

Enforcing End to End Security Policy **cisco** Live !

BRKSEC-2565

Tim Snow
Senior Solutions Engineer, APJ

Asif Khan
Solutions Engineer, ANZ

Your Speaker – Tim Snow



- IT Architect with domain experience in Enterprise Networks, Security and Application Development
- 25+ Year CCIE, CISSP
- 20 Years at Cisco in multiple roles

Prior to Cisco

- Comp. Sci major – Michigan 
- Developer
- TAC L3 and SecOps

About Me



- Canadian, Husband, Father
- Tinkerer – IOT systems (automate the things that don't need to be automated)
- 3D Printing and Robotics
As a way to show my kids tech
- Retro Arcade gaming – growing up in the 80's
- Lifelong beginner at golf

Your Speaker – Asif Khan



- 15+ Years at Cisco in multiple roles
- 2 x CCIE, CISSP, CISM, CISA
- Prior to Cisco: Solution Integration Architect, Field Implementation Engineer, Data Warehousing Engineer, Software Developer

Outside Work

- Hiking
- Rollerblading
- Traveling

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

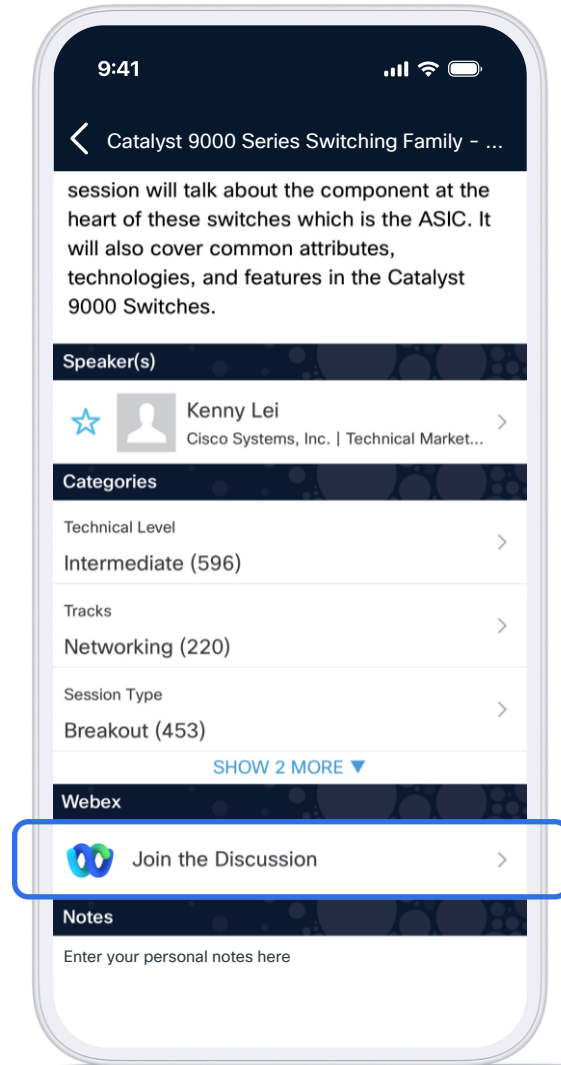
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

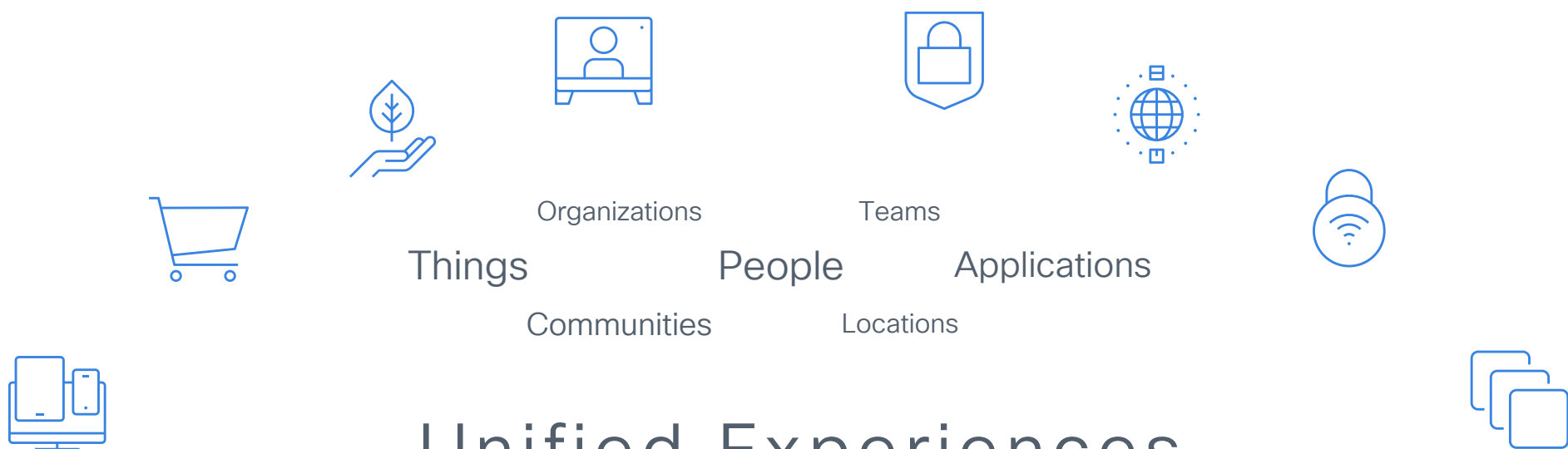
Webex spaces will be moderated by the speaker until 14 November 2025.

Join the Webex Room

<https://ciscolive.ciscoevents.com/clmel25/BRKSEC-2565/>

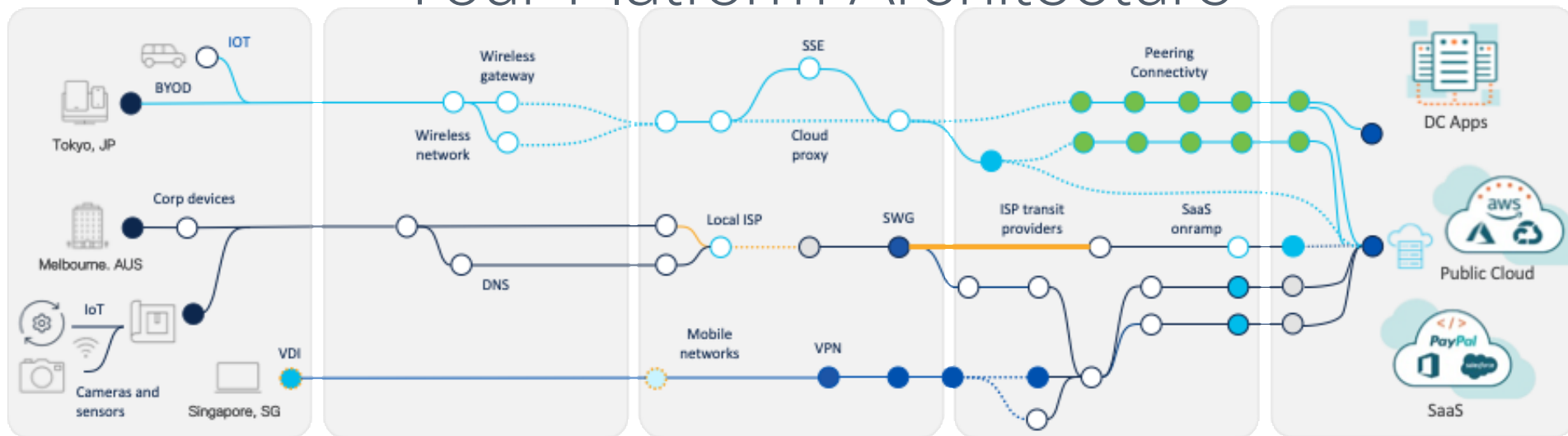
Short Link <http://cs.co/2565>





RELY ON

Your Platform Architecture

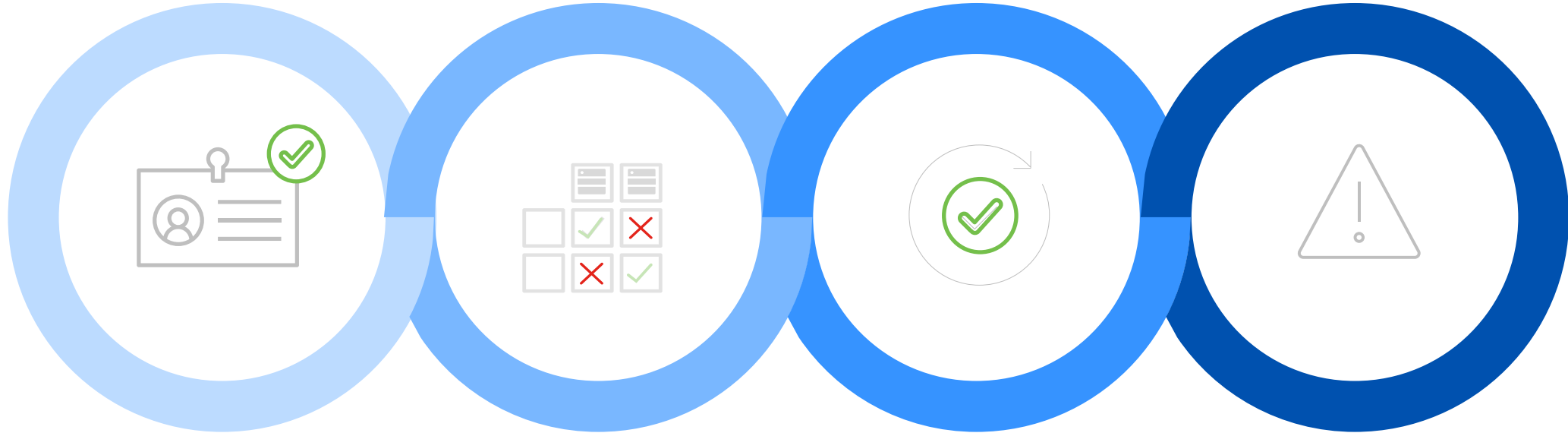


Subject

Transport & Security Services

Resource

Reviewing the Zero Trust Lifecycle



Establish
Trust

User/Machine
Authentication,
Validation and
Health Assessment

Enforce Trust
Based Access

Network
Segmentation
enabled by
Granular Context

Continuously
Verify Trust

Identity
Intelligence,
Behaviour and
Network Analytics

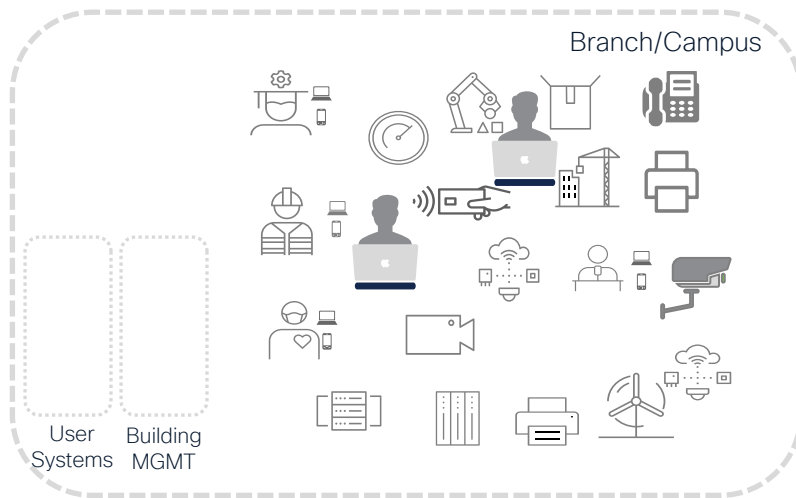
Respond to change
in trust (or threats)

Adaptive
Network Control with
Platform Integration

Enforcing Consistent Policy for End to End Security

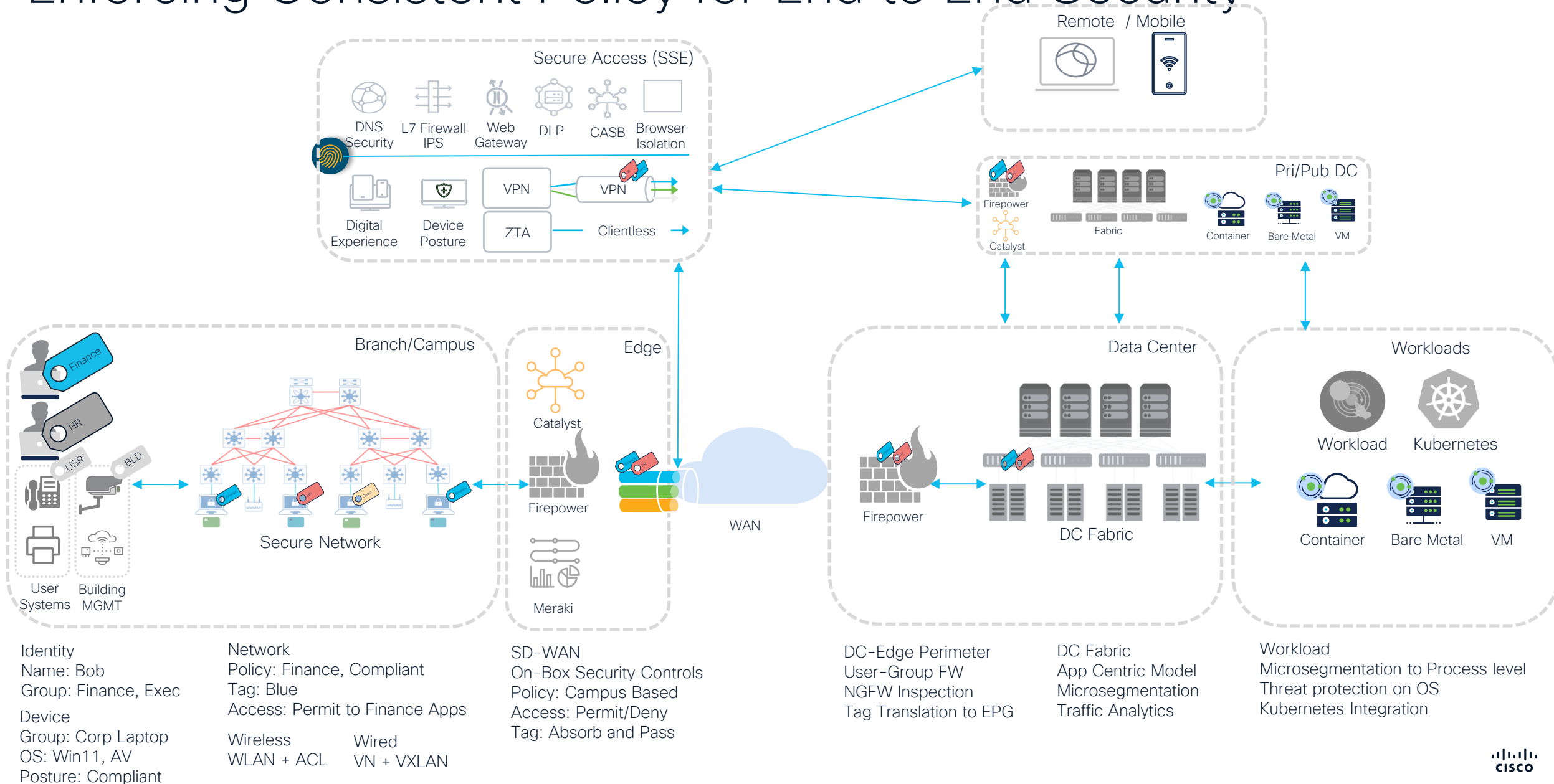
Current Challenges with unknown devices sprawling networks, interconnected everything

- Manual Network Management
Configuration Compliance
Software Versioning
Advisory Responses
- Inventory of all assets on the Network (NIST,CISA)
- Knowing what we have , Who they are, where they are
- Inability to apply policy at scale
- Lack of controls that follow the user/device
- Inability to detect user/entity behaviour changes (NDR)
- Inability to take a response action to contain a threat (response)



"In the next 60 seconds, dozens of devices will try to access your network.
Do you know which ones to trust?"

Enforcing Consistent Policy for End to End Security



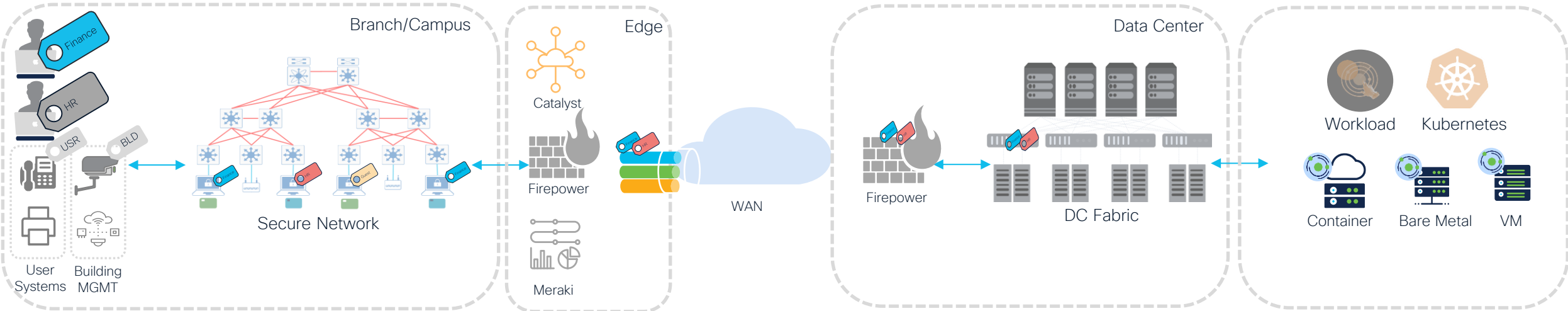
Cisco Solutions that make it happen

	Adaptive Policy for Threat Response	
	Authenticate / Validate / Authorize Device Profiling Device Compliance	Enforcement
		Resources
	Secure and Compliant Infrastructure Endpoint Analytics Network Analytics (Flow)	Devices
		X ✓ X ✓ ✓ ✓
		✓ ✓ X ✓ X X

	Security Capabilities embedded Robust Application QOE Scale and Integrations
	SGT and Access Policy Decryption, URL, IPS SD-WAN Capabilities
	Meraki Cloud Ease of Use Integrated Security Features XDR Expansion

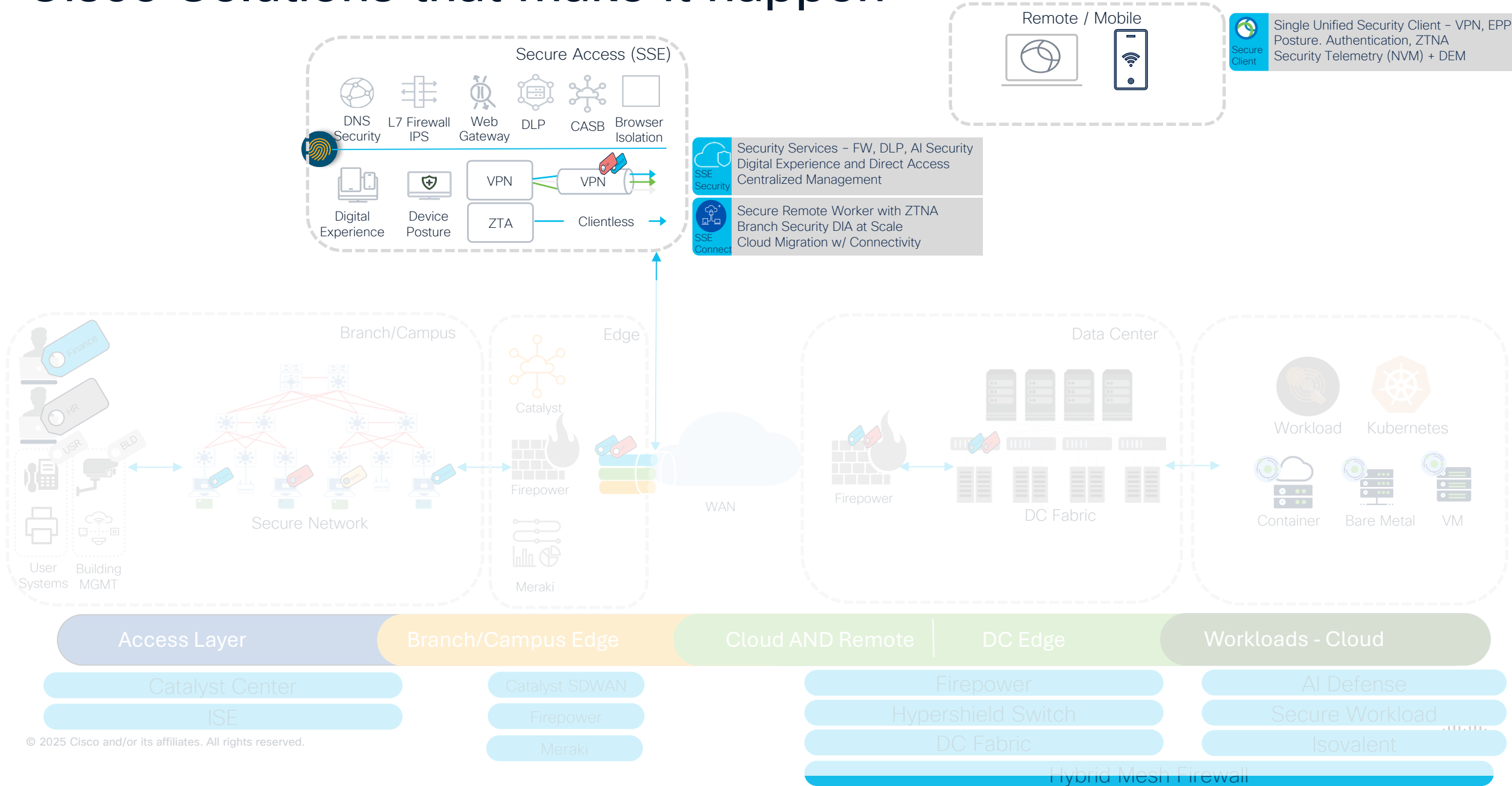
	Firepower Integration – Rules and Visibility
	Data Center Edge Scale and Features TrustSec Segmentation Integrations with DC Fabric and Workload
	Centralized Infra Management Policy Lifecycle – Define, Apply and Monitor Firewall Integration for Scale and Adaptability

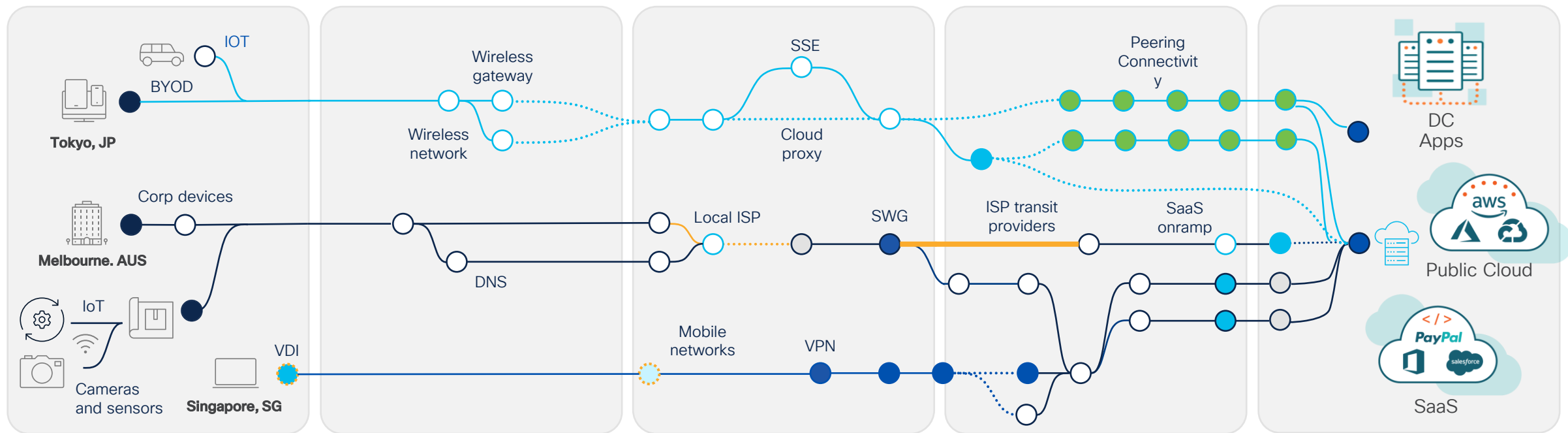
	Workload ingest of K8S resources
	Process Level Visibility Microsegmentation at OS level Traffic and Vulnerability Visibility
	Automated ingestion of inventory Application dependency mapping Container Microsegmentation



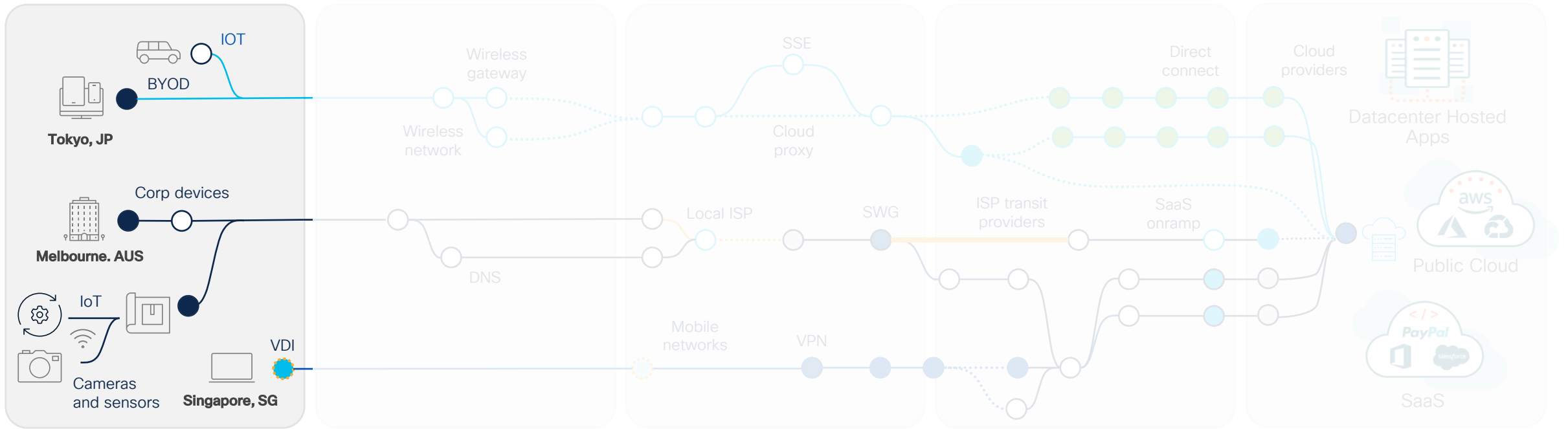
Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads - Cloud
Catalyst Center	Catalyst SDWAN		Firepower	AI Defense
ISE	Firepower		Hypershield Switch	Secure Workload
	Meraki		DC Fabric	Isovalent eBPF
			Hybrid Mesh Firewall	

Cisco Solutions that make it happen





Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads - Cloud
<p>Visibility, Identification, Segmentation</p> <p>Device Profiling</p> <p>Identity Authorization</p> <p>Segmentation</p> <p>Access Control Policies</p>	<p>Policy Enforcement & Service Availability</p> <p>Context Sharing</p> <p>Segmentation</p> <p>Access Control Policies</p> <p>Software Defined WAN</p> <p>Cloud (SSE) Integrations</p>	<p>Access Control & Intrusion Prevention</p> <p>Policy Enforcement</p> <p>Service Visibility</p> <p>Traffic Monitoring</p> <p>Breach Prevention</p>	<p>Access Control & Intrusion Prevention</p> <p>DC Edge Access</p> <p>Traffic Visibility</p> <p>Breach Prevention</p>	<p>Workload and App Protection</p> <p>Segmentation</p> <p>Workload baseline</p> <p>SBOM and Inventory</p> <p>Microservice Protection</p>



Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads &Cloud
<p>Visibility, Identification, Segmentation</p> <p>Device Profiling</p> <p>Identity Authorization</p> <p>Segmentation</p> <p>Access Control Policies</p>	<p>Policy Enforcement & Service Availability</p> <p>Context Sharing</p> <p>Segmentation</p> <p>Access Control Policies</p> <p>Software Defined WAN</p> <p>Cloud (SSE) Integrations</p>	<p>Access Control & Intrusion Prevention</p> <p>Policy Enforcement</p> <p>Service Visibility</p> <p>Traffic Monitoring</p> <p>Breach Prevention</p>	<p>Access Control & Intrusion Prevention</p> <p>DC Edge Access</p> <p>Traffic Visibility</p> <p>Breach Prevention</p>	<p>Workload and App Protection</p> <p>Segmentation</p> <p>Workload baseline</p> <p>SBOM and Inventory</p> <p>Microservice Protection</p>

Authentication (AuthN)

Can the identity be trusted?

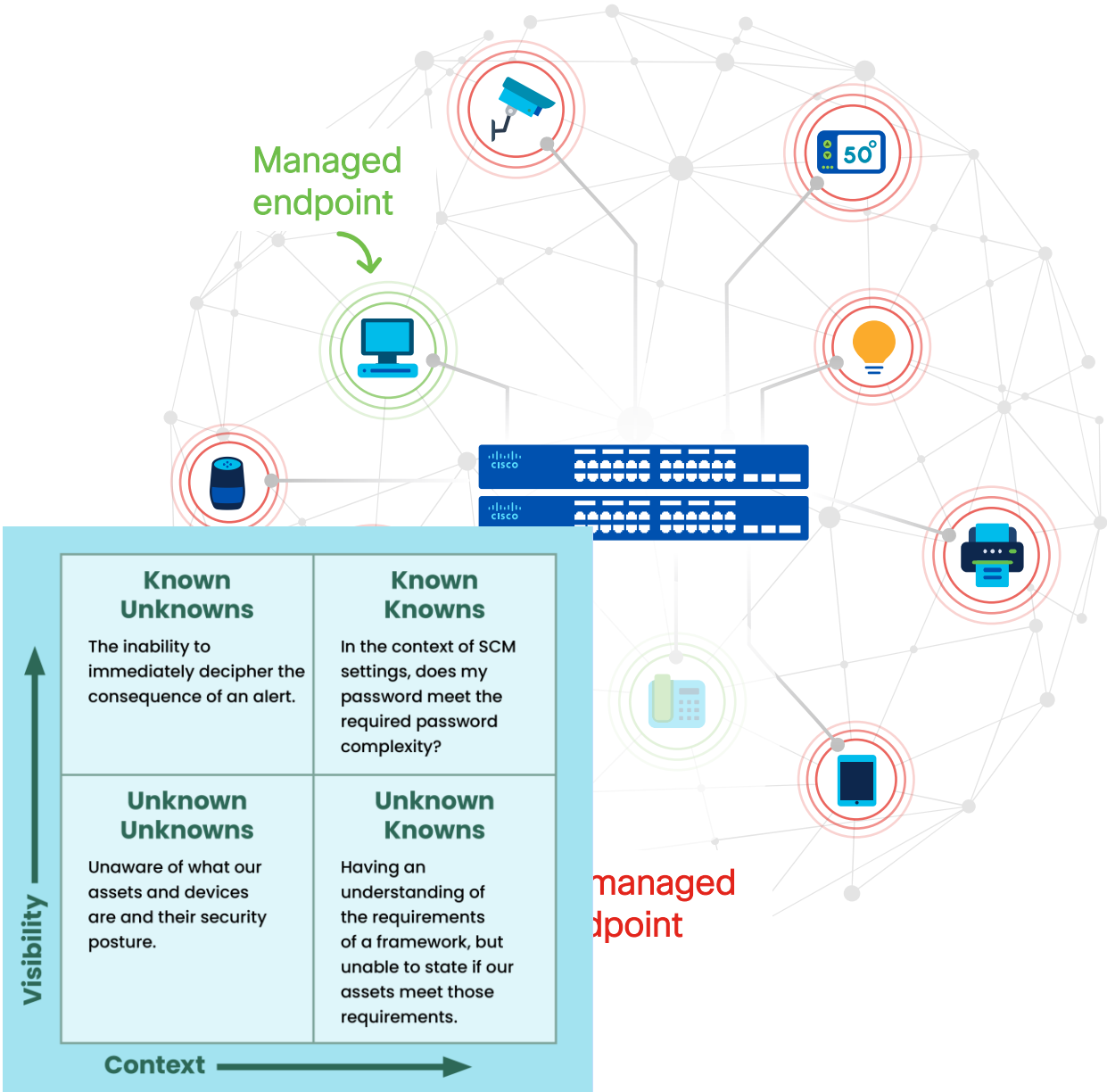
The Principle of Least Trust.

Authorization (AuthZ)

What access level should they receive?

The Principle of Least Privilege.

Who and what is on YOUR network?



1:3 Or More 

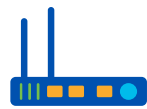
Unmanaged device proliferation.
1:3+ managed to **unmanaged endpoint ratio**



Unmanaged endpoints are difficult to patch and **most vulnerable to cyber attacks**



Secure authentication mechanisms unusable on unmanaged endpoints



Open, unsegmented networks with IOT devices put organizations at risk

Isn't it just all about the User? Not really.

Visibility and control doesn't stop at the end user

Threats

Zero Trust Solution

Unknown non-user devices such as Printers, Phones, Medical carts, etc with unrestricted access can make the entire infrastructure vulnerable



Provide **confined access** to essential services through macro and micro-segmentation

Unauthorized endpoints or devices with **unhygienic posture** can disrupt productivity



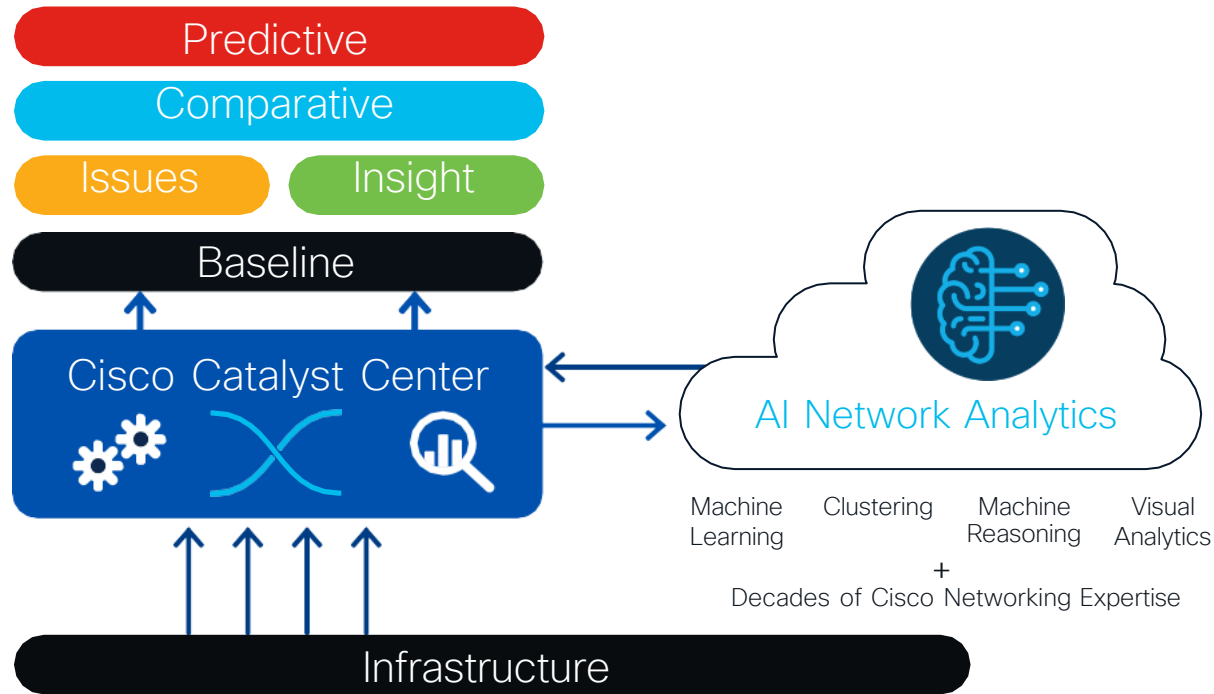
No network access until **endpoint trust is evaluated** (authenticate and evaluate system health)

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**

Branch/Campus – Infra Capabilities Overview



SOC Response
Anticipate and Prevent Failures

Threat
Response

Behaviour & Analytics
User and Entity Behaviour and
Performance Analytics

Behaviour &
Analytics

Compliance & Segmentation
System validation and enforced policy

Compliance &
Segmentation

Configuration and Operations
Full lifecycle of onboarding, configuring,
monitoring and reporting of infrastructure

Day 0 + 1
Operations

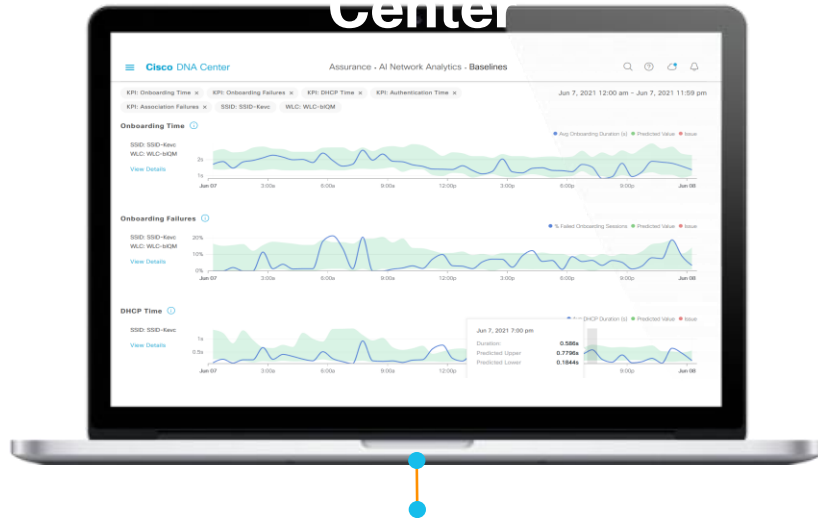
Trusted Infrastructure
Secure Boot, Validated Software and
Configuration Revisioning

Trusted
Network

Cisco Catalyst Center is a foundational platform technology

Your single tool for management LAN, WAN and Wireless (Meraki and more!)

