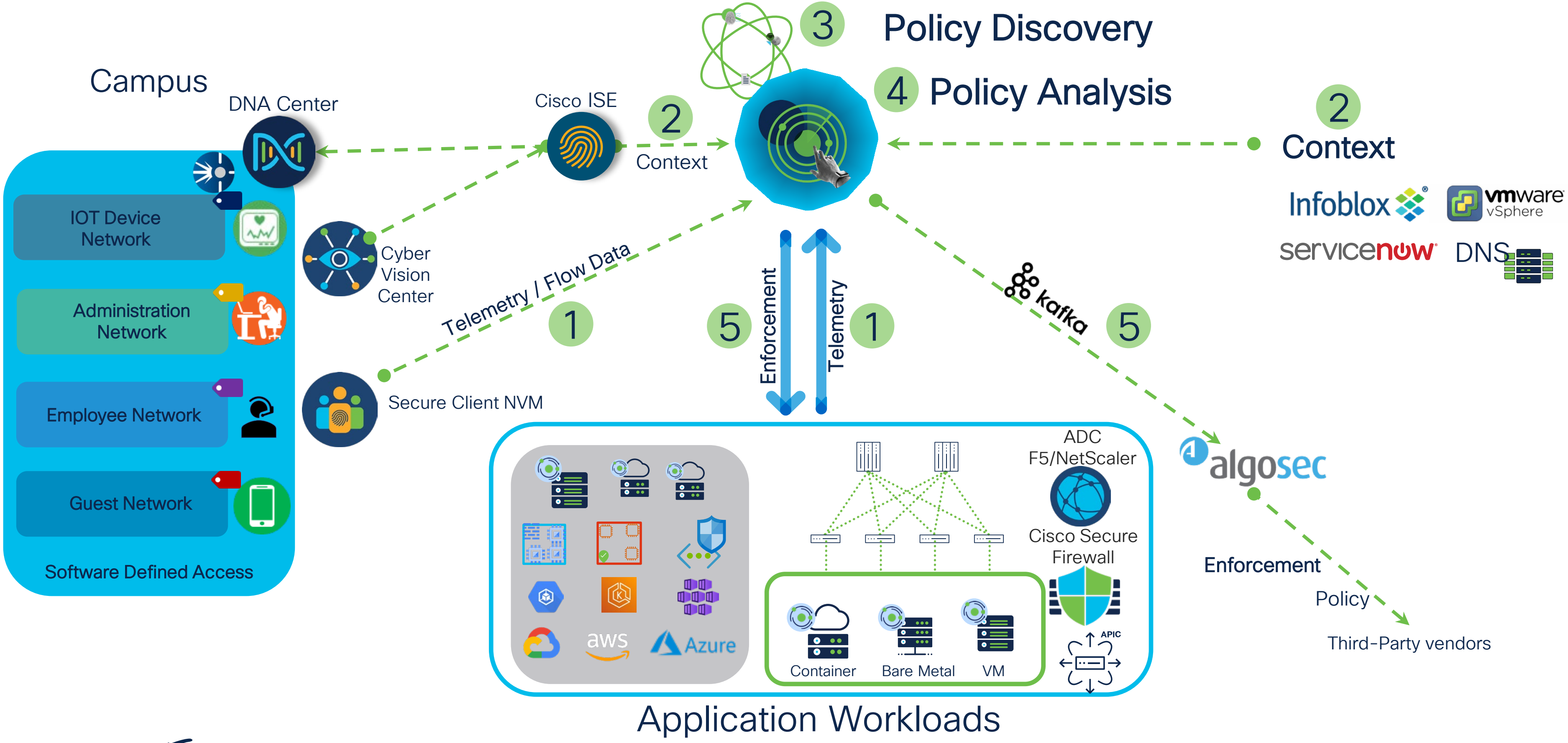
Multiple teams and organizations

Covering multiple dynamic environments

Independent policy models and enforcement points

Inconsistent and siloed islands of policy controls

Harmonize your Zero Trust Segmentation Policy

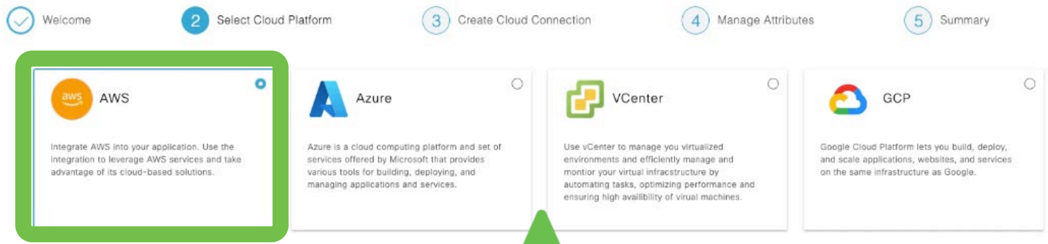


cisco Engage

#CiscoEngage

Classifying Cloud Workloads

ISE 3.4P1



✓ Welcome

2 Select Cloud Platform

3 Create Cloud Connection

4 Manage Attributes

5 Summary

● AWS

Integrate AWS into your application. Use the integration to leverage AWS services and take advantage of its cloud-based solutions.

○ Azure

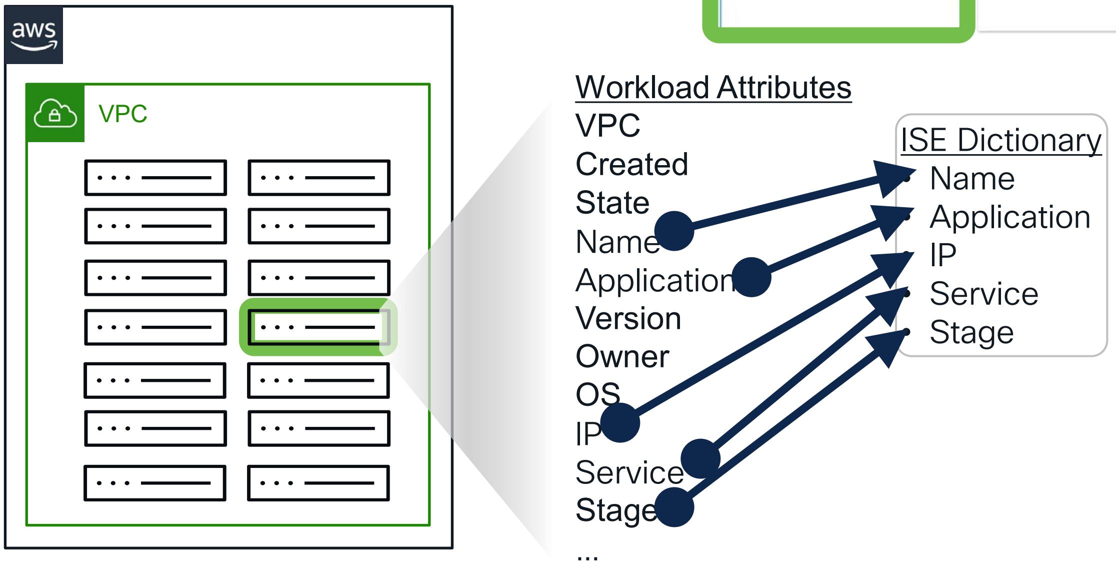
Azure is a cloud computing platform and set of services offered by Microsoft that provides various tools for building, deploying, and managing applications and services.

○ VCenter

Use vCenter to manage you virtualized environments and efficiently manage and montior your virtual infracstructure by automating tasks, optimizing performance and ensuring high availibility of virual machines.

○ GCP

Google Cloud Platform lets you build, deploy, and scale applications, websites, and services on the same infrastructure as Google.



Workload Attributes
VPC
Created
State
Name
Application
Version
Owner
OS
IP
Service
Stage
...

