

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Keeping Up with Zero Trust

Jerry Lin, Principal Security Engineer
BRKSEC-2176

CISCO *Live!*

#CiscoLiveAPJC



“Reconciliation” – Dustin Koa Art

About Jerry Lin

- 20+ years at Cisco; Security CCIE#6469
- Distinguished Speaker Hall of Fame at Cisco Live
- Coauthor; “NAC Appliance: Enforcing Host Security with CleanAccess”, Cisco Press
- Cisco Security Reference Architecture
- Favorite sport; marathons! Boston



CL Hall of Fame



Coauthor



www.cisco.com/go/sra RSAC 2023

CISCO *Live!*

Cisco Webex App

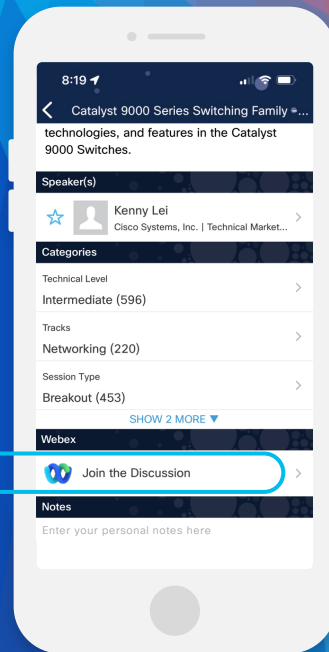
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2176>

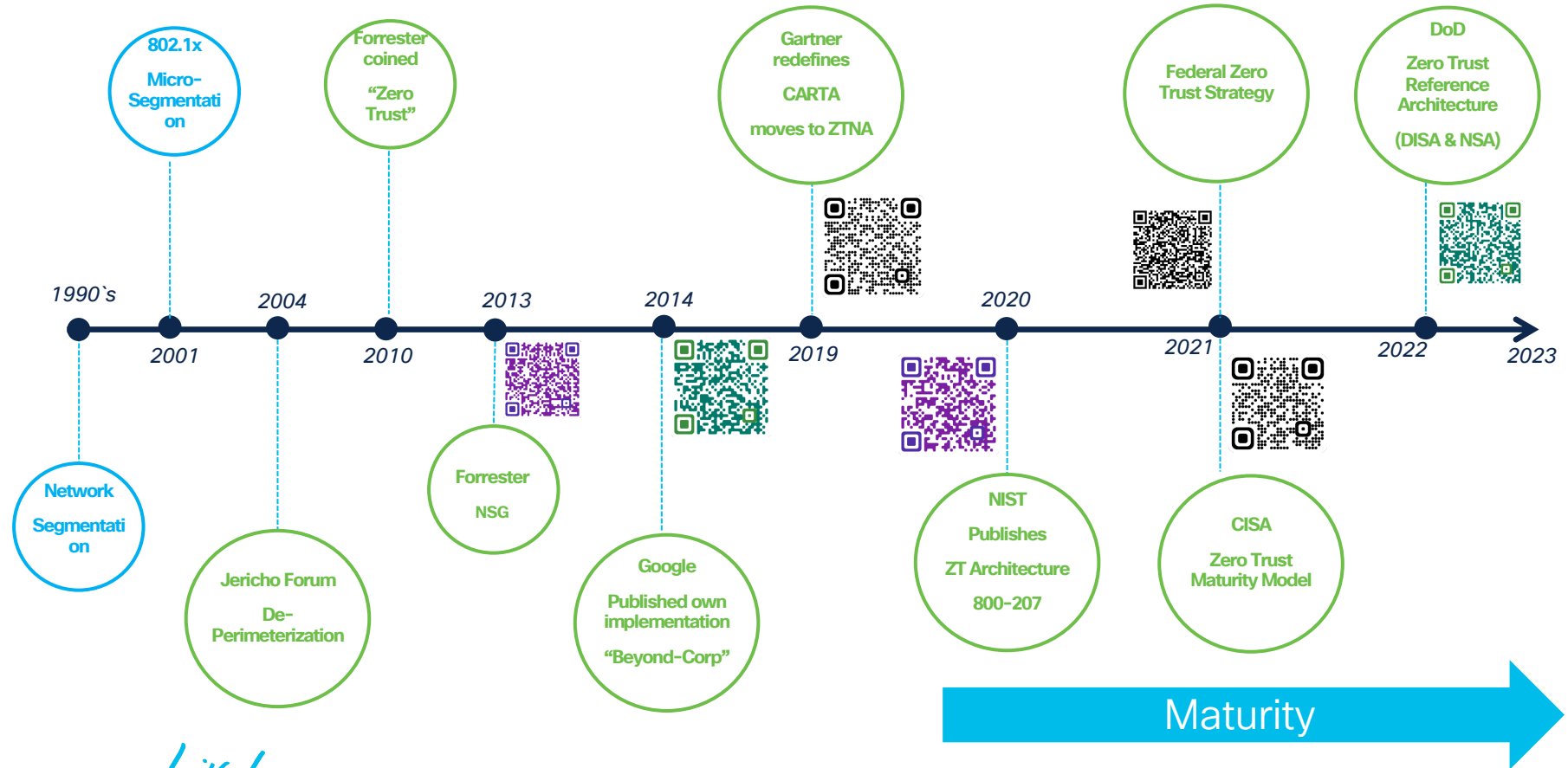
Agenda

- Zero Trust Evolution
- Keeping Up with Zero Trust
- Zero Trust Use Cases
- Summary

What Zero Trust Means to Us



History and Evolution - Zero Trust



Security Outcomes Report for Zero Trust

<https://www.cisco.com/c/en/us/products/security/zero-trust-outcomes-report.html>

86.5% have started on at least 1 ZT pillar

- Identity, Device
- Network & Workload
- Automation and Orchestration

Survey participants

We surveyed **4,751** active information security and privacy professionals from **26** countries.

Data analysis by Cyentia institute

Reduction in probability of incident type when completing zero trust pillar

Identity



Device



Incident Type

Network and Workload



Rise in Data Breach cost

**USD 4.45
million**

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

51%

51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

Source; <https://www.ibm.com/reports/data-breach>

Zero Trust Message Expansion

THEN (“where”)

Cisco Zero Trust
for Workforce



User & Device Security

Visibility /
Analytics /
Orchestration

Cisco Zero
Trust for
Workloads



Workload, Application &
Data Security

cisco
SECURE X

TALOS

Cisco Zero
Trust for
Workplace

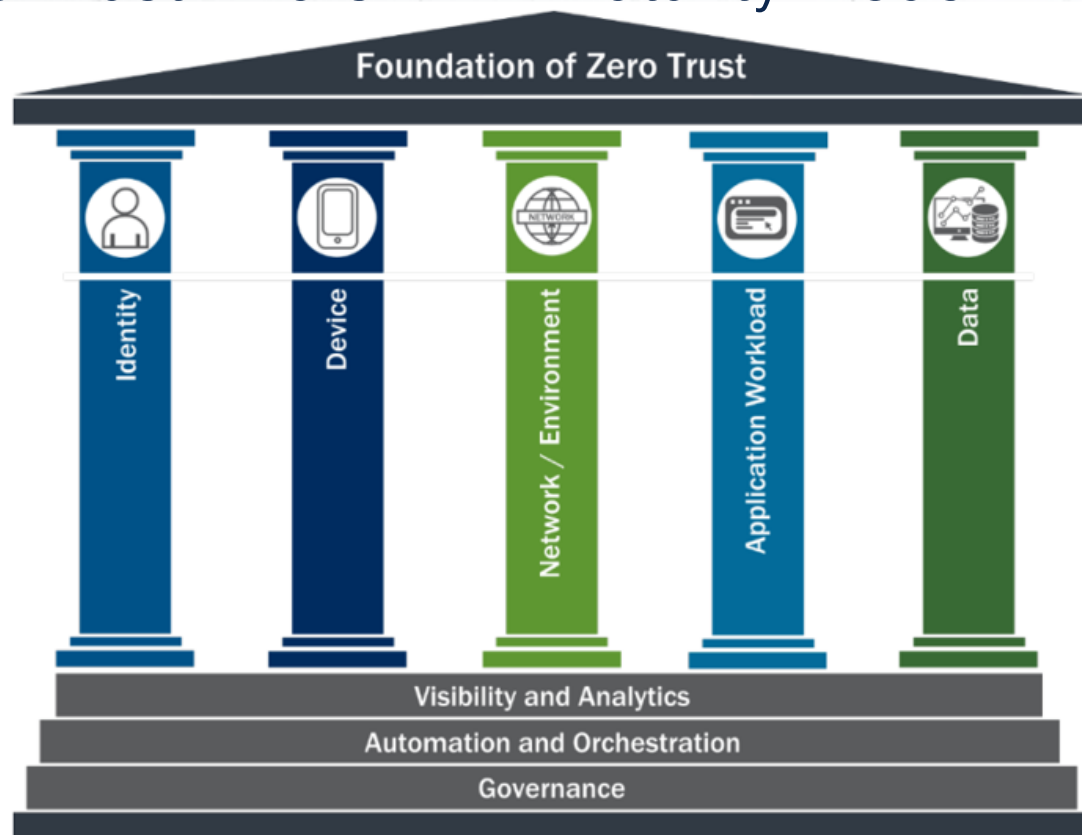


Network & Cloud Security

CISA - Zero Trust Pillars - ZT Maturity Model



CISA =
Cybersecurity
Infrastructure and
Security Agency



Maturity Levels:

- *Traditional*
- *Advanced*
- *Optimal*

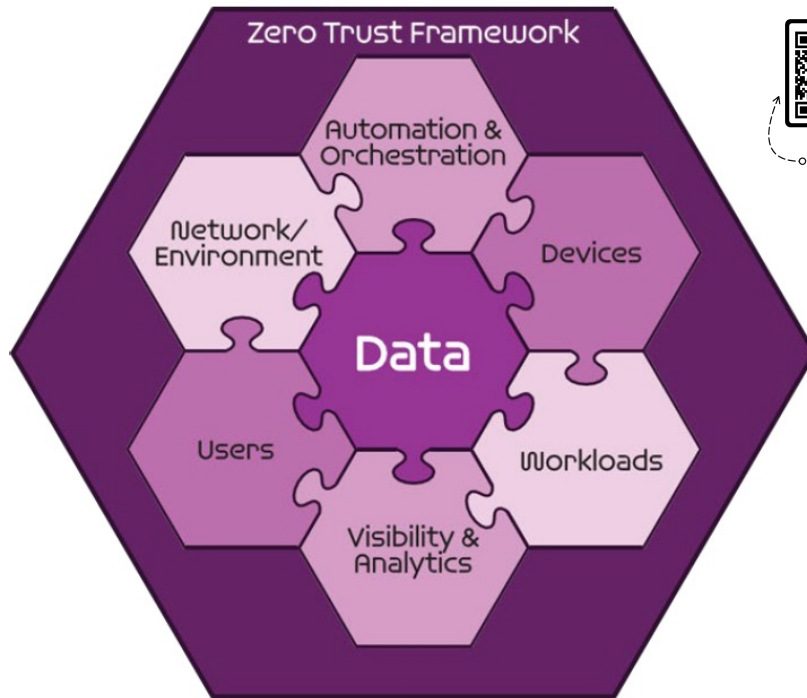
https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Dynamic - Continuous - Integrated - Optimized - Automated
Behavior and posture analytics – suspicious and malicious behaviors

DISA Zero Trust Framework

Defense Information Systems Agency

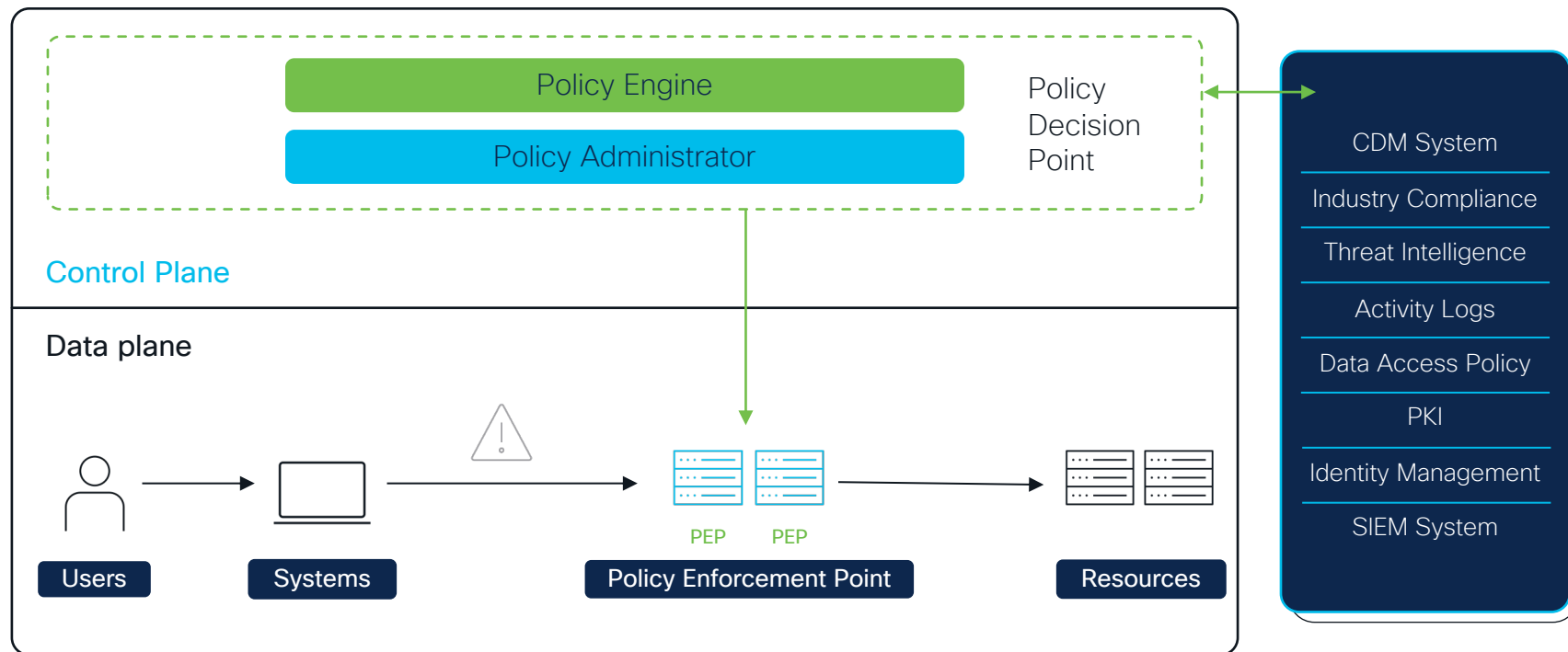
- 7 pillars of DoD ZT Architecture
- Prepared by DISA and NSA(National Security Agency, July 2022



SCAN ME

[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)

NIST 800-207 – Zero Trust Architecture



What it takes to get Zero Trust right

Zero Trust requirements



Establish & Continuously Verify Trust

- User / device / posture / context
- Risk-based authentication
- Behavior monitoring – threat activity
- Vulnerability Management

★ Identity Security
Posture Management



Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit access (ZTNA)



Respond to Change in Trust

- Prioritized incident response
 - Orchestrated remediation
 - Integrated + open workflows
- ★ Identity Threat Detection & Response

★ New Capabilities
CISCO *Live!*



 Threat Intelligence

 Extended Detection and Response

 ZERO TRUST

 SASE

 User / Device Security

 Cloud Edge Network

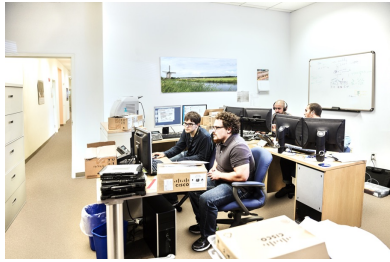
 On Premises Network

 Workload, Application, and Data

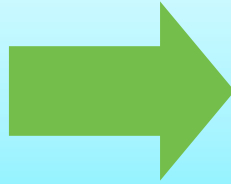
 Platform

Zero Trust Use Cases

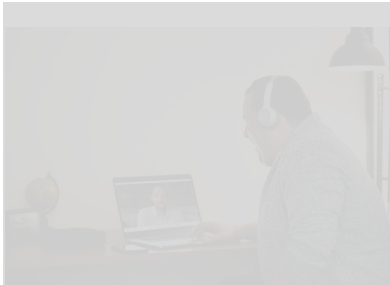
Zero Trust Use Cases



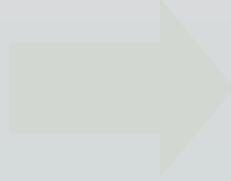
On-
Premises
User &
IOT



- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps



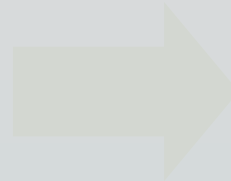
Remote
User



- ZT access to public SaaS
- ZTNA to private apps
- Unified ZTNA client
- Client-based VPN private app access