Cisco Catalyst Center



Physical and virtual infrastructure
Cisco and third-party



Centralized Management of Wired, Wireless and WAN. Automation and workflows, Day 0+1 Operations, Configuration Versioning, updates, AI streamlines and simplifies common tasks



AI/ML and insights to ensure the health, performance and reliability of applications and infrastructures



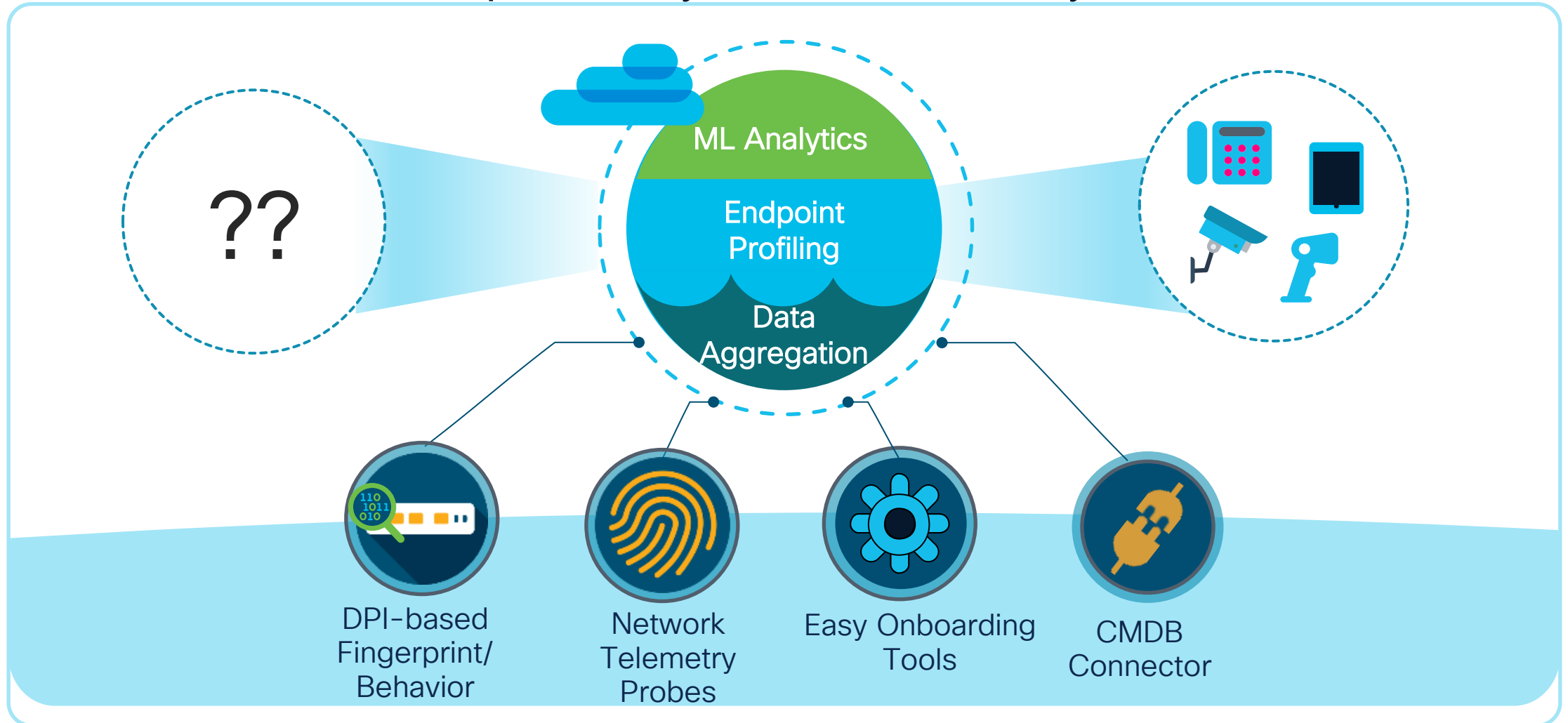
AI/ML and DPI identify and classify endpoints, enforce security policies and mitigate threats for a complete workplace Zero Trust solution



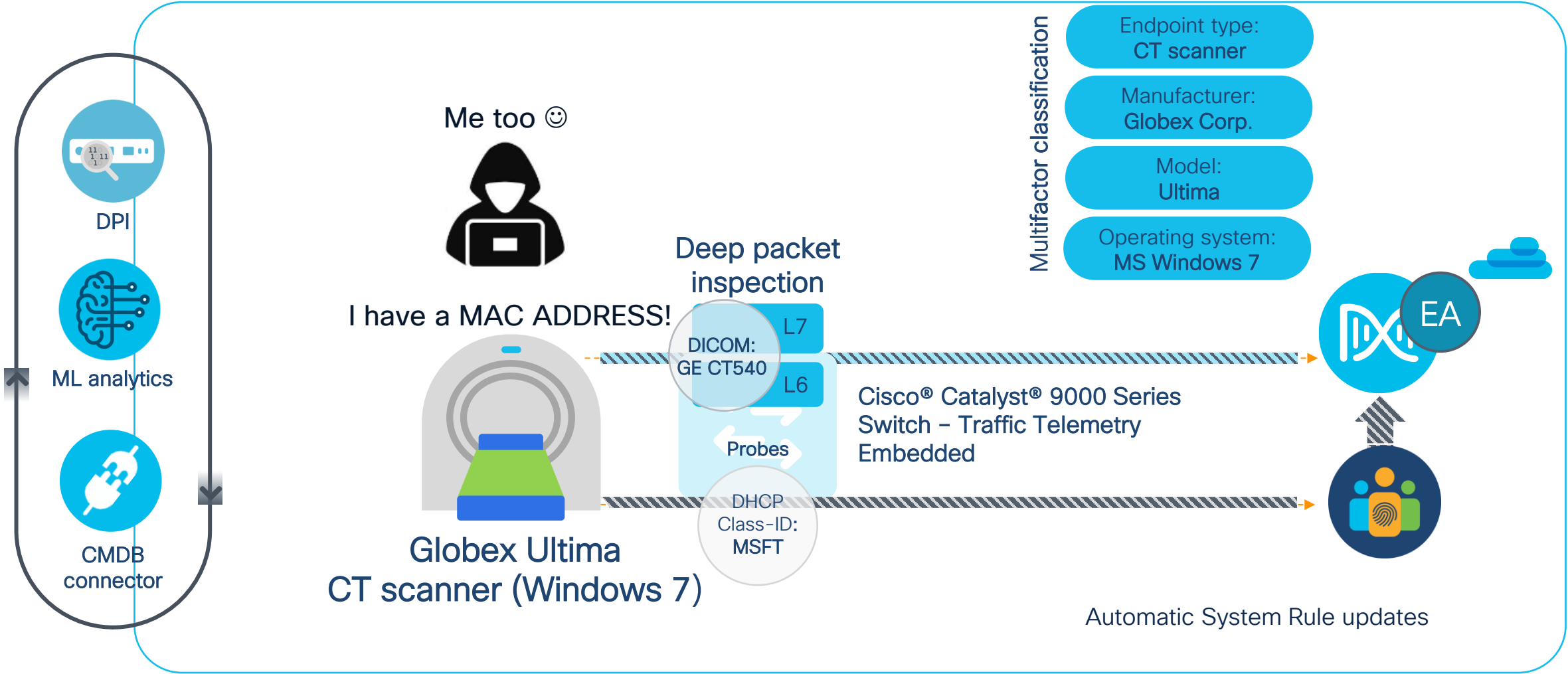
Mature APIs, SDKs, and closed-loop integrations, untangle the complexities of interconnecting third-party systems

Rapidly reducing the unknowns – aggregating data from sources

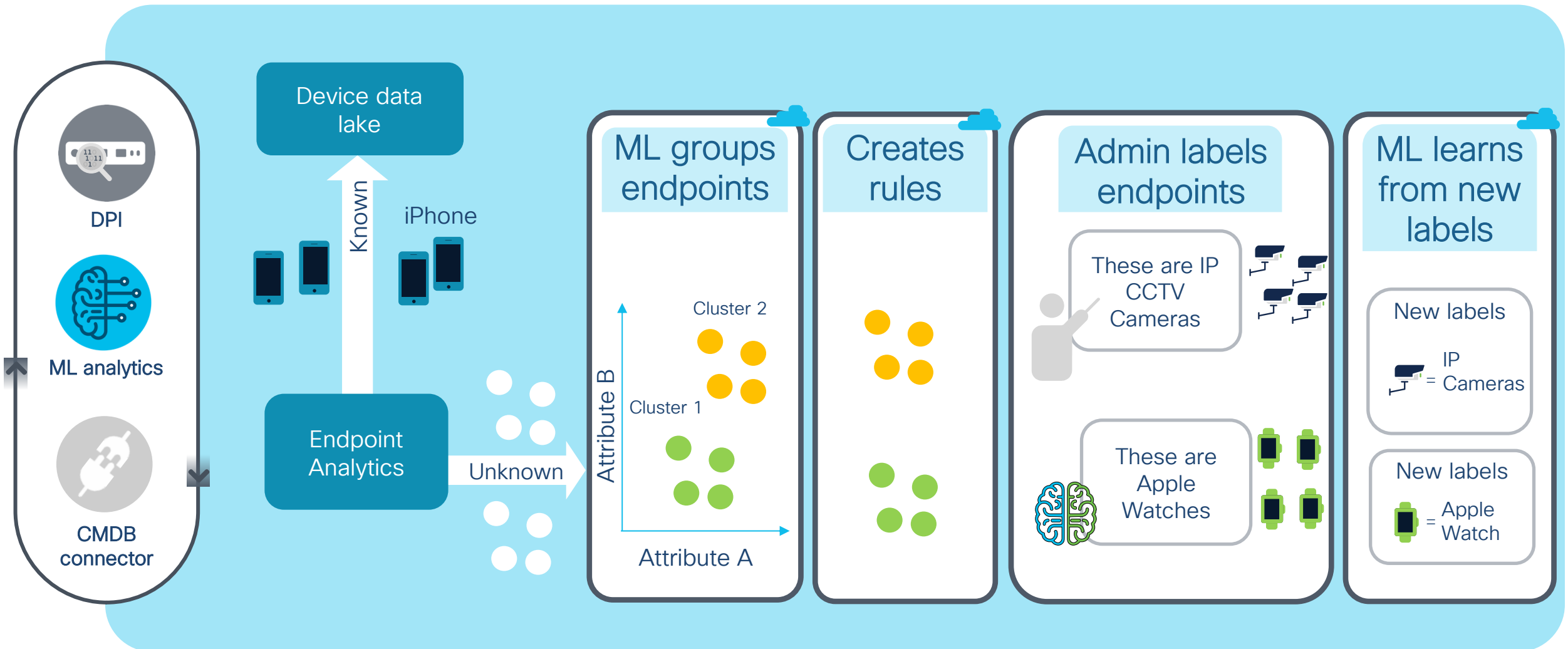
AI Endpoint Analytics On Cisco Catalyst Center



Classification Based On DPI

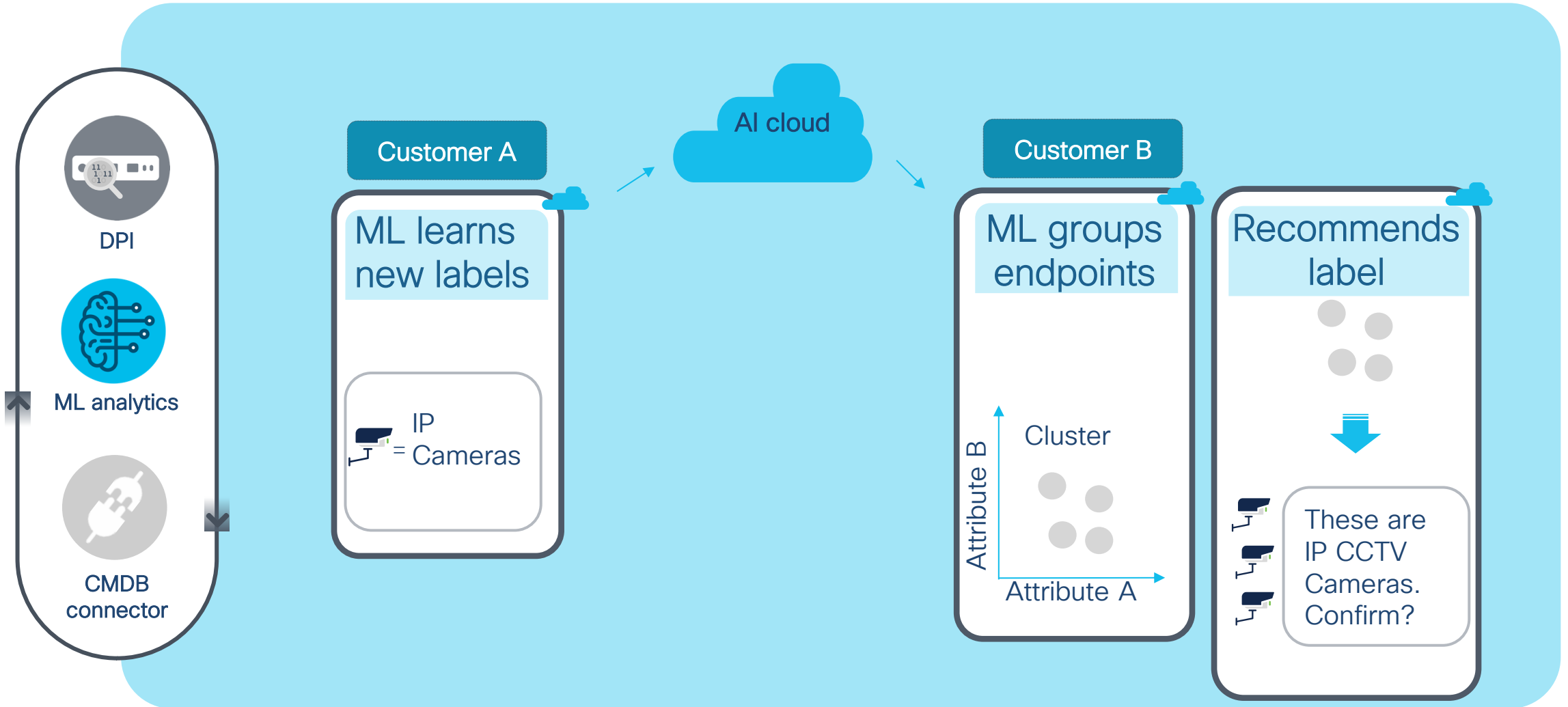


Reducing Unknowns With Machine Learning



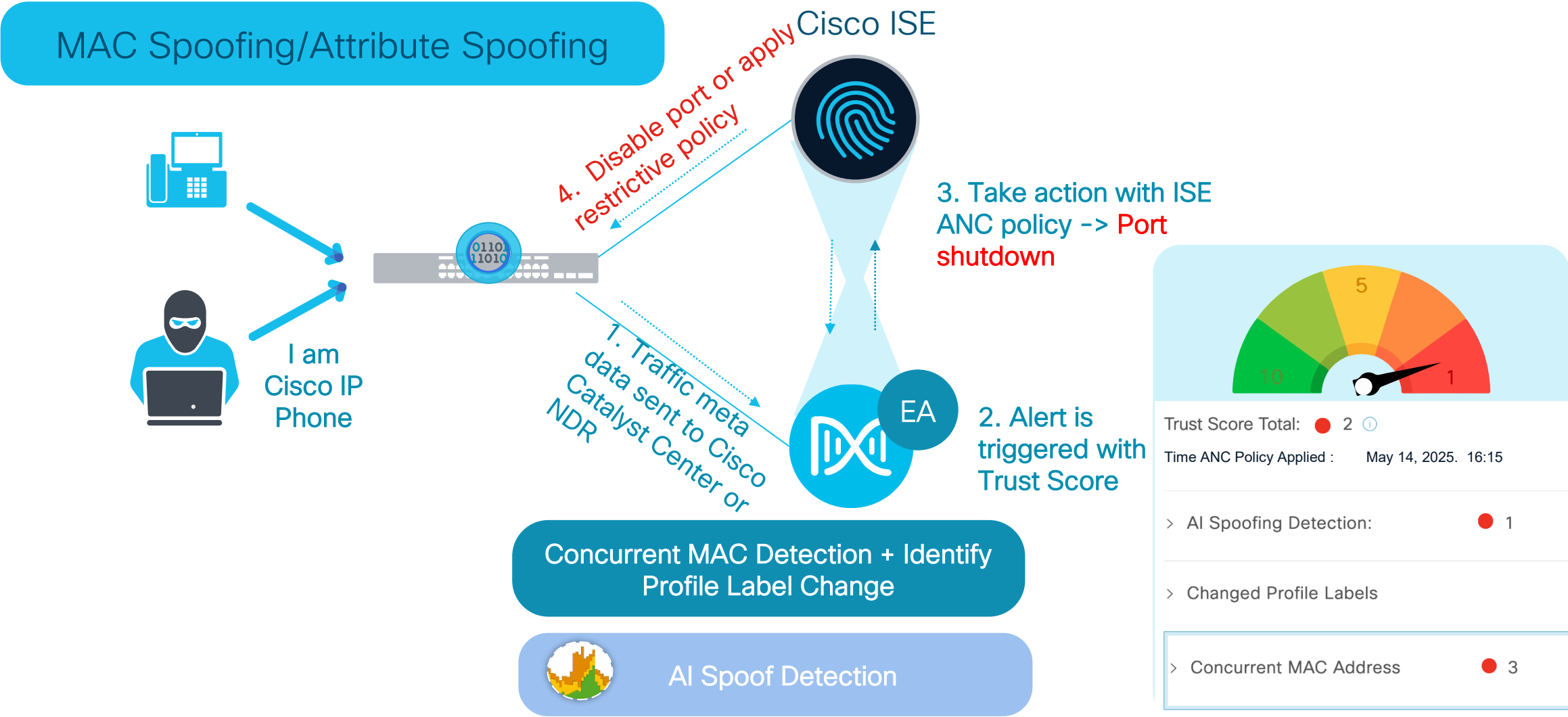
 = done in cloud

Crowdsourcing With Machine Learning



 = done in cloud

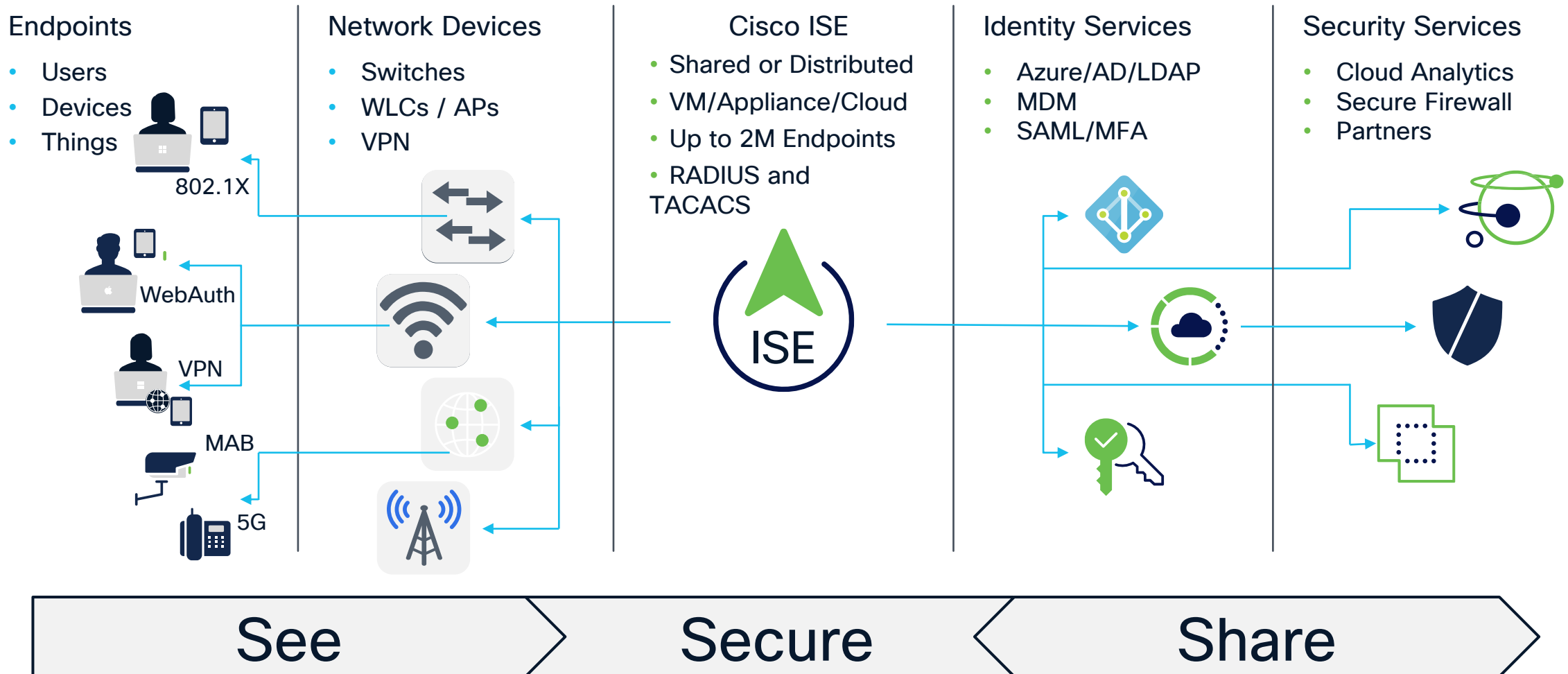
Spoofing Detection And Mitigation



ISE Provides Zero Trust for the Workplace

Enterprise

Security



How Identity Services Engine enforces Zero Trust

Connecting trusted users and endpoints with trusted resources

Trust continually verified

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

Endpoint Request Access

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

Endpoint classified, and profiled into groups

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

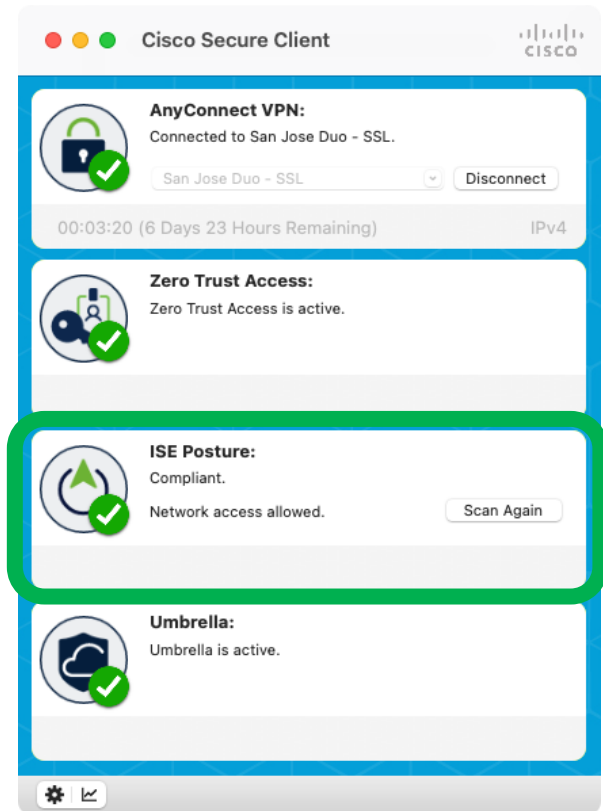
Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved



ISE Posture with Cisco Secure Client

Checks



System Checks

- Hardware Inventory
- USB Checks
- File Checks
- Registry Checks
- Service Checks
- Disk Encryption

Software/ Application Checks

- Application Checks
- Application Inventory
- Anti-Malware Checks
- Firewall Installation Checks

Custom Scripts and external Conditions

- Custom scripts
- External Conditions (AD, Location)
- Compound condition support

Script Remediation

Script Remediation

- Patch Management - MS SCCM
- Windows Update
- WSUS remediation (legacy)

Windows updates Patch Management

Remediation/ Reassessment

- Application, Antimalware, File, Firewall, USB Block, Link
- Passive Reassessment

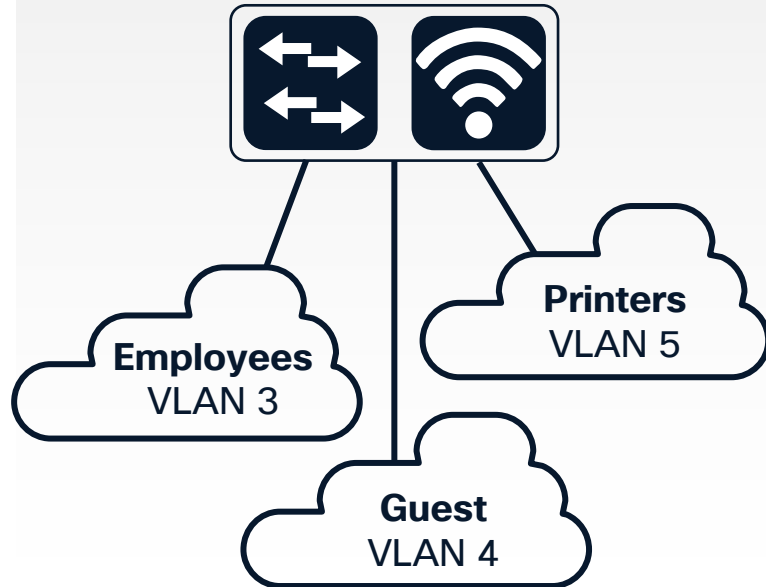
Remediations

Post Auth and Posture - ISE Segmentation Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

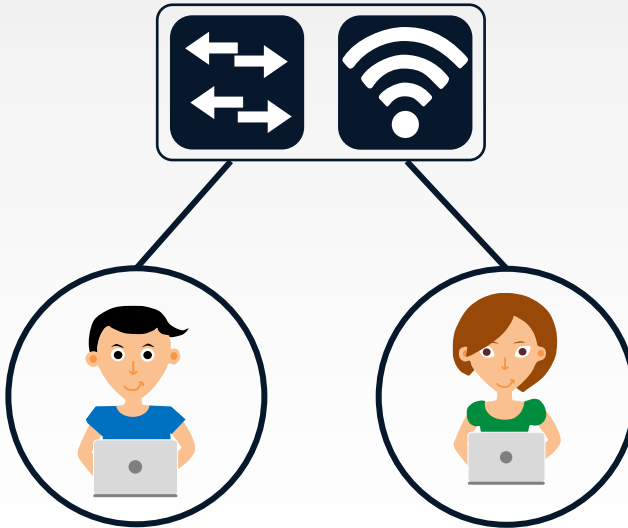
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

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



Employee

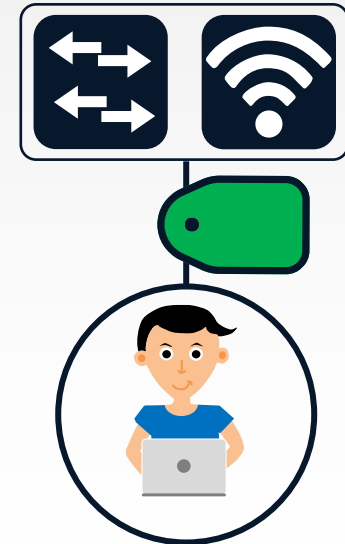
```
permit ip any any
```

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

Work Centers / TrustSec

 Evaluation Mode 86 Days

Egress Policy

Matrices List

Matrix

Source Tree

Destination:

Network Device Authorization

Egress Policies (144) Matrix · Production ▾

Matrix · Production ▾

Only show this dropdown and the 'Matrices List' tab when multi-matrix is enabled in settings.

[+ Create Policy](#)
[⦿ Monitor All Enabled](#)
[▶ Deploy](#)
[⛔ Verify Deploy](#)
[↶ Reset All Policies](#)
[⬇ Import](#)
[⬆ Export](#)

As of Today @ 2:45p (PST) View: **Default View** Default Policy: **Permi**



SGTabc_abcd...
4/0004

Destination

SGTabc_abcd...
6/0006



c_abcdef...
2/0002

c_abcdef...
3/0002

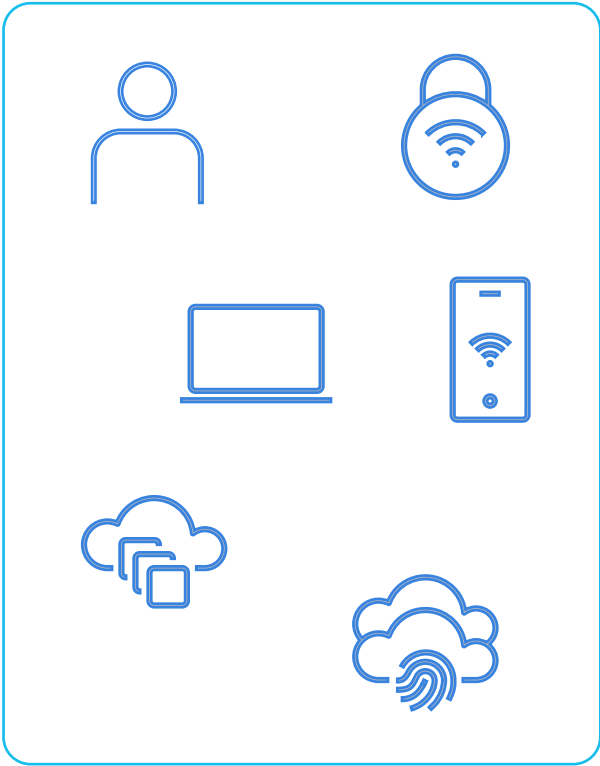
c_abcdef...
/0004

Source

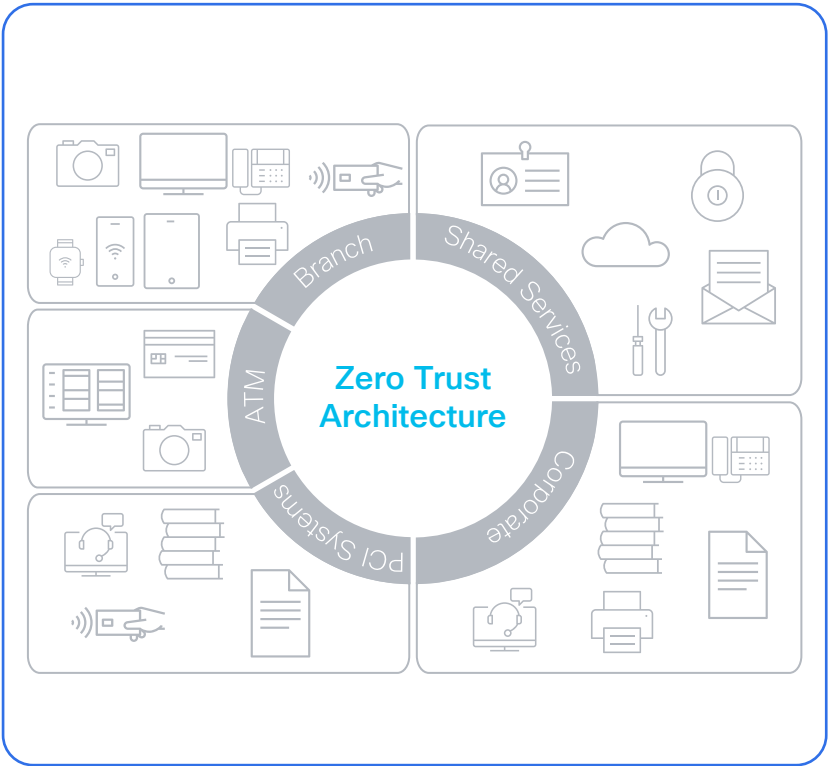
```
deny icmp
deny tcp dst eq 22
deny udp dst eq 53
deny udp dst eq 67
deny udp dst eq 68
deny udp dst eq 69
deny tcp dst eq 135
deny tcp dst eq 137
deny tcp dst eq 138
deny tcp dst eq 139
deny tcp dst eq 445
deny tcp dst eq 689
deny udp dst eq 1025
deny udp dst eq 1026
deny tcp dst eq 3389
permit ip
```

Source 24

Zero Trust Network - See, Profile, Segment



Visibility



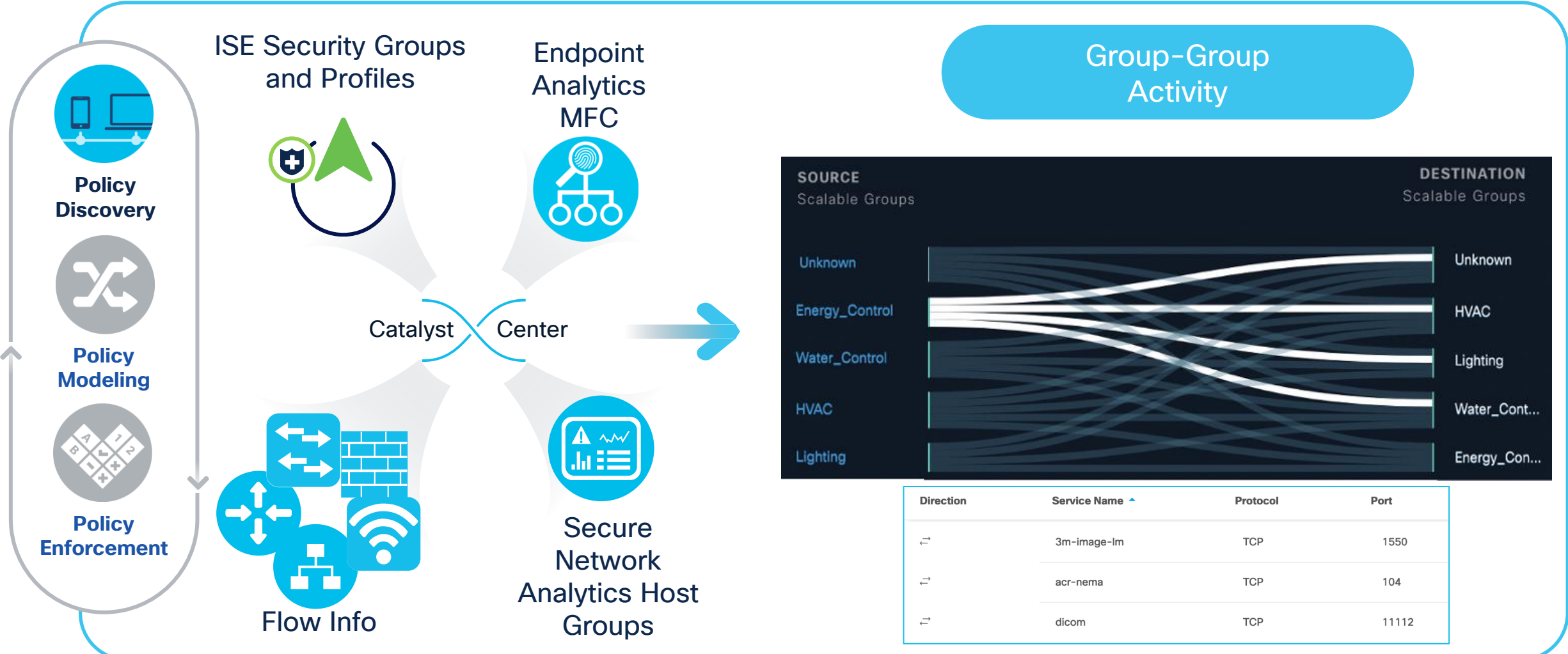
Segmentation



Microsegmentation

Group-Based Policy Analytics (GBPA)

Application on Catalyst Center



The unseen hero – NDR (Formally NBAD)

Compliance

- Policy Violation
- Insecure protocols
- Rogue/new devices
- Torrent/File Sharing
- Bypass of proxy
- Application Identification
- Monitoring Users
- Geographically unusual traffic

Forensic Investigation

- Anomaly
- C2 traffic
- Data Ex
- Data Hoarding
- DDOS Attack
- Beaconing
- Bogon Traffic
- Cryptomining
- Fake Apps
- Malware (including in encrypted traffic)
- P2P traffic
- Insider Threats
- Brute Force Attacks
- Lateral Movement

Incident Response

- Integrating with:
- Identity Solutions
 - SIEM
 - SOAR
 - Packet Capture
 - CI
 - OT Systems

Network Visibility

- Visibility Assessment
- Rogue DHCP / DNS Servers
- Unauthorized Hosts in a Bypass VLAN
- Unknown or Malicious Scanning
- Investigating Slow Network Performance
- Monitoring Remote Workforce

Threat Detection

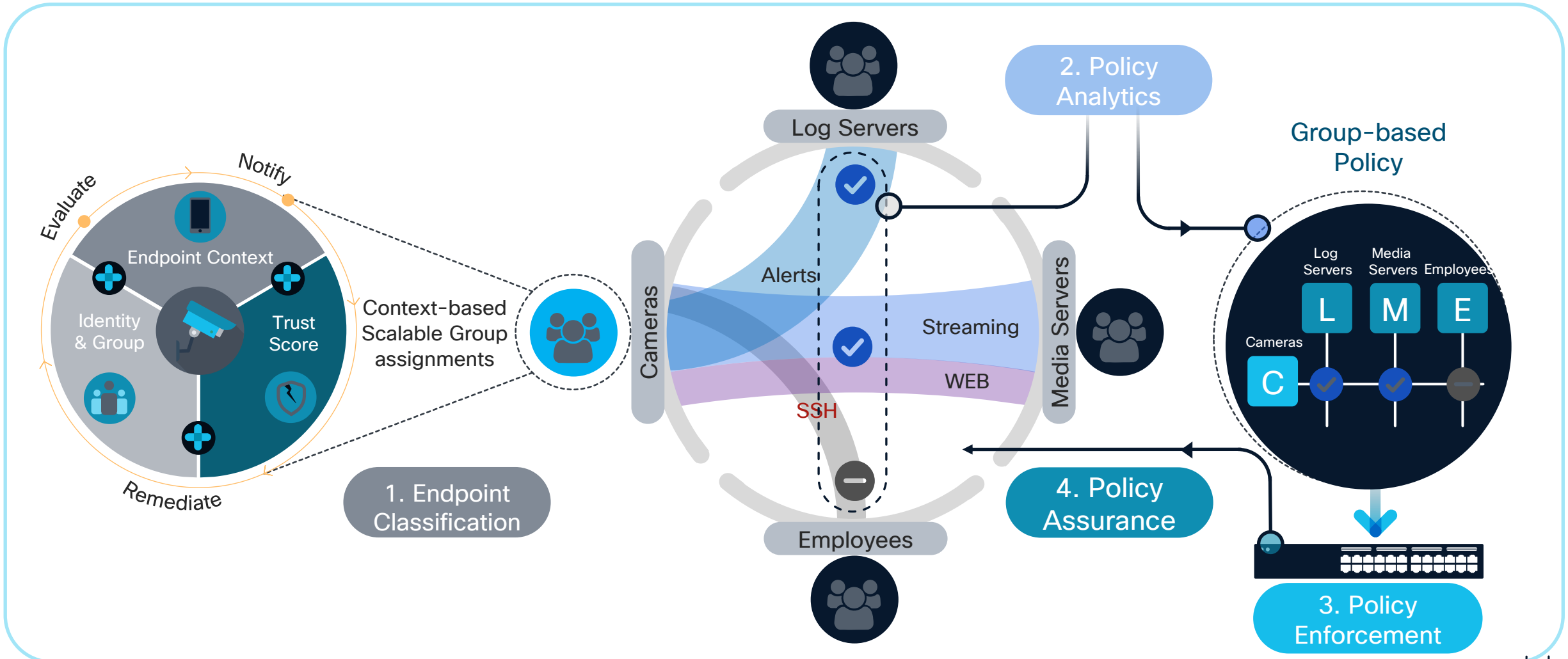
- Anomaly
- C2/Data Ex/Data H
- DDOS Attack
- Exploitation
- High Concern & High index
- Policy Violation
- Recon
- Beaconing
- Bogon Traffic
- Cryptomining
- Fake Apps
- Malware
- P2P traffic
- Insider Threats
- Brute Force Attacks
- Lateral Movement

Bring it all together



Catalyst Center and ISE

Visibility Driven Segmentation



Rapid Threat Containment (RTC)