ISE Dictionary
Name
Application
IP
Service
Stage

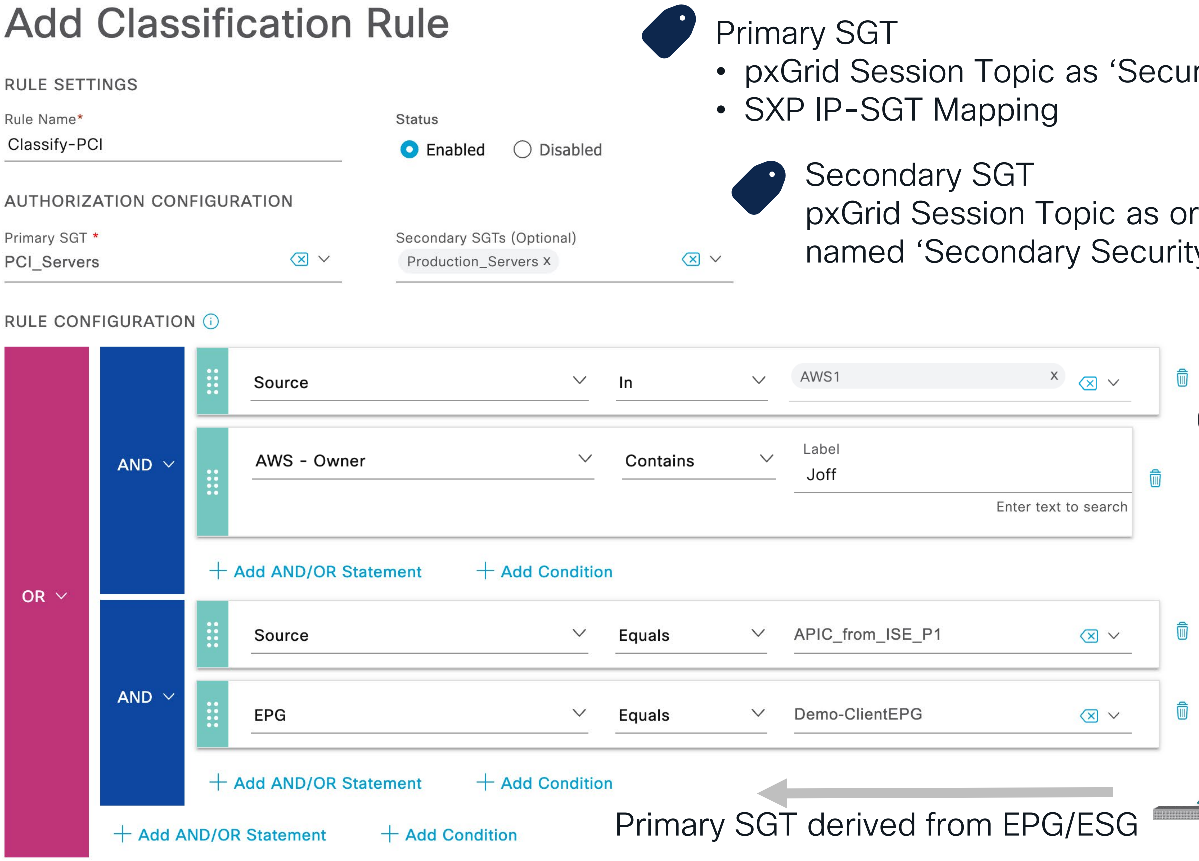
Classification Policy

Primary SGT
Secondary SGT
SXP: SGT-to-IP

ISE Workload Classification Rules

Assign Primary & Secondary SGTs

Classification Conditions



Add Classification Rule

RULE SETTINGS

Rule Name* Classify-PCI

Status ● Enabled ○ Disabled

AUTHORIZATION CONFIGURATION

Primary SGT * PCI_Servers

Secondary SGTs (Optional) Production_Servers x

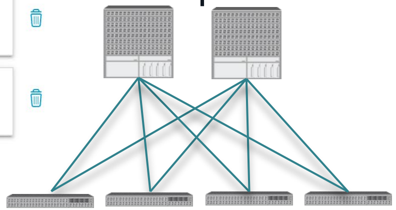
RULE CONFIGURATION

OR	AND	Source	In	AWS1 x
		AWS - Owner	Contains	Label: Joff (Enter text to search)
		+ Add AND/OR Statement	+ Add Condition	
	AND	Source	Equals	APIC_from_ISE_P1
		EPG	Equals	Demo-ClientEPG
		+ Add AND/OR Statement	+ Add Condition	
	+ Add AND/OR Statement	+ Add Condition		

Primary SGT
- pxGrid Session Topic as ‘Security Group’
- SXP IP-SGT Mapping

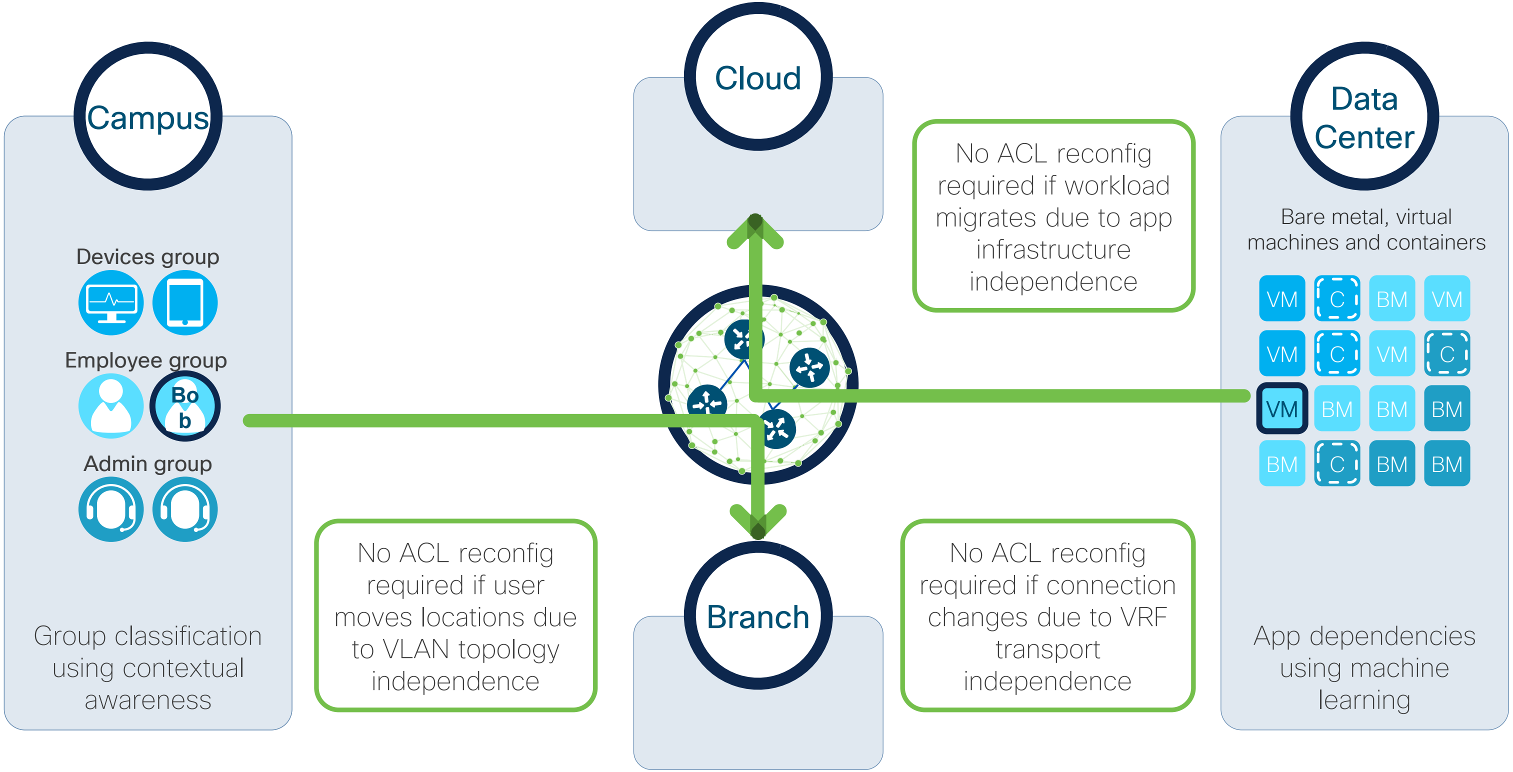
Secondary SGT
pxGrid Session Topic as ordered array named ‘Secondary Security Groups’

ACI Optional



Primary SGT derived from EPG/ESG

Zero-trust access follows user & app anywhere



Group classification using contextual awareness

No ACL reconfig required if user moves locations due to VLAN topology independence