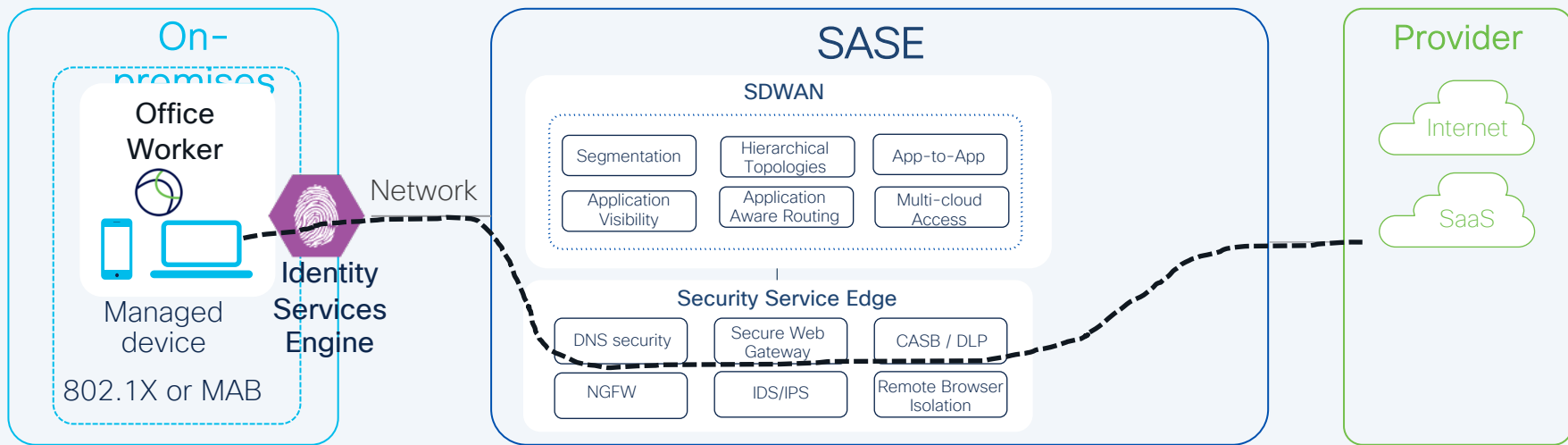


App-to-
App



- App-to-App across multi-cloud

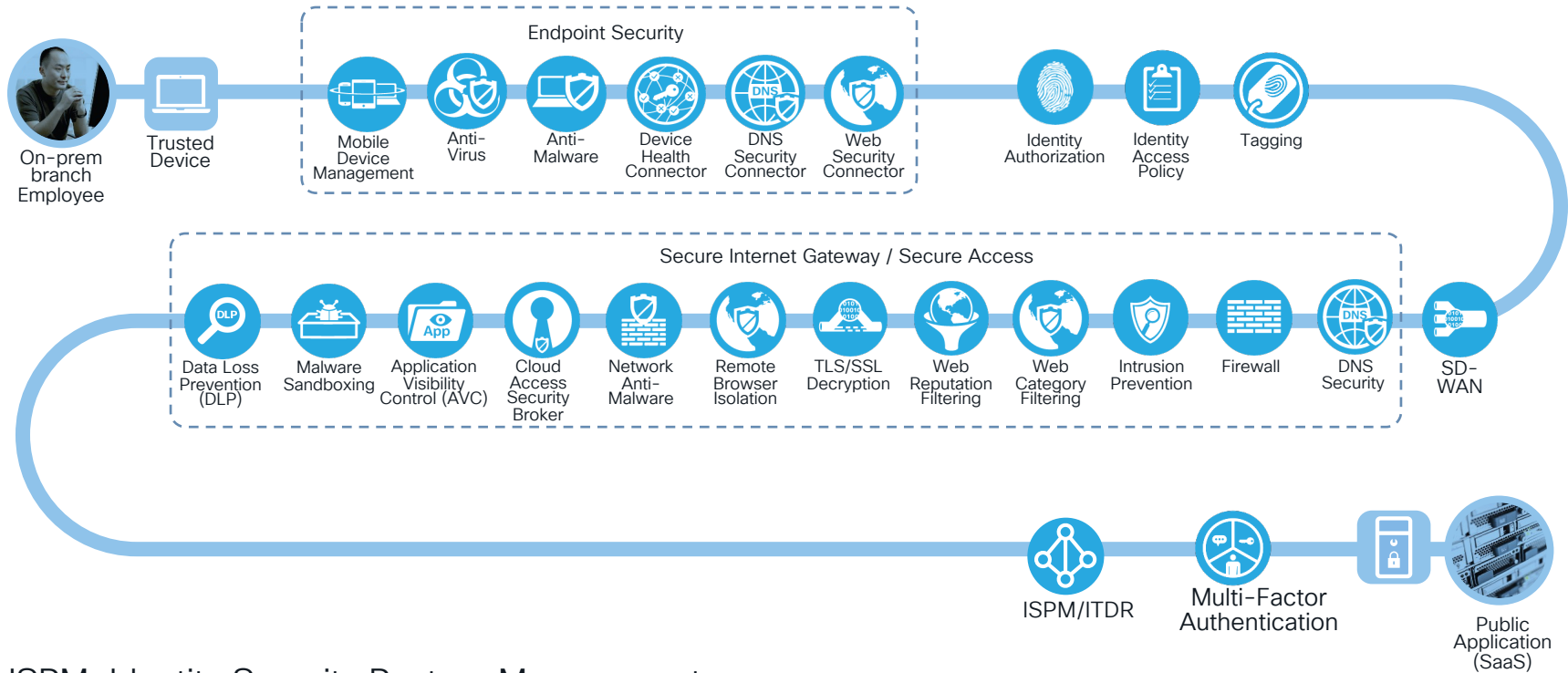
On-Premises Worker to Public SaaS/Internet



On-premise worker to public SaaS/Internet

Business Driver	IT Risk/Initiative	Cybersecurity Risk
Employee Productivity Return to Office(RTO)	Unauthorized/Excessive Access	Aging on-premise security and maturity
Improved application performance and user experience	Direct Internet Access, IPSec Tunnel Management to the Security Service cloud	Malware, Data leakage, ransomware, etc
Improve employee satisfaction or employee retention	Aging technology, poor performance	Lack of visibility and control, new threats

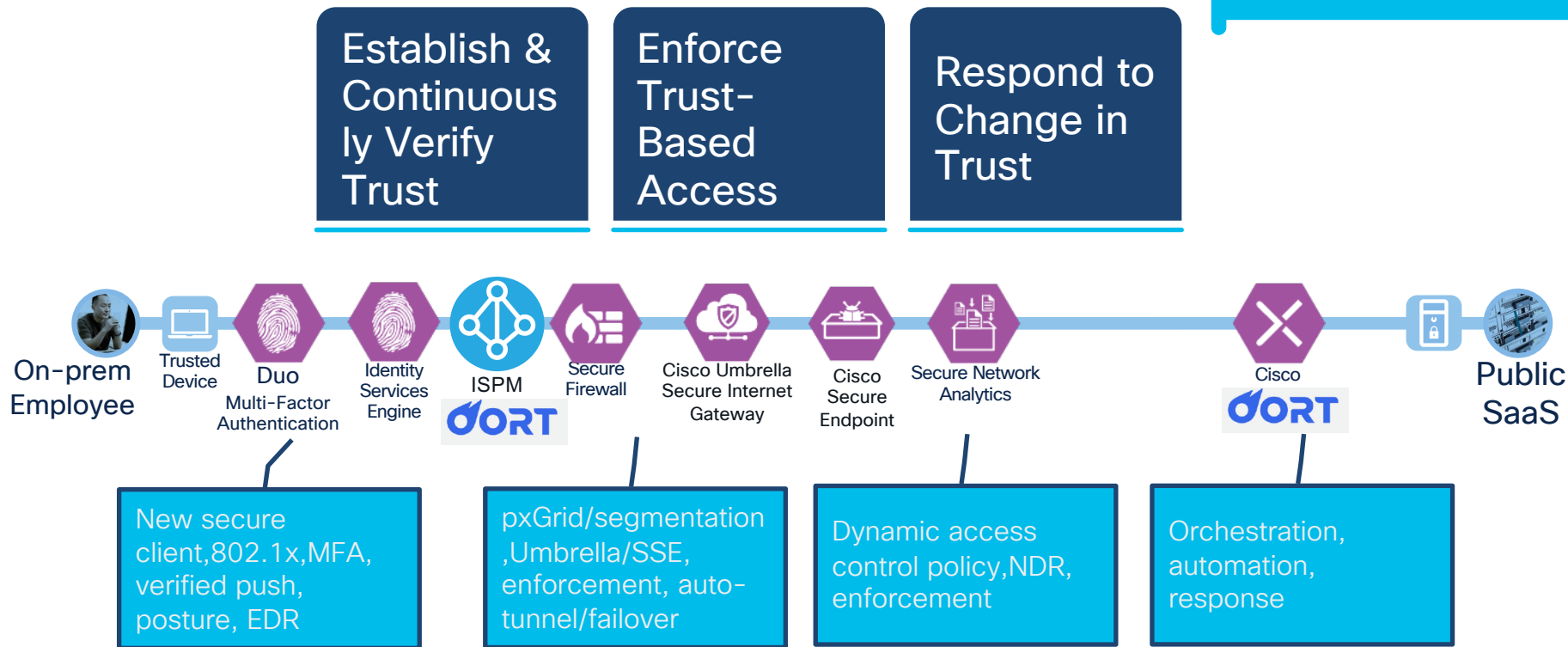
On-premise branch user to public SaaS/Internet



ISPM=Identity Security Posture Management
ITDR=Identity Threat Detection Management