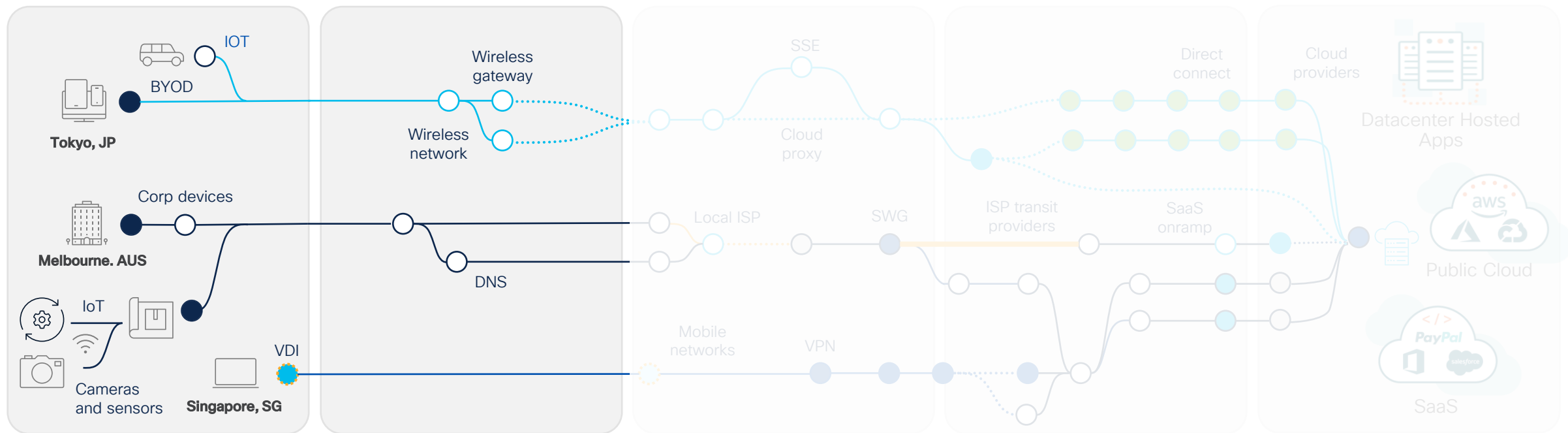


ISE is the Core of Cisco's Common Policy Data Center

Campus

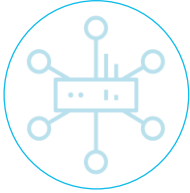
IoT





Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads & Cloud
Visibility, Identification, Segmentation Device Profiling Identity Authorization Segmentation Access Control Policies	Policy Enforcement & Service Availability Context Sharing Segmentation Access Control Policies Software Defined WAN Cloud (SSE) Integrations	Access Control & Intrusion Prevention Policy Enforcement Service Visibility Traffic Monitoring Breach Prevention	Access Control & Intrusion Prevention DC Edge Access Traffic Visibility Breach Prevention	Workload and App Protection Segmentation Workload baseline SBOM and Inventory Microservice Protection

Simplifying Branch Deployments



Cisco SD-WAN

- Best in class SD-WAN
- Converged Security
- Multicloud optimized
- Existing install and new Secure 8k Router



Cisco Secure Firewall

- Best in class Security
- Simplified Management
- Intelligent Path Selection
- East/West Branch protect
- XDR + Splunk Integrated
- Easy SSE Connect



Meraki

- Best in class visibility and troubleshooting
- Ease of Deployment “Lean IT”
- Unified Threat Management
- XDR and Splunk Integrated

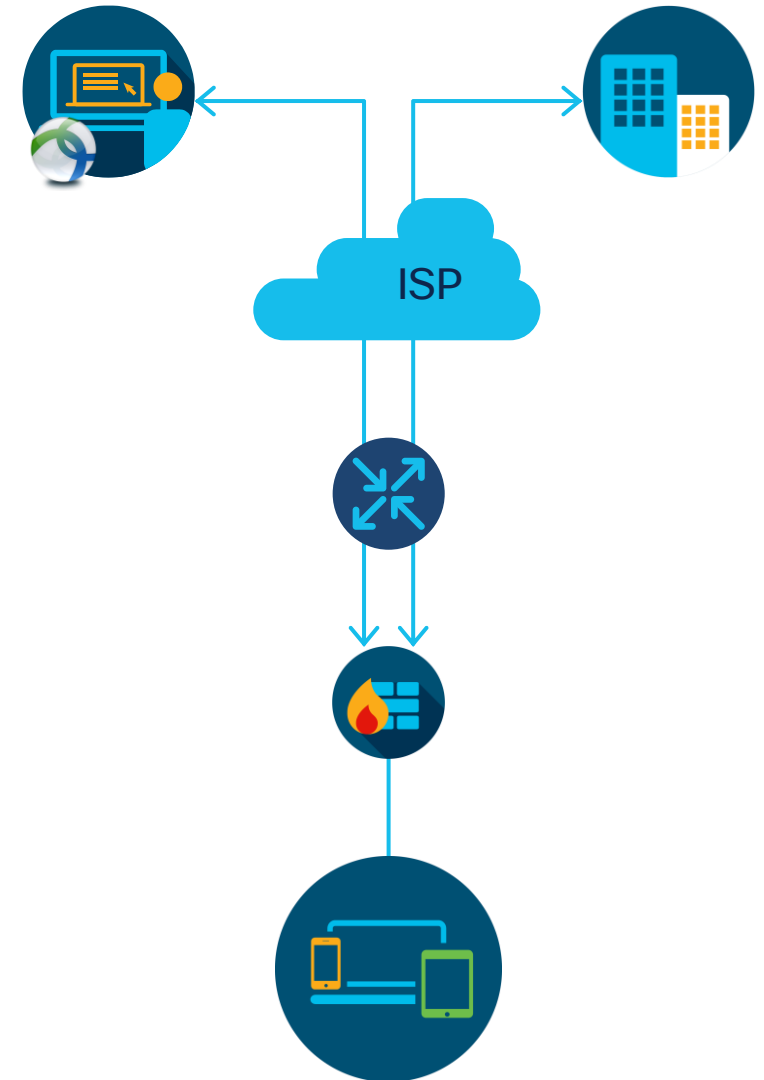
Branch

Customer Requirements

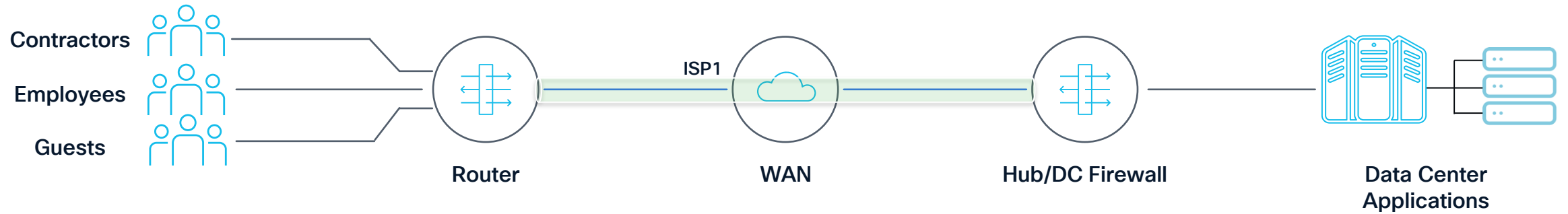
- Advanced Access Control options
- Remote Access VPN
- Site to Site VPN
- Dual ISP Support
- Block access to malicious IPs, URLs, DNS
- Block traffic to 3rd party lists
- Detecting malicious network traffic
- Visibility and tracking of file transfers, Blocking of malicious files
- Dynamic analysis of unknown files

Secure Firewall Capabilities

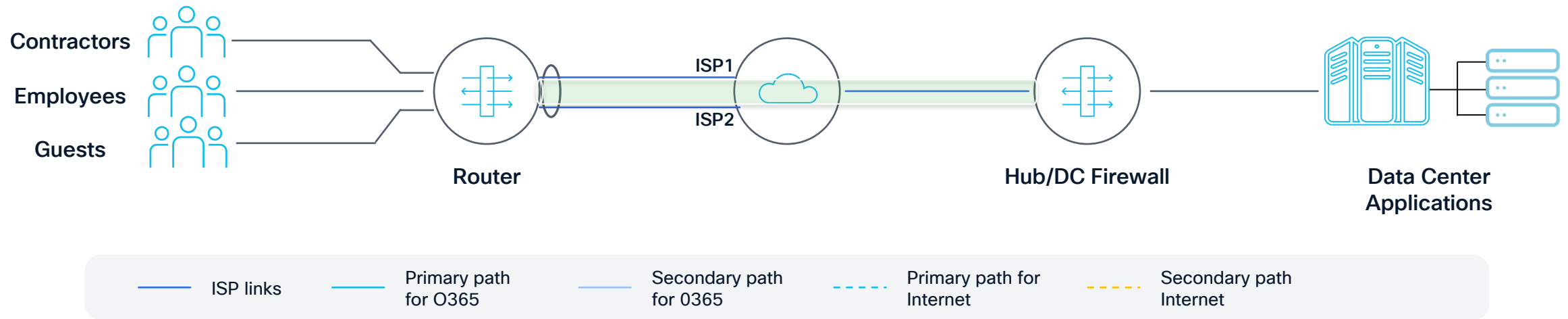
- Applications, URLs, Users, and TrustSec Policy using SGTs
- Client/Clientless VPN/ZTNA
- Route Based VPN
- IP SLA or Traffic Zones
- Talos Security Intelligence
- Unified Policy across Firewall estate
- Threat Intelligence Director
- Snort IPS
- Cisco Secure Malware Analytics



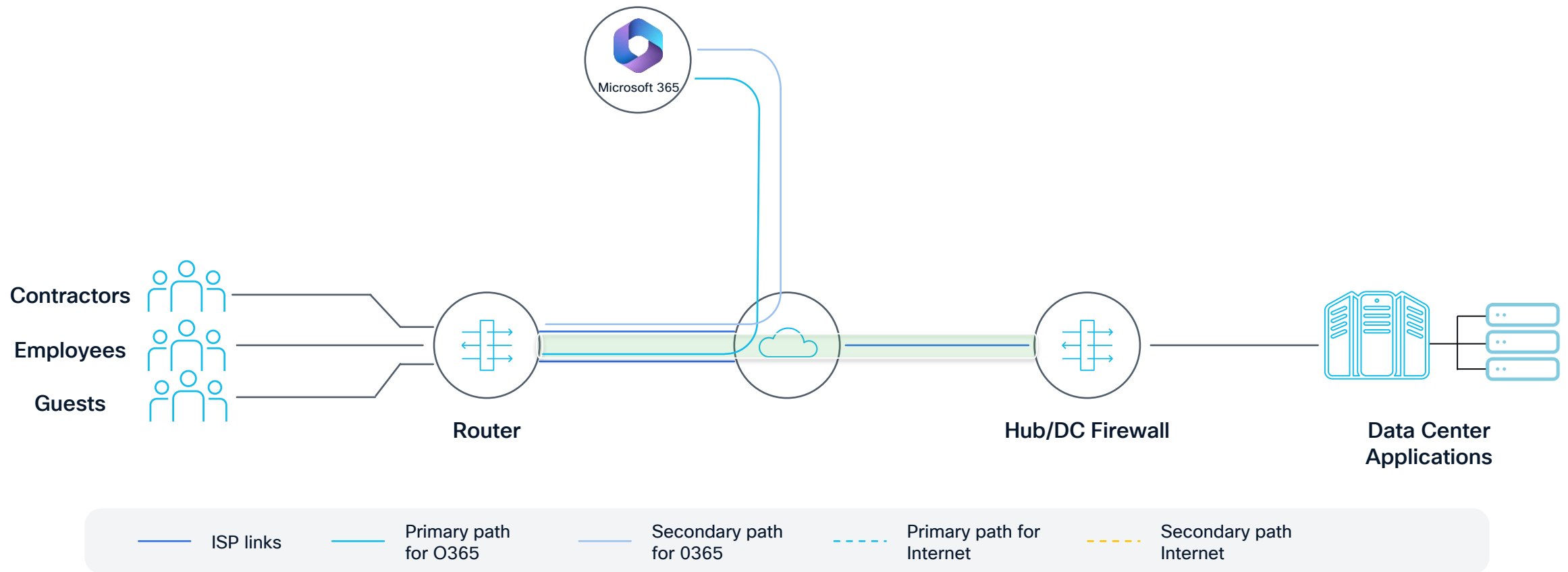
Simple WAN



Redundant WAN

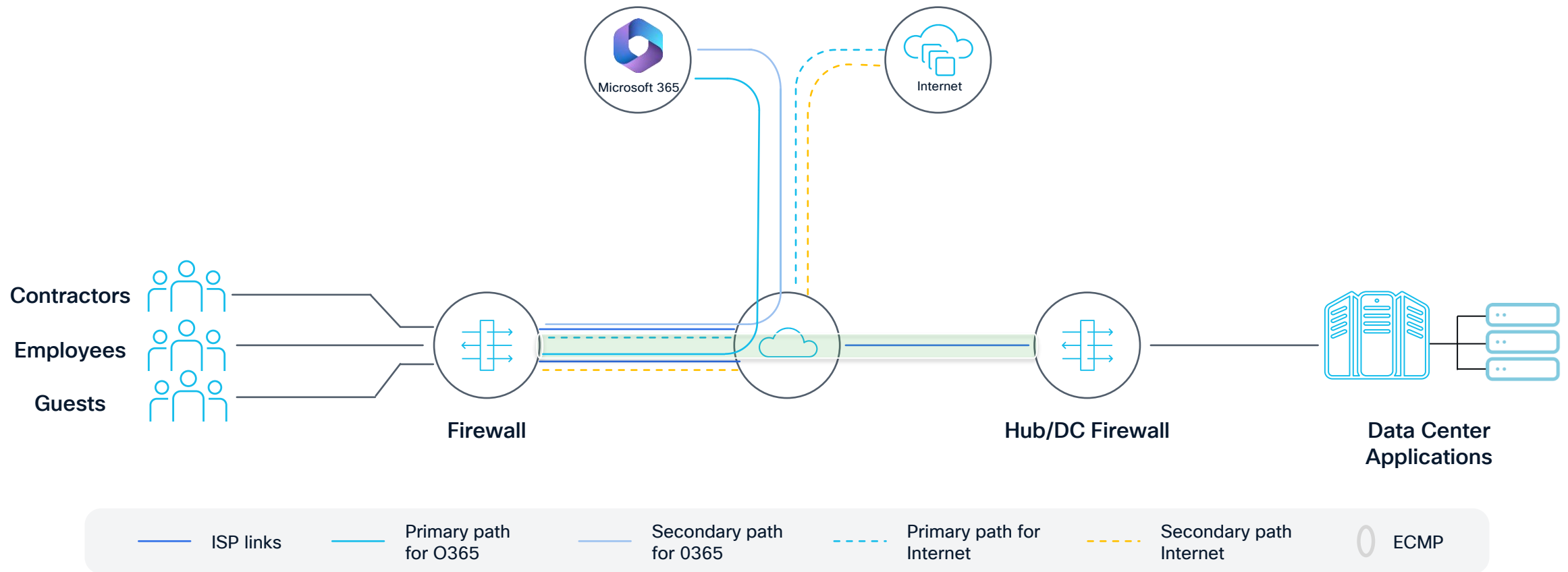


Redundant WAN with select SaaS services



DIA brings requirements for security compliance

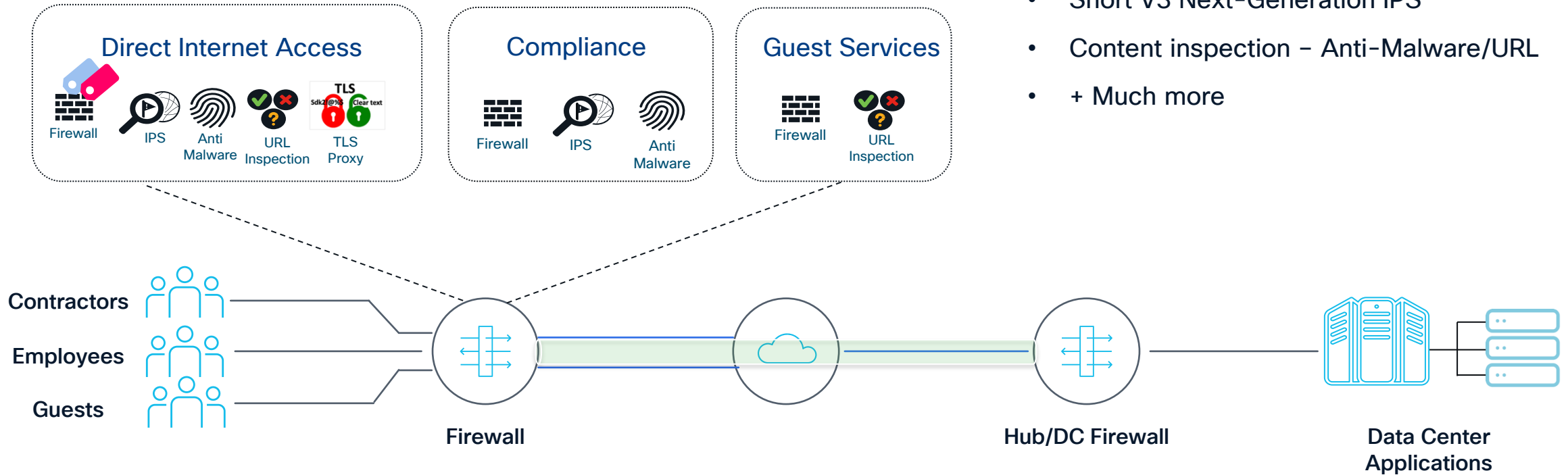
Redundant WAN + SaaS Direct + Direct Internet Access



Firewall @ Branch Security Services

Embedded Security Services

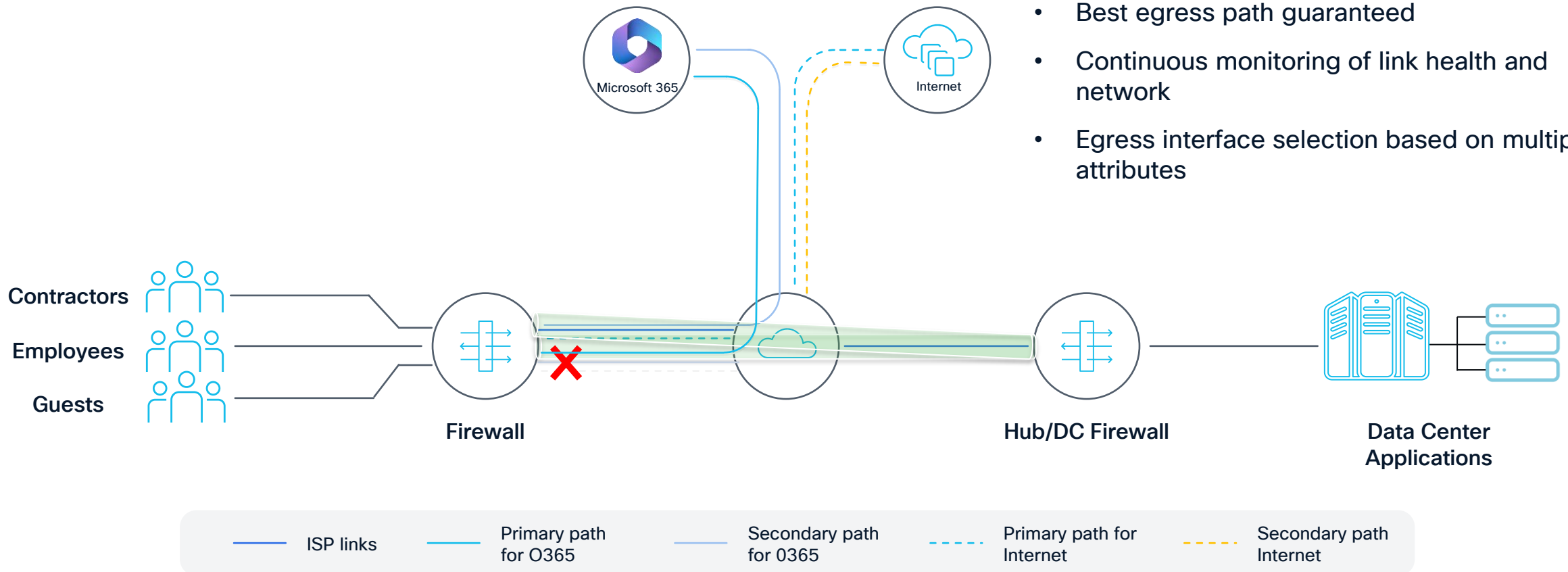
- Layer 7 Firewall with Application Visibility
- TLS Decryption
- Snort V3 Next-Generation IPS
- Content inspection – Anti-Malware/URL
- + Much more



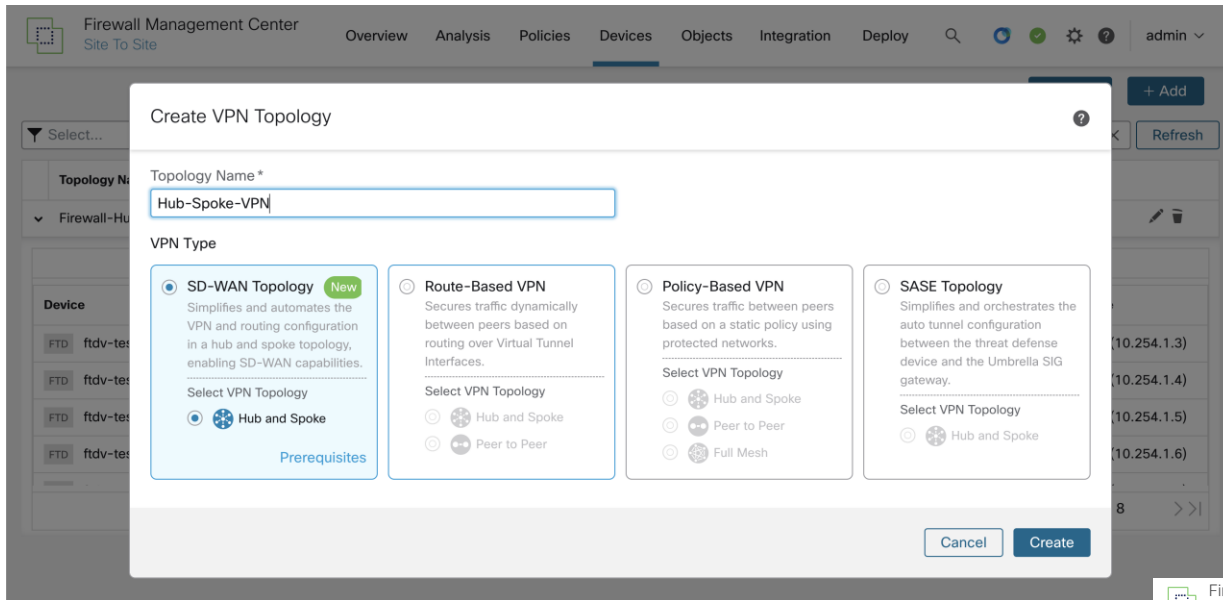
Firewall SD-WAN – Protection with Failover

Intelligent Routing Services

- Intelligent application routing
- Dynamic path selection using real time metrics
- Best egress path guaranteed
- Continuous monitoring of link health and network
- Egress interface selection based on multiple attributes



SD-WAN Wizard – FTD 7.6

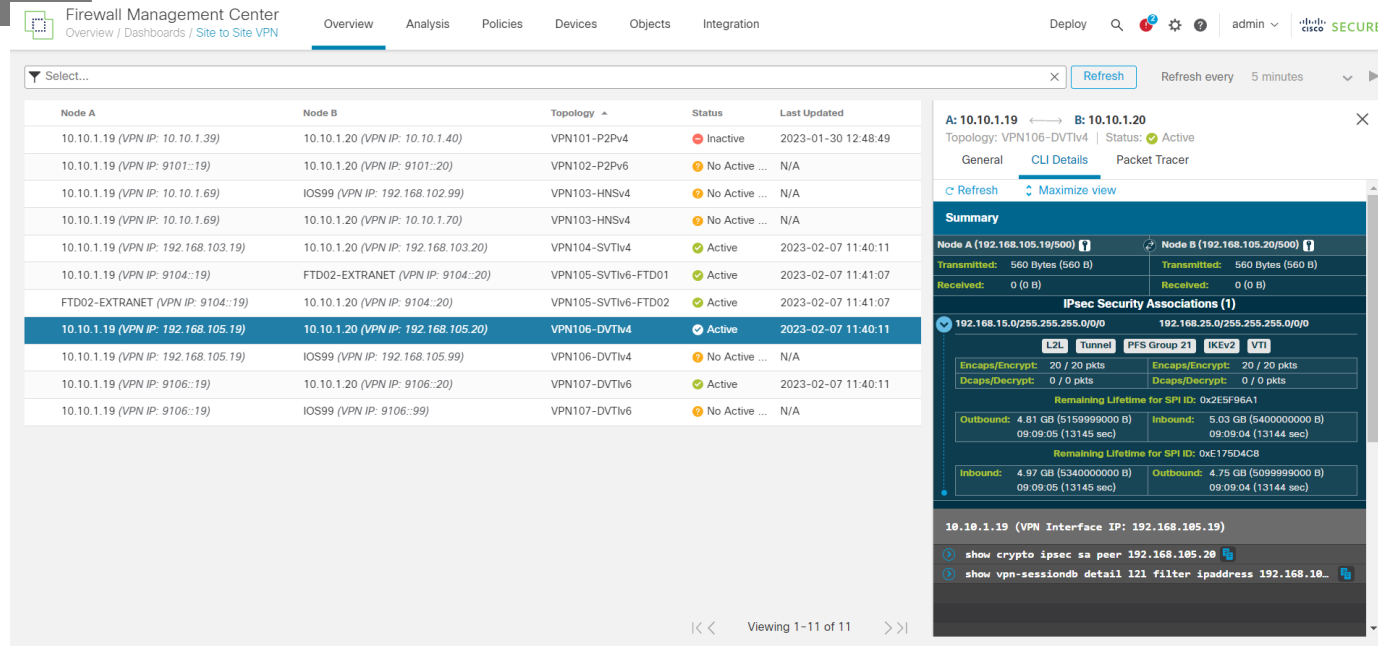


SDWAN Topology Wizard

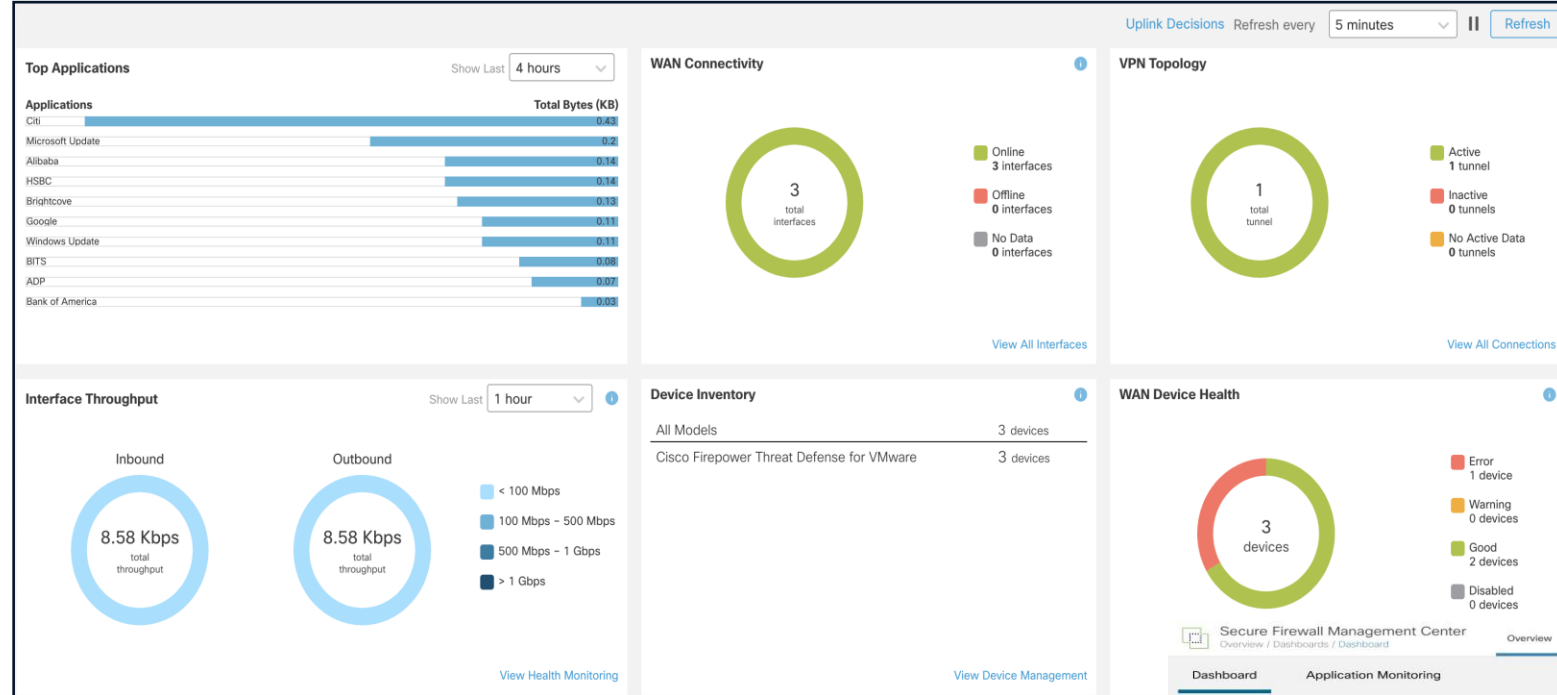
- Policy Templates
- Bulk Branch Onboarding Templates
- Bulk Pre-Provisioning Templates for LTP
- Tunnel/Route Setup Wizard

Unified Viewer

- Easily analyze VPN traffic flow
- Easy to view and understand the configuration of VPN peers



SD-WAN Monitoring

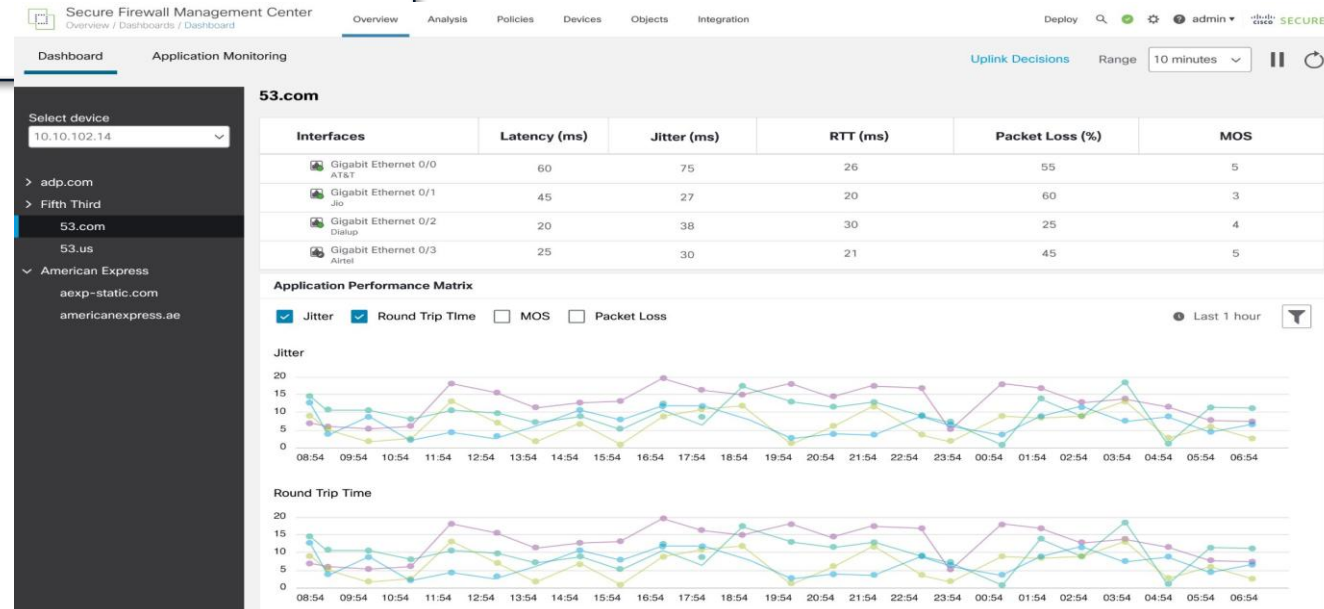


SD-WAN Summary

- Top Applications
- WAN Connectivity (WAN Link status)
- Interface Throughput on WAN Links
- VPN Topology (VPN Tunnel status)
- WAN Device Inventory and Device Health

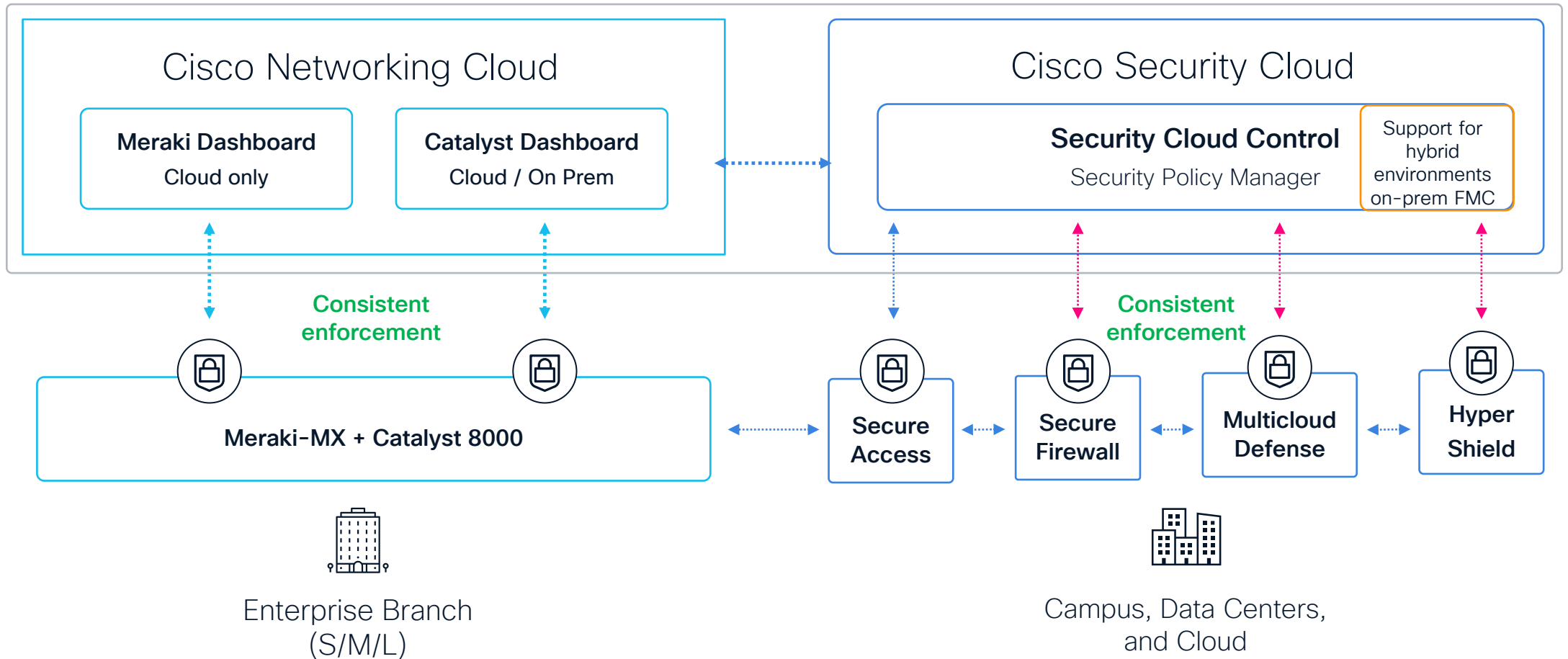
Application Monitoring

- Easily monitor all interfaces where policy is enabled
- Detailed application performance metrics for Jitter, Round Trip Time, MOS and Packet Loss
- Custom monitoring of services

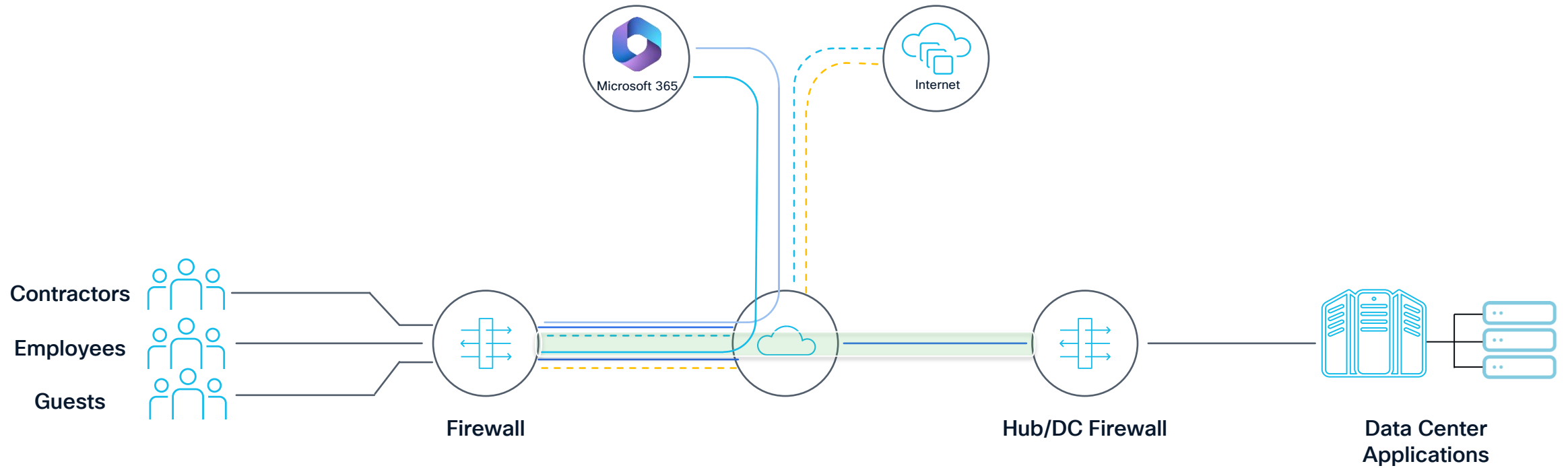


Unified Secure WAN experience

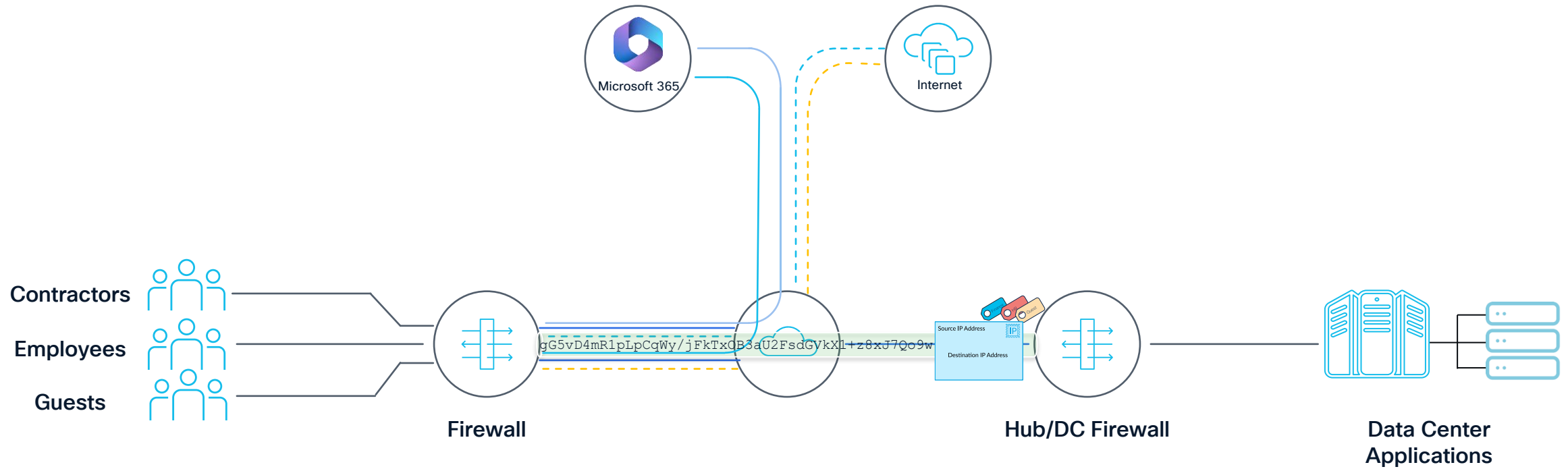
Centralized security policy with consistent enforcement at WAN Edge



Branch to DC and Cloud options



Branch Firepower DIA, Hub/DC



Intent based policy using SGT over tunnels

FTD 10.0.0
(prev 7.8)

SGT over VTI (Tunnel)

- Customers with Cisco SDA fabrics and Firewalls can now extend segmentation over tunnels
- Ex: If a pkt arrived with a valid tag from LAN, it will egress with the same tag over tunnel to a datacenter.
- Policies are applied in DC based on the tag either in firewall, Switch or a Cisco Router
- Extends capabilities beyond Campus Access networks into DC

Firewall Management Center
Devices / VPN / Site To Site

Edit VPN Topology

Topology Name:*
RB-HnS-VPN

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Session Settings

☒ Enable VPN Idle Timeout
30 Minutes (Range 1 - 35791394)

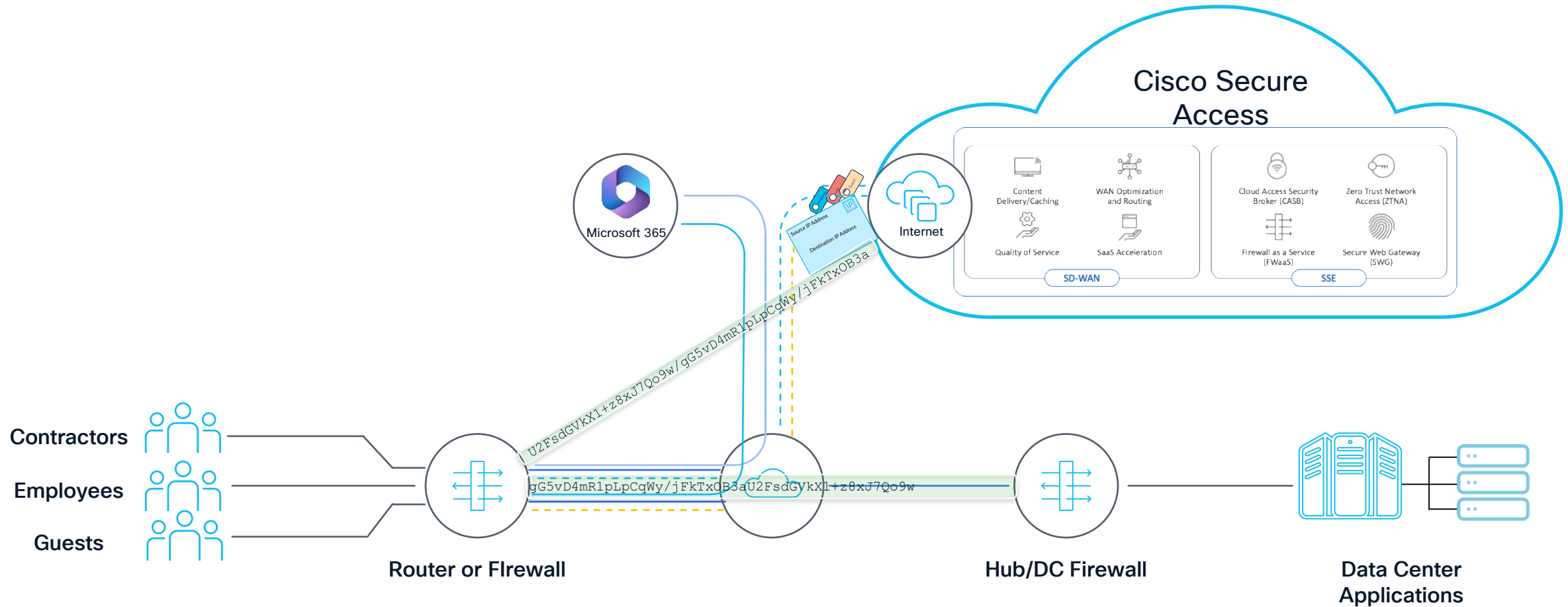
TrustSec (SGT) Settings

☐ Enable SGT propagation over Virtual Tunnel Interfaces
This option enables global Security Group Tag (SGT) propagation over SVTIs and DVTIs. To enable SGT propagation on a specific SVTI or DVTI, configure it in individual devices. Threat Defense device must be Version 7.8.0 and later.