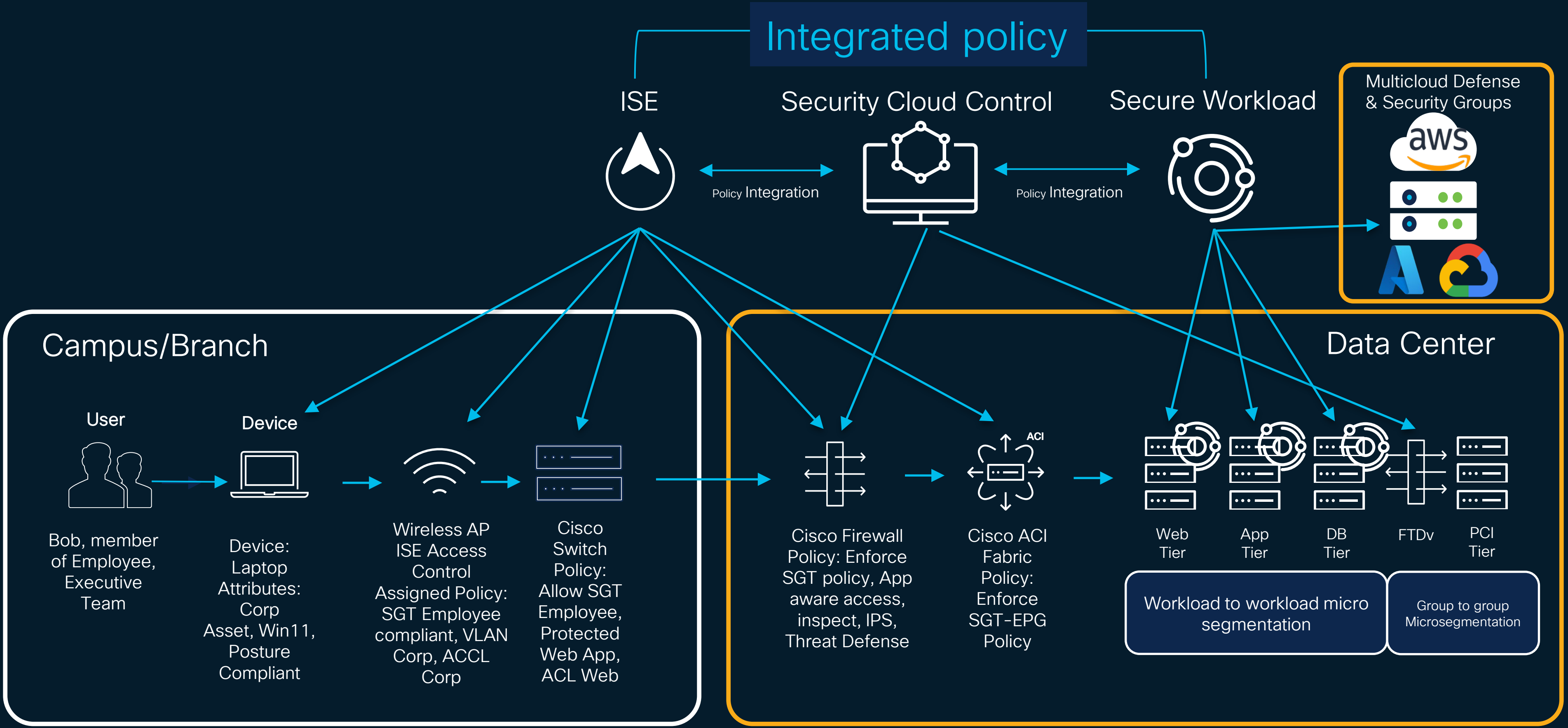
No ACL reconfig required if workload migrates due to app infrastructure independence

No ACL reconfig required if connection changes due to VRF transport independence

Bare metal, virtual machines and containers

App dependencies using machine learning

Cisco End-to-End Zero Trust Segmentation (ZTS)



Integrated policy

ISE

Security Cloud Control

Secure Workload

Multicloud Defense & Security Groups

Campus/Branch

User

Bob, member of Employee, Executive Team

Device

Device: Laptop Attributes: Corp Asset, Win11, Posture Compliant

Wireless AP ISE Access Control Assigned Policy: SGT Employee compliant, VLAN Corp, ACCL Corp

Cisco Switch Policy: Allow SGT Employee, Protected Web App, ACL Web

Data Center

Cisco Firewall Policy: Enforce SGT policy, App aware access, inspect, IPS, Threat Defense

Cisco ACI Fabric Policy: Enforce SGT-EPG Policy

Web Tier

App Tier

DB Tier

FTDv

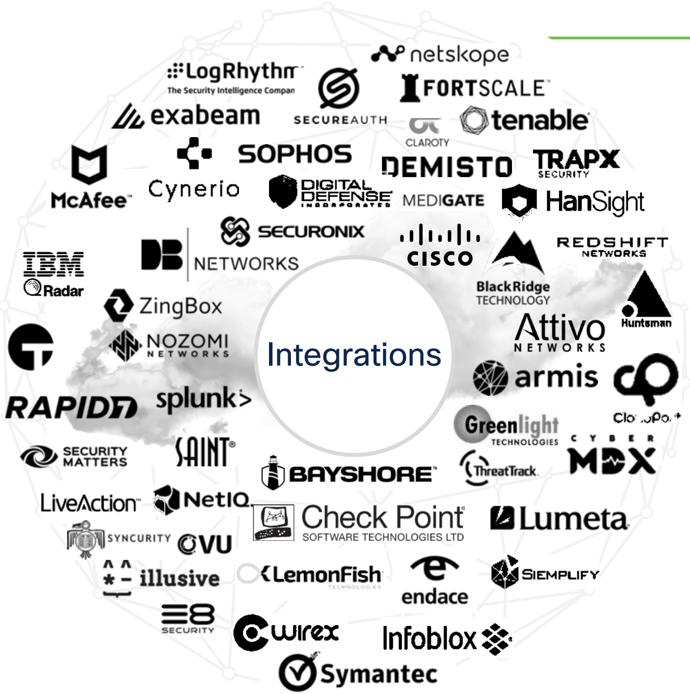
PCI Tier

Workload to workload micro segmentation

Group to group Microsegmentation

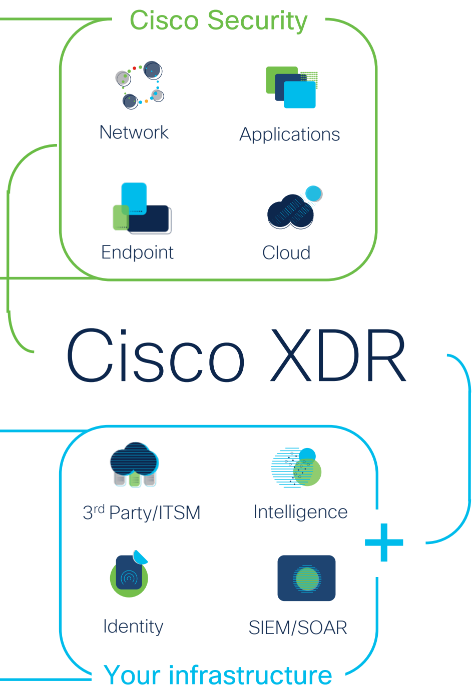
Cisco XDR and Zero Trust

Combing threat and trust centric security with the power of integrations and the simplicity of operations