On-premise branch user to public SaaS/Internet

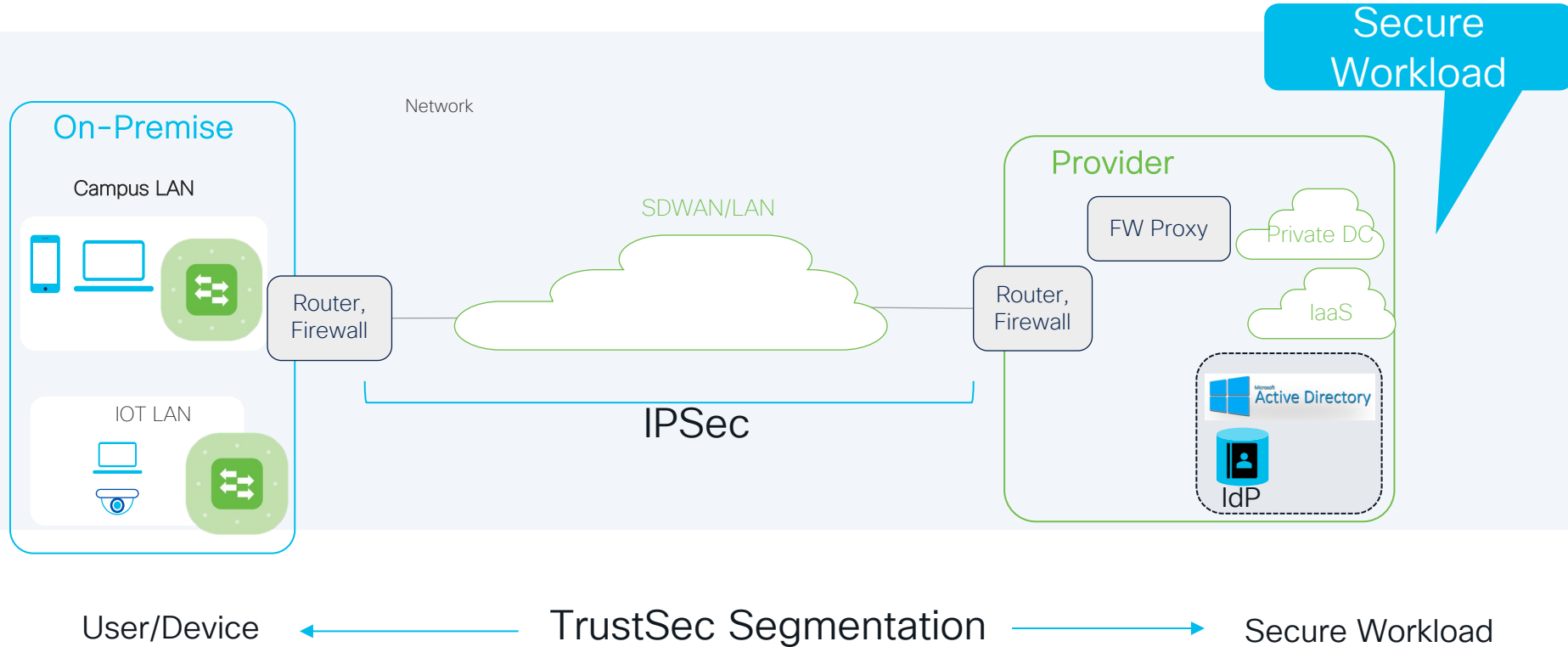
Recommendations



On-premises Access

-user & IoT to private apps

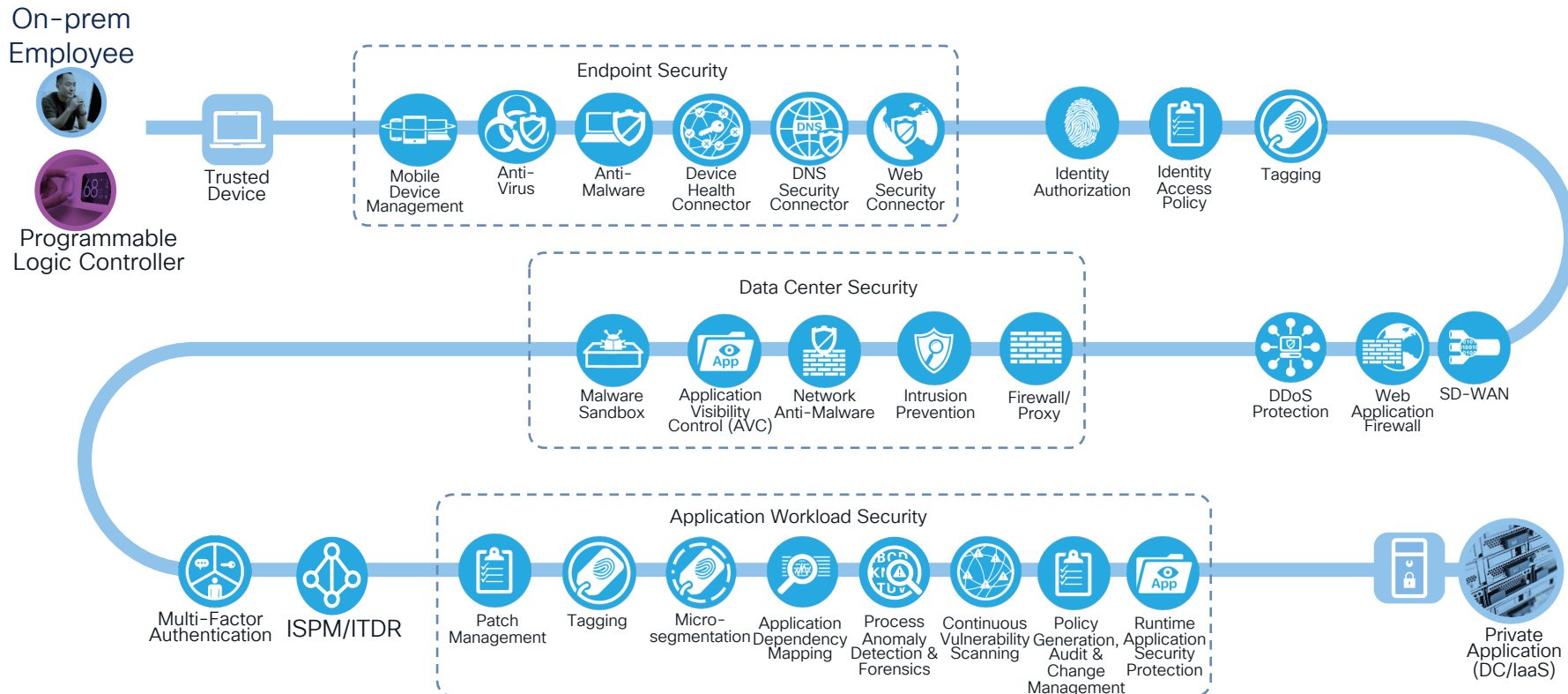
On-Premise branch user & IOT to private apps



On-Premise branch user & IOT to private apps

Business Driver	IT Risk	Cybersecurity Risk
Employee Productivity Return To Office (RTO)	Unauthorized Access Excessive Access	Aging on-premise security controls and their maturity
Intellectual property protection requires retaining legacy apps	Maintaining access to legacy apps which don't support modern authentication methods	Consistency of access control policies on a per app basis between legacy and modern apps
Business continuity requires retaining critical legacy apps	Maintaining legacy infra and controls (on-prem & cloud)	Vulnerabilities due to lack of updates/patching, no granular access controls

On-prem user & IOT to private applications (DC/laaS)



ISPM=Identity Security Posture Management
ITDR=Identity Threat Detection Management

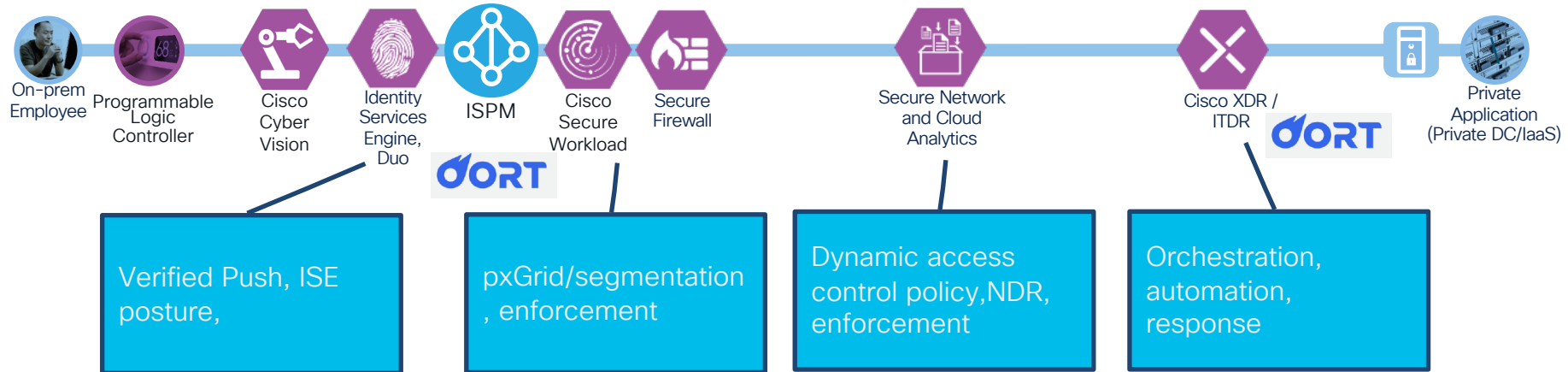
On-prem Employee and IOT to Private Apps

Recommendations

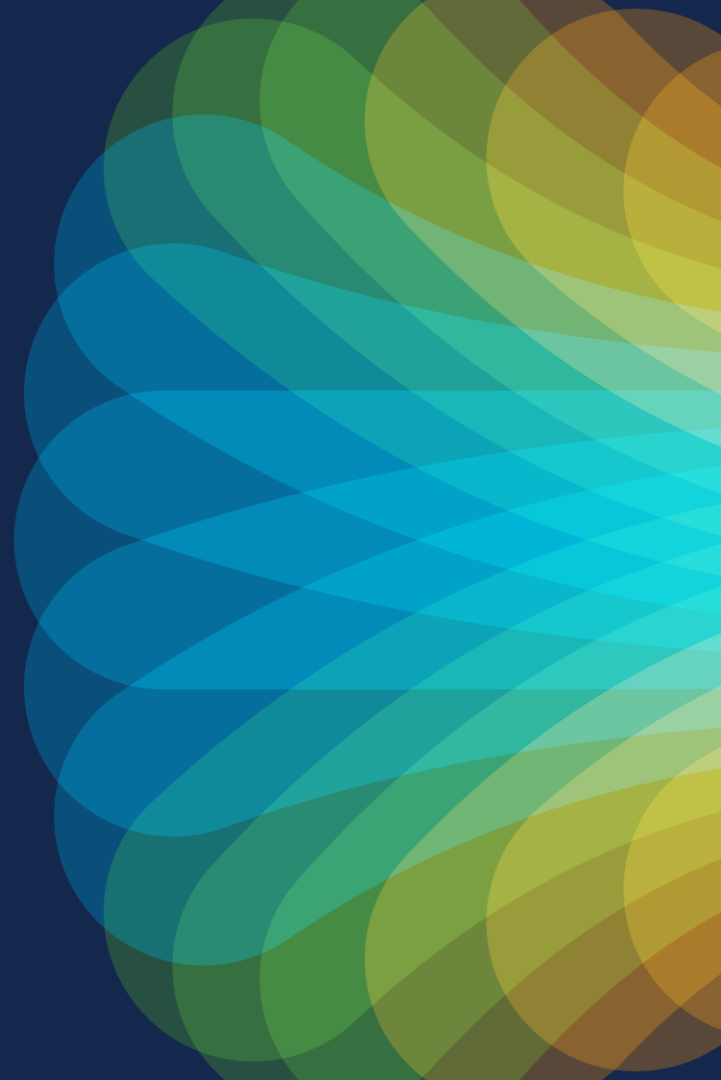
Establish &
Continuously
Verify Trust

Enforce
Trust-
Based
Access

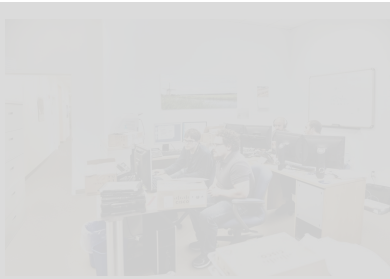
Respond to
Change in
Trust



OT Security with Cybervision



Zero Trust Use Cases



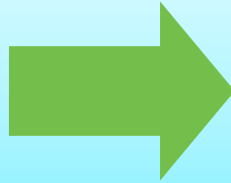
On-
Premises
User &
IoT



- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps



Remote
User



- ZT access to public SaaS
- ZTNA to private apps
- Unified ZTNA client
- Client-based VPN private app access