Access Control for VPN Traffic

☐ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the

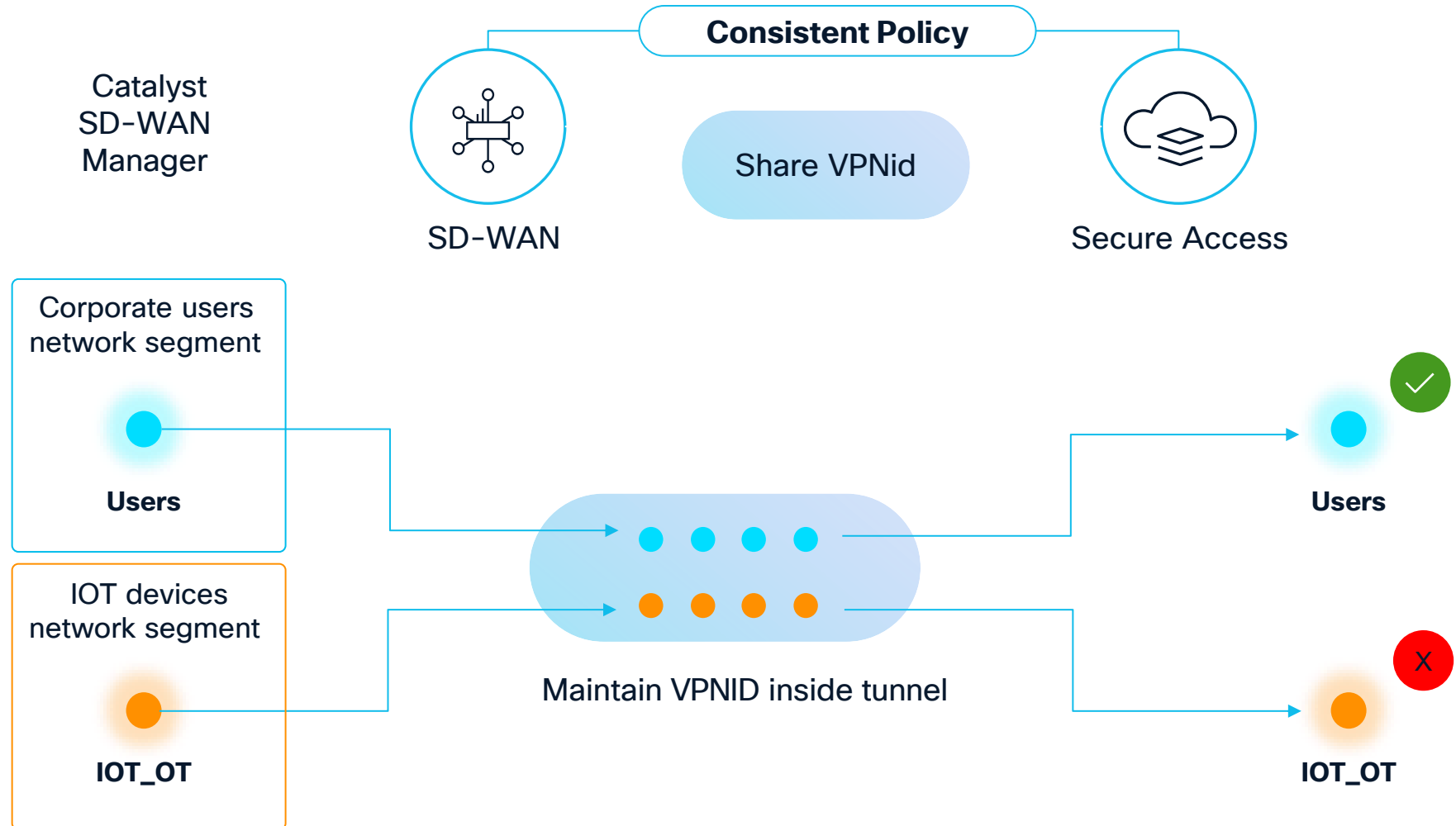
Branch Firepower DIA, Hub/DC and Secure Access SSE



Catalyst SD-WAN

VPNid support for consistent segmentation

- VPNid Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Catalyst SD-WAN

Monitor

Configuration

Analytics

Workflows

Tools

Reports

Maintenance

Administration

Explore

Catalyst SD-WAN

configuration.policies.viewSecureServiceEdge

SGTDemos-Context

SSE Provider

Cisco Secure Access

Zscaler

Context Sharing

VPN

SGT

Tracker

Source IP address

192.168.100.100

Name	Threshold	Interval	Multiplier	API URL Of Endpoint	Action
Tracker	300	60	3	http://www.cisco.com	

Configuration

Interface Name	Description	Shutdown	TCP MSS
ipsec101		false	
ipsec102		false	

Region

Canada (Central)

Secure Access

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name

Intent

2

Object

Settings

Reset all

5 Results

#	Rule name	Access	Action	Sources	Destinations	Security
1	Robots Allow	Internet	Allow	Robots	Any	
2	IOT Devices	Internet	Block	Cell1	Alcohol +13	
18	IOT branch	Internet	Allow	IOT_OT	Any	
28	IOT Devices to HMI	Private	Allow	Cell1	HMI	
29	Block Cell1 to Any	Private	Block	Cell1	Any	

0 result from Default Access Rules

Rule name	Action	Sources	Destinations	Security
-----------	--------	---------	--------------	----------

IOT Devices

Internet

1115

App Risk Profile

Disabled

Sources

1 source

Security Group Tags (1)

Cell1

Destinations

14 destinations

Content Categories (14)

Alcohol

Illegal Activities

Illegal Downloads

Web-based Email

Chat and Instant Messaging

Illegal Drugs

News

Shopping

Sports and Recreation

Streaming Video

+ 4 More

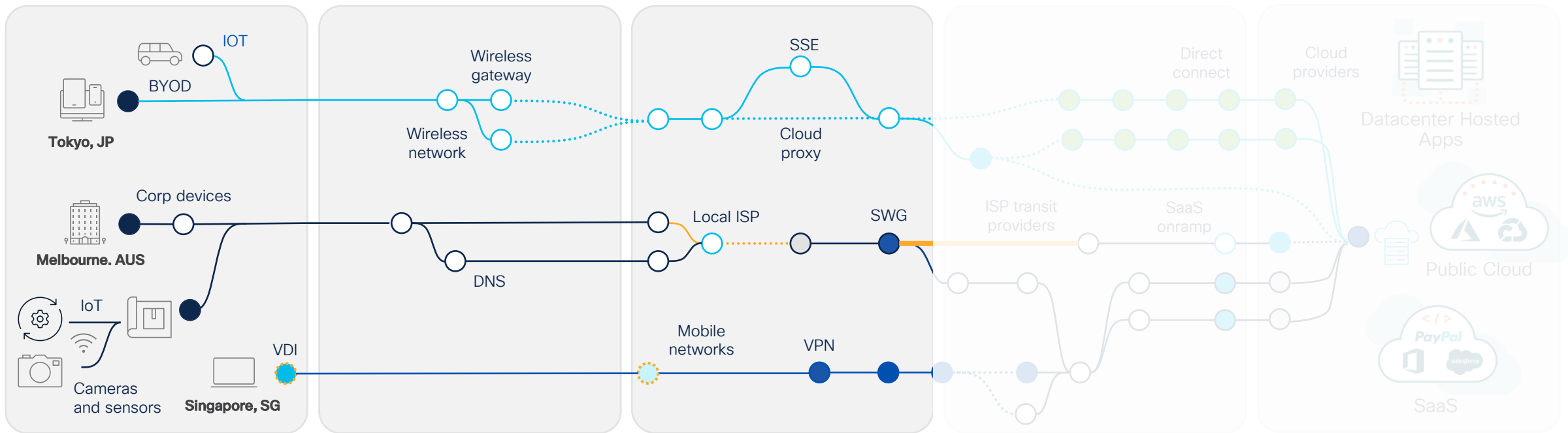
Security

1 Security Control

Delete

Cancel

Edit



Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads & Cloud
<p>Visibility, Identification, Segmentation</p> <p>Device Profiling</p> <p>Identity Authorization</p> <p>Segmentation</p> <p>Access Control Policies</p>	<p>Policy Enforcement & Service Availability</p> <p>Context Sharing</p> <p>Segmentation</p> <p>Access Control Policies</p> <p>Software Defined WAN</p> <p>Cloud (SSE) Integrations</p>	<p>Access Control & Intrusion Prevention</p> <p>Policy Enforcement</p> <p>Service Visibility</p> <p>Traffic Monitoring</p> <p>Breach Prevention</p>	<p>Access Control & Intrusion Prevention</p> <p>DC Edge Access</p> <p>Traffic Visibility</p> <p>Breach Prevention</p>	<p>Workload and App Protection</p> <p>Segmentation</p> <p>Workload baseline</p> <p>SBOM and Inventory</p> <p>Microservice Protection</p>

Customer Challenges We Consistently Hear

- User frustration with cumbersome experiences
 - Risks from unmanaged devices/BYOD (contractors)
 - Risks from AI app/platform use
- Identity attacks are accelerating
 - Security gaps from “things” (IT, OT, IOT)
 - Difficult to verify identity as user behavior/locations change
- Interruptions/slowdowns impede productivity
 - Problem detection/remediation is not fast enough
 - Policy changes create unintended consequences

Solving these challenges requires network and security convergence

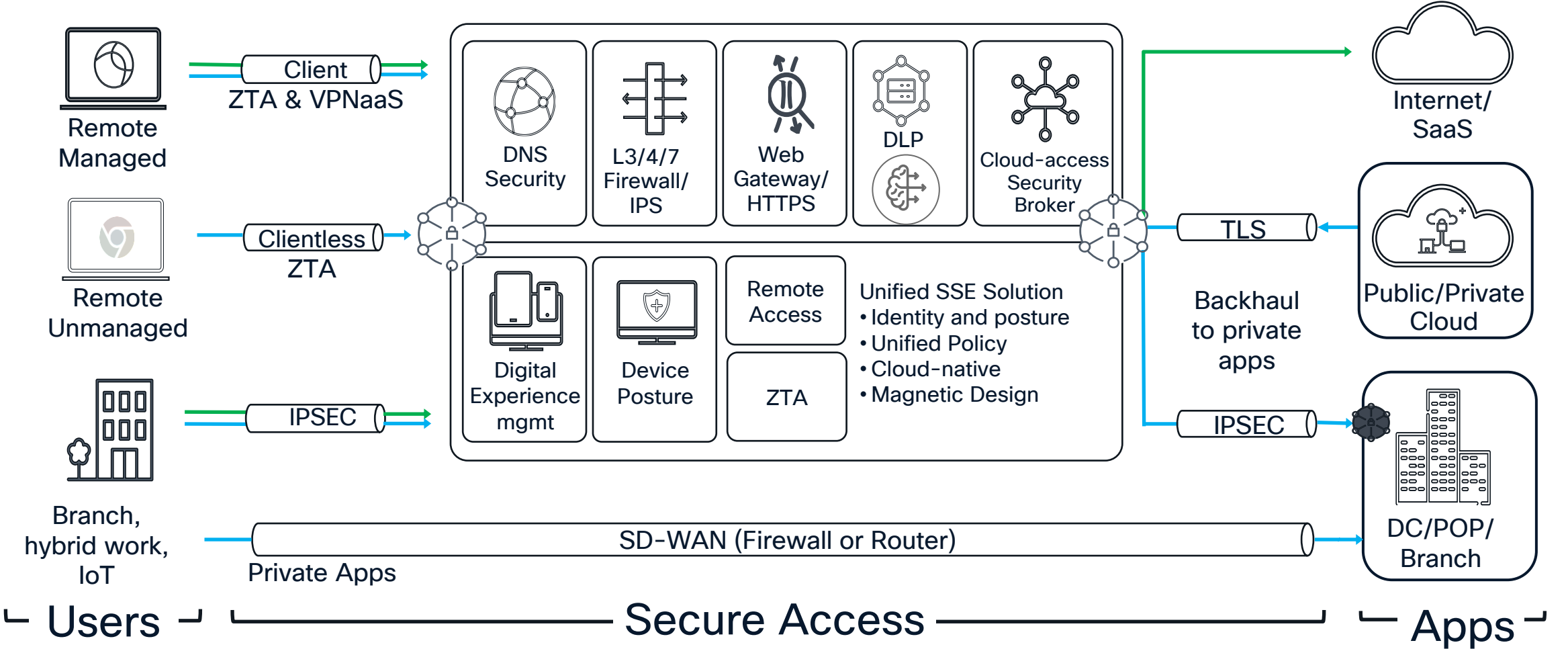
How to connect Users to Cisco Secure Access (CSA)

1 Connect to a network

2 Get to work

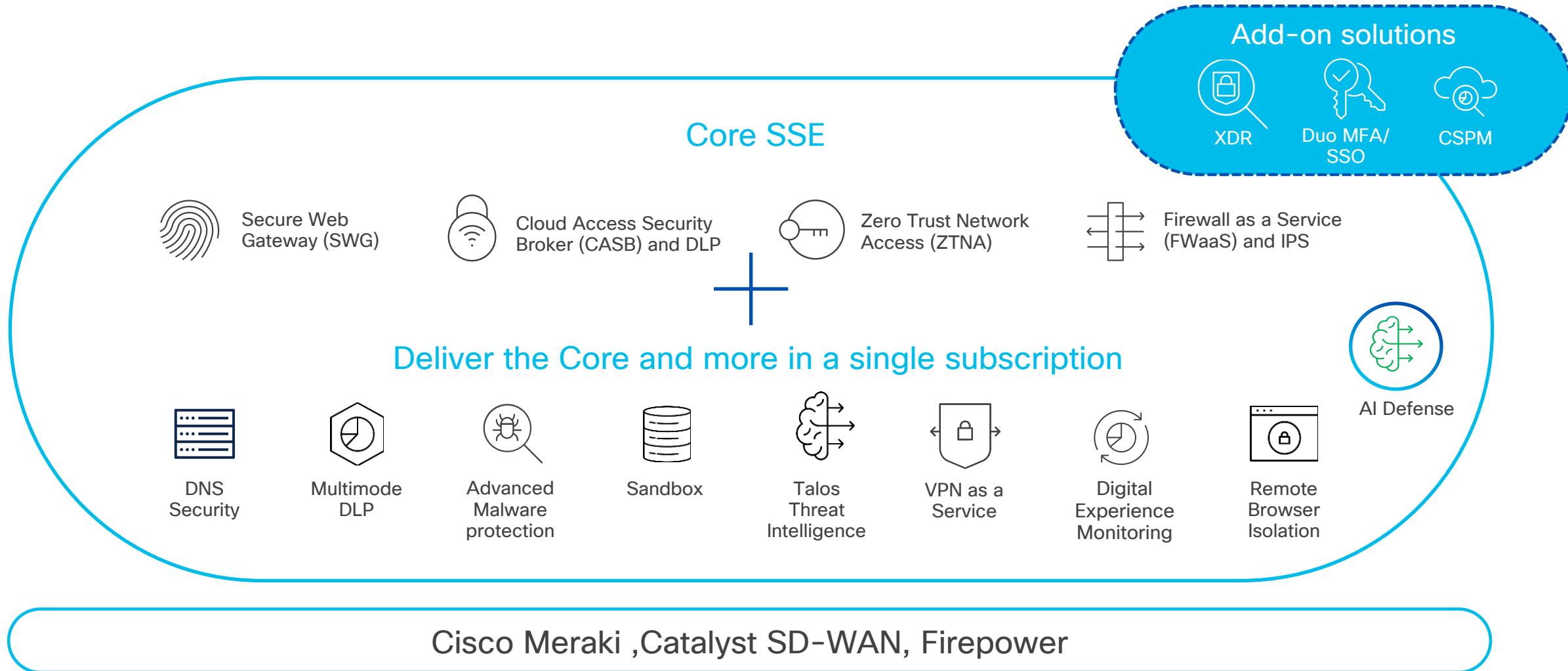


Cisco Secure Access



Cisco Secure Access – Security Capabilities

Go beyond core Security Service Edge (SSE)



Unified Access Policy

Source + Destination = Action | Posture + Security Controls

Identity,
Address,
SG Tag,
NTG,
Device,
etc...

Application,
Address,
Geolocation,
Category,
etc...

Allow,
Block,
Warn,
Isolate

OS ver.
Browser,
AV,
Firewall,
Disk Encr.
etc...

IPS Profiles
AV
Security Profiles
etc...

What is the intent?

Under which conditions

Secure Access – Policy Table and Logic

16 Rules

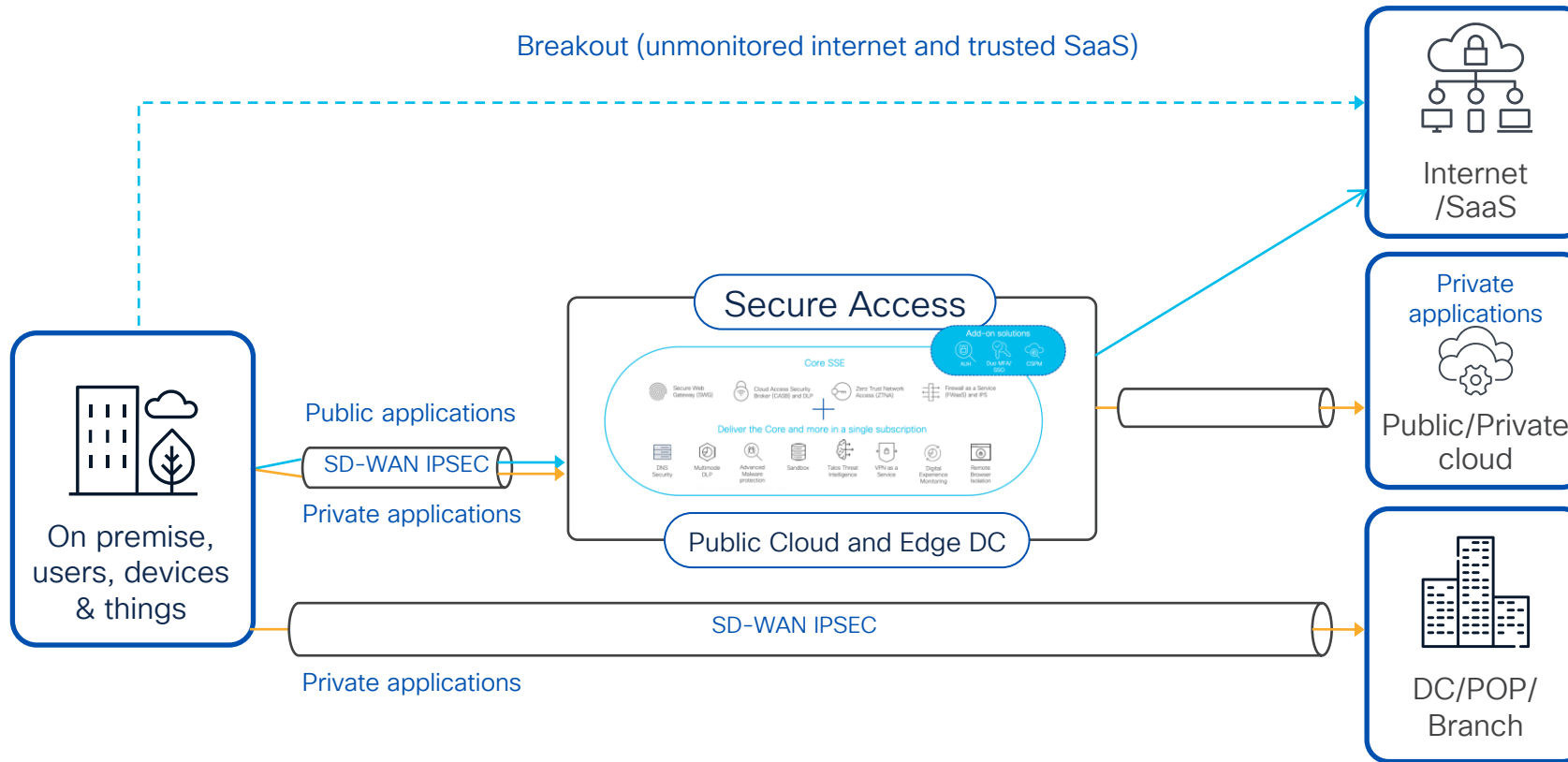
Customize view

☐	#	Rule name	Access	Action	Sources	Destinations	Security	Logging	Posture
☐	1	RBI for Risky Destinations	Internet	Isolate	SSE Incubati...	Potentially ...		Enabled	-
☐	2	Allow Gmail → Block Uploa...	Internet	Allow	SSE Incubati...	Gmail		Enabled	-
☐	3	Block SSH → Outside World	Internet	Block	Marko Tanask...	ssh		Enabled	-
☐	4	Trigger SAML → Outside	Internet	Allow	Any	DL_MSFT_Azur...		Enabled	-
☐	5	Block Illegal Content → Ou...	Internet	Block	Any Network ... +1	Illegal Acti... +5		Enabled	-
☐	6	NTG Secure Access → Out...	Internet	Allow	NTG DE	Any		Enabled	-
☐	7	Roaming Devices → Outside	Internet	Allow	Computers (m...	Any		Enabled	-
☐	8	DNS AND PROXY - REGIST...	Internet	Allow	FraHome4 +1	Any		Enabled	-
☐	9	Default Access Rules ⓘ							
☐	10	Rule name	Action		Sources	Destinations	Security	Posture	
☐	11	For all private access	Block		Any	Any private destination	-	-	
☐		For all Internet access	Allow		Any	Any Internet destination	IPS, Web, Tenant	-	

How to connect Branch Users to CSA

Connect on premise branch and campus users and devices

Internet traffic
Private traffic
Secure tunnel



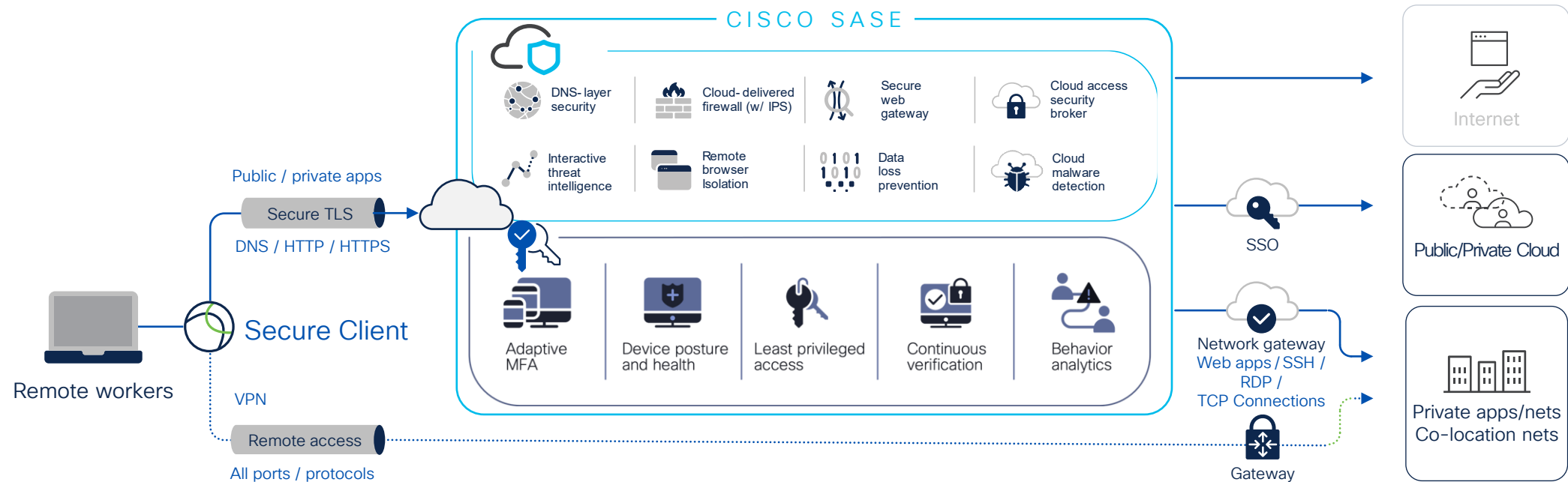
Branch Devices

- Firepower, Meraki, Catalyst SD-WAN
- Catalyst SD-WAN IPSEC Tunnels
- Meraki Auto-VPN connectivity
- Firepower S2S VPN
- UP to 4 Tunnels for scalability and Redundancy
- Load Balancing
- Region Affinity
- Cloud on Ramp

Use Case 1A - Secure client with SSE, MFA and Identity Intel

Work from Anywhere Users

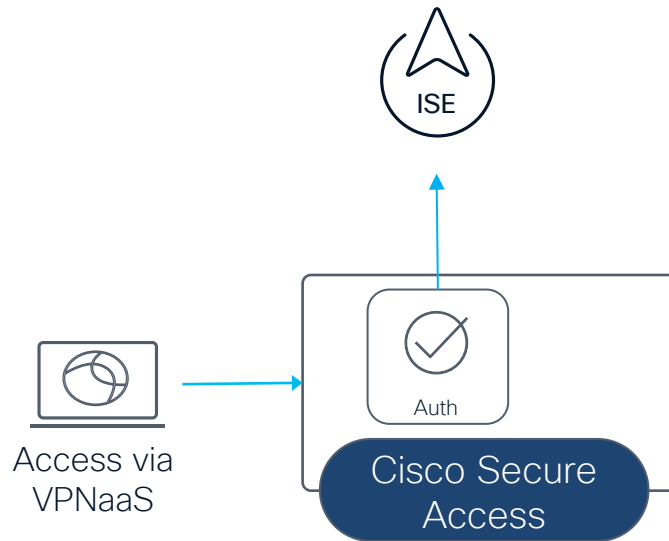
Advanced application experience with comprehensive security



ISE integration with Secure Access VPNaas

VPN-as-a-Service

RADIUS authentication, in addition to SAML authentication

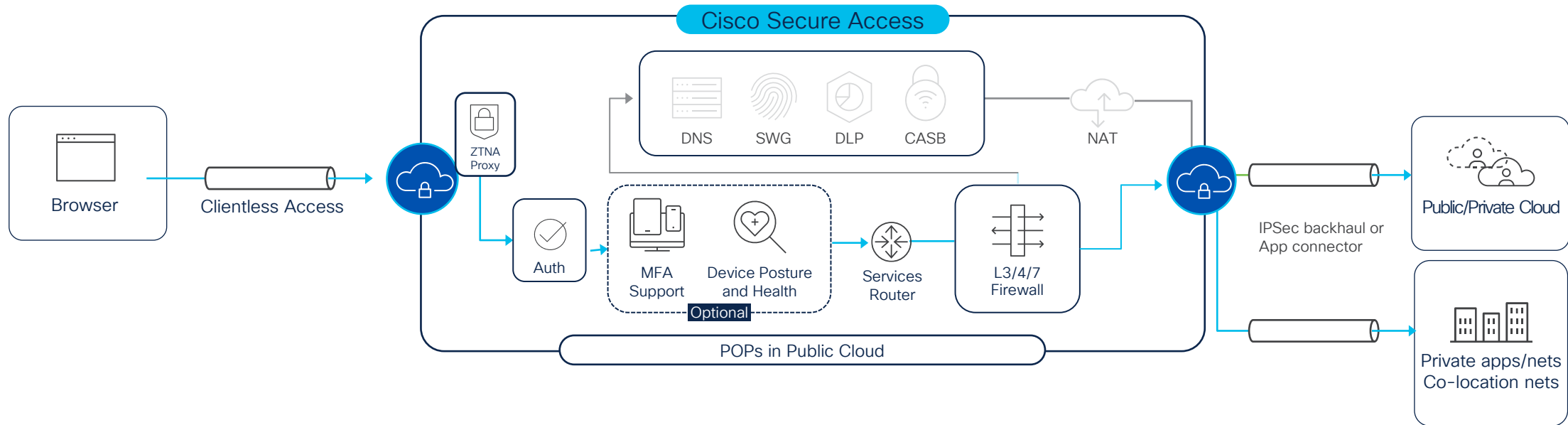


- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- ISE posture supported (optional)
- SGT assignment via authorization (optional)

Use Case 1B – Clientless with Secure Access and Duo

Work from Anywhere Users

Advanced application experience with comprehensive security

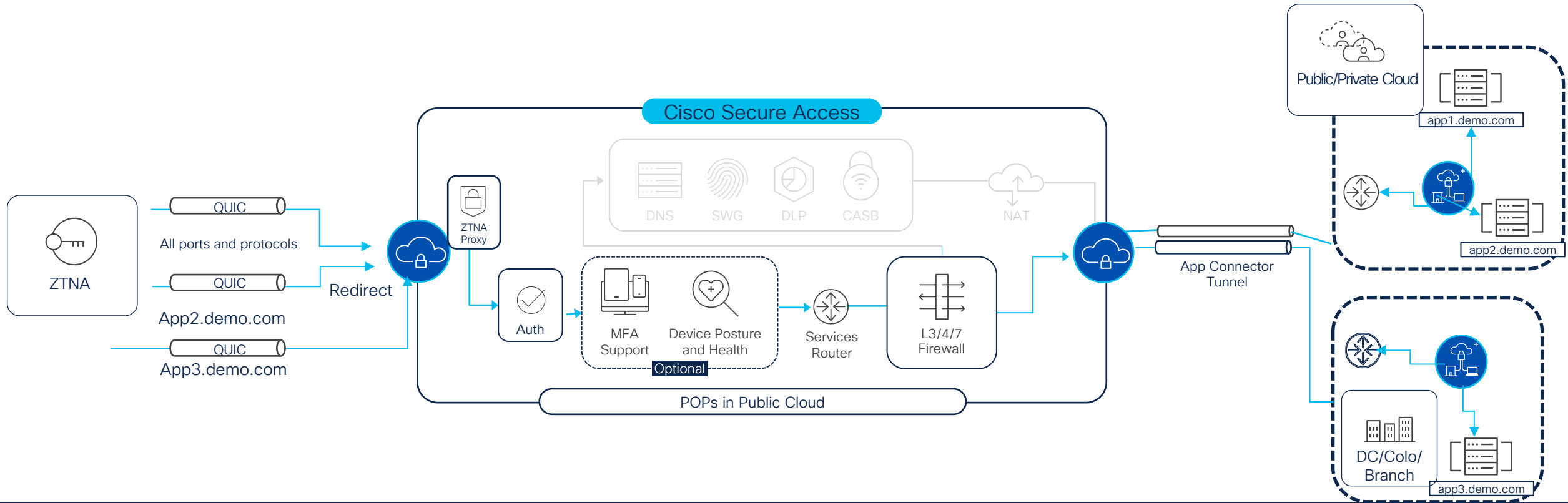


Capabilities

- Clientless
- App-specific access
- Undiscoverable IP address
- Least privileged user access
- Reduced threat surface

Use Case 1C – Secure Private Access (App Connector)

ZTNA supported Apps with App Connector

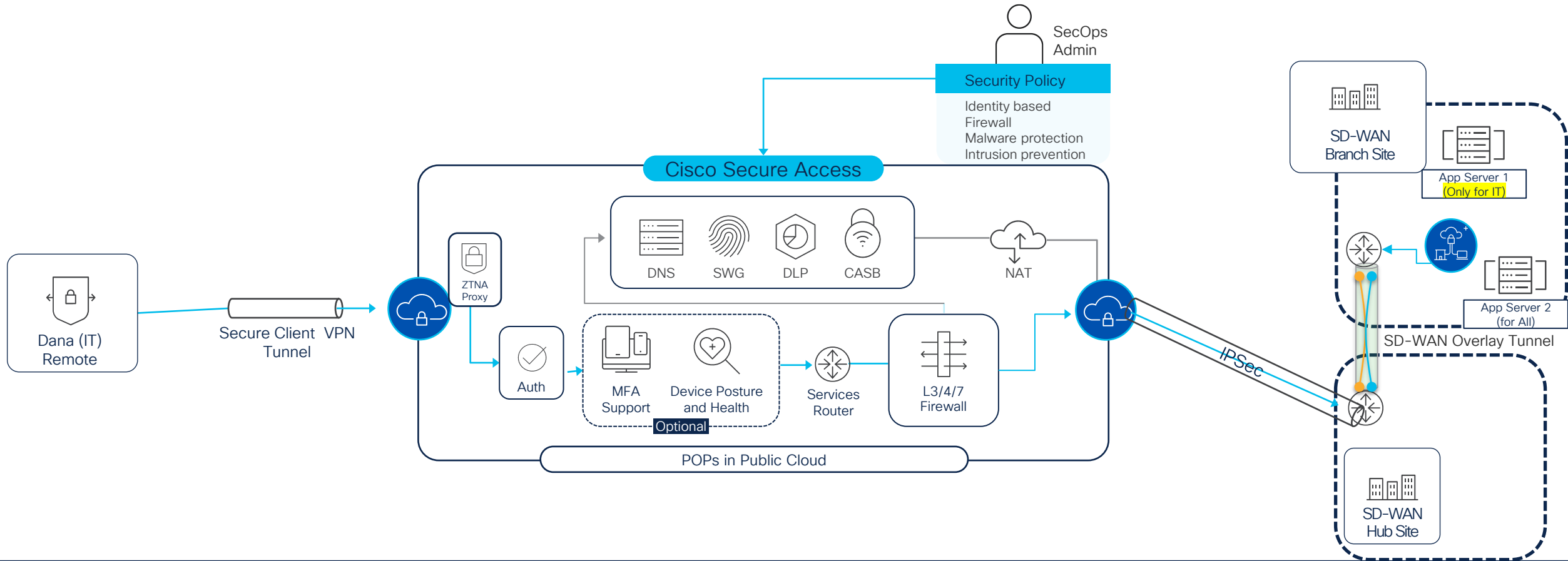


Benefits

- Improved end-user experience
- Improved Security step up auth
- Always on access
- Performance benefits QUIC & MASQUE
- Per App tunnels
- Cloud bypass for sensitive apps (future)
- No routing/network modification on client
- App specific access

Use Case 1D – Secure Private Access (Hybrid)

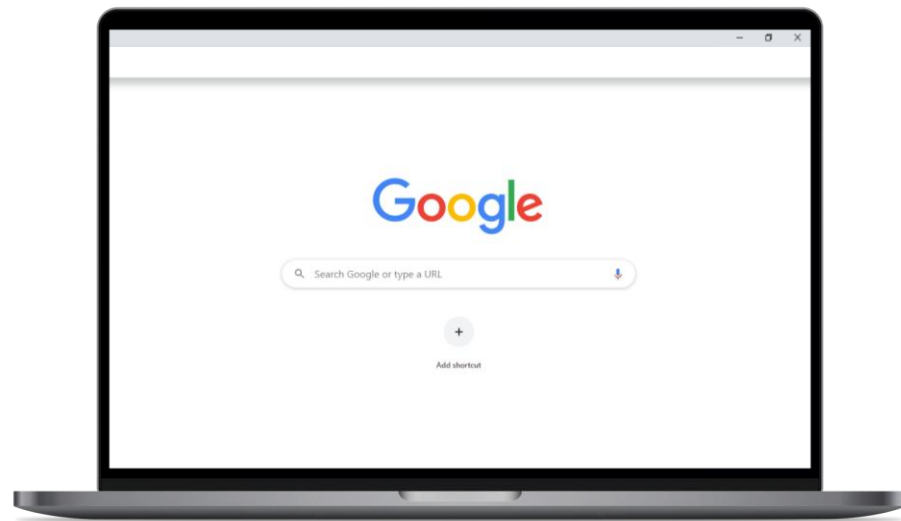
CSA for Secure Private App Access Hybrid