More cross-team use cases simplified with visibility and automation

More integrated products across partner ecosystem and beyond



Cisco Security

Network

Applications

Endpoint

Cloud

Cisco XDR

+

3rd Party/ITSM

Intelligence

Identity

SIEM/SOAR

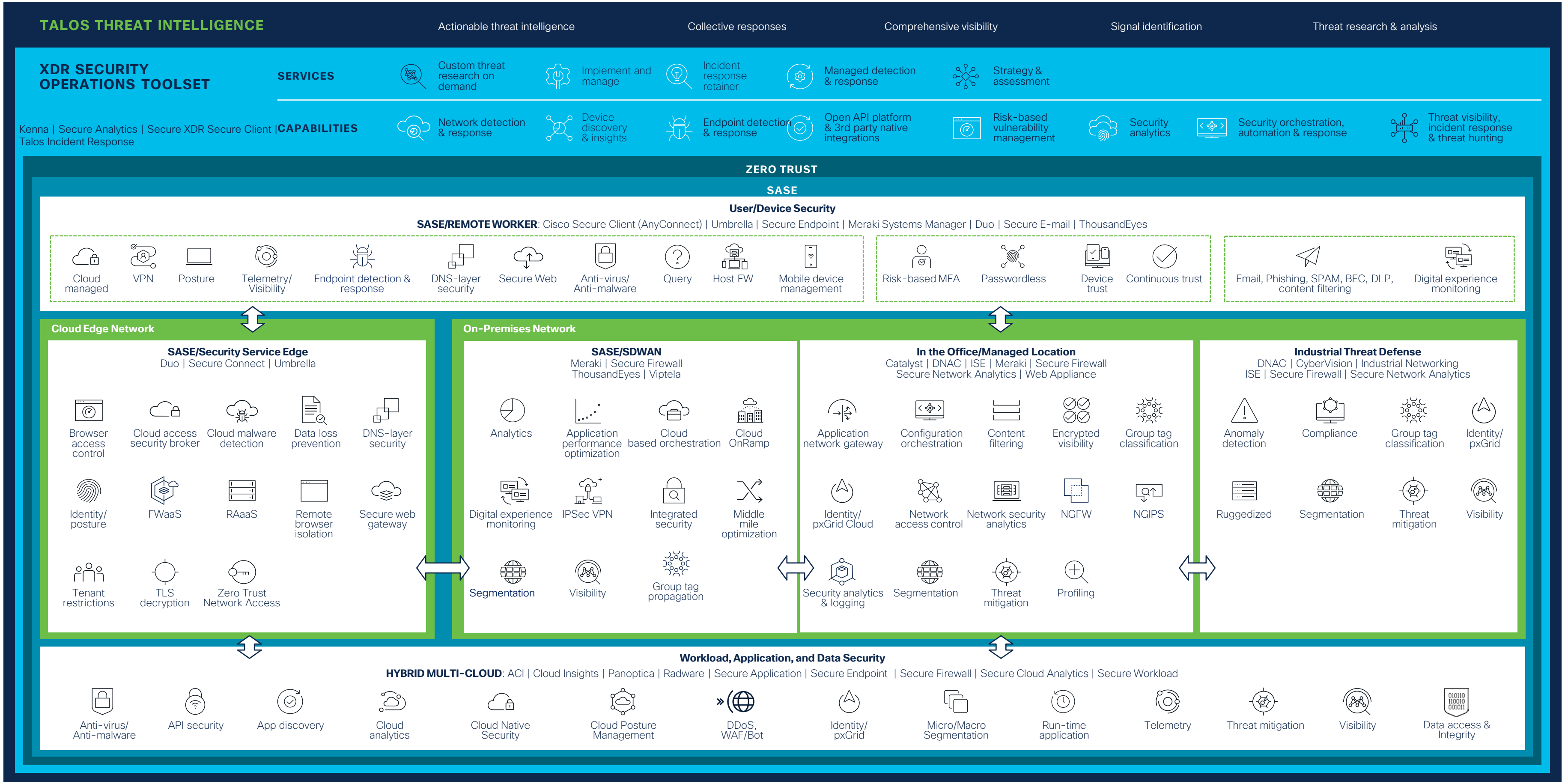
Your infrastructure

Zero Trust Strategy

CISCO SECURE

Security Reference Architecture

cisco.com/go/sra v3.11



TALOS THREAT INTELLIGENCE

Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Kenna | Secure Analytics | Secure XDR Secure Client | Talos Incident Response

SERVICES

Custom threat research on demand | Implement and manage | Incident response retainer | Managed detection & response | Strategy & assessment

CAPABILITIES

Network detection & response | Device discovery & insights | Endpoint detection & response | Open API platform & 3rd party native integrations | Risk-based vulnerability management | Security analytics | Security orchestration, automation & response | Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User/Device Security

SASE/REMOTE WORKER: Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

Cloud managed | VPN | Posture | Telemetry/ Visibility | Endpoint detection & response | DNS-layer security | Secure Web | Anti-virus/ Anti-malware | Query | Host FW | Mobile device management

Risk-based MFA | Passwordless | Device trust | Continuous trust

Email, Phishing, SPAM, BEC, DLP, content filtering | Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge
Duo | Secure Connect | Umbrella

Browser access control | Cloud access security broker | Cloud malware detection | Data loss prevention | DNS-layer security | Identity/ posture | FWaaS | RAaaS | Remote browser isolation | Secure web gateway | Tenant restrictions | TLS decryption | Zero Trust Network Access

On-Premises Network

SASE/SDWAN
Meraki | Secure Firewall
ThousandEyes | Viptela

Analytics | Application performance optimization | Cloud based orchestration | Cloud OnRamp | Digital experience monitoring | IPSec VPN | Integrated security | Middle mile optimization | Segmentation | Visibility | Group tag propagation

In the Office/Managed Location
Catalyst | DNAC | ISE | Meraki | Secure Firewall
Secure Network Analytics | Web Appliance

Application network gateway | Configuration orchestration | Content filtering | Encrypted visibility | Group tag classification | Identity/ pxGrid Cloud | Network access control | Network security analytics | NGFW | NGIPS | Security analytics & logging | Segmentation | Threat mitigation | Profiling

Industrial Threat Defense
DNAC | CyberVision | Industrial Networking
ISE | Secure Firewall | Secure Network Analytics

Anomaly detection | Compliance | Group tag classification | Identity/ pxGrid | Ruggedized | Segmentation | Threat mitigation | Visibility

Workload, Application, and Data Security

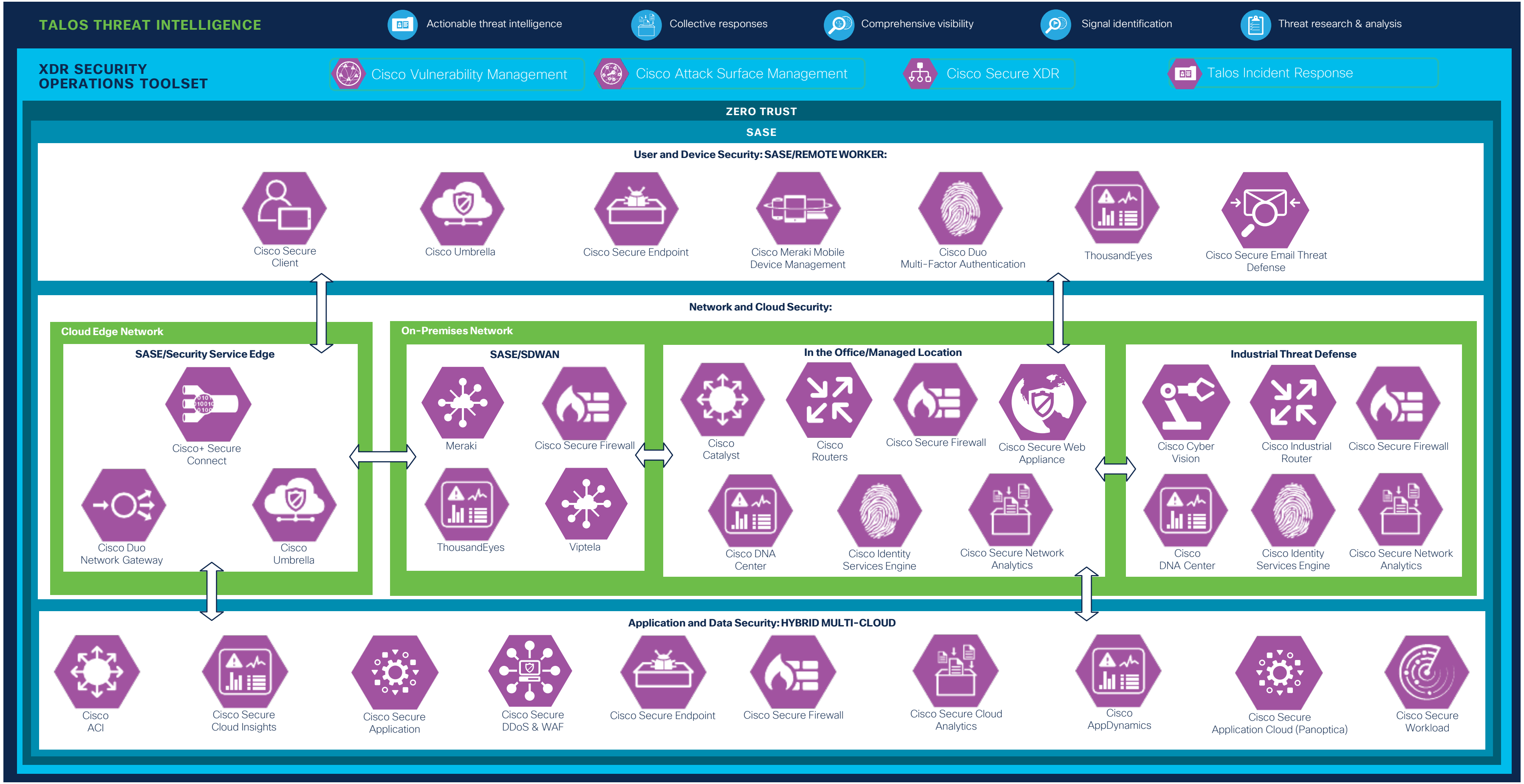
HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Secure Cloud Analytics | Secure Workload

Anti-virus/ Anti-malware | API security | App discovery | Cloud analytics | Cloud Native Security | Cloud Posture Management | DDoS, WAF/Bot | Identity/ pxGrid | Micro/Macro Segmentation | Run-time application | Telemetry | Threat mitigation | Visibility | Data access & Integrity

CISCO Engage

#CiscoEngage

Security Reference Design (SAFE)



TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management

Cisco Attack Surface Management

Cisco Secure XDR

Talos Incident Response

ZERO TRUST

SASE

User and Device Security: SASE/REMOTE WORKER:

Cisco Secure Client

Cisco Umbrella

Cisco Secure Endpoint

Cisco Meraki Mobile Device Management

Cisco Duo Multi-Factor Authentication

ThousandEyes

Cisco Secure Email Threat Defense

Network and Cloud Security:

Cloud Edge Network

SASE/Security Service Edge

Cisco+ Secure Connect

Cisco Duo Network Gateway

Cisco Umbrella

On-Premises Network

SASE/SDWAN

Meraki

Cisco Secure Firewall

ThousandEyes

Viptela

In the Office/Managed Location

Cisco Catalyst

Cisco Routers

Cisco Secure Firewall

Cisco Secure Web Appliance

Cisco DNA Center

Cisco Identity Services Engine

Cisco Secure Network Analytics

Industrial Threat Defense

Cisco Cyber Vision

Cisco Industrial Router

Cisco Secure Firewall

Cisco DNA Center

Cisco Identity Services Engine

Cisco Secure Network Analytics

Application and Data Security: HYBRID MULTI-CLOUD

Cisco ACI

Cisco Secure Cloud Insights

Cisco Secure Application

Cisco Secure DDoS & WAF

Cisco Secure Endpoint

Cisco Secure Firewall

Cisco Secure Cloud Analytics

Cisco AppDynamics

Cisco Secure Application Cloud (Panoptica)

Cisco Secure Workload

Establish Trust

- Device Posture
- Endpoint Security
- Identity Authorization
- Identity Access Policy
- Multi-Factor Authentication
- Mobile Device Management
- SAML & SSO
- Tagging

Enforce Trust-Based Access

- Application Security
- Clientless Remote Access
- Cloud Security
- DDoS Protection
- Firewall
- Intrusion Prevention
- Microsegmentation
- SD-WAN
- Web App Firewall

Continuously Verify Trust

- Anomaly Detection
- Anti-Virus
- Anti-Malware
- Data Loss Prevention (DLP)
- Flow Analytics
- Malware Sandbox
- Network Anti-Malware
- Vulnerability Scanning

Respond to Change in Trust

- Security Orchestration Automation and Response (SOAR)

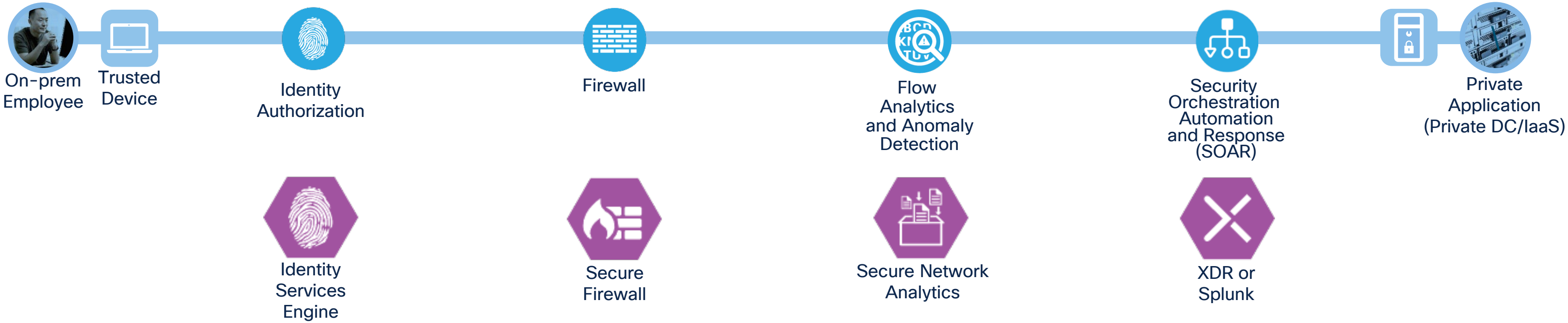
On-prem Employee with Trusted Device:
Accessing Private Application (Private DC/IaaS)

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust



On-prem Employee

Trusted Device

Identity Authorization

Firewall

Flow Analytics and Anomaly Detection

Security Orchestration Automation and Response (SOAR)

Private Application (Private DC/IaaS)

Identity Services Engine

Secure Firewall

Secure Network Analytics

XDR or Splunk

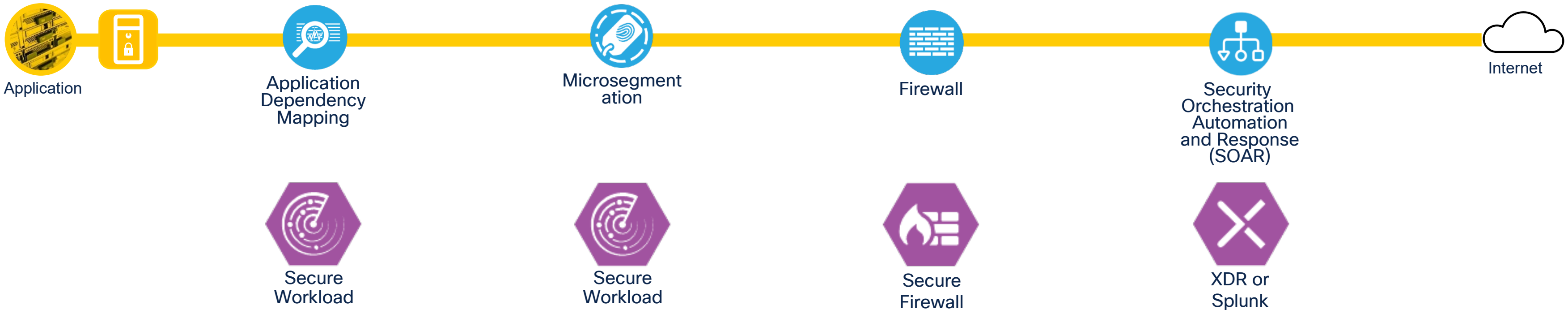
Applications:
API Calls to Internet

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust



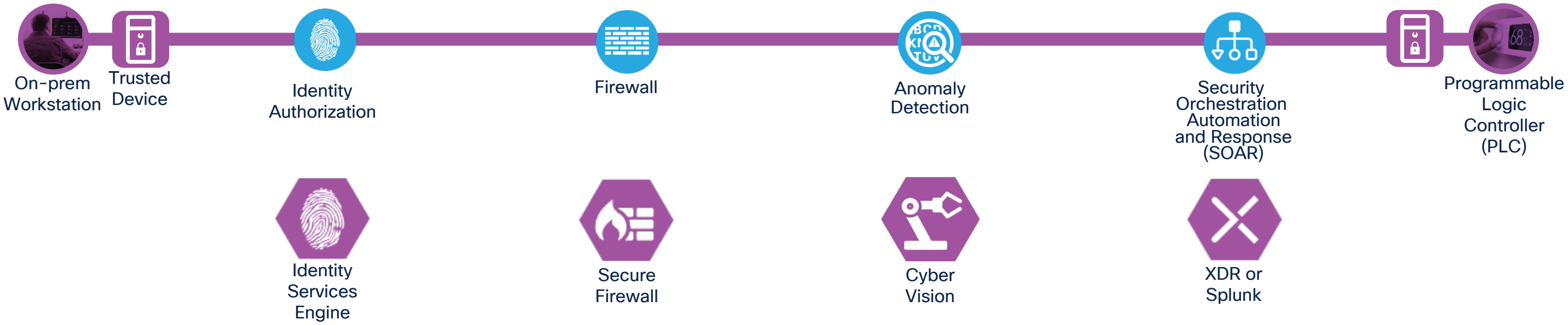
Industrial Security:
On-prem Workstation (Trusted Device) to Programmable Logic Controller

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust



On-prem Workstation

Trusted Device

Identity Authorization

Firewall

Anomaly Detection

Security Orchestration Automation and Response (SOAR)

Programmable Logic Controller (PLC)