App-to-
App

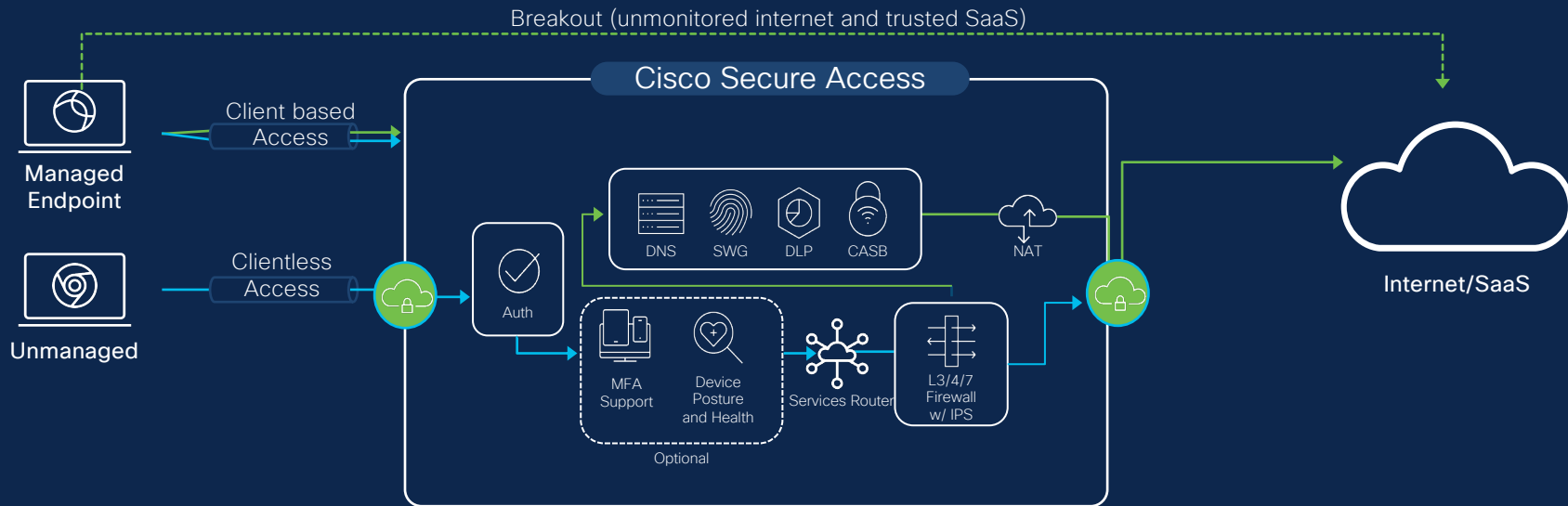


- App-to-App across multi-cloud

Secure Remote Worker

- Public SaaS/Internet

Zero Trust: Secure Remote Worker to SaaS/Internet

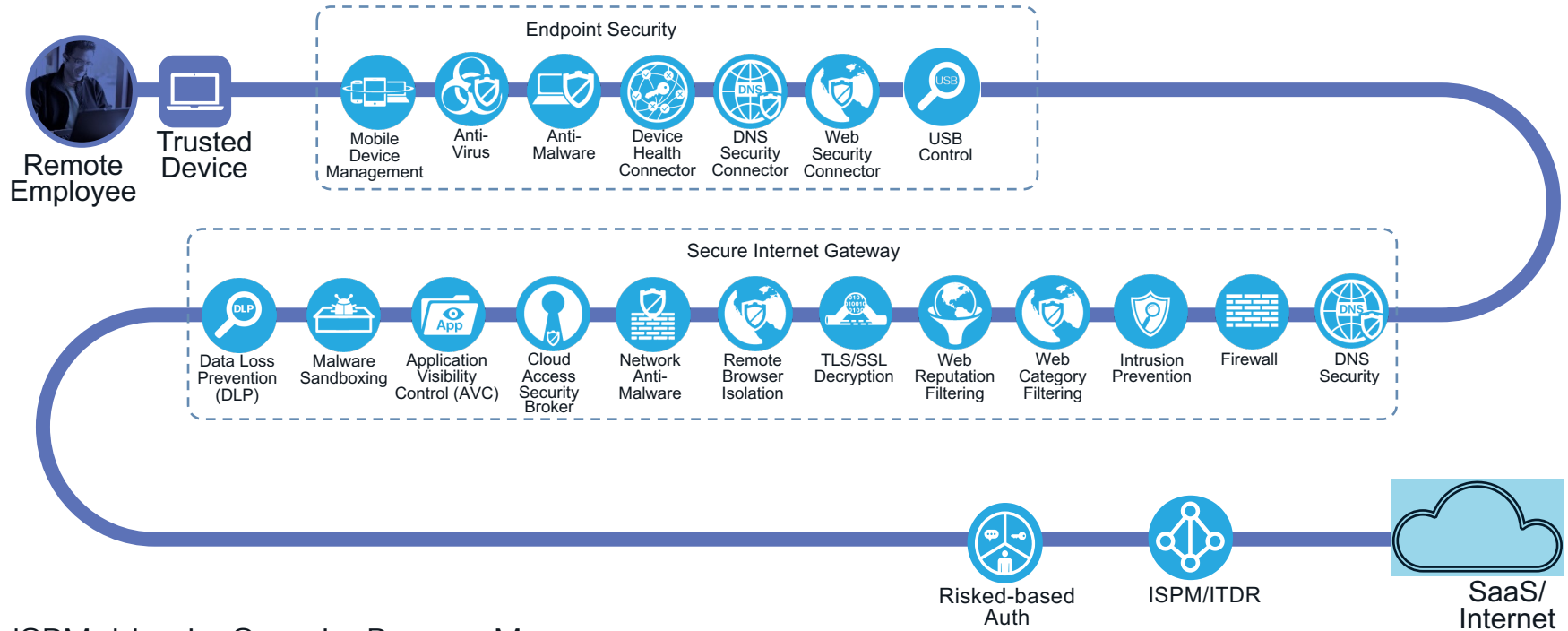


Risks: Remote Worker to SaaS/Internet

Business Driver	IT Risk	Cybersecurity Risk
Work From Home Employee Retention	Complex User support	Phishing, identity theft
Lower TCO of business applications using SaaS	IT resilience in Cloud Platform	Data leakage
Employee productivity with strict secure access	Complex administrative policy	Unauthorized Access to sensitive data. Potential Data Loss.

Remote Worker to public SaaS / Internet

Capabilities Workflow for Trusted Device

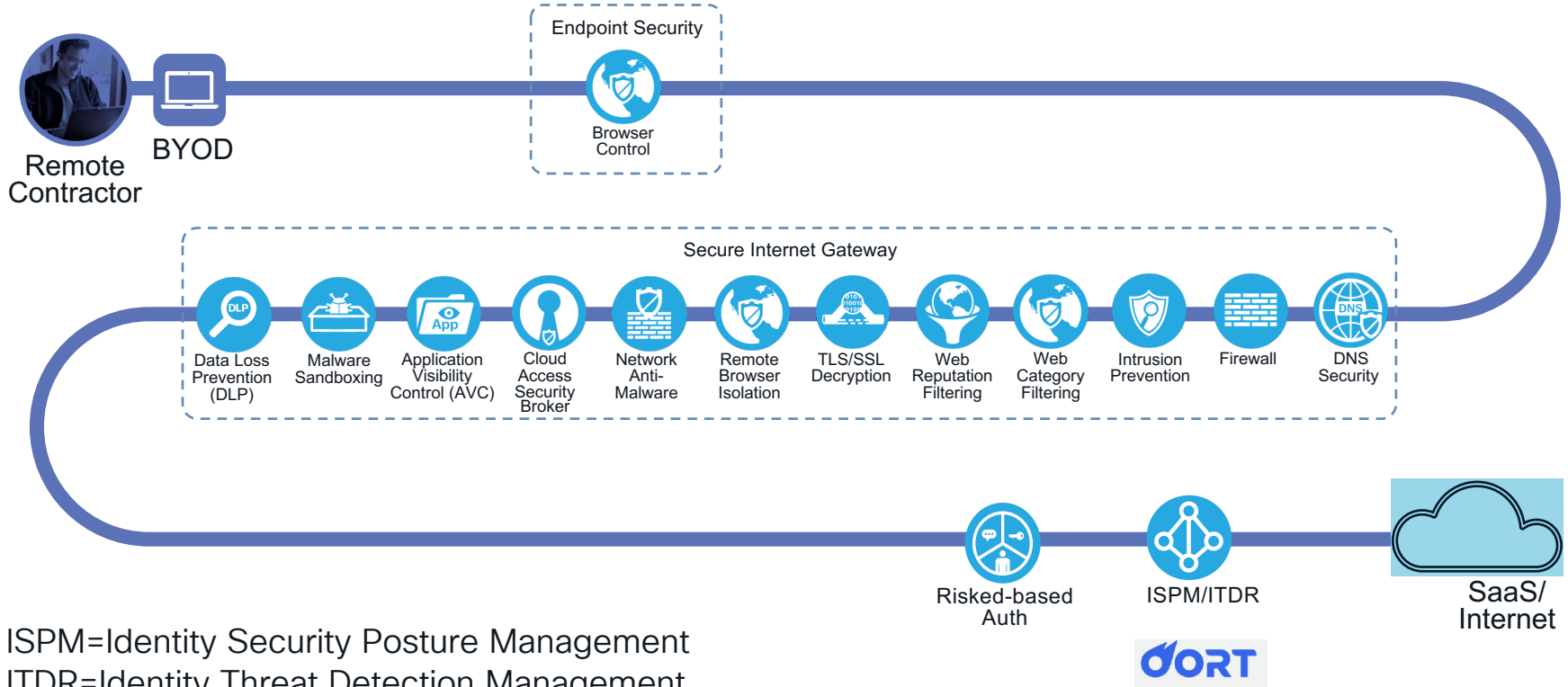


ISPM=Identity Security Posture Management
ITDR=Identity Threat Detection Management