- Uses “As a Service model” to terminate the RA VPN connections at Cisco Secure Access (SSE) & restrict the access to Private Apps hosted on a Cloud Branch

Native Device Support

BYOD via enterprise managed Google Chrome
Advanced protocol support for Apple, Samsung



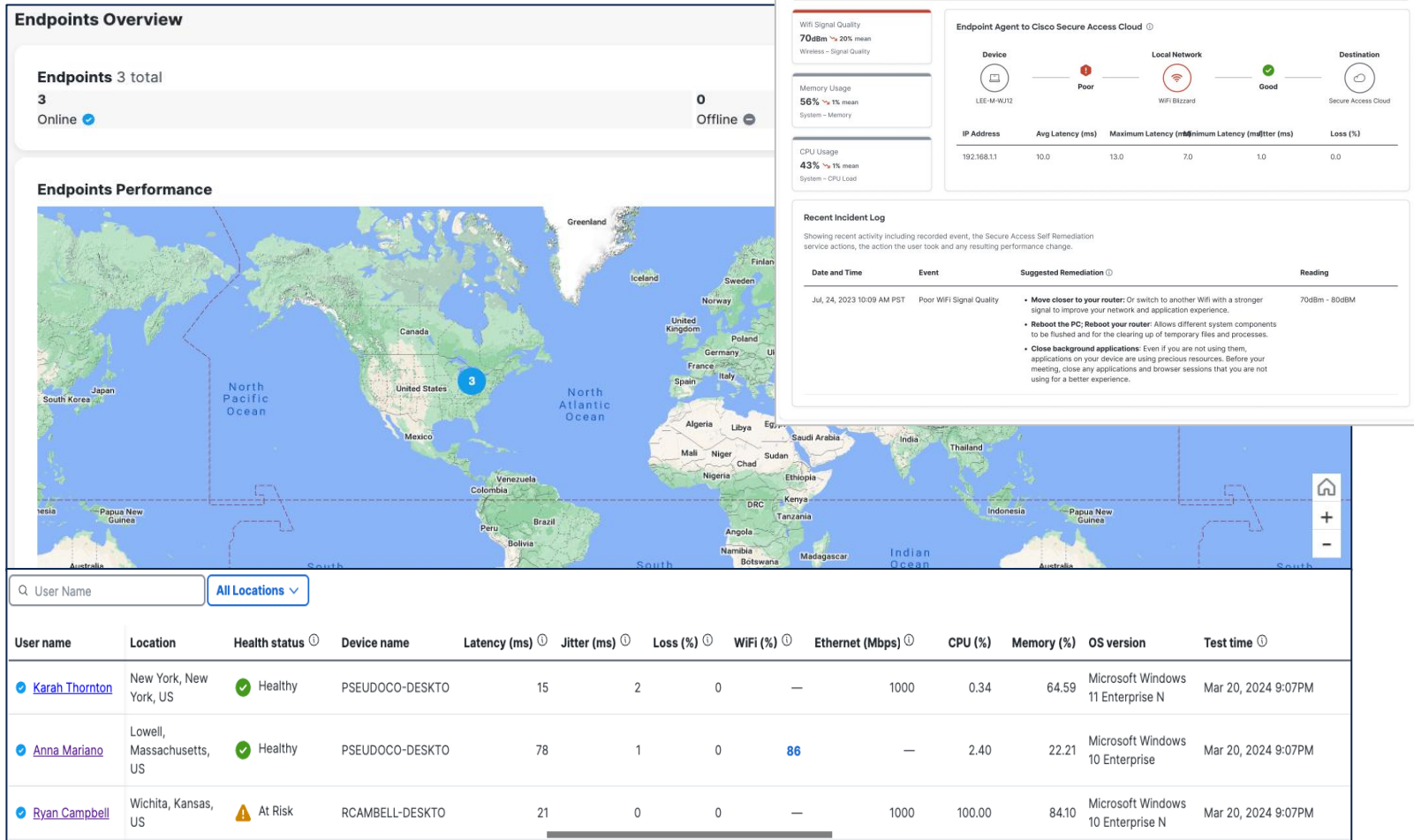
Chrome Enterprise Browser



Native OS Integration

Secure Access Experience Insights

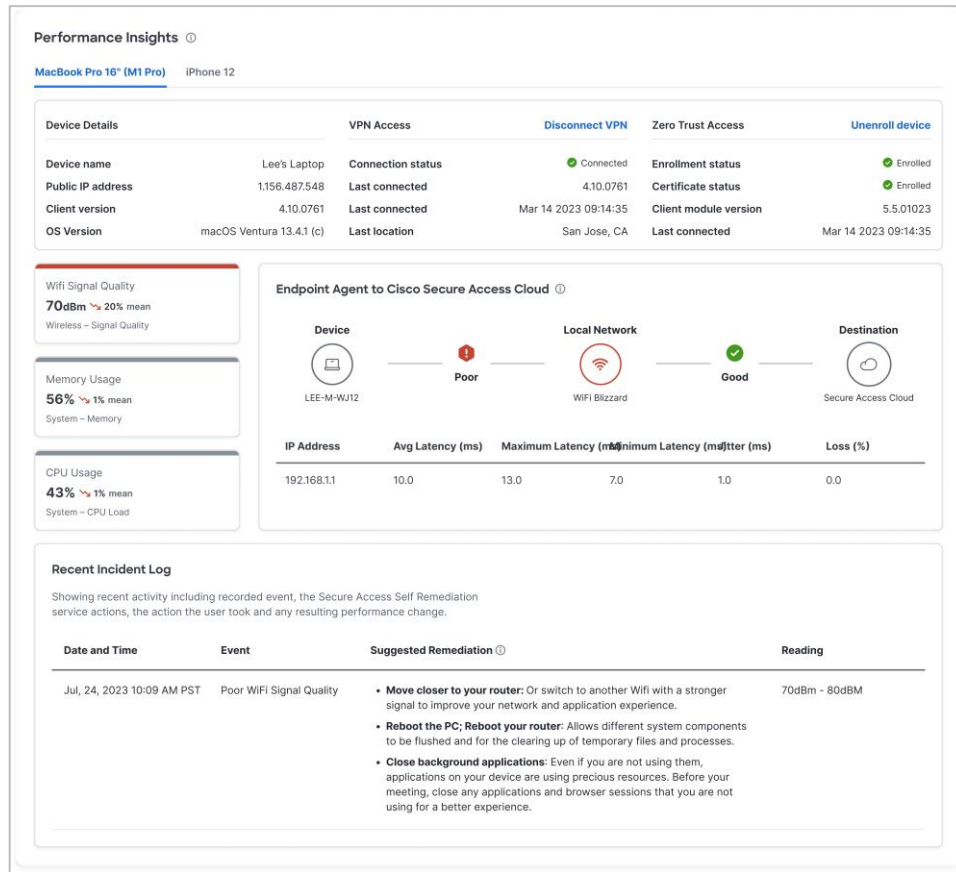
Monitor user digital experience without separate agents or management portals



- Global visibility of registered endpoint status
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent(EPA) as a module in Cisco Secure Client

Cisco Secure Access

Make it easier to operate



Monitor the health and performance of users, applications, and network connectivity.

Optimize user productivity by automatically mining details on the user's end-to-end experience, enabling the IT/security staff to rapidly resolve the issue.

DEM monitoring examples:

- Endpoint performance – CPU, memory, Wifi
- Network performance – endpoint to Secure Access
- Top 20 SaaS applications performance
- User specific events

Secure Access: SSE that truly understands AI

- Powered by AI Defense models to *understand intent*

Intelligent Protection

- Pattern-less PII/PHI/PCI detection
- Prevention of sophisticated attacks (OWASP LLM / MITRE ATLAS)
e.g., prompt injection
- Intent-based toxicity detection

Zero-Friction Security

- Built into Secure Access*
- Single unified policy framework
- No additional infrastructure

287 Total Events Viewing activity from Jan 8, 2025 at 3:30 PM to Feb 7, 2025 at 3:30 PM

Event Type	Severity	Identity	Direction	Destination	Rule	Action	Detected	Detected
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:15 AM	Feb 5, 2025 at 1:15 AM
AI Guardrails	Critical	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM	Action
AI Guardrails	Critical	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM	Monitored
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM	File Name
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM	Form
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	Identity
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	Application
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	OpenAI ChatGPT
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM	Application Category
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:57 AM	Generative AI
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:57 AM	
Real Time	Critical	52.12.127.197	Upload	Mozilla Firefox	Raja_test_rule	Monitored	Feb 5, 2025 at 12:57 AM	
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:56 PM	
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:54 PM	
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM	
AI Guardrails	High	Raymond Wei (raywei@cisc...)	Prompt	OpenAI ChatGPT	AI Demo	Blocked	Feb 4, 2025 at 10:49 PM	
AI Guardrails	High	Raymond Wei (raywei@cisc...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM	
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:46 PM	

Classification

Privacy guardrail

1 Match Privacy

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the \$1.2M deal with ACME Company.

Classification

Safety guardrail

1 Match Toxicity

how to make a bomb

1200+ AI Applications Coverage 100% Top 16 AI Apps Coverage 1 Unified Security Framework

Easy migration to Zero Trust Access

- ✓ You set the pace of ZTNA adoption
- ✓ Same client
- ✓ Common policy



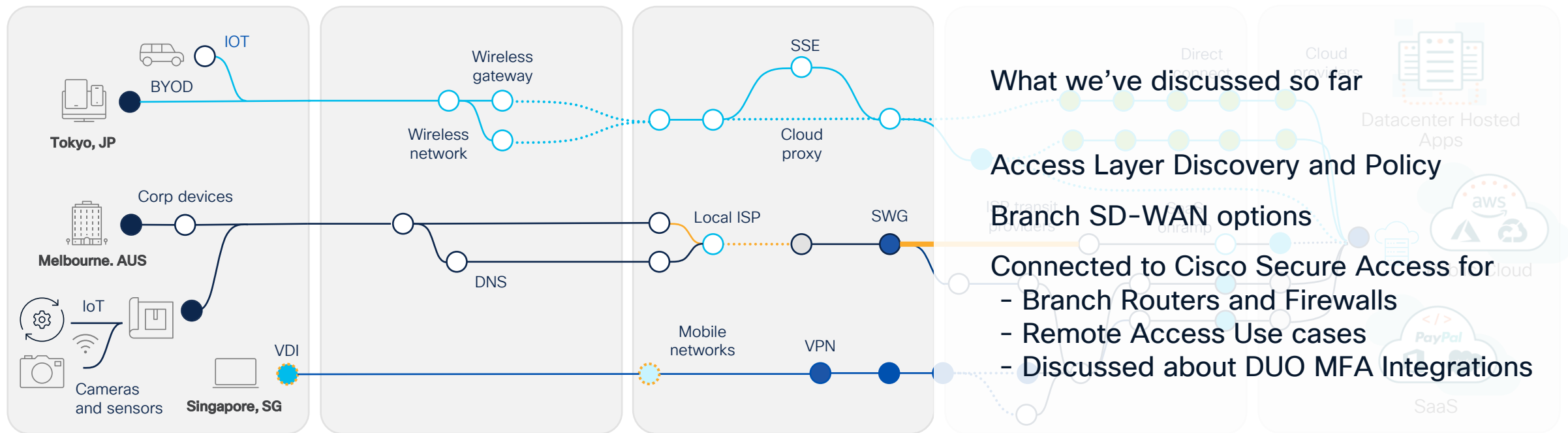
Traditional VPN
Network level access –
cannot control at app level



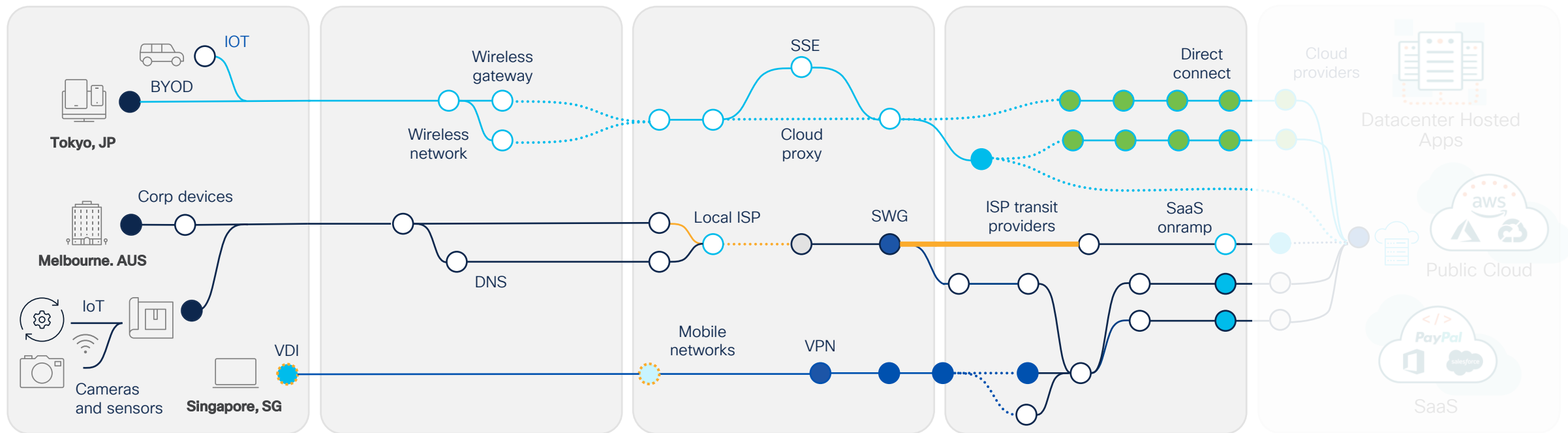
VPN as-a-Service
Lift your VPN to the cloud –
more control and easier to
manage



Unified ZTNA
Granular controls at the
application level + VPNaaS and
Digital Experience Monitoring



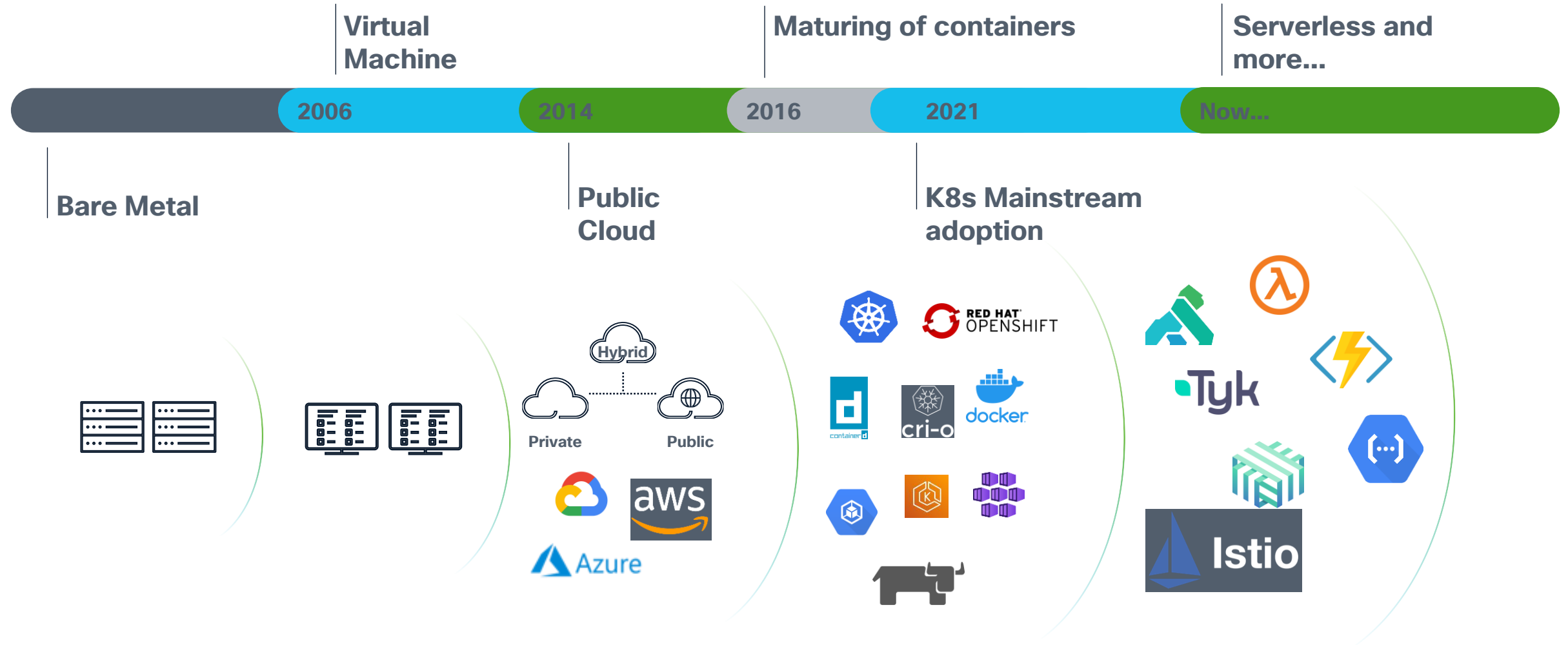
Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads & Cloud
<p>Visibility, Identification, Segmentation</p> <p>Device Profiling</p> <p>Identity Authorization</p> <p>Segmentation</p> <p>Access Control Policies</p>	<p>Policy Enforcement & Service Availability</p> <p>Context Sharing</p> <p>Segmentation</p> <p>Access Control Policies</p> <p>Software Defined WAN</p> <p>Cloud (SSE) Integrations</p>	<p>Access Control & Intrusion Prevention</p> <p>Policy Enforcement</p> <p>Service Visibility</p> <p>Traffic Monitoring</p> <p>Breach Prevention</p>	<p>Access Control & Intrusion Prevention</p> <p>DC Edge Access</p> <p>Traffic Visibility</p> <p>Breach Prevention</p>	<p>Workload and App Protection</p> <p>Segmentation</p> <p>Workload baseline</p> <p>SBOM and Inventory</p> <p>Microservice Protection</p>



Access Layer	Branch/Campus Edge	Cloud AND Remote	DC Edge	Workloads & Cloud
<p>Visibility, Identification, Segmentation</p> <p>Device Profiling</p> <p>Identity Authorization</p> <p>Segmentation</p> <p>Access Control Policies</p>	<p>Policy Enforcement & Service Availability</p> <p>Context Sharing</p> <p>Segmentation</p> <p>Access Control Policies</p> <p>Software Defined WAN</p> <p>Cloud (SSE) Integrations</p>	<p>Access Control & Intrusion Prevention</p> <p>Policy Enforcement</p> <p>Service Visibility</p> <p>Traffic Monitoring</p> <p>Breach Prevention</p>	<p>Access Control & Intrusion Prevention</p> <p>DC Edge Access</p> <p>Traffic Visibility</p> <p>Breach Prevention</p>	<p>Workload and App Protection</p> <p>Segmentation</p> <p>Workload baseline</p> <p>SBOM and Inventory</p> <p>Microservice Protection</p>

Data Centers and Applications are evolving

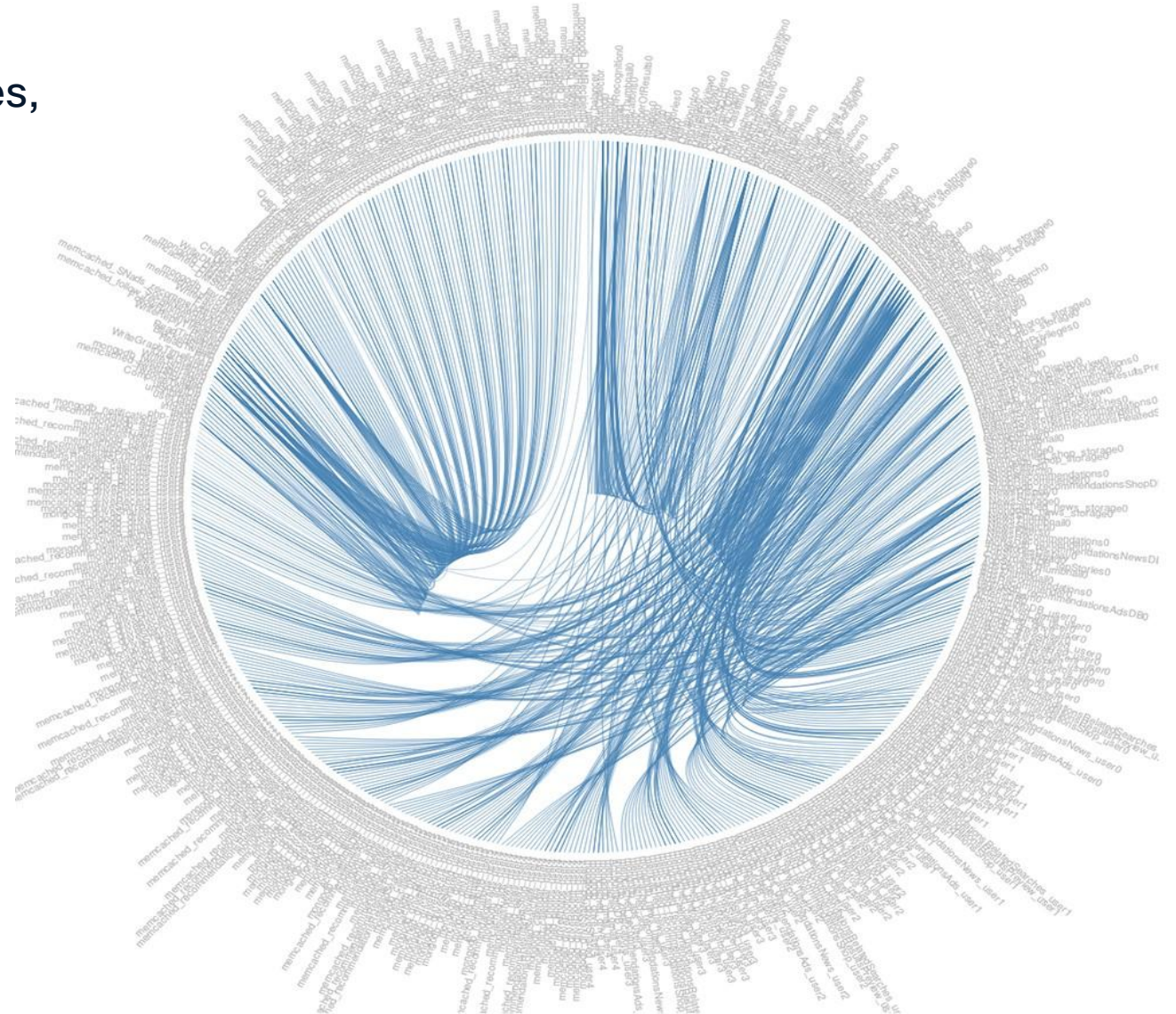
Workload Security is Getting More Complex



The reality of modern applications

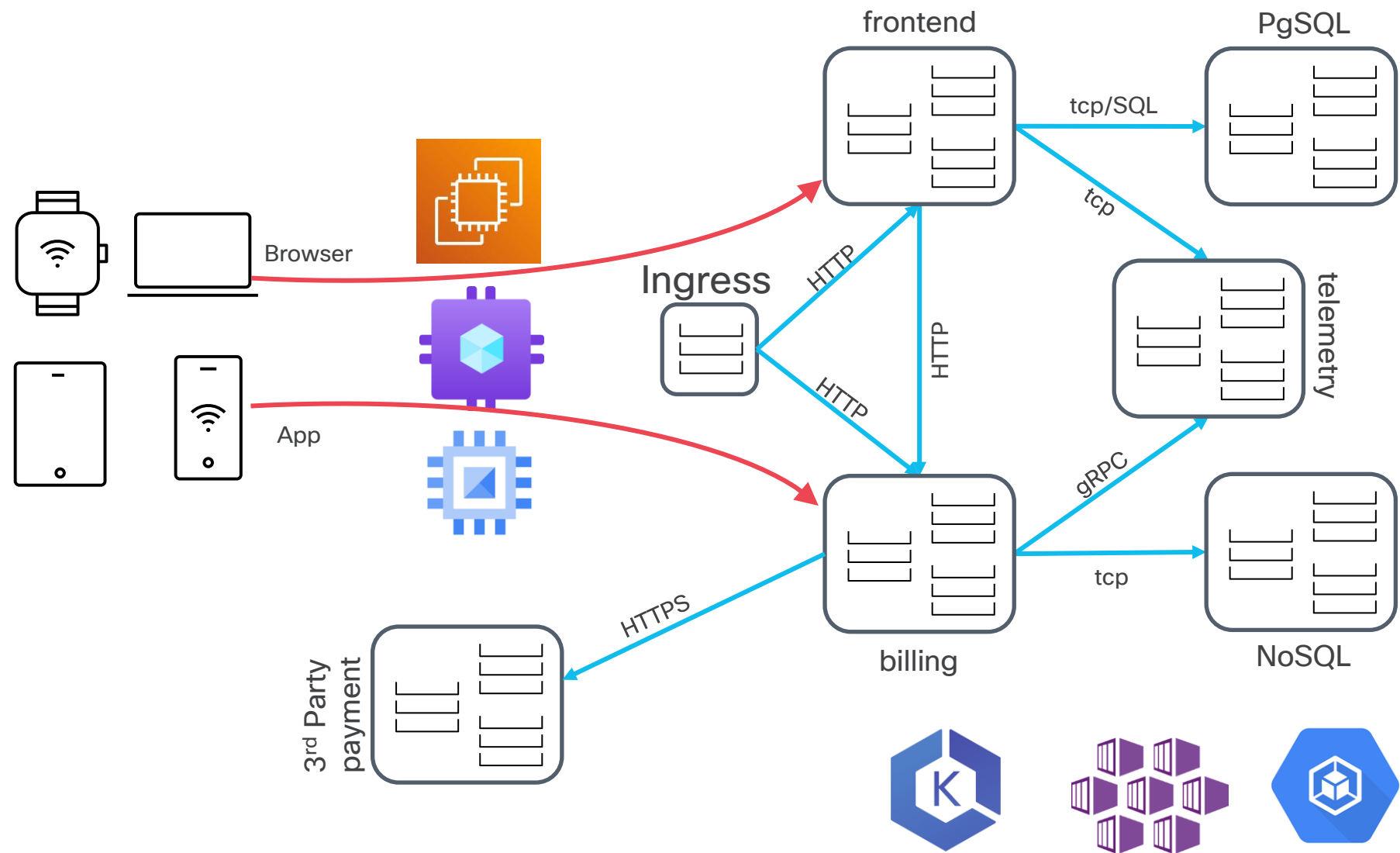
Deployed in Multi-cloud using Microservices, Serverless functions and APIs

- Decoupled
- Dynamic
- Scalable



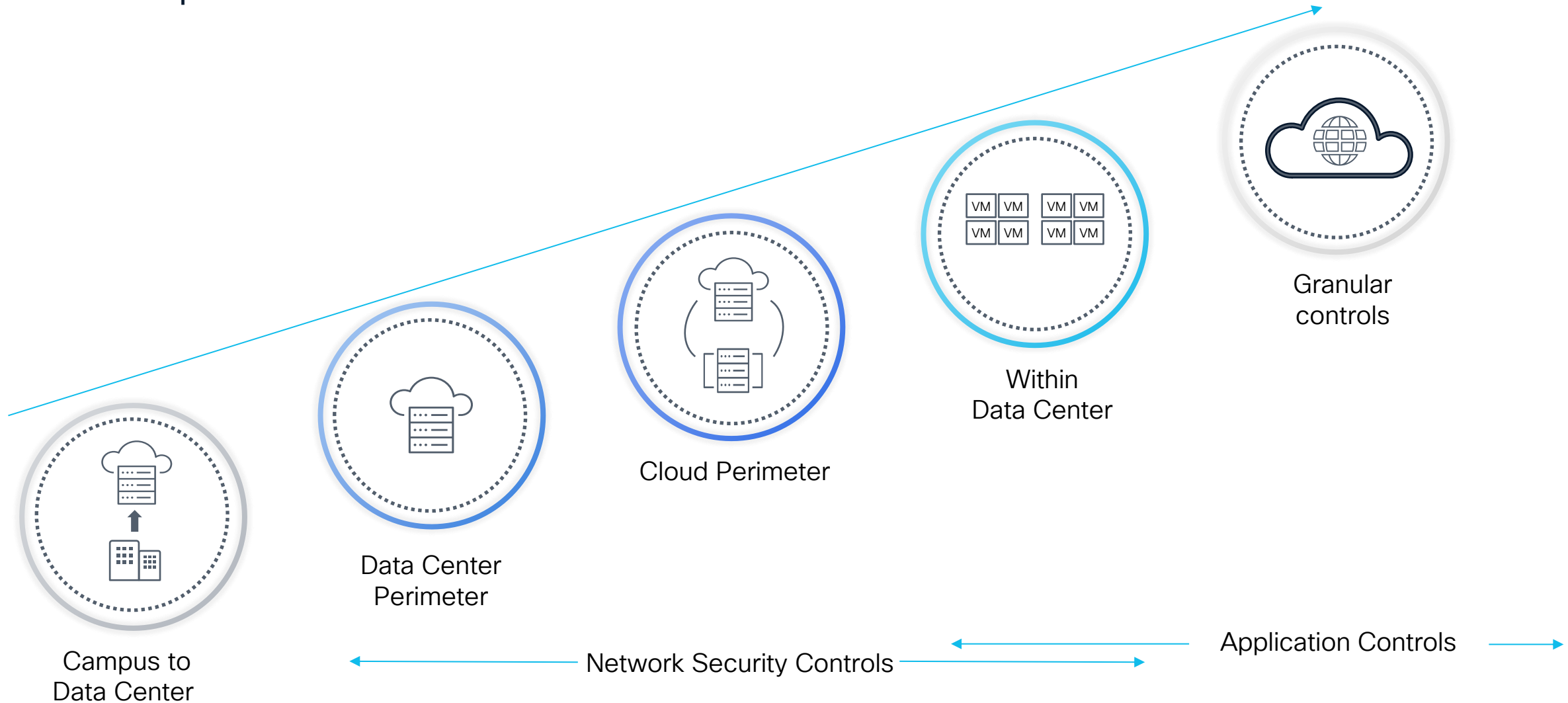
Simple Modern Application

- Micro-services
- Containers and K8s
- Cloud-native services
- Serverless
- API
- Infrastructure as Code
- Orchestration and Automation



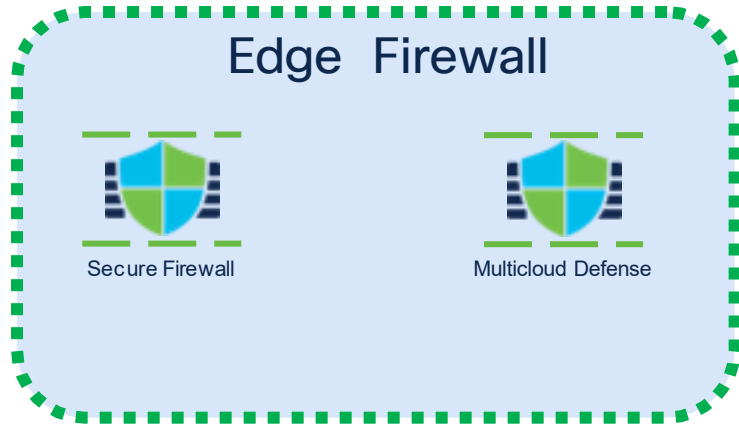
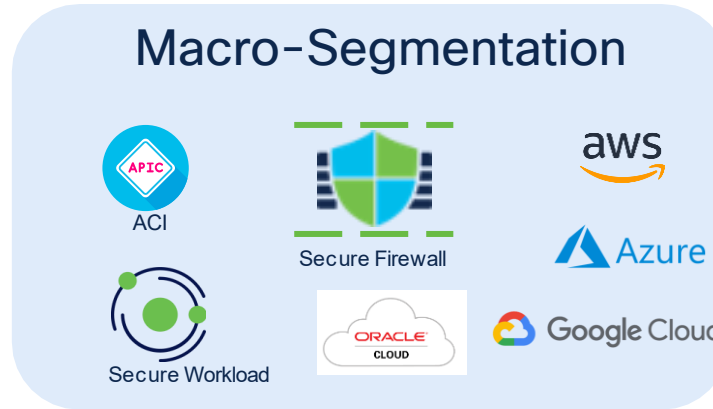
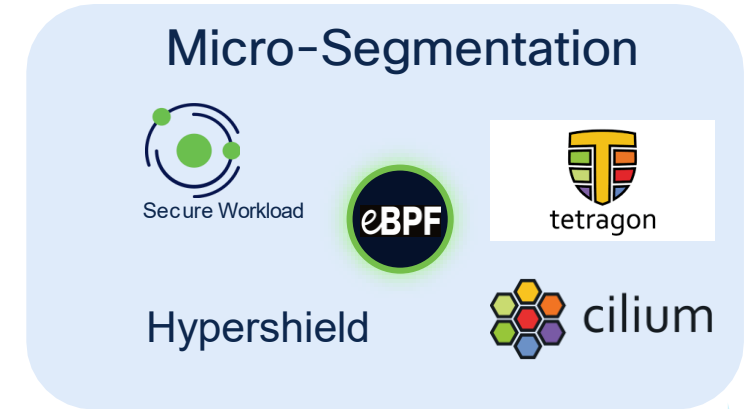
Layers of Defence

New threats require new controls



Layers of Defence

For Robust Security Controls



Application Security Journey

Perimeter Defense

- Robust Ingress & Egress Policy Controls
- Next-Generation Threat Detection and Protection
- Threat Intelligence and Visibility

Zones and Segmentation

- Segment zones within your data center and cloud.
- Context and identity-aware segmentation
- Fabric Security Controls
- Agent-based and Agentless

Granular Application Controls

- Micro-segmentation that creates dynamic, application-centric micro-perimeters
- AI Driven Security controls to enforce least privilege access and prevent lateral threat movement
- Granular surgical controls

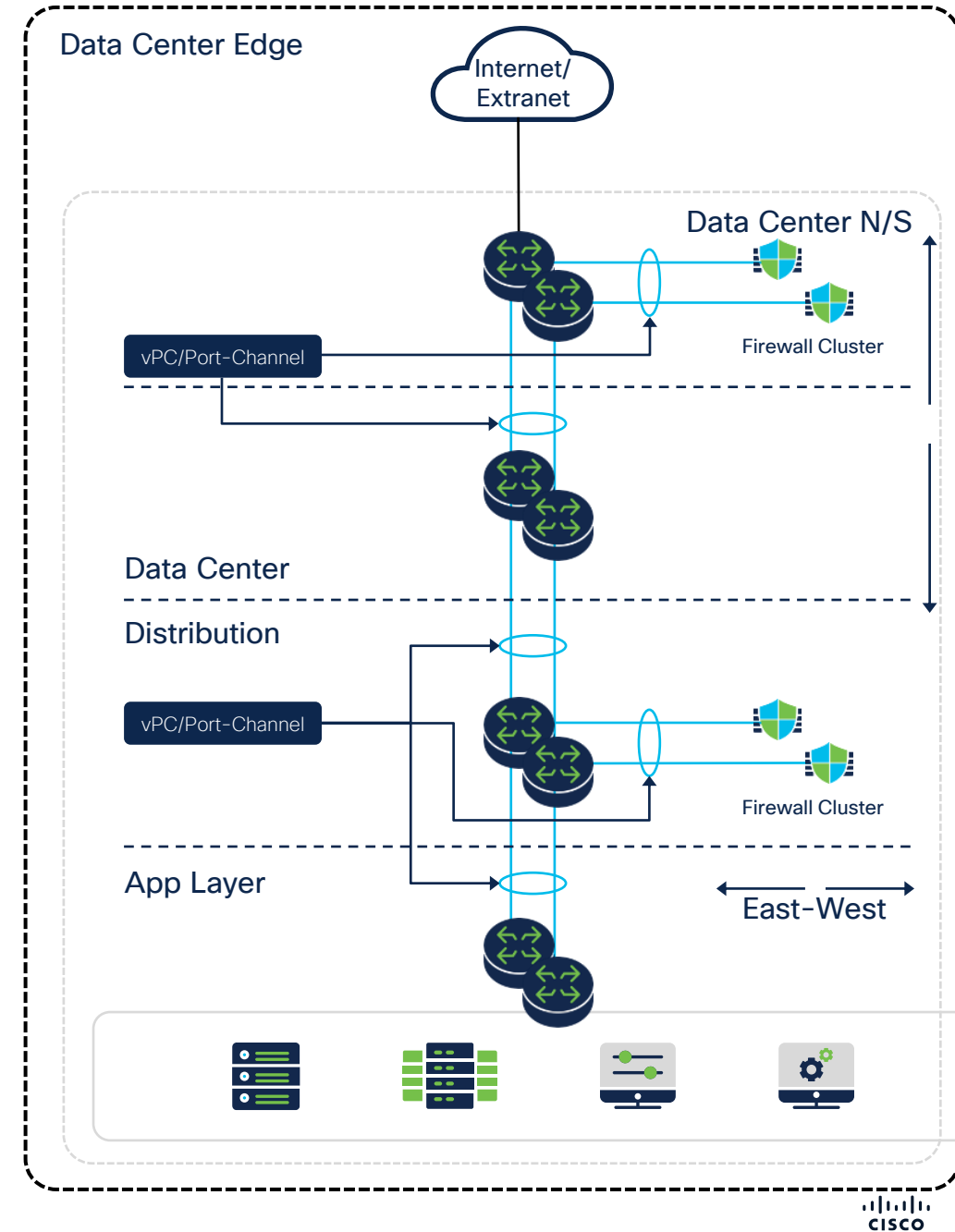
Data Centre Perimeter

Key Functions

- Access Policy Controls (North-South and East-West)
- Advanced Threat Detection and Controls
- Low Latency Capabilities
- Scalability and Resilience

Cisco Secure Firewall

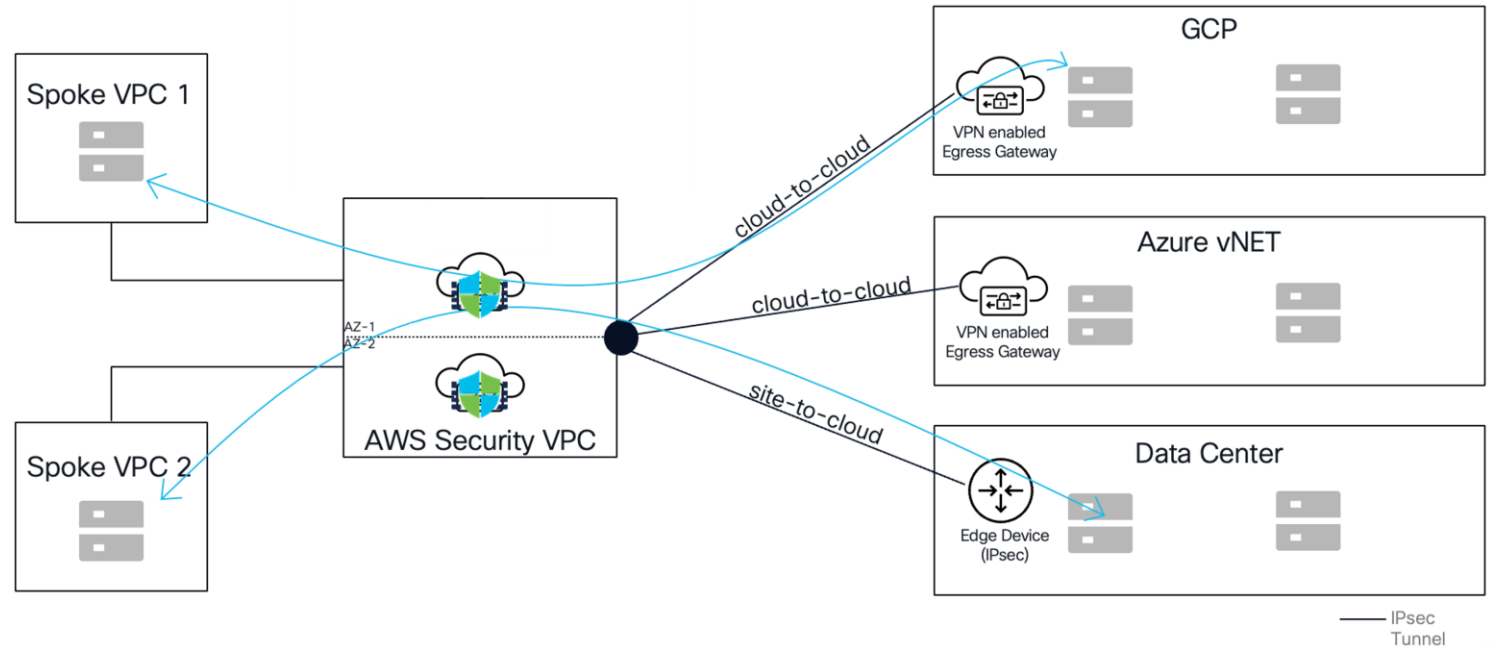
- Zone segmentation, Identity aware intent-based controls, TrustSec Policy using SGTs, ACI Policy Control with EPGs
- Snort and SnortML IPS, Malware Protection, Encrypted Visibility Engine
- Block access to malicious IP's, URL's, DNS, Blacklisted sources using Talos Threat Intelligence
- Hardware Flow Offload
- High Availability, Multi-instance, Intra-site and Inter-site Clustering



Cloud Perimeter

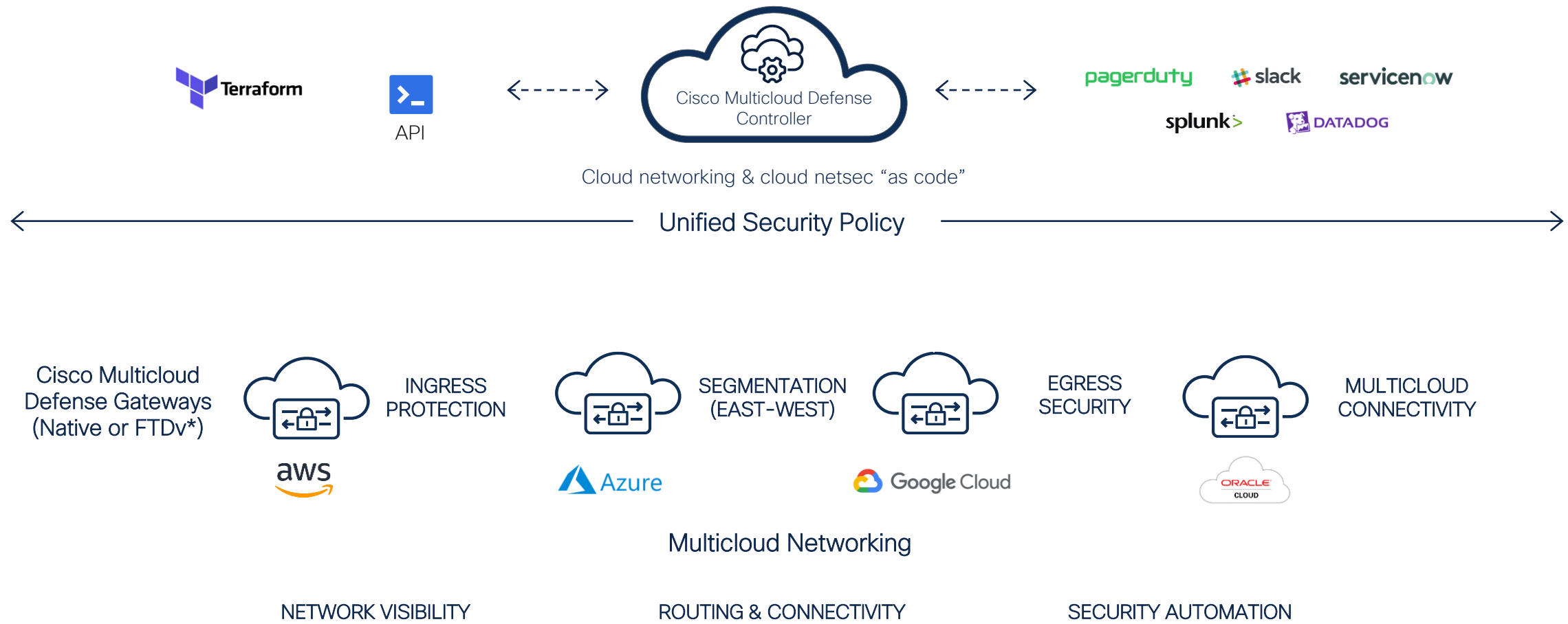
Key Functions

- Policy Controls (North-South and East-West)
- Advanced Threat Detection and Controls
- Virtual Firewalls
- Multicloud Networking
- Automation
- Simplified operations



Cisco Multicloud Defense

Multi-cloud networking, automation, and cloud-native network security controls



Cloud infrastructure is different

What do we need to
configure?