Identity Services Engine

Secure Firewall

Cyber Vision

XDR or Splunk

cisco Engage

SAFE CVD: Cisco Zero Trust Architecture Guide

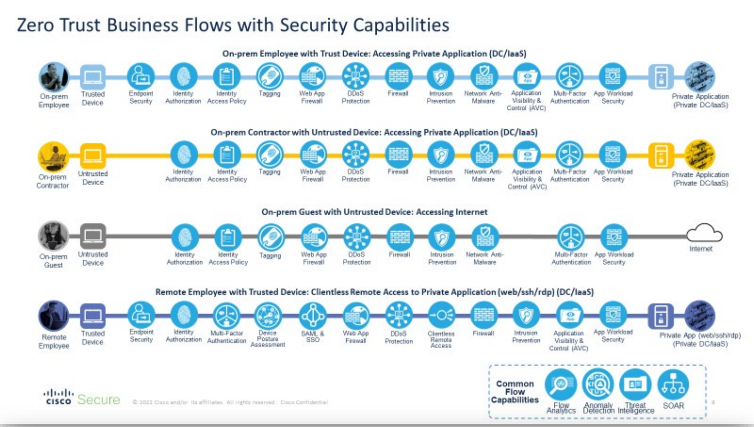
ZT capabilities guidelines

cisco Secure

Cisco Zero Trust Architecture Guide Deck

Solution Architecture Team – SAFE CVDs
July 5, 2022

https://cisco.com/go/safe



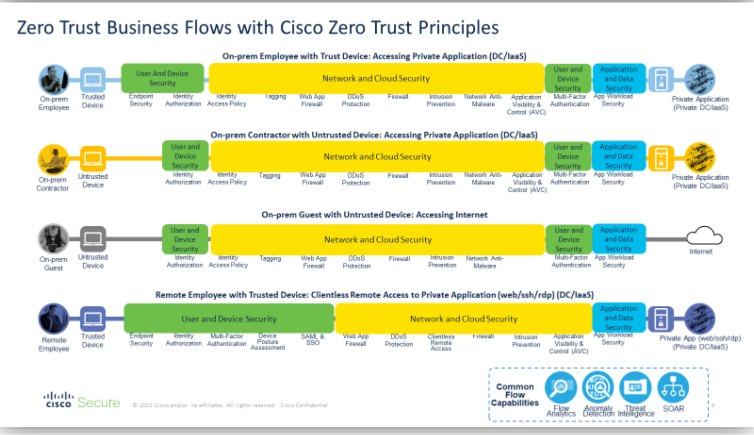
Zero Trust Business Flows with Security Capabilities

On-prem Employee with Trust Device: Accessing Private Application (DC/IaaS)

On-prem Contractor with Untrusted Device: Accessing Private Application (DC/IaaS)

On-prem Guest with Untrusted Device: Accessing Internet

Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)



Zero Trust Business Flows with Cisco Zero Trust Principles

On-prem Employee with Trust Device: Accessing Private Application (DC/IaaS)

On-prem Contractor with Untrusted Device: Accessing Private Application (DC/IaaS)

On-prem Guest with Untrusted Device: Accessing Internet

Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)

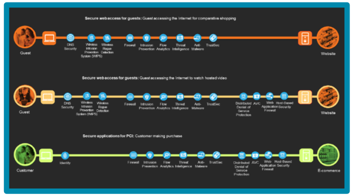
Common Ways to Leverage SAFE

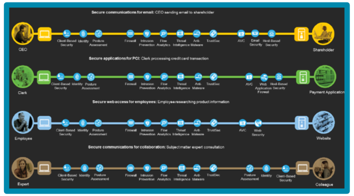
Reference Architectures

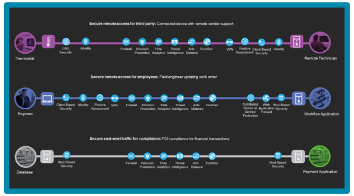
Documented reference materials that provide validated solutions for common architectures and solution needs.

Architecture Workshops

A lightweight process of identifying customer needs and possible missing capabilities to help select the most appropriate solutions.

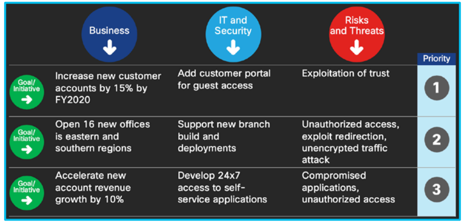




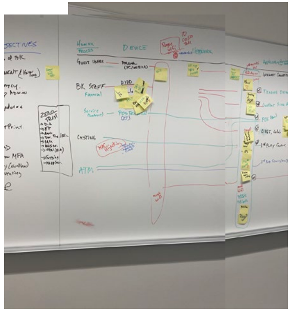


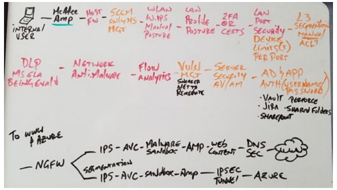
Risk Workshops

Focused on capabilities rather than product; solutions are co-developed with customers to build and prioritize the right product solutions.



	Business	IT and Security	Risks and Threats	Priority
Goal/ Initiative	Increase new customer accounts by 15% by FY2020	Add customer portal for guest access	Exploitation of trust	1
Goal/ Initiative	Open 16 new offices is eastern and southern regions	Support new branch build and deployments	Unauthorized access, exploit redirection, unencrypted traffic attack	2
Goal/ Initiative	Accelerate new account revenue growth by 10%	Develop 24x7 access to self-service applications	Compromised applications, unauthorized access	3




McAfee Amp
Internal User
Host FW
DLP
Network Anti-Malware
Flow Analytics
To www & Azure
NGFW
IPS - AVC - Malware Sandbox - AMP - Web Content - DNS Sec
Segmentation
IPS - AVC - Sandbox - Amp - IPSEC Tunnel - Azure

Typical SAFE Workshop Meeting Flow & Audience

Proposal

SAFE Proposal Meeting(s) (30 Min) – Virtual or Onsite: CxO or BDM, Networking & Security

Discovery

SAFE Discovery: Business (60-90 Min) - Onsite: CxO or BDM, Networking & Security
SAFE Discovery: Domains (60 Min) - Onsite: Networking & Security, Compliance (Optional)
SAFE Discovery: Security (60 Min) - Onsite: Networking & Security

Report

SAFE Report Read-Out (60 Min) - Onsite: CxO or BDM, Networking & Security

SAFE
SIMPLIFIES SECURITY

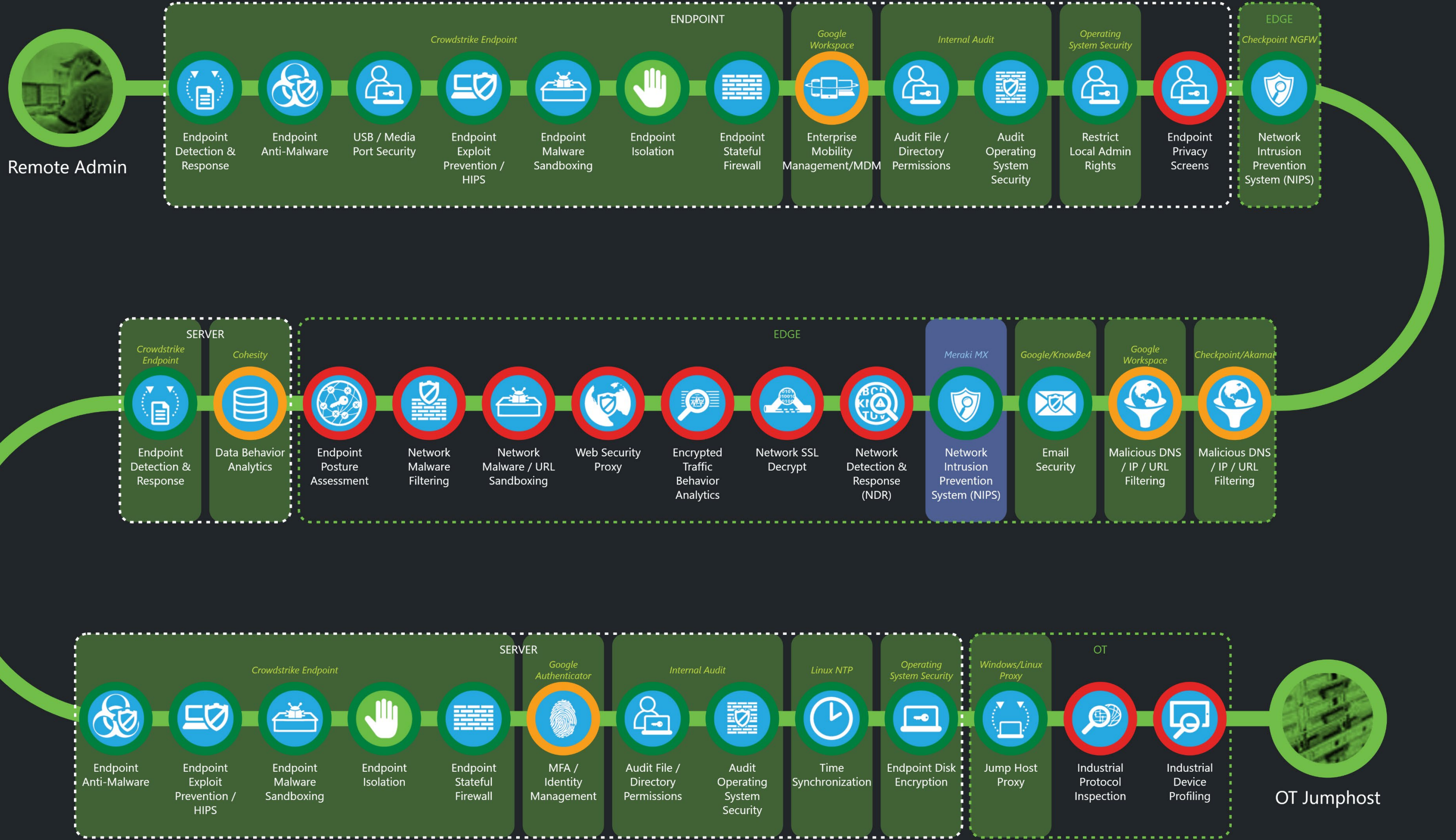
Diagram #3 Remote Admin to OT Jumphost

(Gap Analysis)