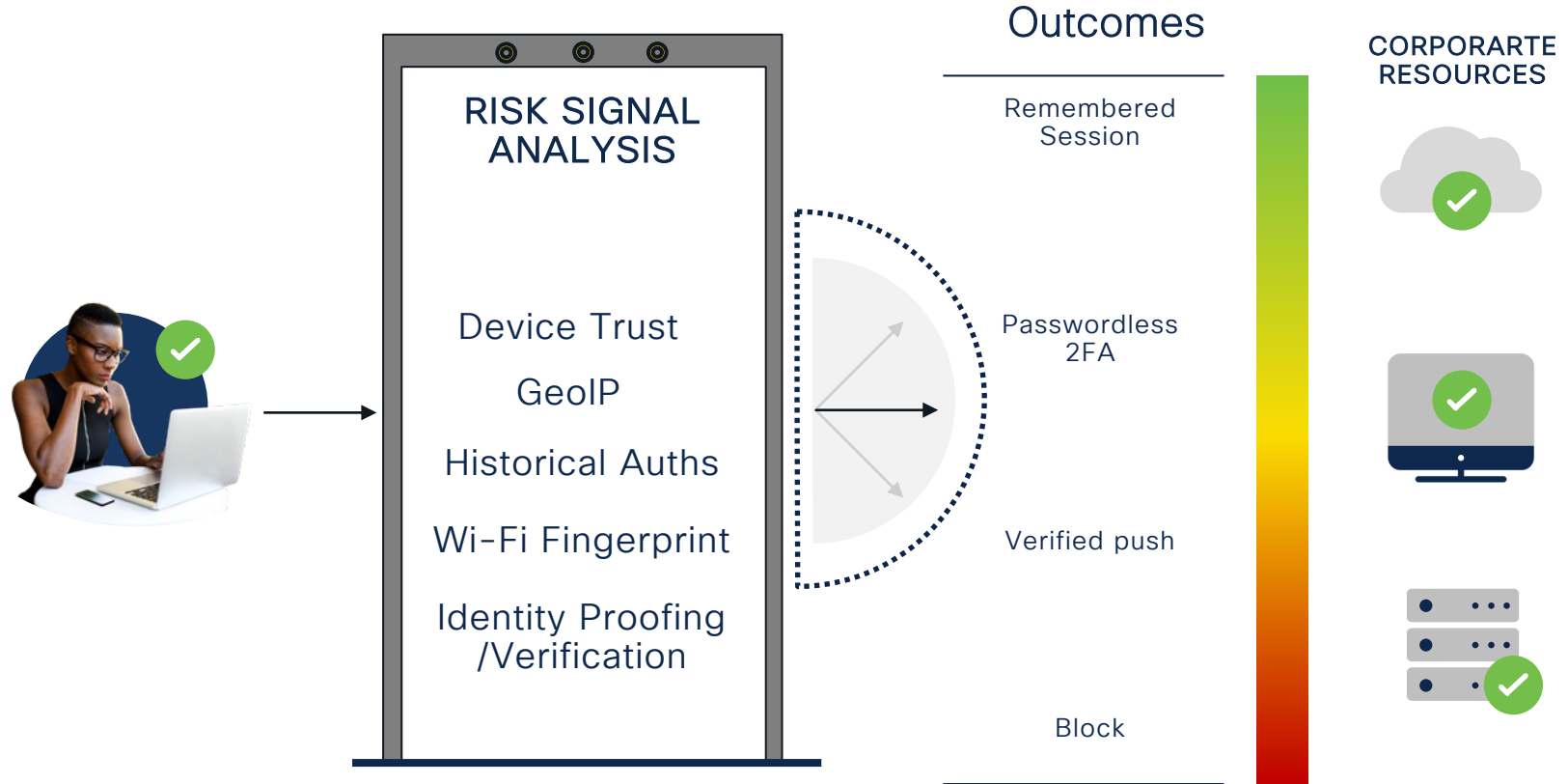
CISCO *Live!*

Remote Worker to public SaaS / Internet

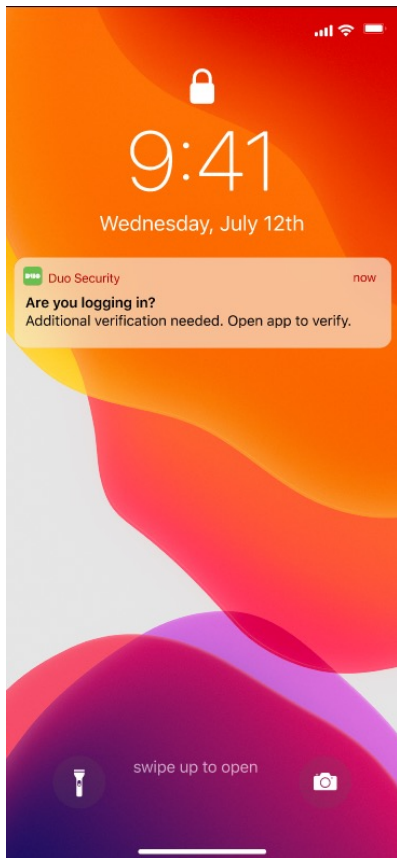
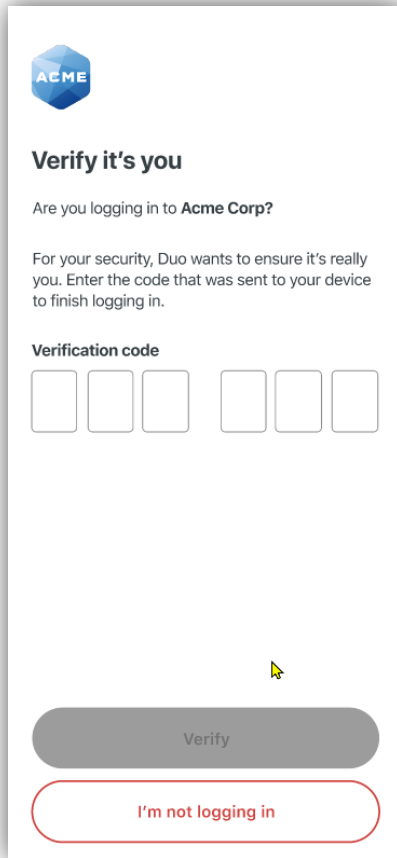
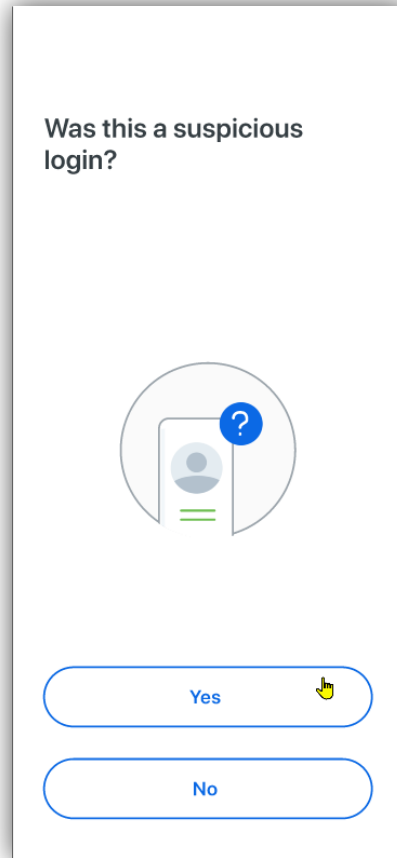
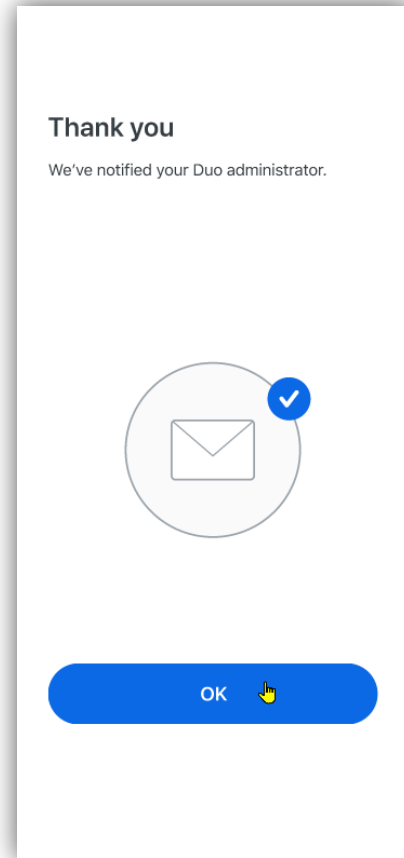
Capabilities Workflow for BYOD (Untrusted Device)



Duo Risk-Based Authentication



RBA triggers Verified Push to establish trust



Risk-Based Factors

- User marked fraud
- Push harassment (attacking a user)
- Push spray (attacking multiple users)
- Unrealistic travel
- Country code mismatch
- Novel ASN

Risk-based factor selection

 To enable these policy settings, applications must have the Universal Prompt activated or use the named "Duo Auth API" application. [Learn more about requirements for this policy.](#)

When Duo detects a [higher risk authentication](#), users will be limited to authentication methods that best protect against the risk.

☒ Limit available authentication methods based on risk ⓘ **Risk-based factor selection enabled**

[^ Hide available authentication methods](#)

Passcodes and tokens

Passcodes from the Duo Mobile app and hardware tokens, and bypass codes. API-based authentications will be limited to these methods only.

Roaming and platform authenticators

WebAuthn FIDO2 security keys with biometric or PIN verification, and authenticators or biometric sensors built into the device like Touch ID or Windows Hello.

Verified Push

A more secure version of Duo Push that requires users to enter a code from the authentication prompt on their mobile device.

Verified Duo Push Code Length

Users will get a verification code of digits through the authentication prompt.

Identity Sprawl



Microsoft
Active Directory



Azure Active Directory

okta



GitHub

CISCO *Live!*

- jelin@cisco.com
- jerrylin@gmail.com
- jeremylin@gmail.com
- Jerry@ID.onmicrosoft.com
- jerrylin949@dropbox.com
- + more

Google



 PingIdentity®

 Dropbox

 slack

Identity Threat Detection and Response (ITDR)

“...a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems.

It works by implementing detection mechanisms, investigating suspicious posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure...”