Security VPCs

VPC and DNS Flow Log capture

Network Load Balancer

Gateway Load Balancers

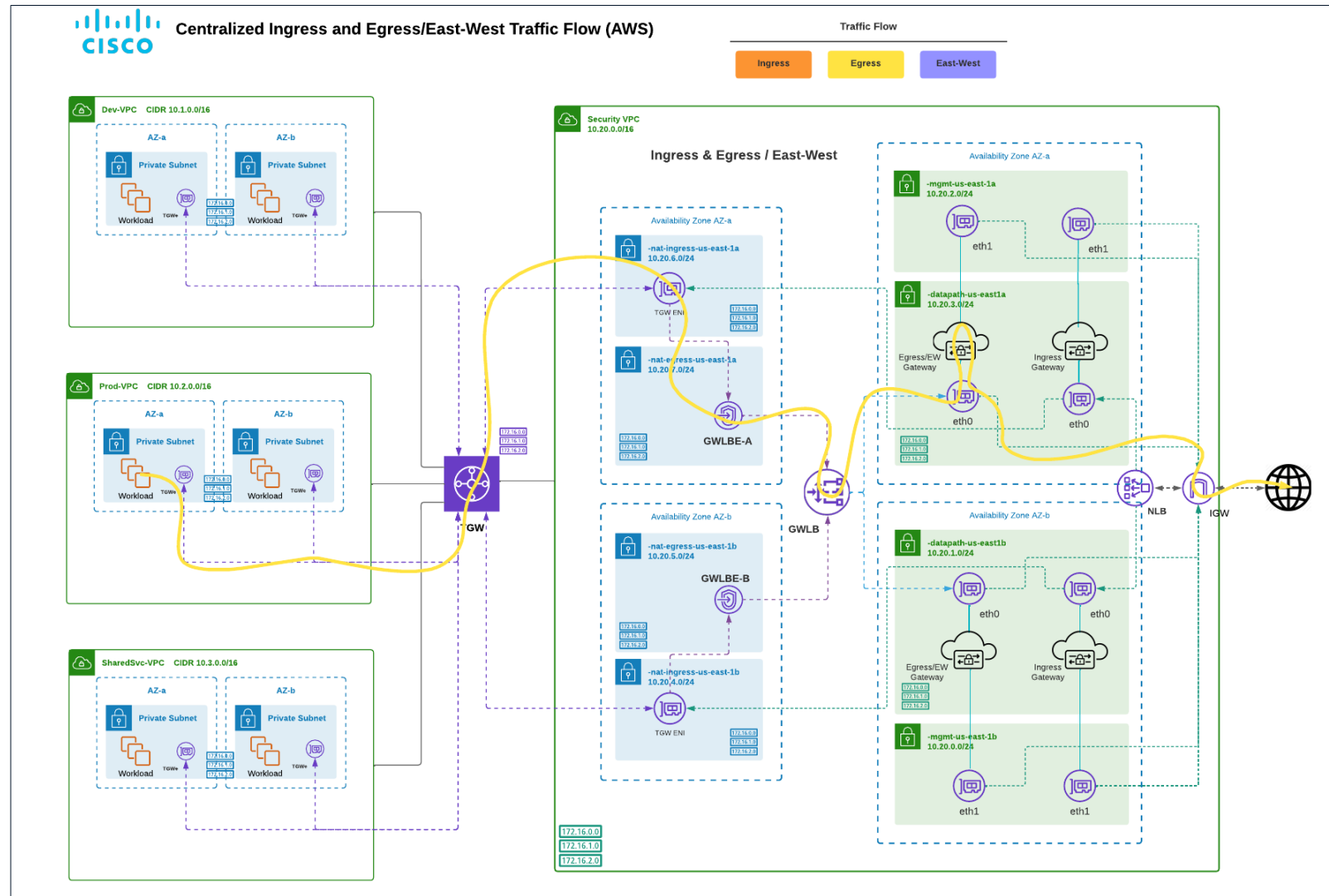
Gateway Firewall

(Deployment, Insertion, Autoscaling)

AWS Transit Gateways

(New or existing, TGW attachment)

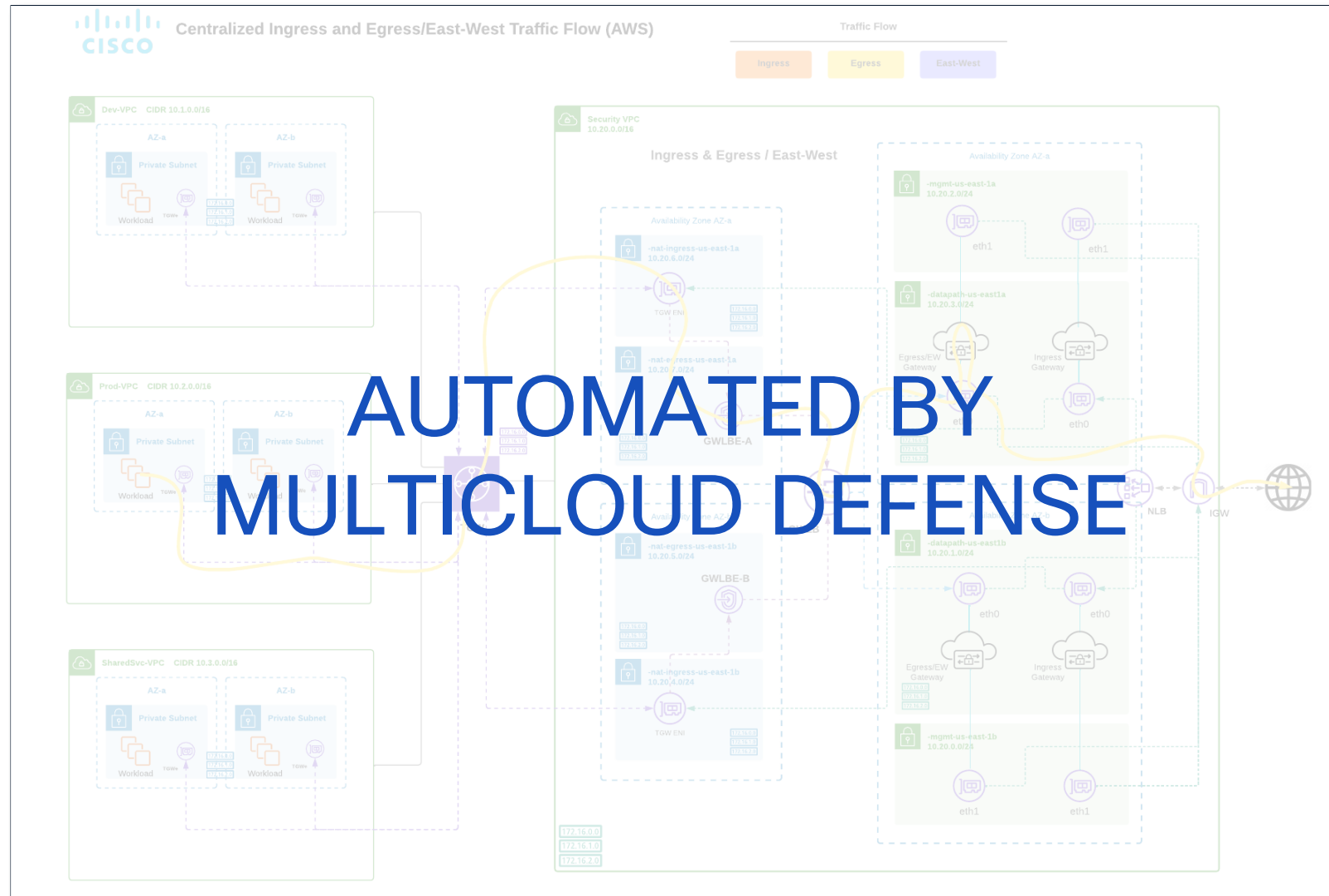
VPC subnet routing to TGW



Simplified operations with Cisco Multicloud Defense

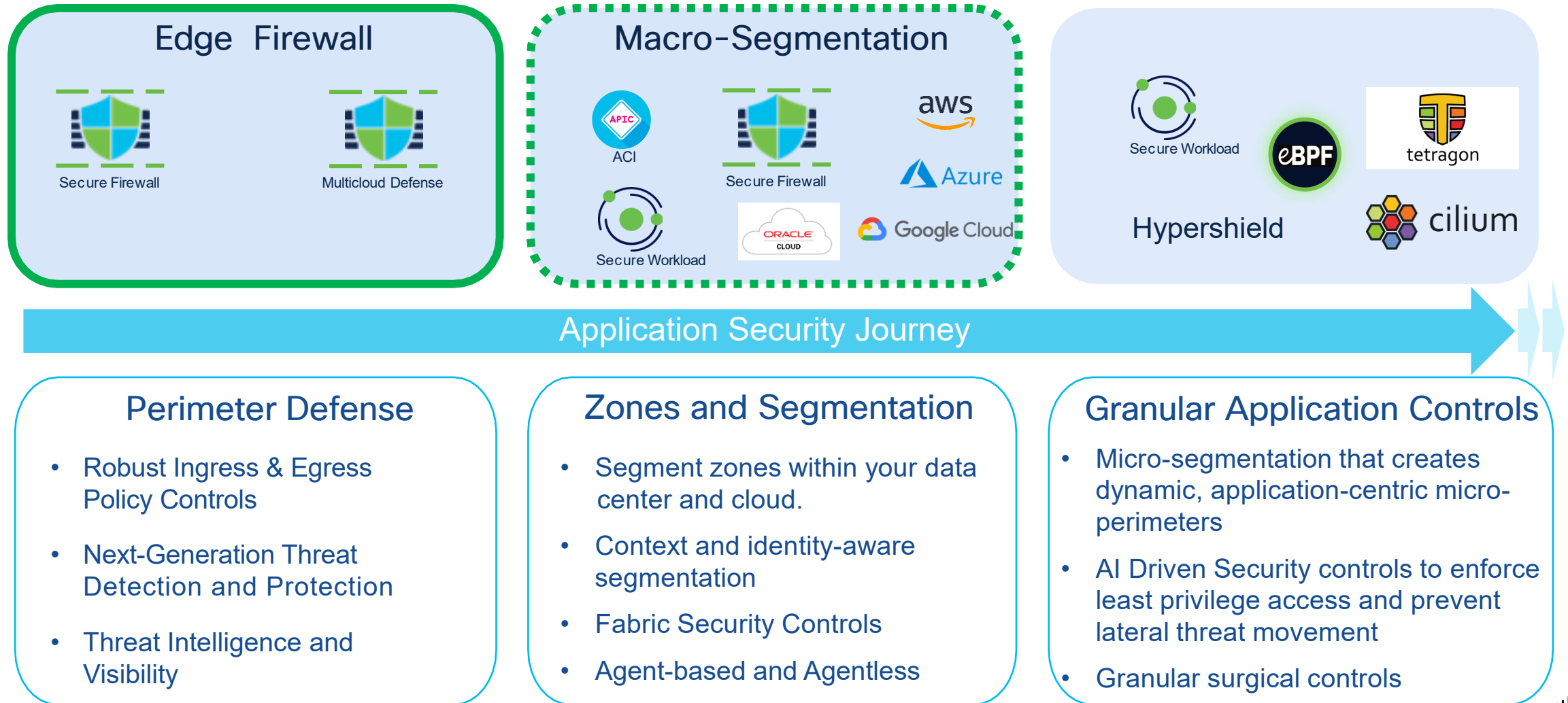
What do we need to
configure?

**AUTOMATED
BY
MULTICLOUD
DEFENSE**



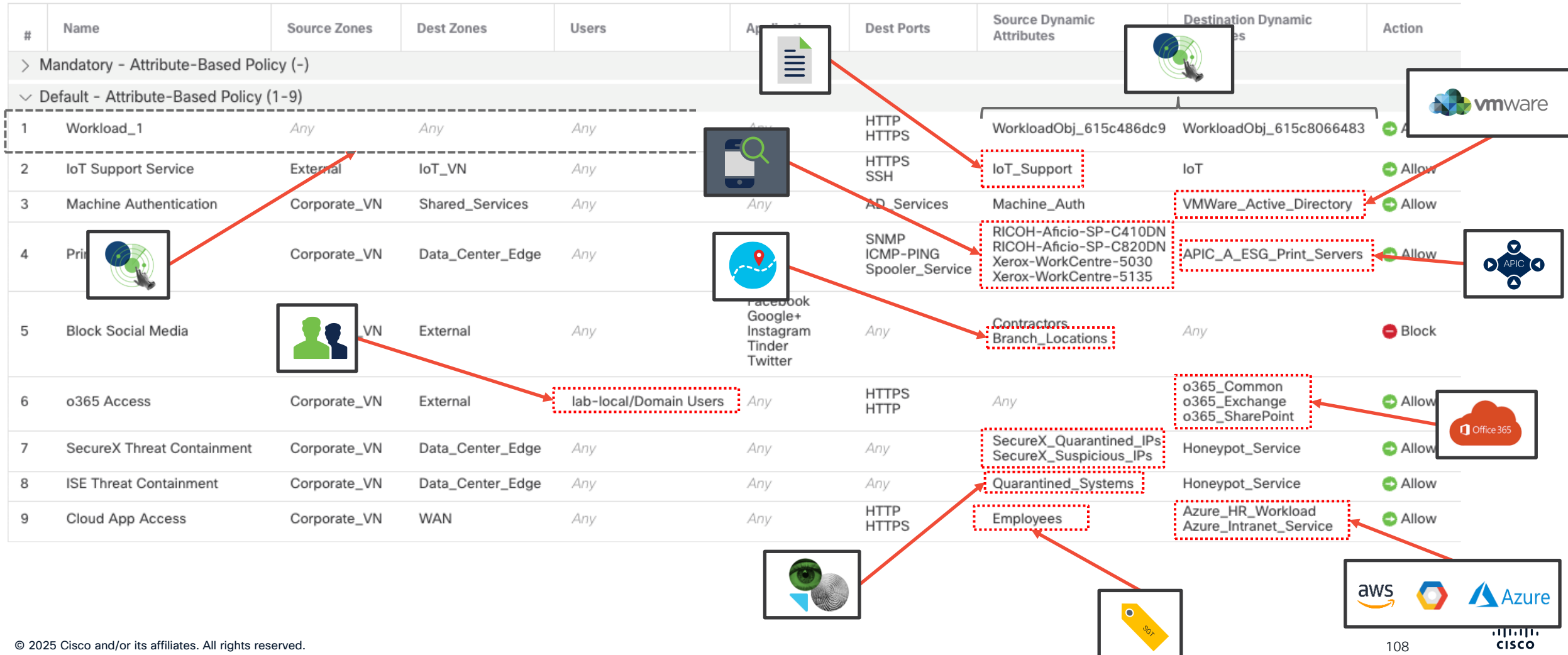
Layers of Defence

Going beyond Perimeter Defense



Intent based Access Controls

Access Control should adapt when identity and context changes



Cisco Secure Dynamic Attribute Connector

Keep security policies up to date in dynamic environment

Cloud Connectors



Azure



Azure Service
Tags



vCenter/
NSX-T



GCP



AWS

Public Feeds Connectors



O365



GitHub



Webex



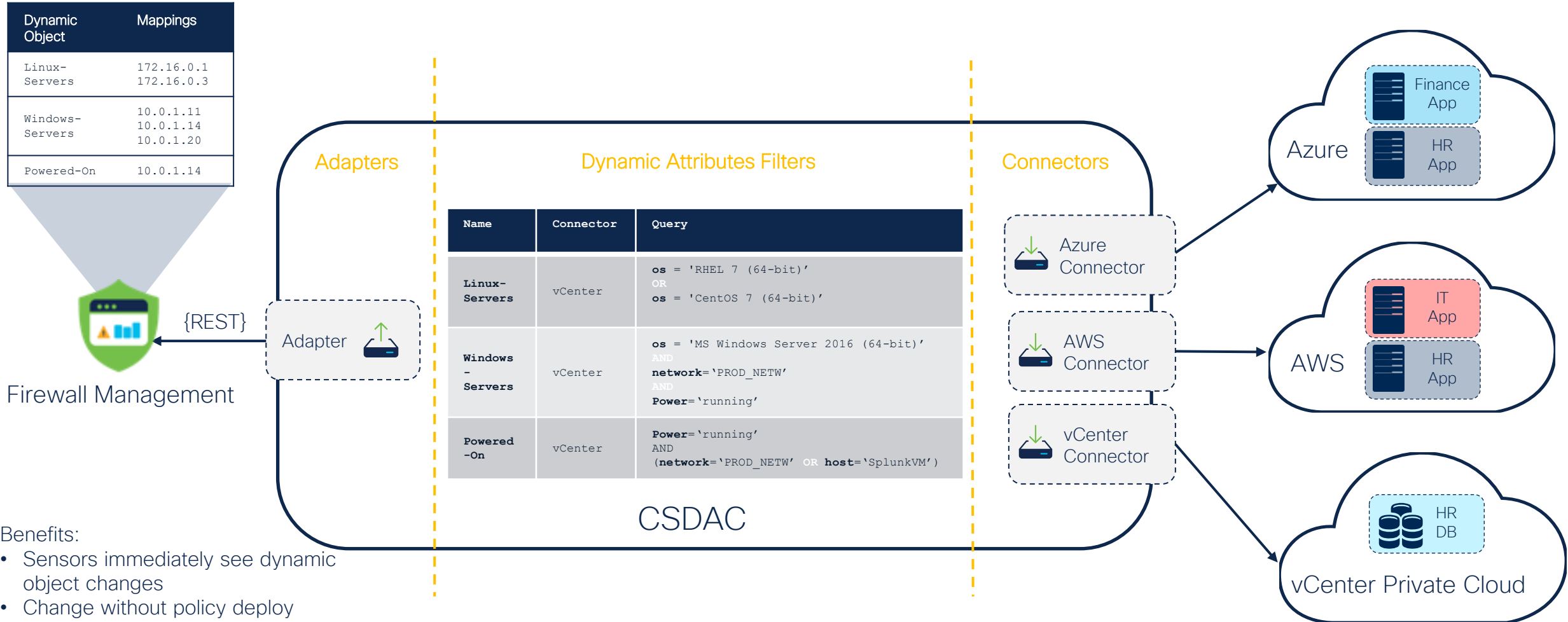
Zoom



Generic
TXT

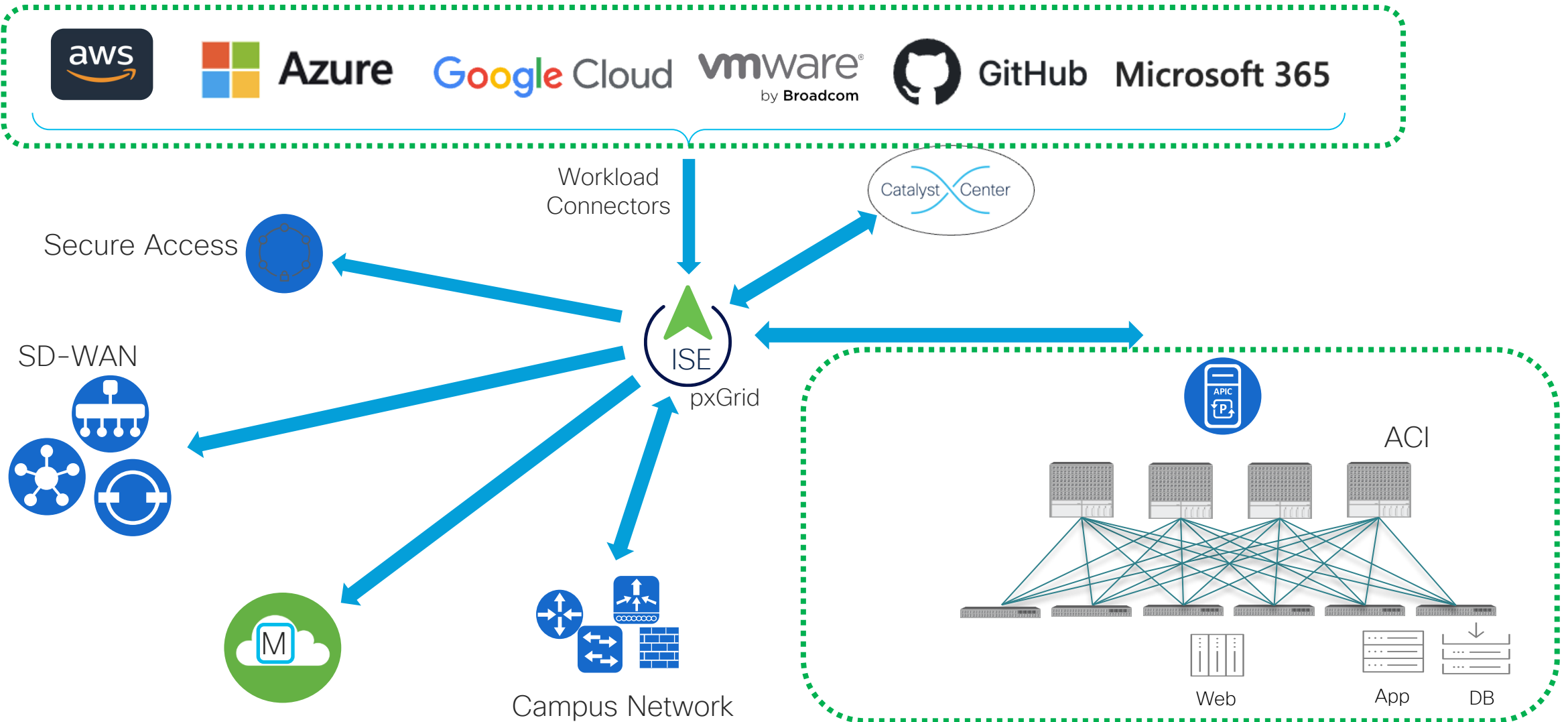
Cisco Secure Dynamic Attributes Connector

Use existing workload attributes to classify and normalize



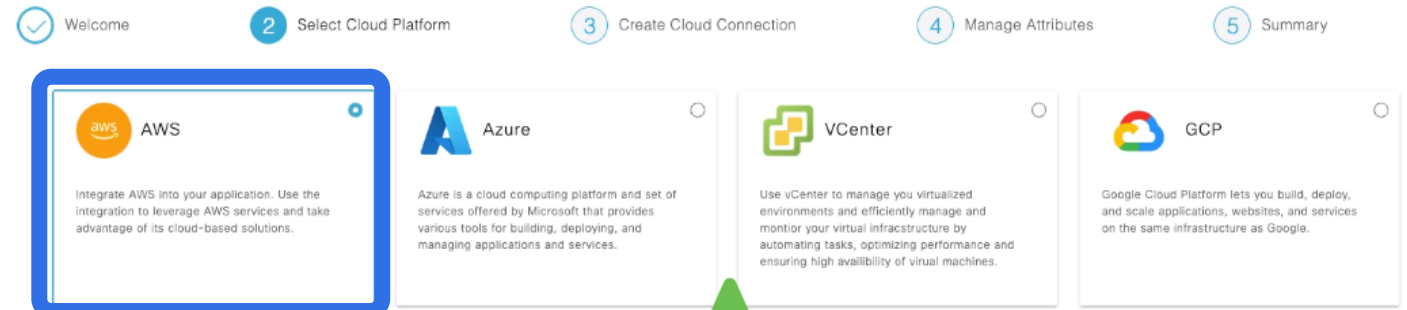
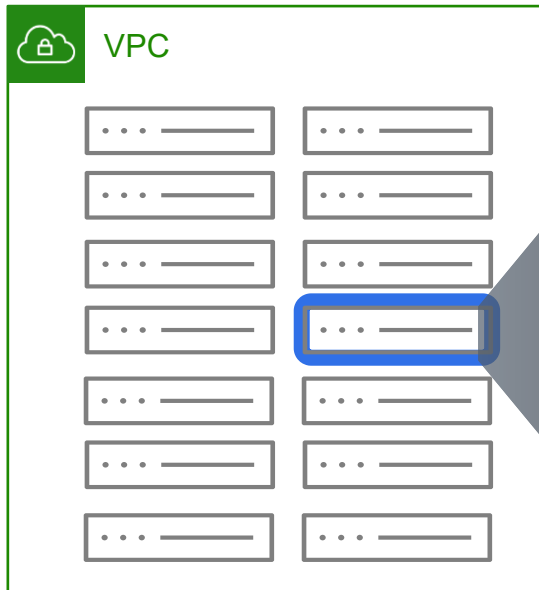
Classifying Workloads with Cisco ISE

Use existing workload attributes to classify and normalize



Classifying Workloads

Use existing workload attributes for classification



Workload Attributes

VPC

Created

State

Name

Application

Version

Owner

OS

IP

Service

Stage

...

ISE Dictionary

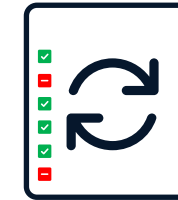
Name

Application

IP

Service

Stage



Classification Policy

ISE Workload Classification

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

AWS - Owner

Contains

Label
Joff

+ Add AND/OR Statement

+ Add Condition

AND

Source

Equals

APIC_from_ISE_P1

EPG

Equals

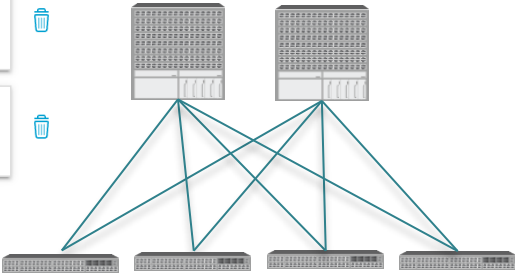
Demo-ClientEPG

+ Add AND/OR Statement

+ Add Condition

+ Add AND/OR Statement

+ Add Condition



Dynamic Parameters for Access Controls

Example: Cisco Firewall - Controls change dynamically when identity changes

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
v Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	➔ Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	➔ Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	➔ Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	➔ Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	🚫 Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	➔ Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	➔ Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	➔ Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	➔ Allow

Fabric Security Controls

Example: Dynamic Segmentation using Nexus Dashboard

Automated configuration process

Define your micro-segmentation policies from a single pane

Intuitive and dynamic

Create security groups with a few clicks to define all necessary policies and matching attributes.

Security Matrix

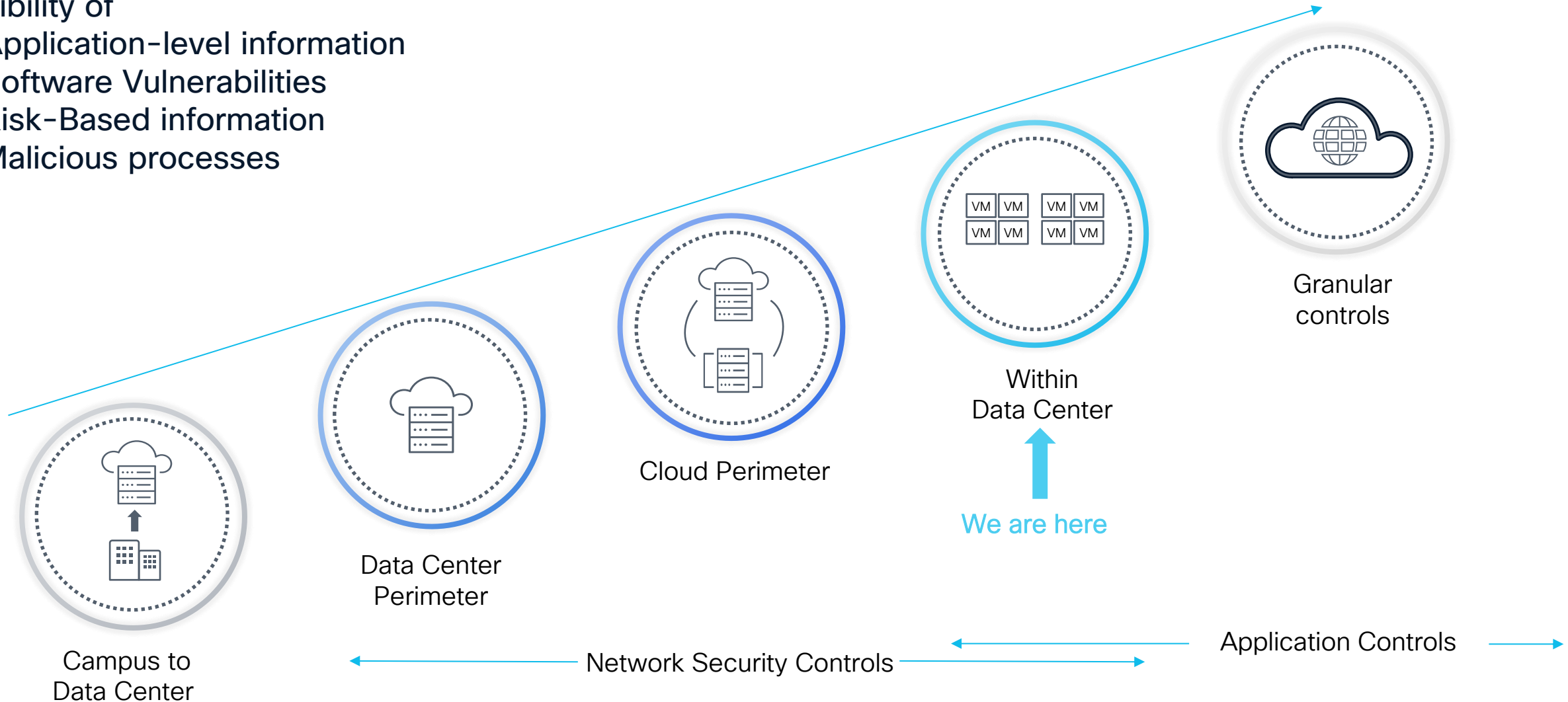
Visualize all your groups and contracts and get further details with ease



Beyond network-layer visibility and controls

Visibility of

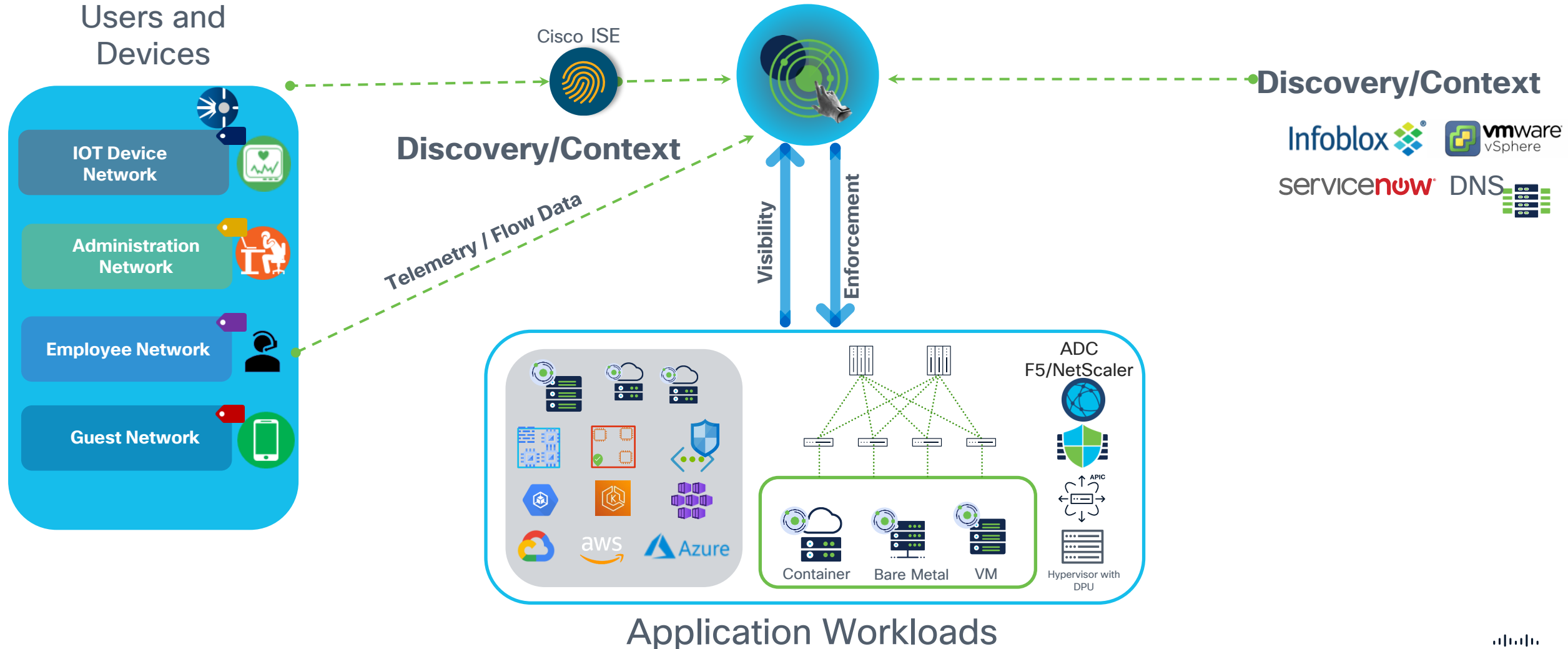
- Application-level information
- Software Vulnerabilities
- Risk-Based information
- Malicious processes