Solution Success

Challenges / Deficiencies

Not deployed or successful



Remote Admin

ENDPOINT

Crowdstrike Endpoint

Endpoint Detection & Response

Endpoint Anti-Malware

USB / Media Port Security

Endpoint Exploit Prevention / HIPS

Endpoint Malware Sandboxing

Endpoint Isolation

Endpoint Stateful Firewall

Google Workspace

Enterprise Mobility Management/MDM

Internal Audit

Audit File / Directory Permissions

Audit Operating System Security

Operating System Security

Restrict Local Admin Rights

Endpoint Privacy Screens

EDGE

Checkpoint NGFW

Network Intrusion Prevention System (NIPS)

SERVER

Crowdstrike Endpoint

Endpoint Detection & Response

Cohesity

Data Behavior Analytics

EDGE

Endpoint Posture Assessment

Network Malware Filtering

Network Malware / URL Sandboxing

Web Security Proxy

Encrypted Traffic Behavior Analytics

Network SSL Decrypt

Network Detection & Response (NDR)

Meraki MX

Network Intrusion Prevention System (NIPS)

Google/KnowBe4

Email Security

Google Workspace

Malicious DNS / IP / URL Filtering

Checkpoint/Akamai

Malicious DNS / IP / URL Filtering

SERVER

Crowdstrike Endpoint

Endpoint Anti-Malware

Endpoint Exploit Prevention / HIPS

Endpoint Malware Sandboxing

Endpoint Isolation

Endpoint Stateful Firewall

Google Authenticator

MFA / Identity Management

Internal Audit

Audit File / Directory Permissions

Audit Operating System Security

Linux NTP

Time Synchronization

Operating System Security

Endpoint Disk Encryption

OT

Windows/Linux Proxy

Jump Host Proxy

Industrial Protocol Inspection

Industrial Device Profiling

OT Jumphost

SAFE Risk Report Deliverable Summary

- **Risk Prioritized, Vendor-Agnostic Gap Analysis** based on each place of the network and architecture

- **Risk, Gap and Final-State Flow Diagrams** based on Risk Score and/or Cisco Best Practice Security Designs (SSE, XDR, Zero Trust)

- **Cisco Recommendations**
  - Stop-Gap
  - Short-Term Projects
  - Long-Term Projects
  - Integration Opportunities
  - Consolidation Opportunities

Cisco SAFE Workshop Report

Prepared for: [CUSTOMER]

Prepared by: [Lead TSA]
[TSA Title]
Mon YYYY

Do not share outside [CUSTOMER] or the Cisco account team for [CUSTOMER]

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1

June 8 - 12
San Diego

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

OT Segmentation

Cisco Tech Day Colorado

Andrew Usankin & Ambika Harit, Industrial IoT

cisco Engage

#CiscoEngage

Agenda

- Introduction
- Importance of Visibility
- Enlist your Network
- Demo

Securing industrial operations starts with OT visibility

Identify OT assets and their communications

Spot vulnerabilities to patch or protect

Segment networks with access policies

Detect bypass or leaks in the IDMZ

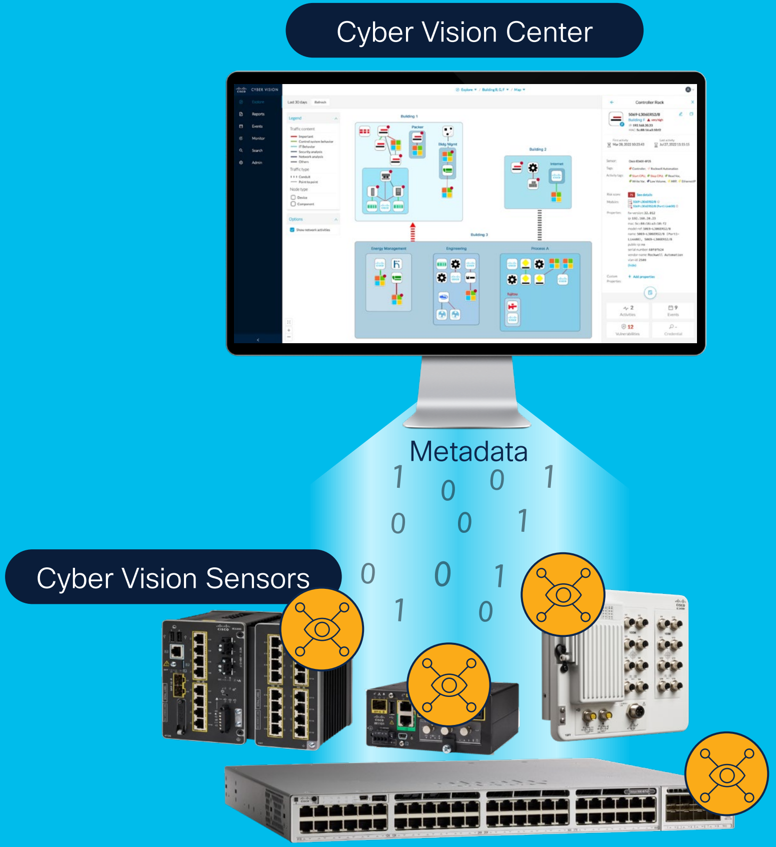
Drive compliance and governance

Visibility helps drive IT/OT collaboration to secure industrial operations

Enlist your network to gain OT visibility at scale

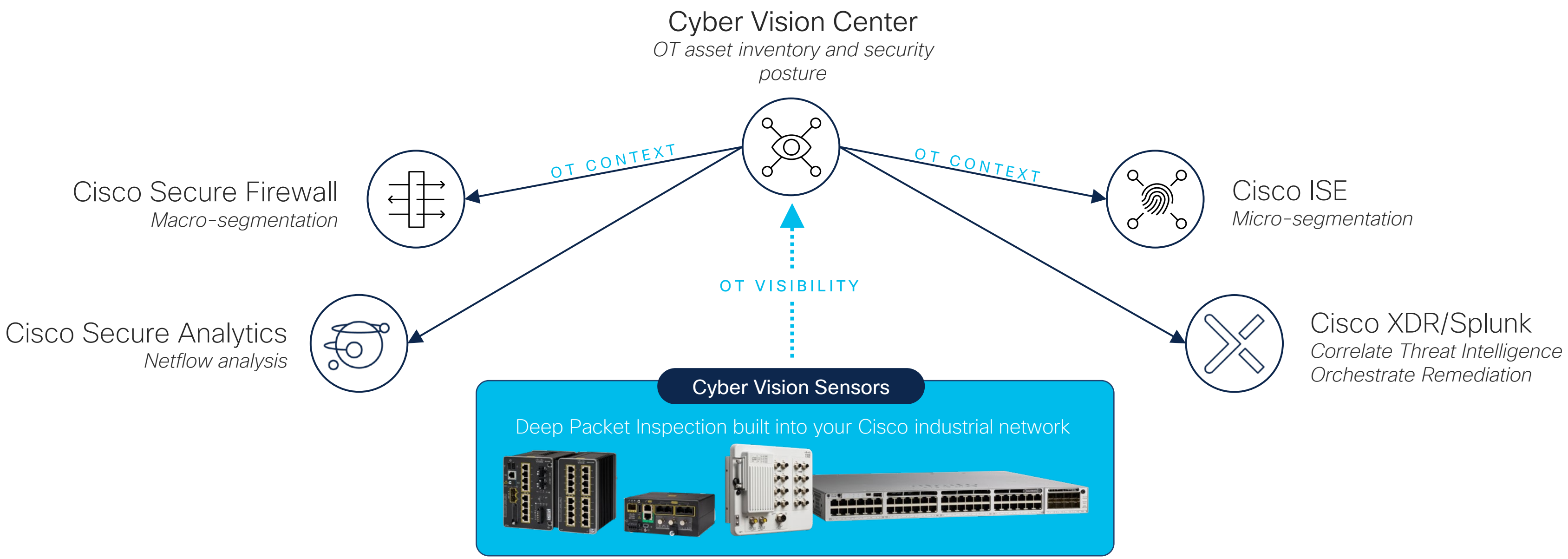
Cisco Cyber Vision

- Visibility sensor is a software feature running in switches and routers
- No additional hardware needed
- No need for an out-of-band collection network
- Sends metadata to monitoring console (only ~5% extra traffic)
- Active discovery requests see pass NAT and firewall boundaries
- Centralized deployment and management
- No impact on network performance