Gartner Analyst

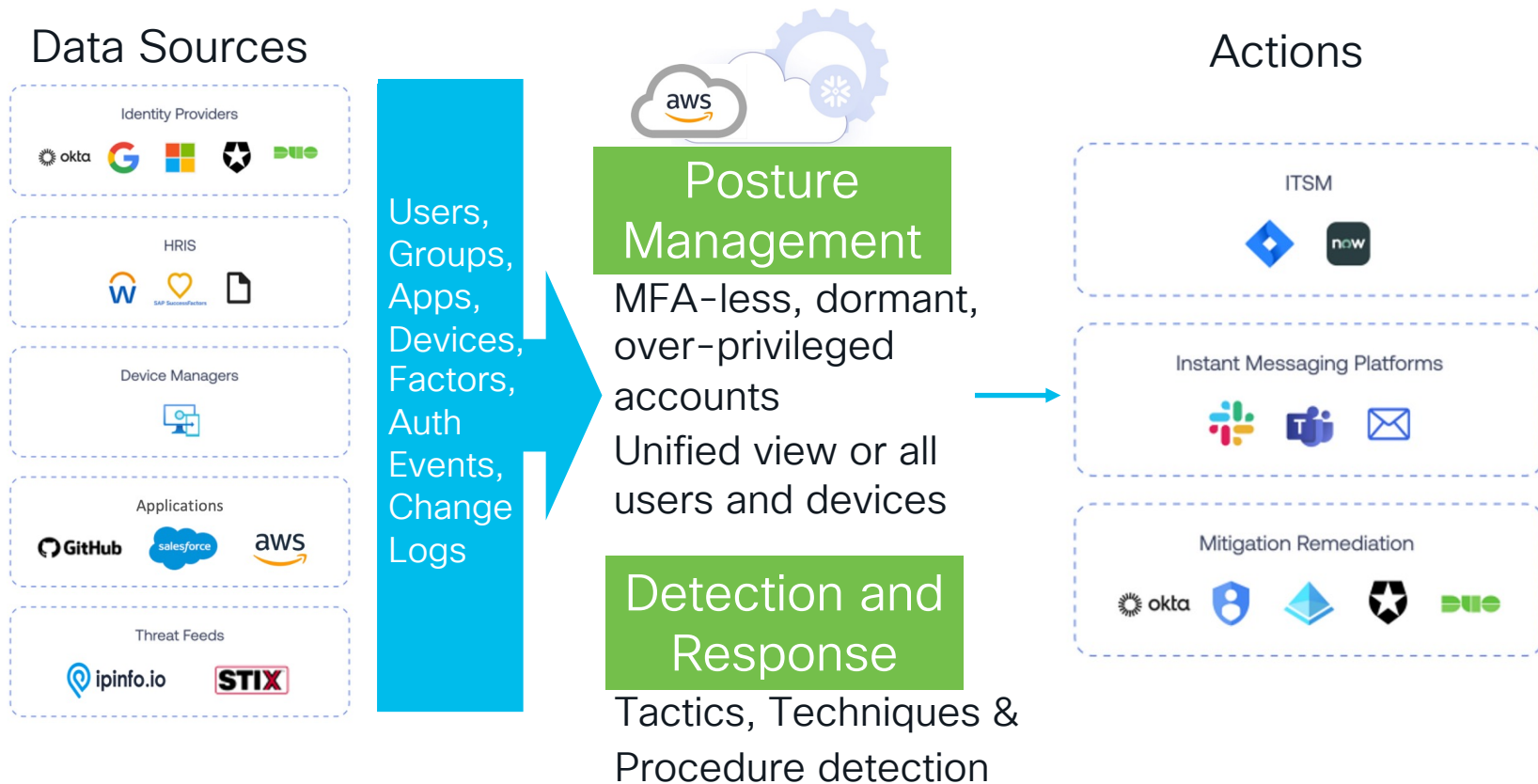
By 2026, 90% of organizations will be using some type of embedded identity threat detection and response function from access management tools as their primary way to mitigate identity attacks

Gartner: Magic Quadrant for Access Management, Nov 2022

Identity Security Posture Management (ISPM)

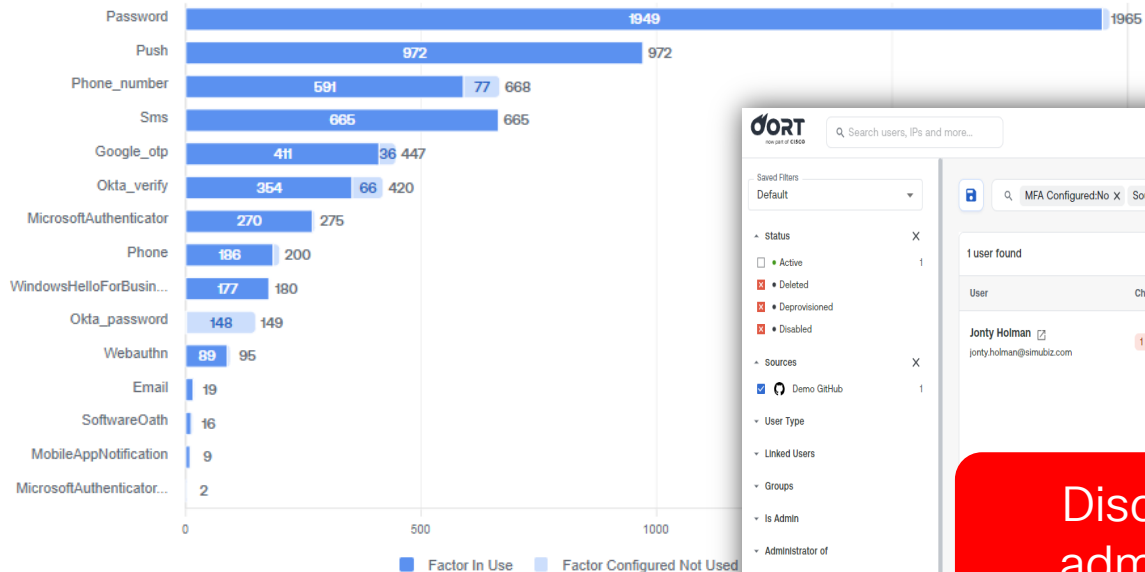
- Enables organizations to manage and protect identities proactively by monitoring and analyzing an organization's identity security posture to detect weaknesses and misconfigurations
 - No or weak MFA
 - Dormant accounts
 - Over-privileged users (especially partners, contractors, etc)
 - Administrative account overuse
 - SSO bypass
 - User inconsistencies

Cisco Identity Threat Detection & Response



Inconsistent Authentication policies

MFA Prevalence by User Count



MFA	Providers	Status
		Active

Search users, IPs and more...

Dashboard Users Checks Integrations

MFA Configured: No X Sources: Demo GitHub X NOT Status: (3 conditions) X Search users, names, groups, applications and IPs

1 user found

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Jonny Holman jonny.holman@simulabz.com	1	0	N/A	11 Hours Ago Nov 8, 2023 04:10:46	N/A	N/A			Active

Discover which Github user or administrator is not using MFA

Overall MFA compliance view

Unified User Inventory

Problem: Identity Sprawl

Likely same user

Multiple IdPs

Linked Users

User		User Type	Last Seen (UTC)	Last Location	MFA	Providers
Aalto Helmig  aalto.h@simubiz.com	• Transient	Internal	5 Hours Ago Oct 25, 2023 11:46:11	N/A		
Aalto Helmig  aalto.helmig@simubiz.com	• Active	External	19 Hours Ago Oct 24, 2023 22:00:05	Fort Lauderdale, Florida, US		
Aalto Helmig  helmig@simubiz.com	• Active	Internal	13 Hours Ago Oct 25, 2023 04:11:07	N/A		  

Identity Hygiene

- Link multiple ID's as one user based UserID, email, UPN, etc
- Prevent unauthorized logins if employee leaves organization

Merged account view

OORT new part of CISCO

Search users, IPs and more...

Dashboard Users Checks Integrations

AW Andy Winiarski admin - oort

Saved Filters: Default

▲ Status X

- Active 13
- Deleted
- Deprovisioned
- Disabled
- Inconsistent 6

▲ Sources (AND) X

- Azure AD Integration for Oort 20
- okta dev 17
- AWS Oort AWS 27
- Oort Dev Auth0 72
- Oort Duo Dev 22
- Oort GitHub 23
- Oort GSuite 33
- Oort Okta 45
- Oort Salesforce 23
- Oort Slack 38

▼ User Type

▼ Linked Users

▼ Groups

▼ Is Admin

▼ Administrator of

▼ MFA Configured

▼ Protected Population

▼ Has Tickets

Sources:(2 conditions) (AND) NOT Status:(3 conditions)

Search users, names, group, applications and IPs

<> Advanced X

19 users found

User ↓	Checks ↑	# IPs ↑	# Logins ↑	Last Seen (UTC) ↑	Last IP Address ↑	Last Location	MFA ↑	Providers
Alex Zaslavsky 2 zasalex@oort.io	2	13	72	2 Hours Ago Nov 8, 2023 17:02:43	N/A	N/A		
Andy Winiarski 1 andy@oort.io	3	17	69	5 Hours Ago Nov 8, 2023 14:07:30	N/A	N/A		
Anna Tutt anna@oort.io	3	14	4	23 Days Ago Oct 16, 2023 16:25:07	71.121.221.178	Parkville, Maryland, US		
Anton Khitrenovich 1 anton@oort.io	5	22	65	2 Hours Ago Nov 8, 2023 17:23:30	N/A	N/A		
Desiree Davies desiree.davies@oort.io	1	22	51	5 Hours Ago Nov 8, 2023 14:42:09	N/A	N/A		
Didi Dotan 1 didi@oort.io	2	13	48	3 Hours Ago Nov 8, 2023 16:44:13	N/A	N/A		
Joel Rader joel@oort.io		0	2	6 Months Ago May 23, 2023 13:20:22	N/A	N/A		
Josefa Riveros josefa@oort.io	3	15	48	A Day Ago Nov 7, 2023 20:02:33	130.44.149.163	Somerville, Massachusetts, US		
Matt Caulfield matt@oort.io	3	73	19	2 Days Ago Nov 6, 2023 17:07:52	N/A	N/A		

Consolidated
IdP view

Service-account misuse

Service Account Successful Sign In (First reported: Less than 1 day ago) [View activity from all IPs](#) ✕

Please track if this sign in is legitimate.
Consider reviewing the list on a weekly basis or connecting to the digest email.

Ip Details

5.173.12.88 ⚠ New ISP

Browser: **CHROME**

Country: **PL**

State: **Pomerania**

Other users using the same IP: 1

weirauch.fohr@simubiz.com

User Title engineer i

1 event found [View in activity](#)

Date (UTC)	Source	Event	Result	
Nov 7, 2023 20:01:44		user.session.start	Success	See in context

New unknown ISP
and IP

Detect and stop service account access from unknown locations

Inactive Guest Accounts

Remove inactive accounts to minimize attack surface

The screenshot shows the Cisco DuoORT interface. The top navigation bar includes the logo, a search bar, and links to Dashboard, Users, Checks, and Integrations. The user profile for Michael Marriott is visible. The main content area shows the user profile for Pantomima Visholdo, with tabs for Overview, Activity, Networks, Devices, Applications, Groups, and Checks. The 'Actions' menu is highlighted with a red box. A confirmation dialog is open, asking for confirmation to delete the user from Microsoft Entra ID. The dialog includes a warning that the account may be recovered before automatic deletion.

Checks / Inactive Guest Users / panto.visho@simubiz.com

Pantomima Visholdo • Active

Overview Activity Networks Devices Applications Groups Checks **Actions**

Failing Checks

Name	Result	Times Excluded	First Reported (UTC)
Inactive Guest Users	Failure	0	Nov 8, 2023 04:23:51
No MFA Configured	Failure	0	Nov 8, 2023 04:23:51

Delete user from Microsoft Entra ID (formerly Azure AD)

Are you sure you want to delete this user account from Microsoft Entra ID?