Beyond network-layer visibility and controls

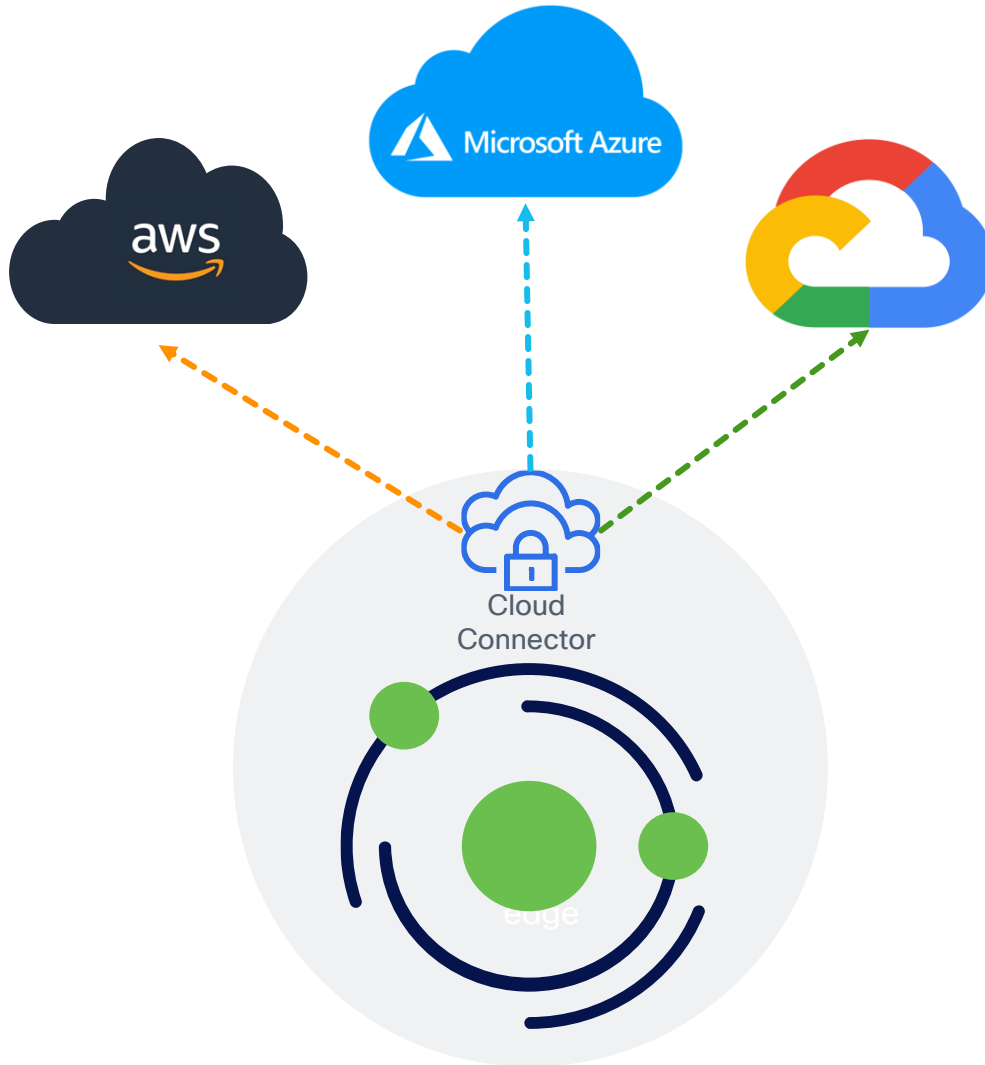
Cisco Secure Workload: Agentless or Agent-based deployment

Cisco Secure Workload



Cloud Workloads

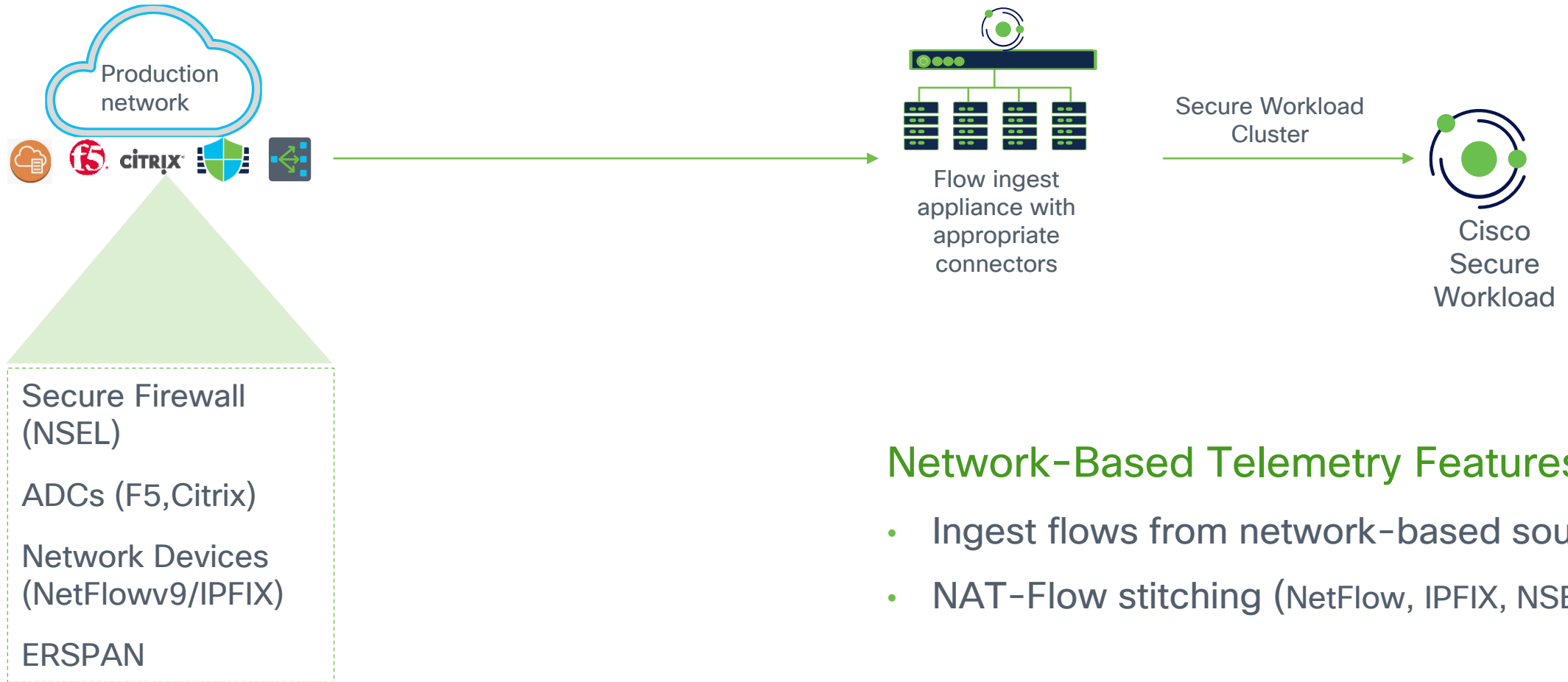
Agentless



- Centralized cloud-onboarding experience
 - Cloud connectors
 - Single point of management
- Visibility
 - Near real-time discovery of workloads and labels
 - Flow telemetry via VPC/VNets flow-logs
- Enforcement
 - Security Groups (AWS)
 - Network Security Groups (Azure)
 - Firewall (GCP)

Workload visibility at the network level

Agentless



Network-Based Telemetry Features

- Ingest flows from network-based sources
- NAT-Flow stitching (NetFlow, IPFIX, NSEL)

Host Agent

Windows servers
(Virtual machines and bare metal)



Windows desktop
(VDI and Workstation)



Linux servers (x86)
(virtual machine and bare metal)



IBM zSystems
(z/Linux operating system)



IBM PowerPC and pSeries systems
(AIX operating system)



Oracle SPARC 

Container host
(Linux container host OS with DaemonSet)



Application Flow Observability

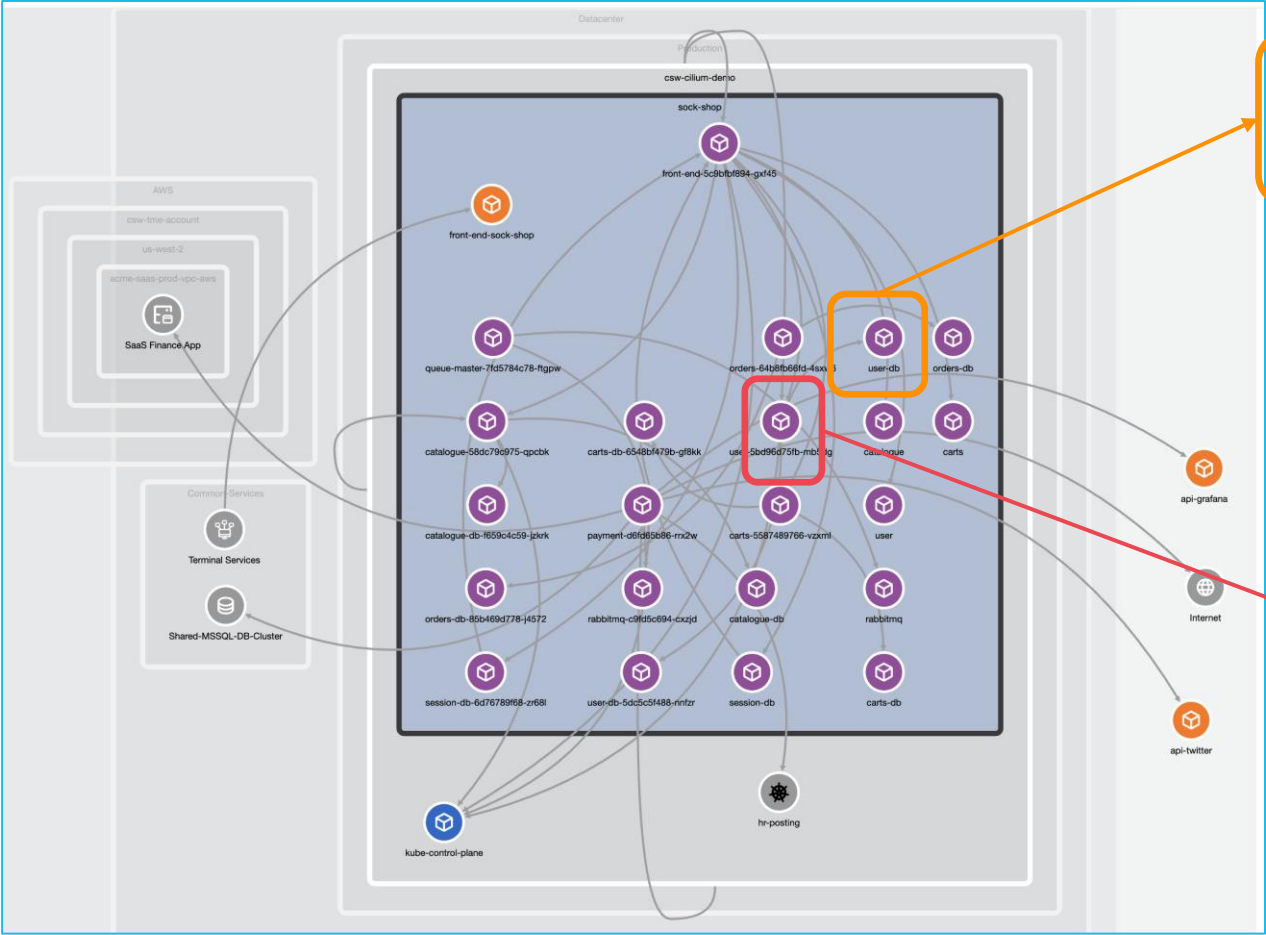
- Process Flow Details from Workloads
- Flow-level information
 - 5-tuple flow information
 - Flags, Bytes, Packet Count, SRTT
 - TLS/SSH and DNS/FQDN information
 - Malicious destinations
- Application-level information
 - Process Details
 - User Information



Aug 13 03:32:00 am (CEST)		
	Consumer ⓘ	Provider ⓘ
Flags	PSH ACK	PSH ACK
ICMP Type and Code		
Byte Count	68,616 (1,038,747,838 so far)	60,960 (1,030,287,456 so far)
Packet Count	544 (7,855,211 so far)	428 (7,727,024 so far)
SRTT	10.3ms	
Process	/usr/sbin/mysqld --wsrep_start_position=2afd6776-ce1d-11ec-9166-6af94ddd0dd5:769	/usr/sbin/mysqld --wsrep_start_position=2afd6776-ce1d-11ec-9166-6af94ddd0dd5:696
User	mysql	mysql
Drop Reason	N/A	N/A

Granular Application Visibility

End to End Application Discovery



Cluster

user-db

Full cluster details

Name

user-db

Description

The cluster was formed from the following sources: Service name: user-db

Query (5 alternates)

`* orchestrator_system/service_name = user-db and * orchestrator_system/namespace = sock-shop`

Neighbors 1

user-5bd96d75fb-mb5dg

Enter attributes...

Search Inventory

Services 1

Pods 0

Workloads 0

IP Addresses 0

1 of 1 Services

Service Type

Service Name

Scope Name

* orchestrator_applicati

ClusterIP

user-db

Production : csw-cilium-demo : sock-shop

... 5 more

Cluster

user-5bd96d75fb-mb5dg

Full cluster details

Name

user-5bd96d75fb-mb5dg

Description

The cluster was formed from the following sources: ReplicaSet name: user-5bd96d75fb

Query (5 alternates)

`( * orchestrator_name = user and * orchestrator_pod-template-hash = 5bd96d75fb ) and * orchestrator_system/namespace = sock-shop`

Neighbors 3

front-end-5c9bfbf894-gx45

user-db

user-db-5dc5c5f488-nmfzr

Enter attributes...

Search Inventory

Services 0

Pods 1

Workloads 0

IP Addresses 0

1 of 1 Pods

Pod Name

Address

Scope Name

* orchestrator_applic

user-5bd96d75fb-mb5dg

10.0.1.243

Production : csw-cilium-demo : sock-shop

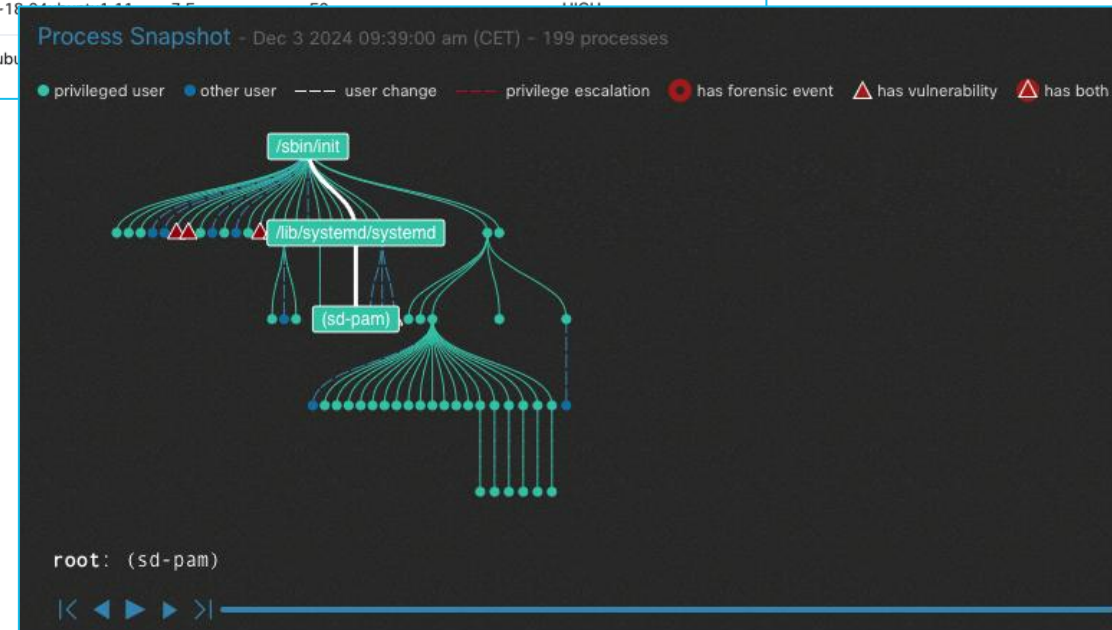
... 5 more

Workload Runtime Observability

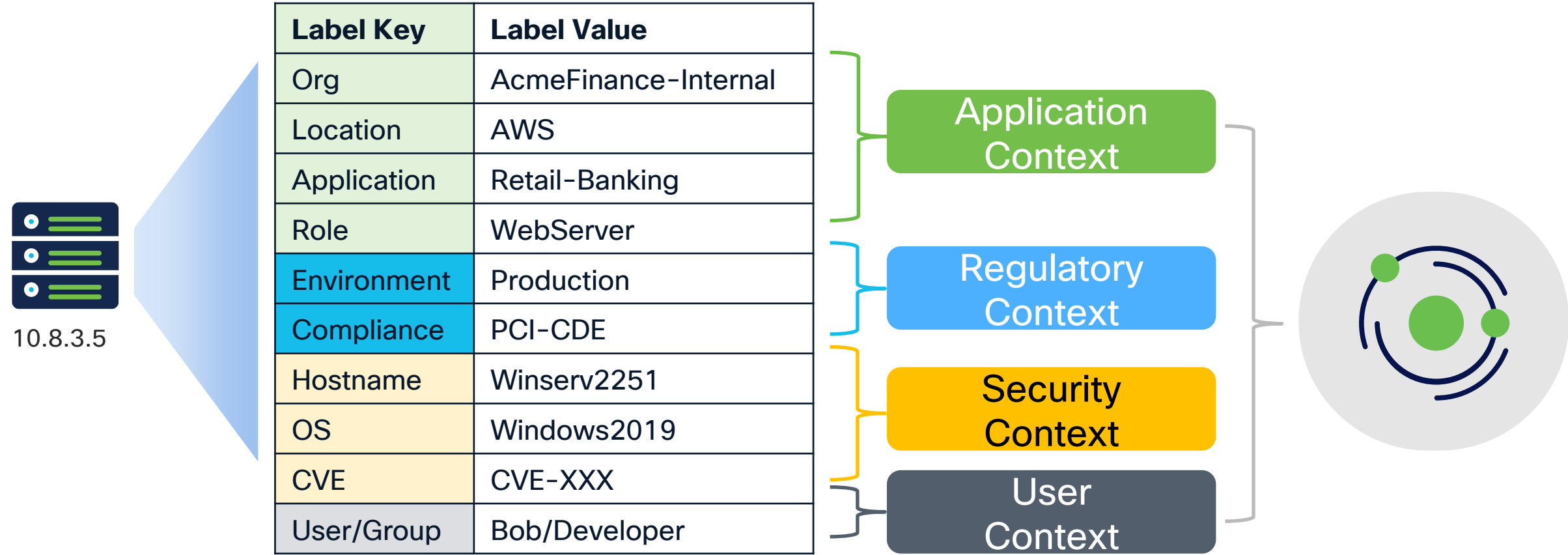
In-Depth Visibility of Workload Estate

- Processes information
- Resource consumption
- Malicious processes
- Software packages
- Vulnerabilities
- Risk-Based information
- Process-tree and forensics

Vulnerabilities						
<input type="text" value="Enter attributes..."/> Filter						
Displaying 417 of 417						
▼	CVE ↓	Package Name ↑↓	Package Version ↑↓	Score (V3) ↑↓	Cisco Security Risk Score ↑↓	Base Severity (V3) ↑↓
	CVE-2024-7592	libpython2.7	2.7.17-1~18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	libpython2.7-minimal	2.7.17-1~18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	libpython2.7-stdlib	2.7.17-1~18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	python2.7	2.7.17-1~18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7592	python2.7-minimal	2.7.17-1~18.04ubuntu1.11	7.5	50	HIGH
	CVE-2024-7264	curl	7.58.0-2ubuntu1.1	7.5	50	HIGH



Workload Identity and Discovery with Context



Enforcing Granular Intent-Based Policy

Top-Down: Phased Enforcement

Workspaces

Datacenter-SJC14

PRIMARY

Version 0

View Version History

Matching Inventories

Policies

Filters

Conversations

Provided Services

Policy Analysis

Enforcement Status

Enforcement

Filter Policies ...

Absolute and Default Policies

Catch All

Grouped

Ungrouped

Action

Consumer

Provider

Protocols and Ports

DENY

PCI OOS Workloads

PCI CDE Workloads

TCP : Any

Ecommerce-Prod

PRIMARY

Version 0

View Version History

Policies

Filters

Conversations

Provided Services

Policy Analysis

Enforcement Status

Enforcement

Filter Policies ...

Default Policies

Catch All

Grouped

Ungrouped

Priority

Action

Consumer

Provider

Protocol

Port

100

ALLOW

... : Datacenter-SJC-14 : Production : eCommerce

AD-DNS

UDP

53 (DNS)

100

ALLOW

... : Datacenter-SJC-14 : Production : eCommerce

... : Datacenter-SJC-14 : Production : eCommerce

TCP

Any

100

ALLOW

... : Shared Services : Jumphosts

... : Datacenter-SJC-14 : Production : eCommerce

TCP

22 (SSH)

100

ALLOW

... : Shared Services : Jumphosts

100

ALLOW

Any

100

ALLOW

Any

Action

Consumer

Provider

Protocols and Ports

ALLOW

Any

... : Datacenter-SJC-14 : Production : eCommerce

TCP : 80 (HTTP) ...1 more

ALLOW

ecomm-app-tier

Root : Internet

TCP : 25 (SMTP) ...1 more

ALLOW

ecomm-app-tier

ecomm-redis-nfs

TCP : 2049 (NFS) ...1 more

ALLOW

ecomm-app-tier

ecomm-belb01

TCP : 3306 (MySQL)

ALLOW

ecomm-belb01

ecomm-sql

TCP : 3306 (MySQL)

ALLOW

ecomm-sql

ecomm-sql

TCP : 4567 ...1 more

ALLOW

... : Datacenter-SJC-14 : Production : eCommerce

AD-DNS

UDP : 53 (DNS)

ALLOW

... : Shared Services : Jumphosts

... : Datacenter-SJC-14 : Production : eCommerce

TCP : 22 (SSH) ...1 more

Datacenter Level (Phase-1)

Ringfence (Phase-2)

Granular Micro-segmentation (Phase-3)

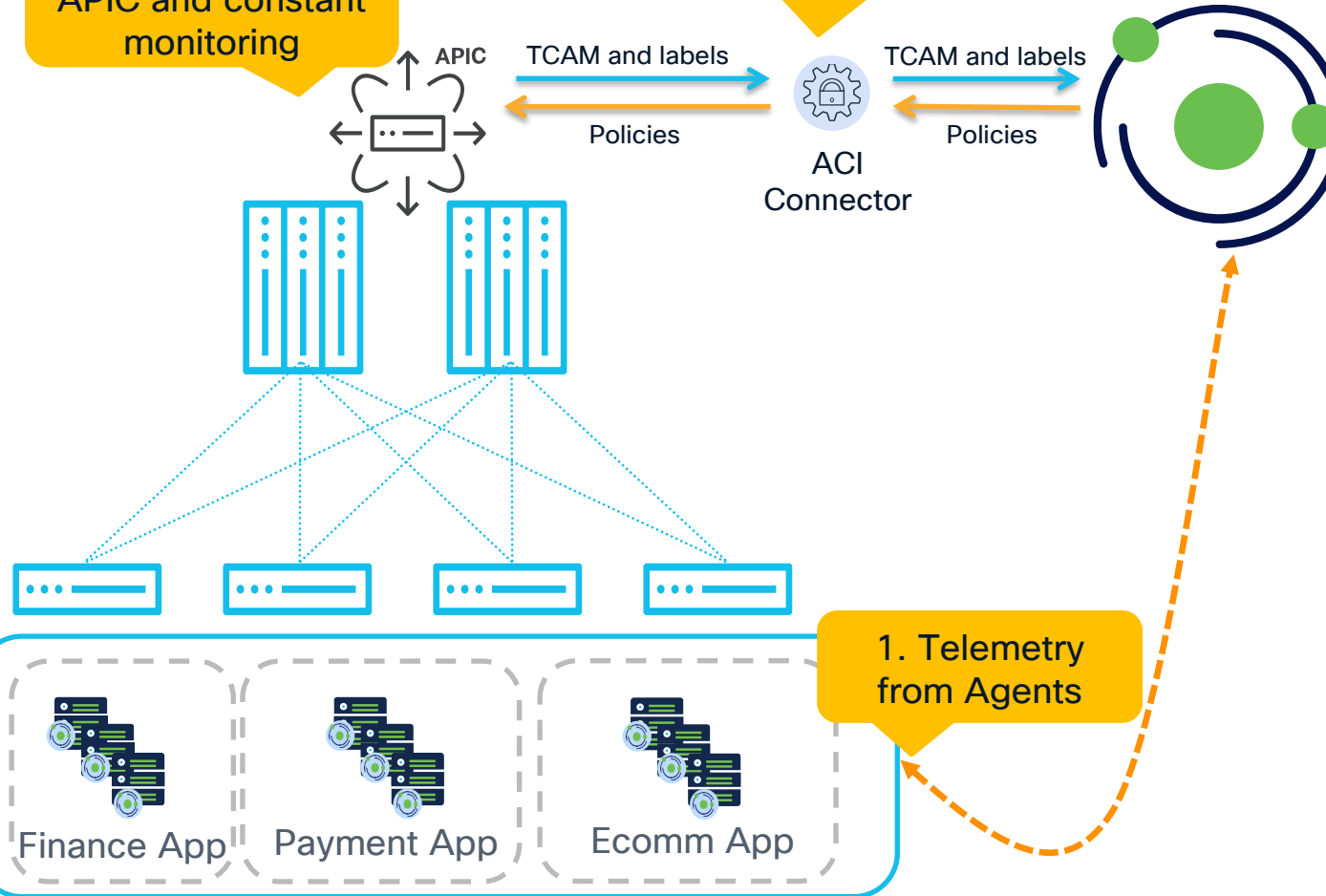
Agentless Controls

ACI Integration

3. Enforcement on APIC and constant monitoring

2. Scope to VRF Mapping and Discovery

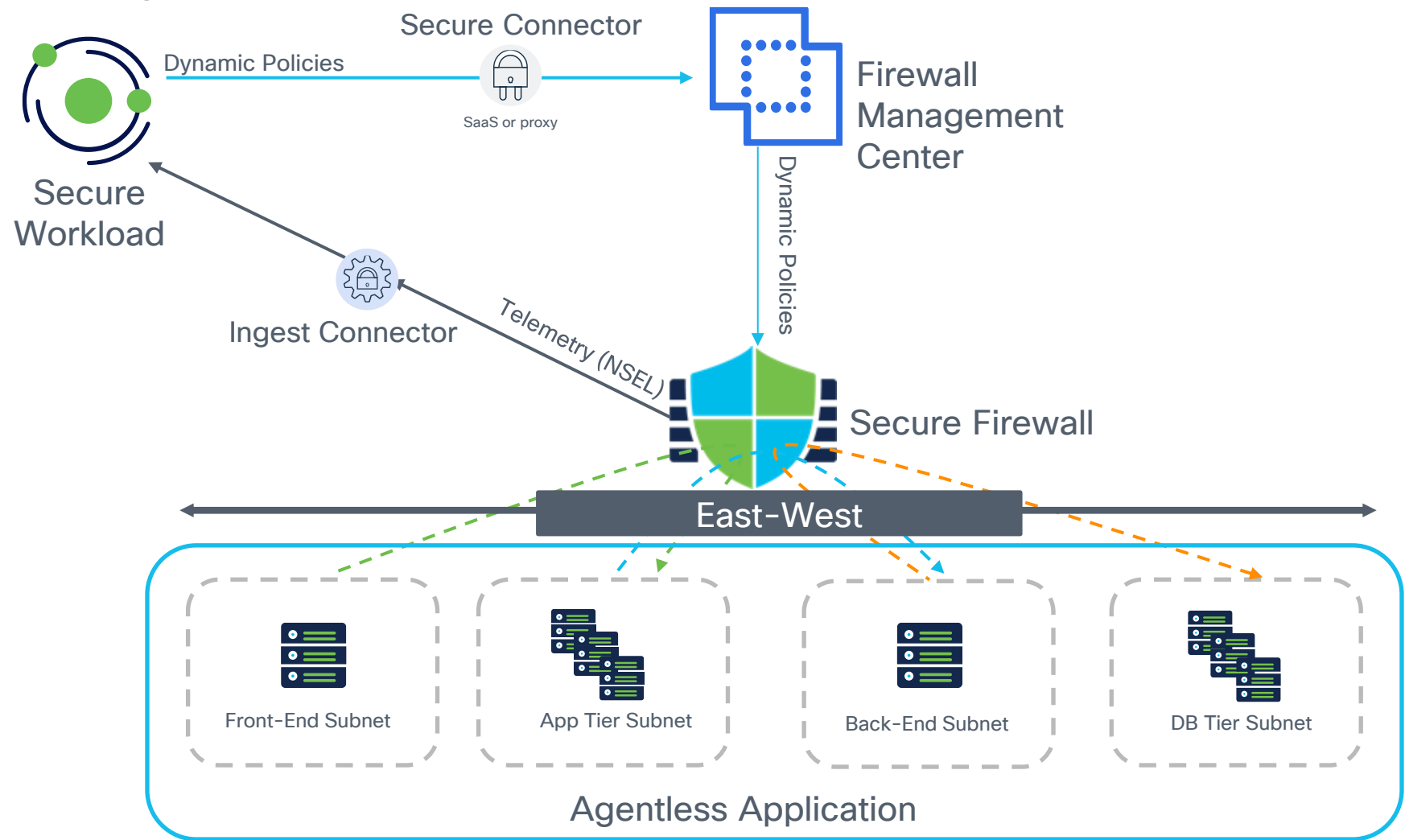
1. Telemetry from Agents



- Telemetry via agents
- Workload Discovery
- Policy optimization and TCAM monitoring
- Dynamic push ESG contracts on ACI

Agentless Controls

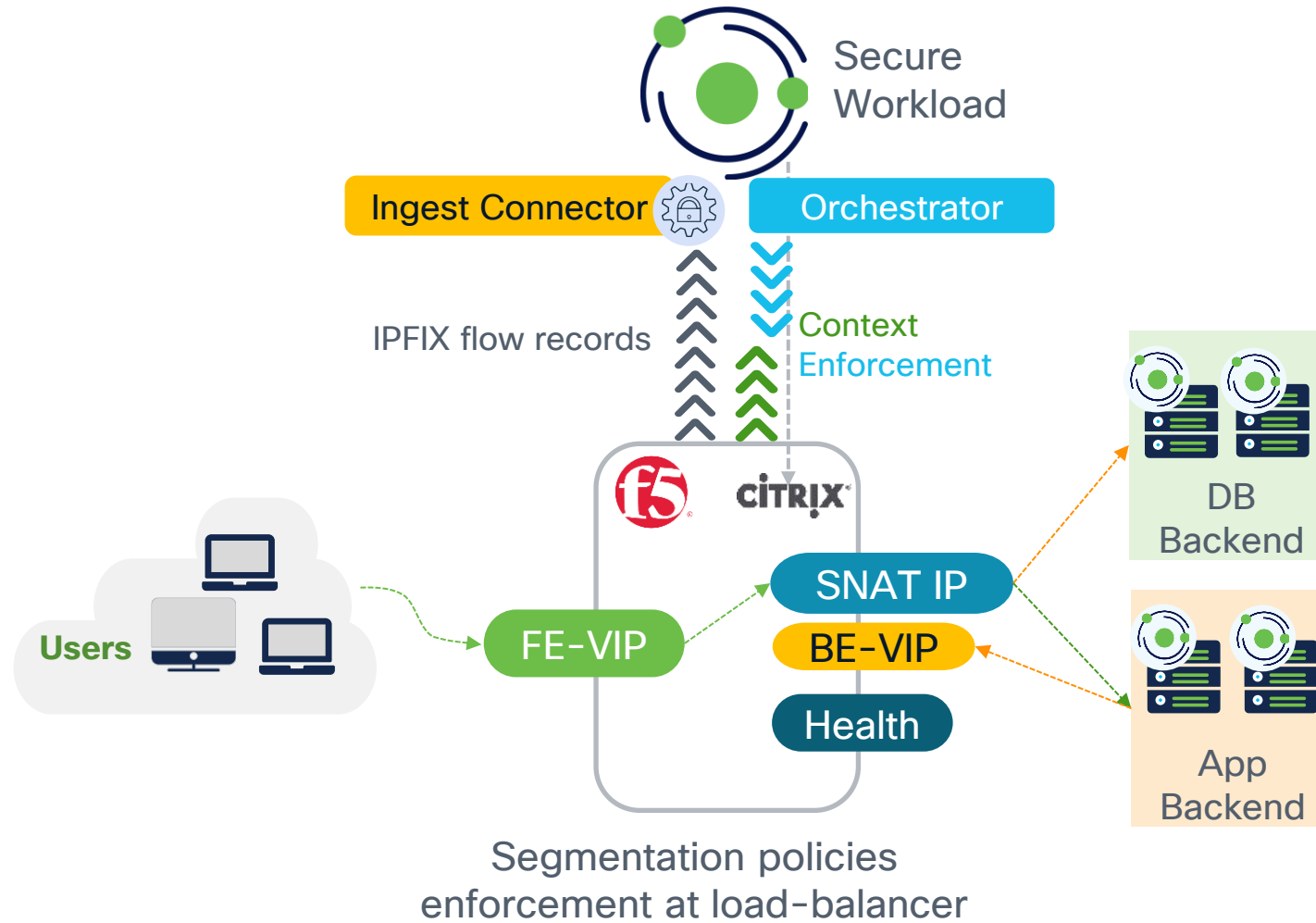
Secure Firewall Integration



Segmentation policies enforcement at firewall

Agentless Controls

Enforcement at load-balancer



Quarantine Workloads Based on CVE/Process

Workloads (VM, Baremetal and containers)



Filters ? CVE Score v3 ≥ 9 Filter

Displaying 2 of 315

Name	Version	Architecture	Publisher
.NET Framework 3.5 Features	3.5	AMD64	Microsoft Corporation
.NET Framework 3.5 (includes .NET 2.0 and 3.0)	3.5	AMD64	Microsoft Corporation

CVE-2016-0033 CVSS Score: (v2: 5) (v3: 7.5)
CVE-2016-0047 CVSS Score: (v2: 5) (v3: 7.5)
CVE-2016-0132 CVSS Score: (v2: 10) (v3: 9.8)
CVE-2016-0145 CVSS Score: (v2: 9.3) (v3: 8.8)
CVE-2016-0149 CVSS Score: (v2: 4.3) (v3: 5.9)
CVE-2016-3209 CVSS Score: (v2: 5) (v3: 5.5)
CVE-2016-3255 CVSS Score: (v2: 5) (v3: 7.5)
CVE-2012-0160 CVSS Score: (v2: 9.3)
CVE-2012-0161 CVSS Score: (v2: 9.3)
CVE-2012-0163 CVSS Score: (v2: 9.3)
CVE-2012-2519 CVSS Score: (v2: 7.9)
CVE-2012-4776 CVSS Score: (v2: 9.3)

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS v2.0 Severity and Metrics:
Base Score: 10.0 HIGH
Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C (V2 legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Complete
Integrity (I): Complete
Availability (A): Complete
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Filter: CVE-Filter-Demo

Query: Package CVE contains CVE-2014-4877

Scope: Tetration

Description: CVE filter for quarantine

Restricted?: No

Public?: No

Endpoints (42)

Absolute Policies 3 Default Policies 9 Catch All DENY Add Absolute Policy

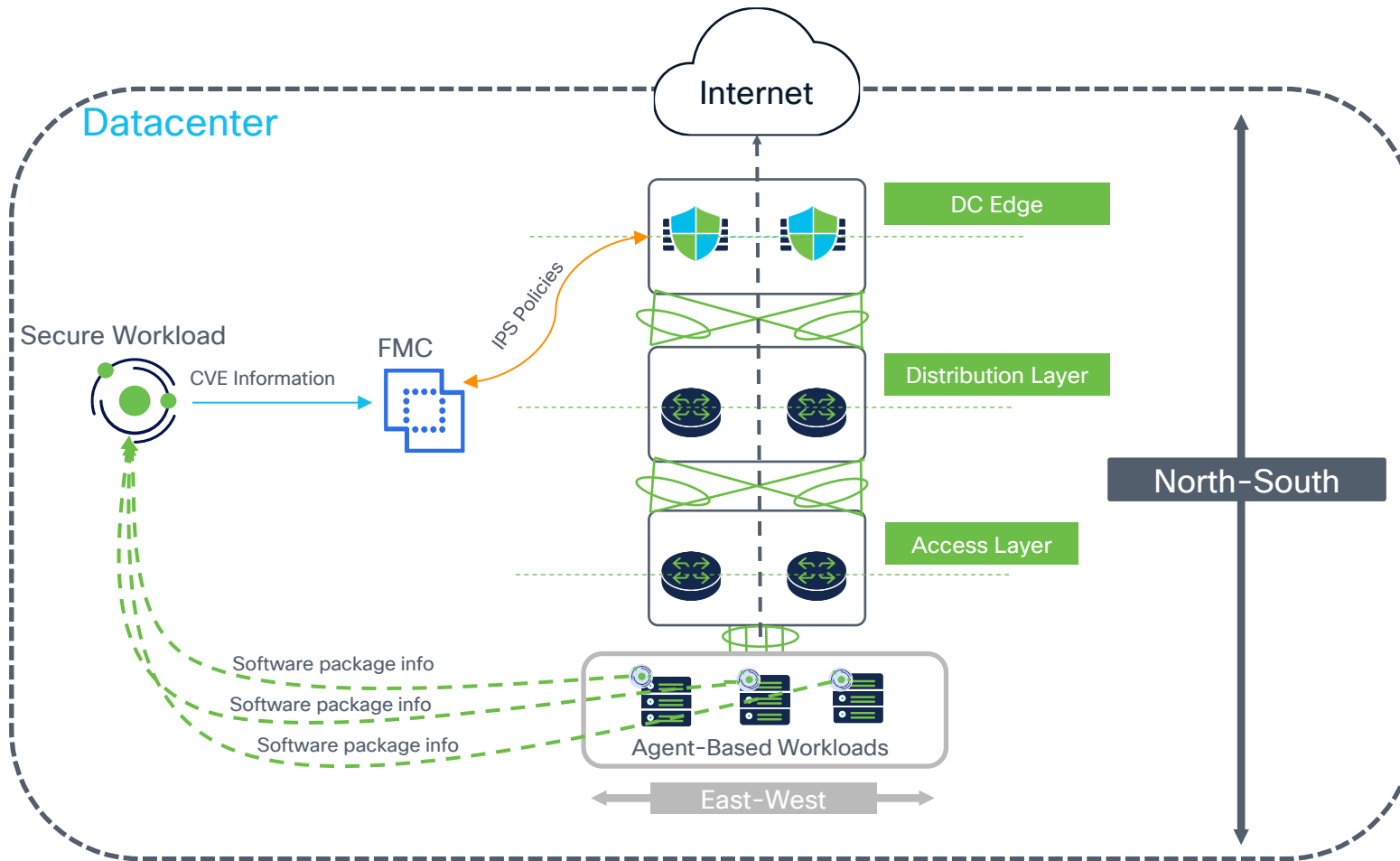
Priority	Action	Consumer	Provider	Services
100	DENY	CVE-Filter-Demo	10.10.0.*	UDP : 0-65535 ...
200	ALLOW	CVE-Filter-Demo	Tetration	TCP : 22

- Visibility into the vulnerability details
- Vulnerability details include:
 - Severity
 - Impact sub-score
 - Exploitability sub-score
- Quickly identify all servers that are running specific vulnerable software package version

- **Inventory filter** – Identity workloads using specific CVEs attributes.
- Policy creation and enforcement to isolate or quarantine the affected workloads (OpenAPI support for XDR integrations)

Compensating Controls with Virtual Patch

Agentless Controls



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

Compensating Controls with Virtual Patch

FMC Virtual Patch

Settings

Segmentation

Virtual Patching

Event Log

Enter attributes...

×

Filter

Rules

Virtual Patch Rule

Sales Web App

Used in Virtual Patching Rule Sales Web App

* Application = Sales-Web and CVE Score v3 > 8

Workloads with Published CVEs

Refresh

Filter Workloads

Rules 1, Workloads 1

CVE List

Vulnerabilities by Source

No Search Constraints [\(Edit Search\)](#)

Third-Party Vulnerabilities Summary

Third-Party Vulnerabilities Details

Table View of Third-Party Vulnerabilities

Hosts

Jump to...