Deep Packet Inspection & Active Discovery **built into your network infrastructure**

Extend IT security to your industrial settings



Cyber Vision Center
OT asset inventory and security posture

Cisco Secure Firewall
Macro-segmentation

Cisco ISE
Micro-segmentation

Cisco Secure Analytics
Netflow analysis

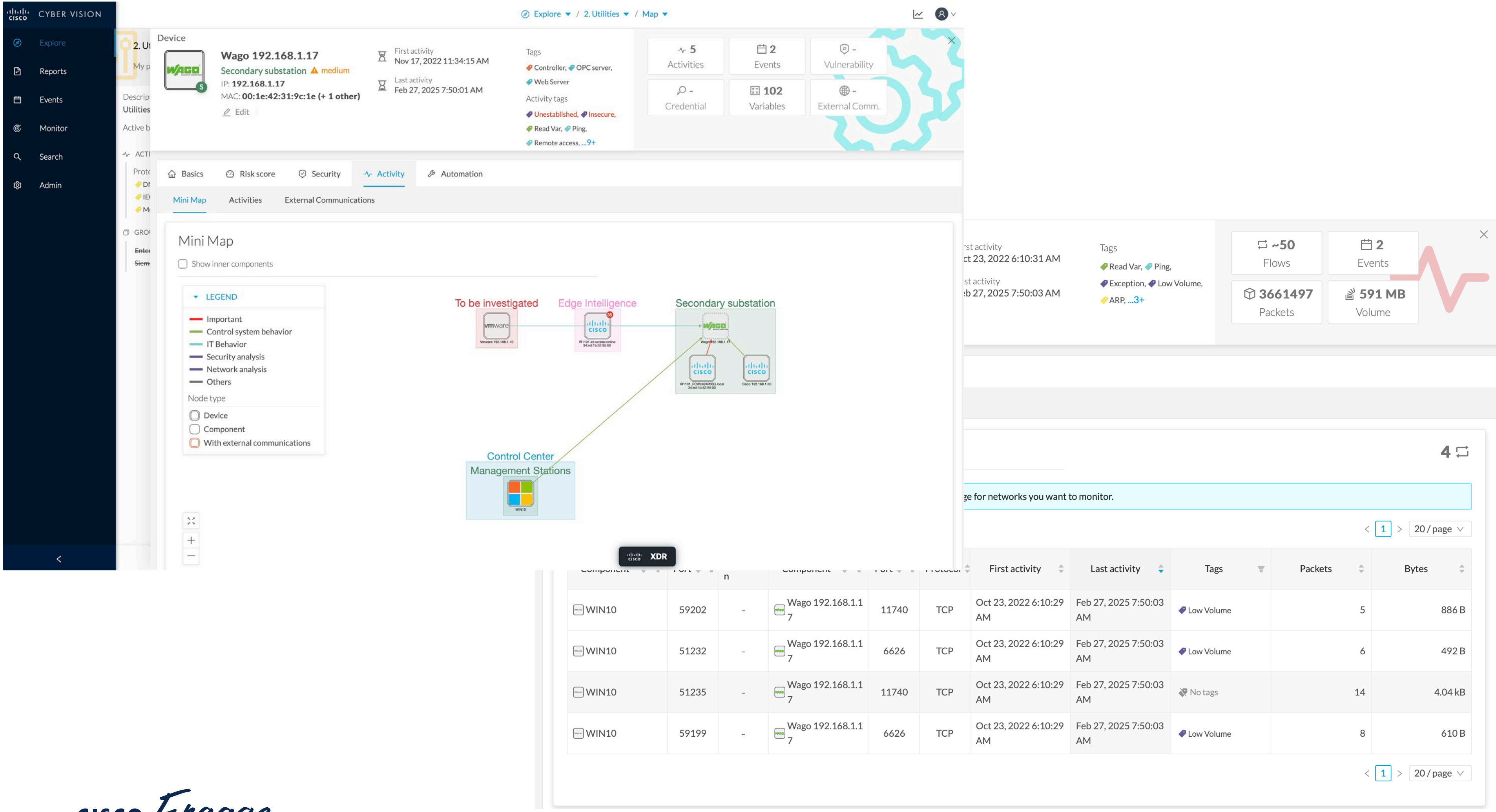
Cisco XDR/Splunk
Correlate Threat Intelligence
Orchestrate Remediation

Cyber Vision Sensors

Deep Packet Inspection built into your Cisco industrial network

The broadest OT security solution on the market ▪ Powered by Talos Threat Intelligence

Demo 2



Device

Wago 192.168.1.17

Secondary substation ⚠ medium

IP: **192.168.1.17**

MAC: **00:1e:42:31:9c:1e (+ 1 other)**

Edit

First activity
Nov 17, 2022 11:34:15 AM

Last activity
Feb 27, 2025 7:50:01 AM

Tags
Controller, OPC server, Web Server

Activity tags
Unestablished, Insecure, Read Var, Ping, Remote access, ...9+

5 Activities	2 Events	- Vulnerability
- Credential	102 Variables	- External Comm.

Basics | Risk score | Security | Activity | Automation

Mini Map | Activities | External Communications

Mini Map

□ Show inner components

LEGEND
- Important
- Control system behavior
- IT Behavior
- Security analysis
- Network analysis
- Others

Node type
- □ Device
- □ Component
- □ With external communications

rst activity
ct 23, 2022 6:10:31 AM

st activity
b 27, 2025 7:50:03 AM

Tags
Read Var, Ping, Exception, Low Volume, ARP, ...3+

~50 Flows	2 Events
3661497 Packets	591 MB Volume

4

ge for networks you want to monitor.

1 | 20 / page

Component	Port	n	Component	Port	Protocol	First activity	Last activity	Tags	Packets	Bytes
WIN10	59202	-	Wago 192.168.1.17	11740	TCP	Oct 23, 2022 6:10:29 AM	Feb 27, 2025 7:50:03 AM	Low Volume	5	886 B
WIN10	51232	-	Wago 192.168.1.17	6626	TCP	Oct 23, 2022 6:10:29 AM	Feb 27, 2025 7:50:03 AM	Low Volume	6	492 B
WIN10	51235	-	Wago 192.168.1.17	11740	TCP	Oct 23, 2022 6:10:29 AM	Feb 27, 2025 7:50:03 AM	No tags	14	4.04 kB
WIN10	59199	-	Wago 192.168.1.17	6626	TCP	Oct 23, 2022 6:10:29 AM	Feb 27, 2025 7:50:03 AM	Low Volume	8	610 B

1 | 20 / page

Thank you

slido

Please download and install the Slido app on all computers you use

Audience Q&A

ⓘ Start presenting to display the audience questions on this slide.

Time	Cisco Tech Day Colorado Agenda Overview
8:30am	Arrivals, Check-In
9:00am	Welcome/Keynote
10:00am	Breakout Sessions • Digital Resilience with Splunk and Cisco • Threat Detection Investigation & Response • Reimagining Work with the New and Improved Webex Suite and Devices • Network Design Clinic
11:00am	Breakout Sessions • Networking: Expanding Your Toolbox to Building Smarter Networks • Monitoring Cloud and APIs with ThousandEyes Innovations • Navigating the Future: Alternatives to expensive virtualization licensing with Cisco compute
12:00pm	Lunch
1:00pm	Breakout Sessions • Advanced Access: Designing Cisco Access Layer Solutions with Wi-Fi 7 • Identity and Secure Access • Unlocking the Future of Data Centers: Cisco HyperFabric and AI Pods with UCS & Nexus • Rapid Incidence Response Workshop/CTF
2:00pm	Breakout Sessions • Unleashing the Power of Cisco Campus Fabric: Simplifying Network Automation and Scalability • Zero Trust Network Segmentation • Improve the Customer Experience through the Webex Engagement Platform
3:00pm	Wrap Up/Raffle
3:30pm	Close

What’s Next?

The bridge to possible

Thank you

cisco Engage

GO **BEYOND**

#CiscoEngage