CVE-to-SnortID Mapping

☐	Vulnerability Source x	Vulnerability ID x	IP Address x	Port x	Bugtraq ID x	CVE ID x	SVID x	Snort ID x	Title x	Description x	Domain x
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000012	192.168.19.20			2018-25032			2018-25032	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000011	192.168.19.20			2023-25690	13499	62297	2023-25690	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000010	192.168.19.20			2022-1271	12936	60757, 60758, 300301	2022-1271	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000009	192.168.19.20			2022-41903			2022-41903	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000008	192.168.19.20			2022-23521			2022-23521	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000007	192.168.19.20			2023-38408			2023-38408	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000006	192.168.19.20			2022-40674			2022-40674	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000005	192.168.19.20			2022-2526			2022-2526	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000004	192.168.19.20			2021-3656			2021-3656	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000003	192.168.19.20			2021-3653			2021-3653	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000002	192.168.19.20			2022-42898			2022-42898	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000001	192.168.19.20			2022-24903			2022-24903	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge
▼	☐ CSW fa6ee20b-2466-00ac-cd81-72be2b38c0df 1	2000000	192.168.19.20			2023-0767			2023-0767	CSW-3.9.1.1, 20240117134505Z	Global \ DC-NS-Edge

© 2025 Cisco and/or its affiliates. All rights reserved.

133

 CISCO

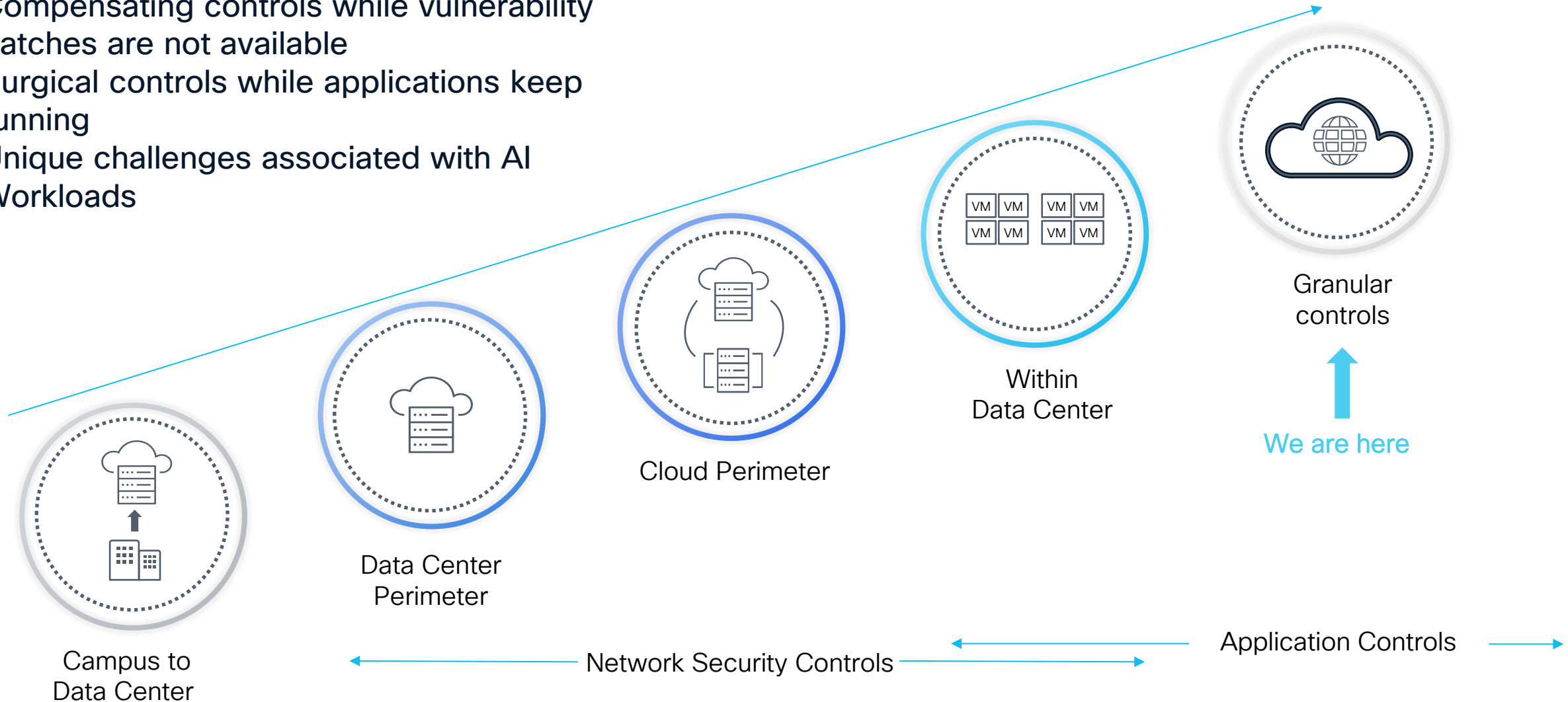
Microsegmentation – Approaches

Compare and Contrast

Criteria	Agent	Agentless-Network	Agentless-Cloud	Comments
Form-Factor Coverage (baremetal, VM, container)	●	●	●	Agentless: Limited coverage for containers
OS Dependency	●	●	●	Agent: Dependencies on OS
Network Infrastructure Dependency	●	●	●	Agentless-Network: Dependencies on network
Observability- Flow (baremetal, VM, container)	●	●	●	Agentless: Limited visibility for containers
Observability - Runtime (vulnerability, processes, behavior)	●	●	●	Agentless: No visibility
Enforcement (Granularity)	●	●	●	Agentless-Network: Segmentation policies granularity depends on the insertion method and form-factor Agentless-Cloud: Limited granularity for container form-factor
Enforcement (Scalability)	●	●	●	Agentless-Cloud: Number of access control rules limited by Cloud Service Provider
Time to Deploy	●	●	●	Agent: Organizational dependencies

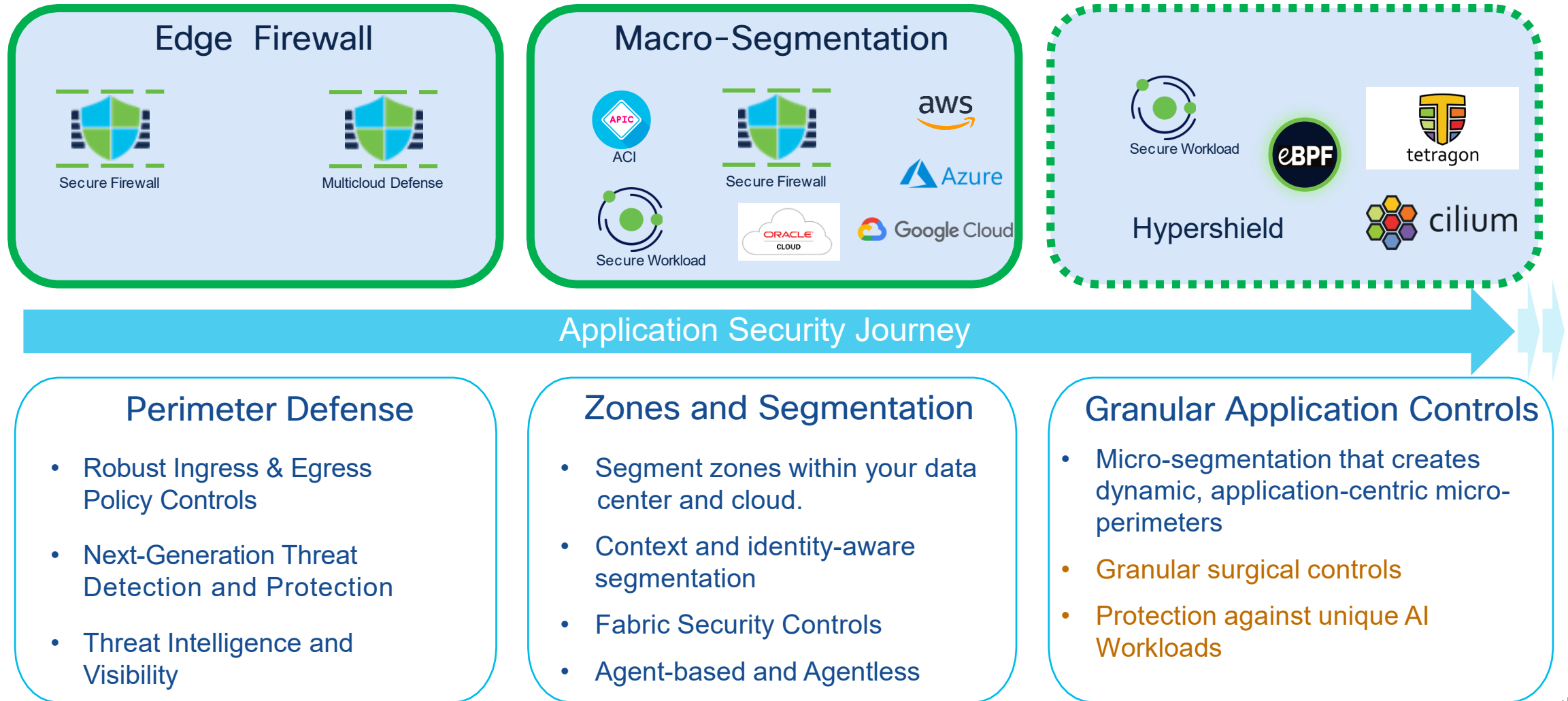
Beyond micro-segmentation

- Compensating controls while vulnerability patches are not available
- Surgical controls while applications keep running
- Unique challenges associated with AI Workloads



Layers of Defence

Going beyond application micro-segmentation



Cisco Hypershield

eBPF – Foundation of Hypershield

- Kubernetes networking
- Load balancing
- Kubernetes services
- Identity-based security
- L7 policies



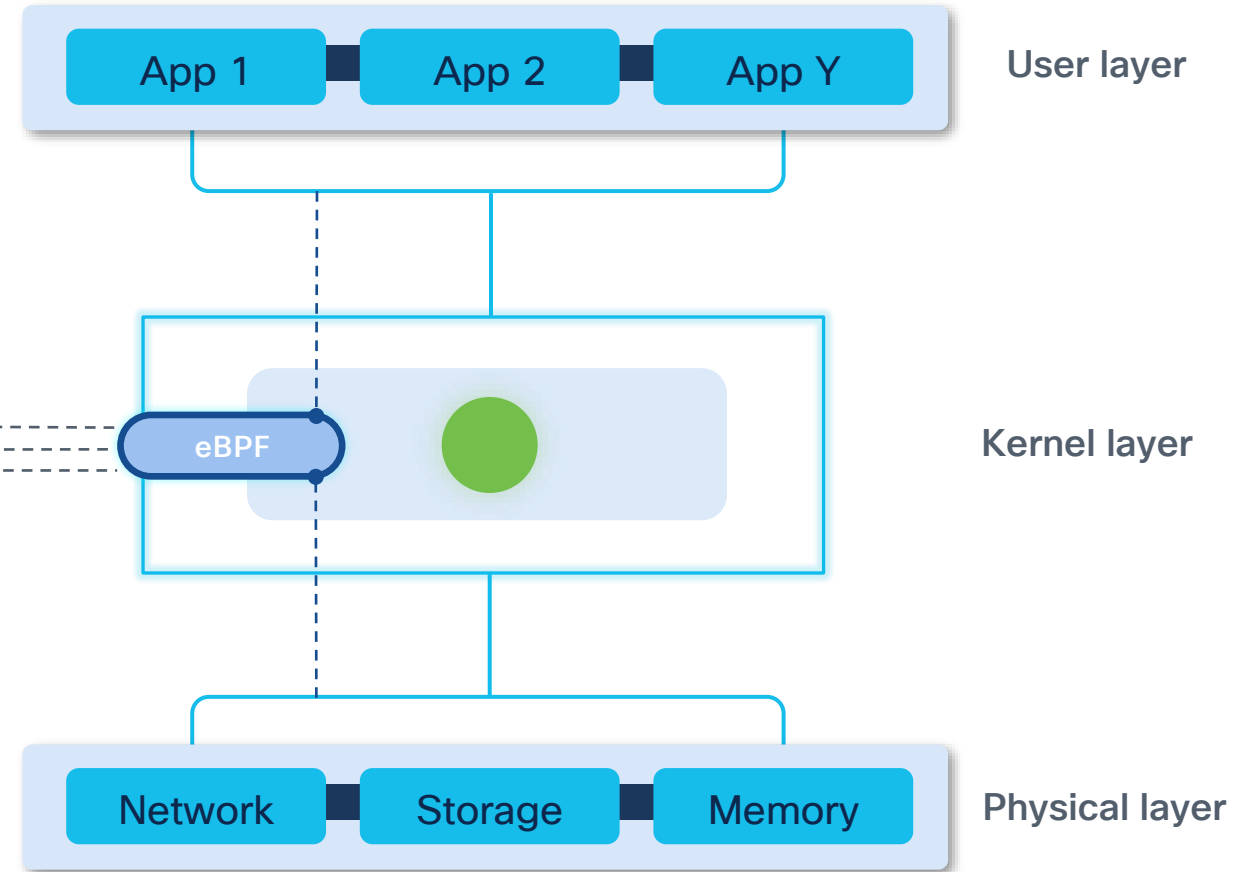
Network filtering

- Dependencies map (service and flows)
- Monitoring and alerting
- App monitoring

Observability

Security policy

- Monitor process execution
- Runtime security policies
- Real time enforcement

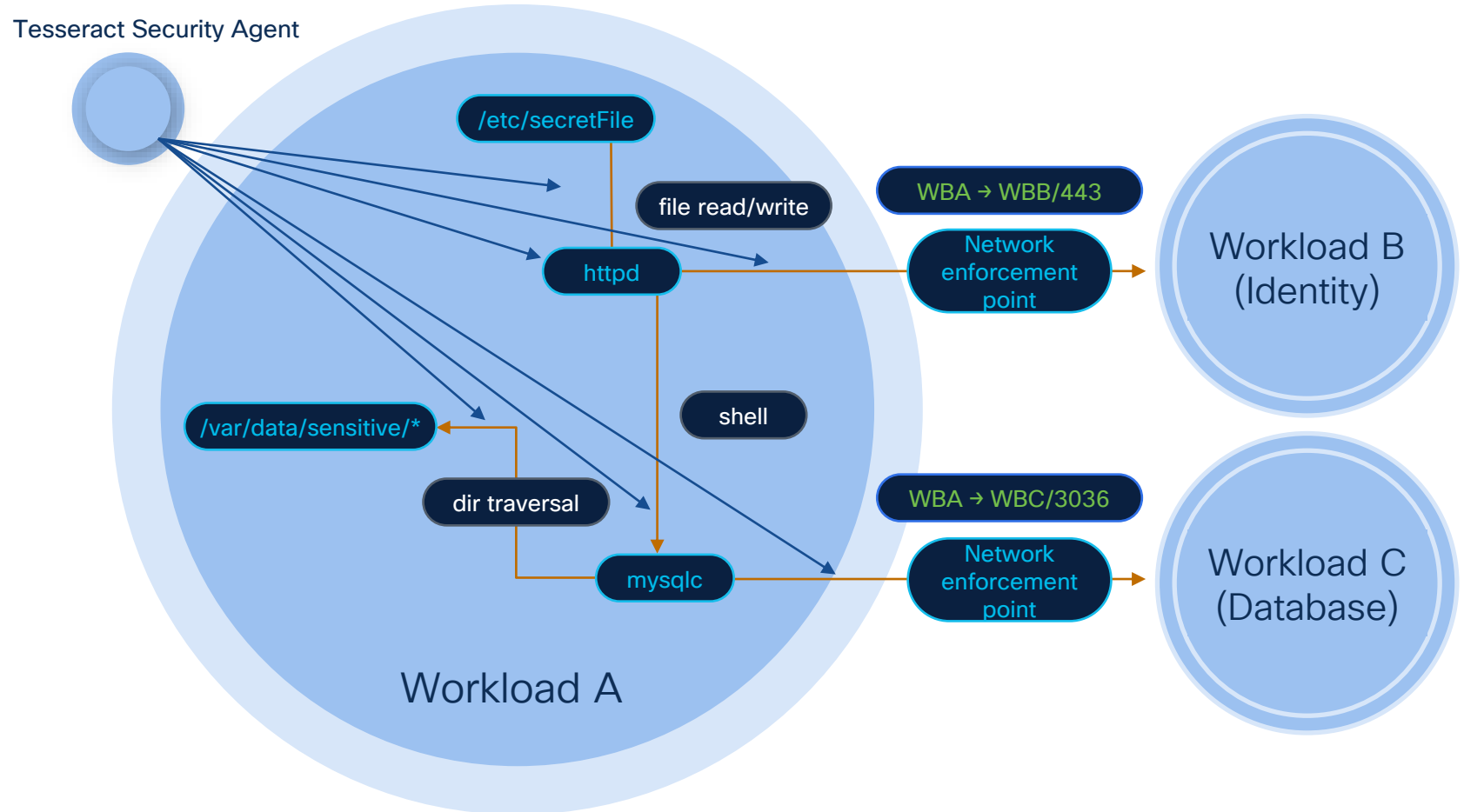


eBPF based visibility & controls in network & workload

Cisco Hypershield (built on Isovalent)

Deep visibility
and enforcement

- Network
- File read/write
- Directory traversals
- Privilege escalations



Surgical mitigating controls

While keeping applications up and running

Distributed Exploit Shield | runc-exec...

Verified

REMEDICATION 1

Recommended

The Distributed Exploit Shield blocks new container processes with a current working directory of "/" in the host namespace.

Reason

Remediates vulnerability **CVE-2024-21626**

Effect

Block and alert

Principal

/usr/local/sbin/runc

Action

sys_execve

Resource

*

Condition

when principal.version <= 1.1.11 or unknown and action.cwd = "host_ns:/"

Deployed by 8,734 other customers

Deploy

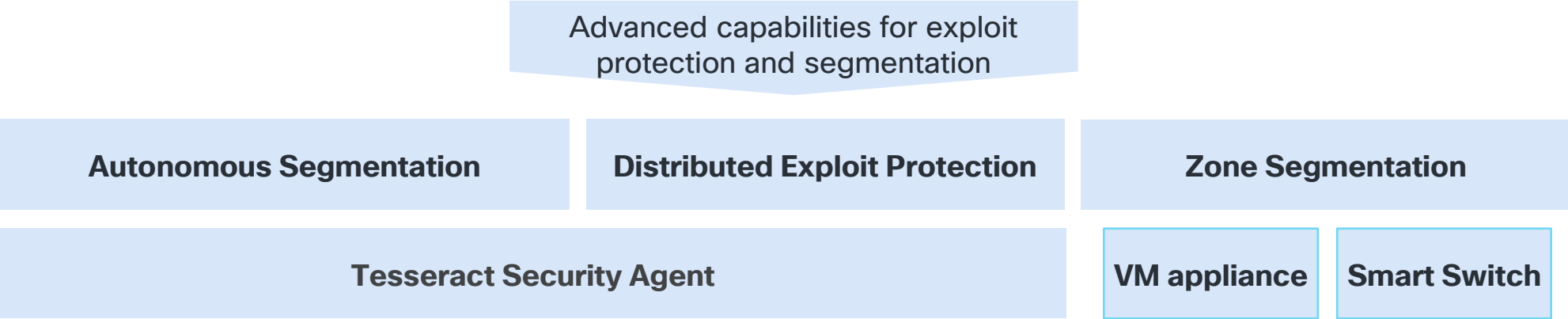
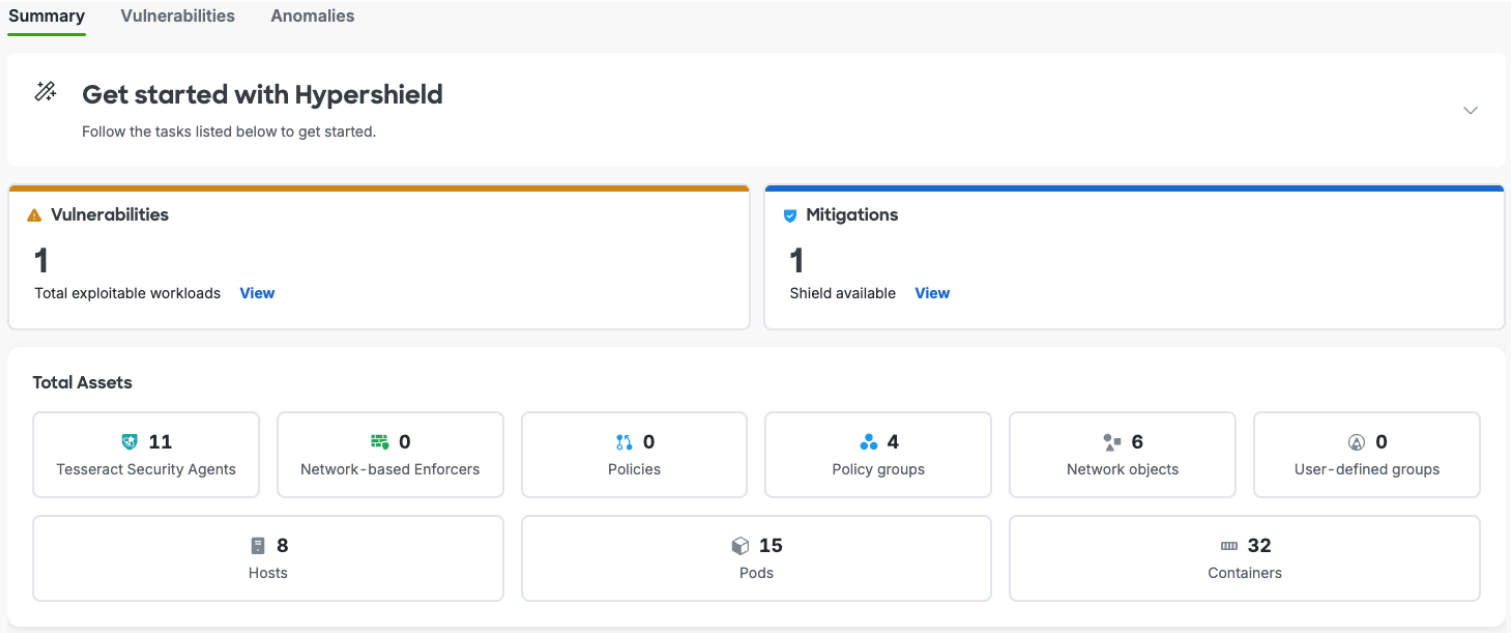
View 3 alternative remediations

Archive

AI generated rule blocking a vulnerable container process:

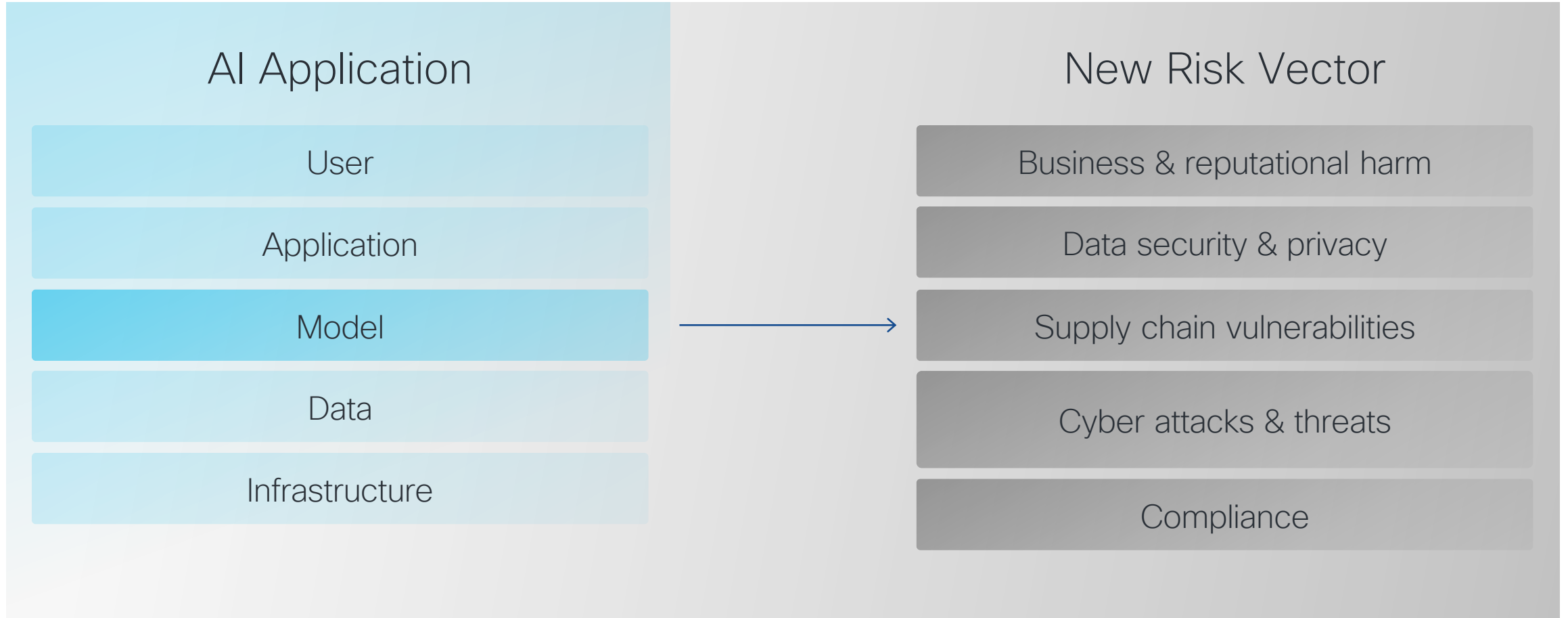
Effect	Block & Alert
Principals	File path / executable
Actions	Execute Permit
Resources	* (act on any resource)
Conditions	Minimum version & namespace

Agent and Agentless Enforcement



AI Applications: Unique Security Requirements

AI Applications can be non-deterministic



Securing AI Applications

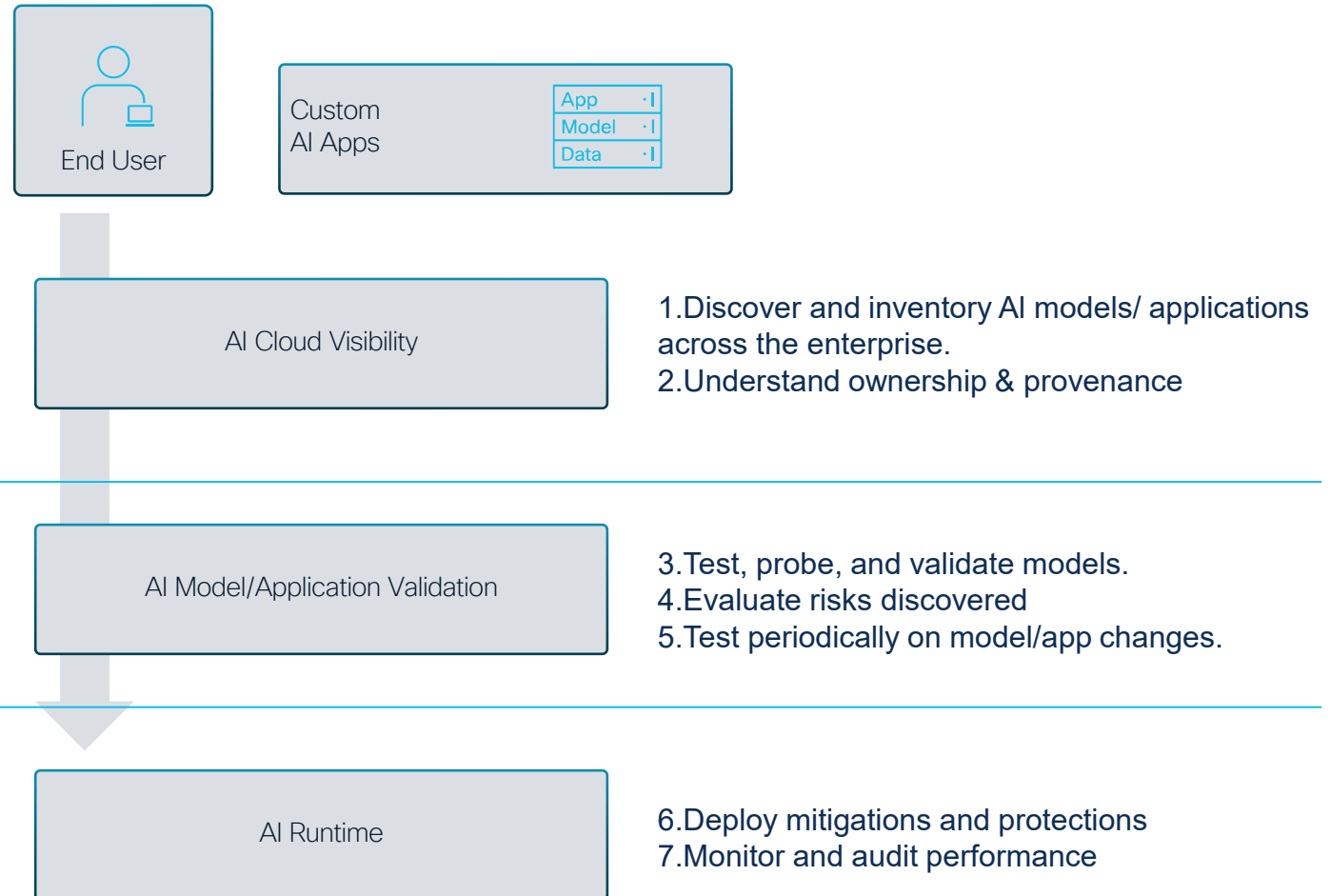
Cisco AI Defense: Secure AI Apps development lifecycle

Enterprise development teams are
Enabling AI rapidly in their applications.

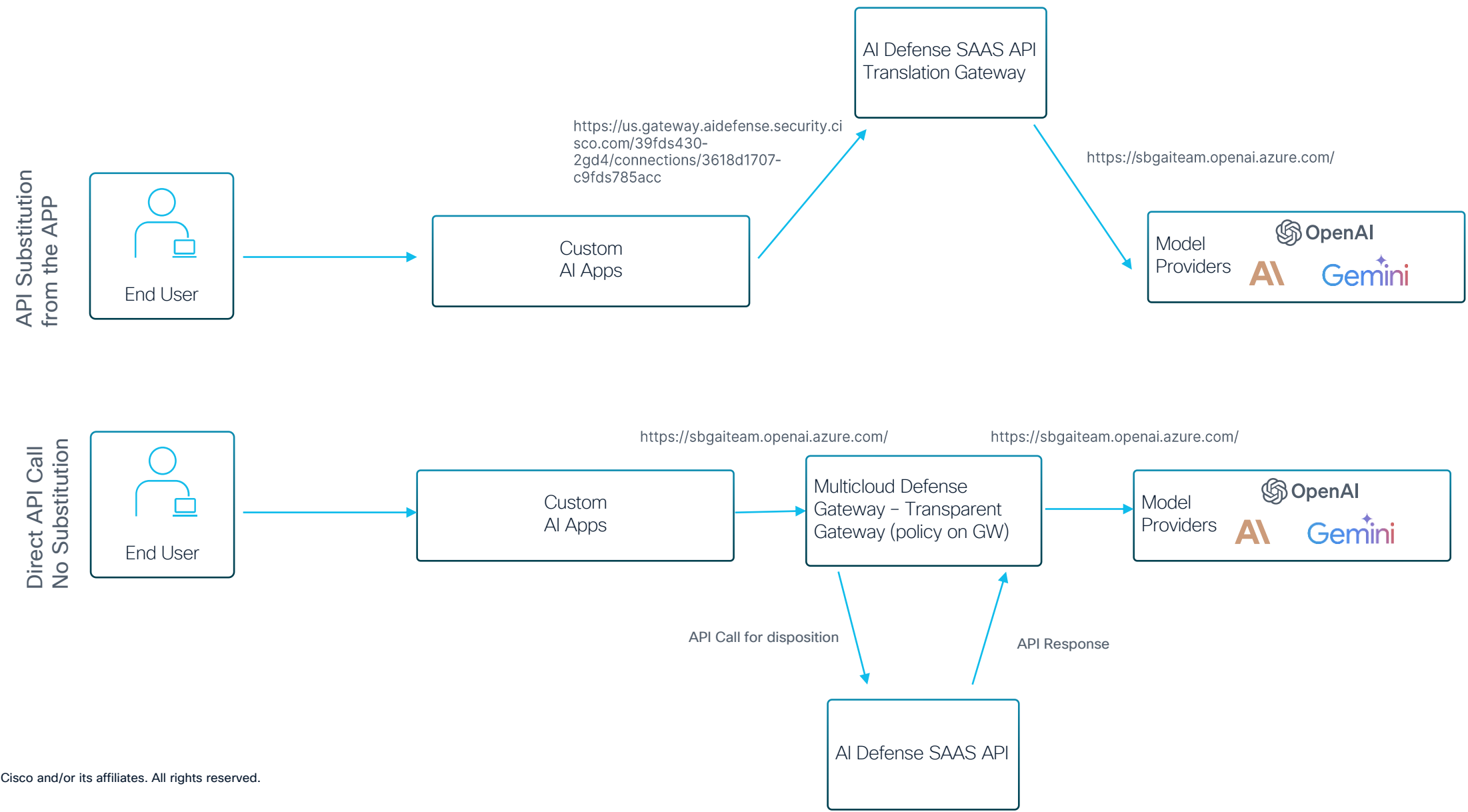
What AI assets are in my cloud?
(including VPCs)

What are the risks associated with these
AI models and apps?

Protect with runtime guardrails



Guardrail Implementation

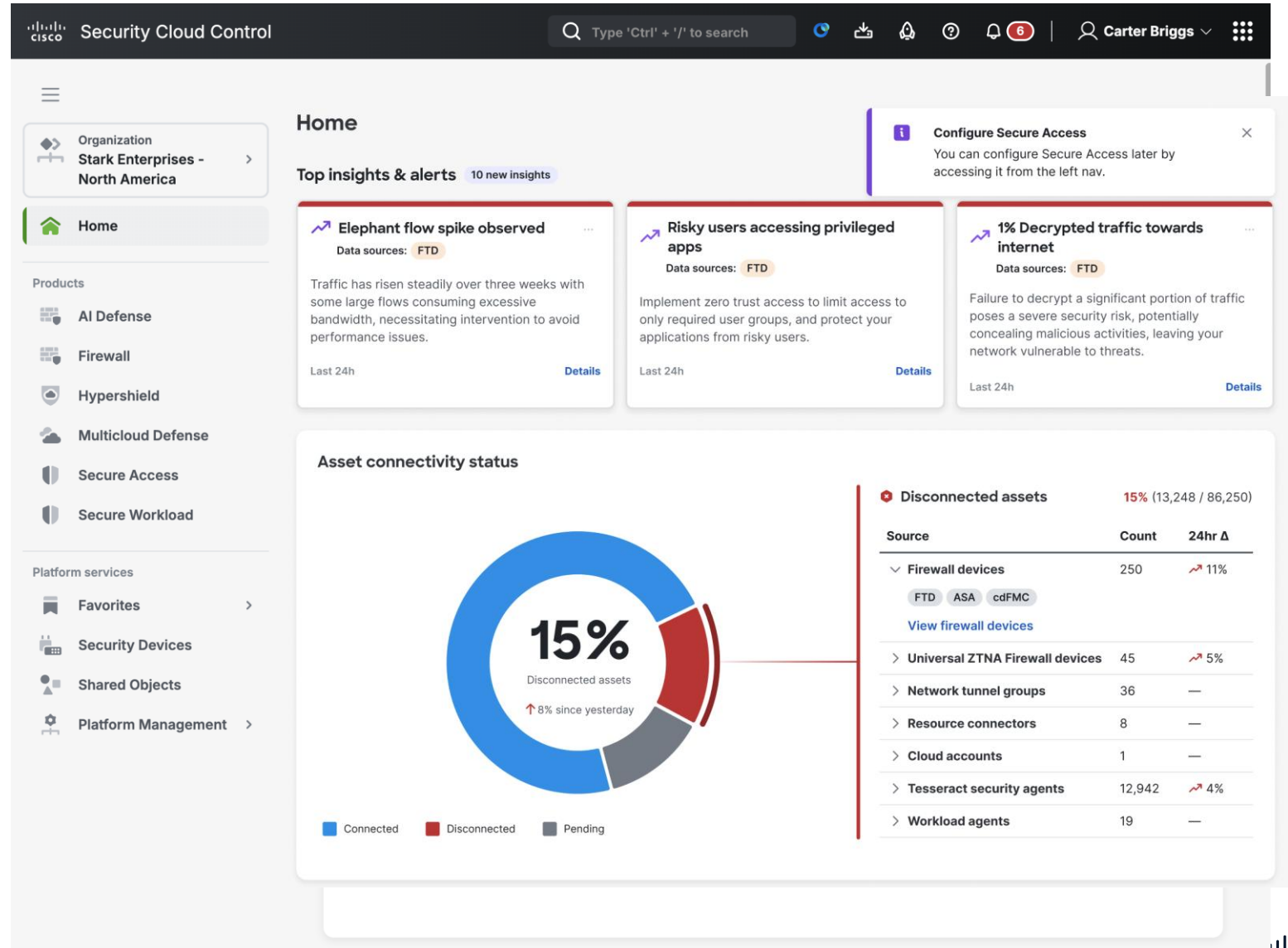


Sprawling Security Controls

But Inefficient Security Operations

Cisco Security Cloud Control helps address:

- Inconsistent policies
- Too many dashboards to manage and monitor
- Obstacles to operate at speed and scale



Addressing the challenges

Challenges

- Evolving infrastructure and changing boundaries
- Disparate control points resulting in inconsistent policies
- Lack of dynamic and shared context
- Having to hunt for which platform shows which data

What we discussed

- • Zero Trust approach to access policy across the architecture
- • Unified Policy Constructs for enforcement and response
- • Cross platform context sharing
- • Unified Dashboard for efficient Security Operations

Solution: A Platform approach to Security

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

CISCO Live !

Unlock insights from the network

Firewall Logs at no additional cost in Splunk*

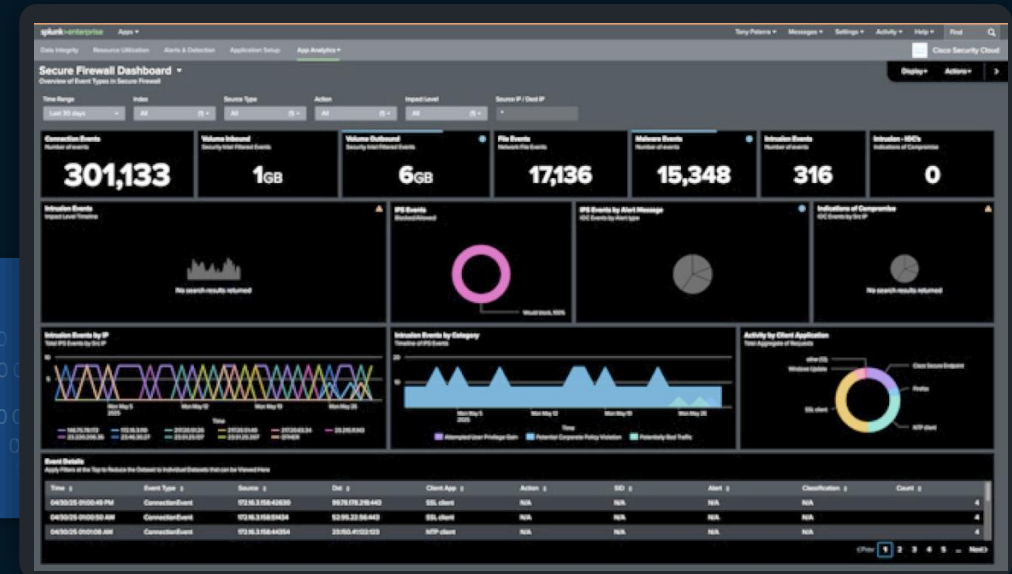
Comprehensive
TDIR



Unleash
Network Insights



Bridging
SecOps + NetOps



New detections | Automated response

*Cisco Firepower (FTD) firewalls are entitled to 5GB of Splunk logging capacity with purchase