The account may be recovered before it is automatically deleted according to Microsoft Entra ID policies.

Cancel Confirm

ITDR Response

Non-compliant user can be quarantined individually or across multiple IdPs



- + Open ticket
- ↻ Reset MFA
- ➡ Log out user
- 🔒 Quarantine
- 📱 Send push verification
- ↻ Refresh User Data
- +👤 Link user

- + Open ticket
- ↻ Reset MFA
- ➡ Log out user
- 🔒 Quarantine
- 📱 Send push verification
- ↻ Refresh User Data
- +👤 Link user

Add to Quarantine Group

Are you sure you want to add this user to quarantine group?

This action will add the selected user in the quarantine group defined in your tenant settings (Quarantine). Please make sure that the proper policies are in place in your Identity Provider instance, to restrict access for users in that group.

Selected action applies to:

- 🔵 Demo Azure AD
- 🔴 Demo GSuite
- ⚙️ Demo Okta



Cancel

Confirm

Add to Quarantine Group

Are you sure you want to add this user to quarantine group?

This action will add the selected user in the quarantine group defined in your tenant settings (Quarantine). Please make sure that the proper policies are in place in your Identity Provider instance, to restrict access for users in that group.

Selected action applies to:

- 🔵 Demo Azure AD
- 🔴 Demo GSuite
- ⚙️ Demo Okta

Cancel

Confirm

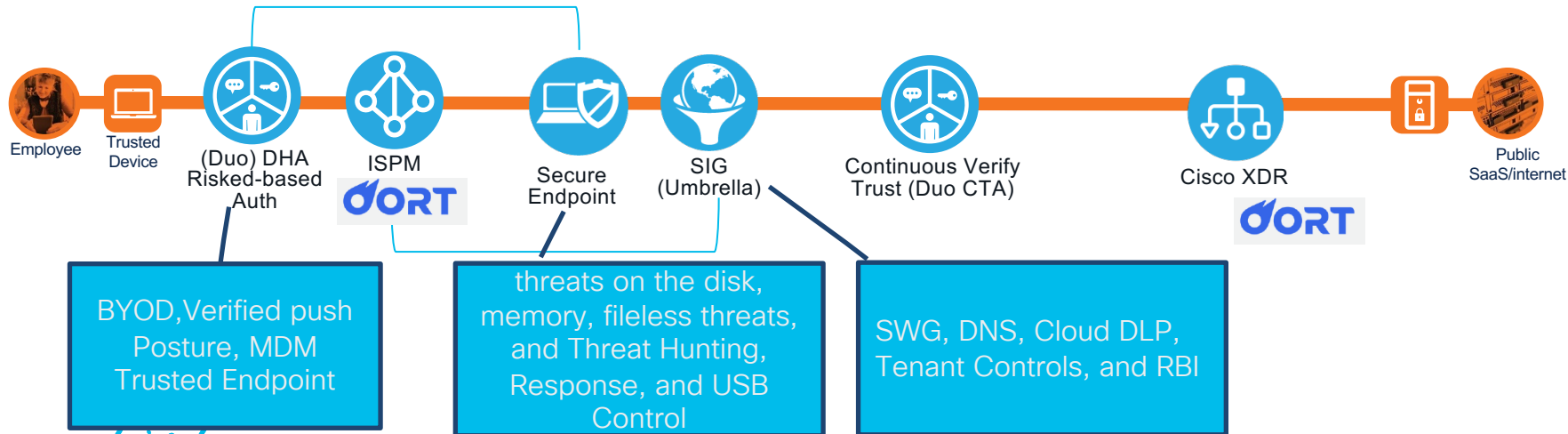
Remote user with Managed Device Accessing public SaaS / Internet

Recommendations

Establish &
Continuous
ly Verify
Trust

Enforce
Trust-
Based
Access

Respond to
Change in
Trust

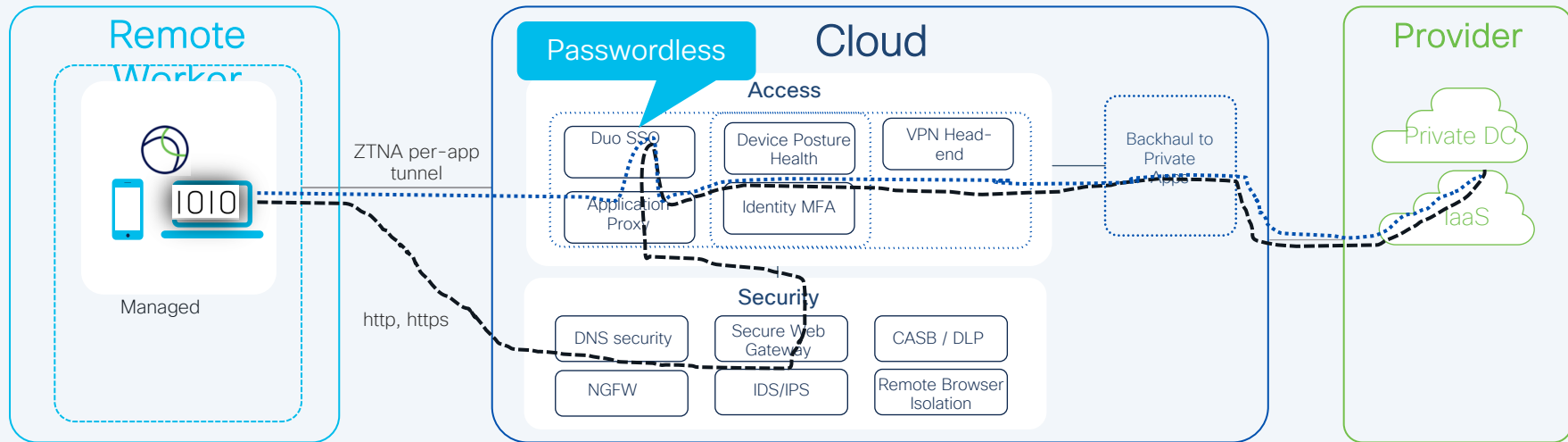


Secure Remote Worker

- ZTNA Private App Access
- Full VPN Client (optional)

Zero Trust Network Access - Remote Worker

Private app access through application proxy

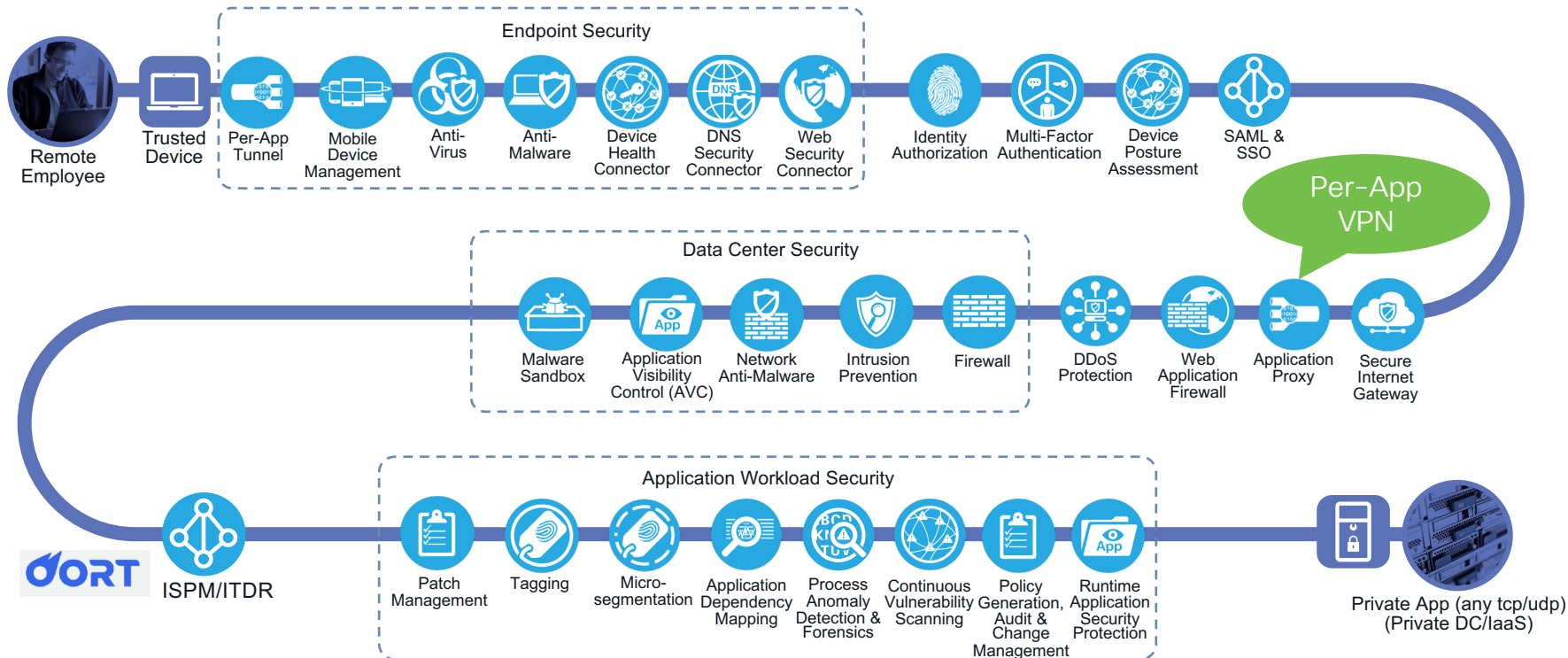


Client ZTNA: all ports/protocols

ZTNA: Remote worker to private apps

Business Driver	IT Risk	Cybersecurity Risk
Work From Home Employee Retention	Complex User support (multiple access methods, multiple agents, etc)	Phishing, identity theft, malware, SPAM, virus, etc.
Intellectual property protection requires retaining legacy apps	Maintaining access to legacy apps which don't support modern authentication methods	Consistency of access control policies on a per app basis between legacy and modern apps
Business continuity requires retaining critical legacy apps	Maintaining legacy infra and controls (on-prem & cloud)	Vulnerabilities due to lack of updates/patching, no granular access controls

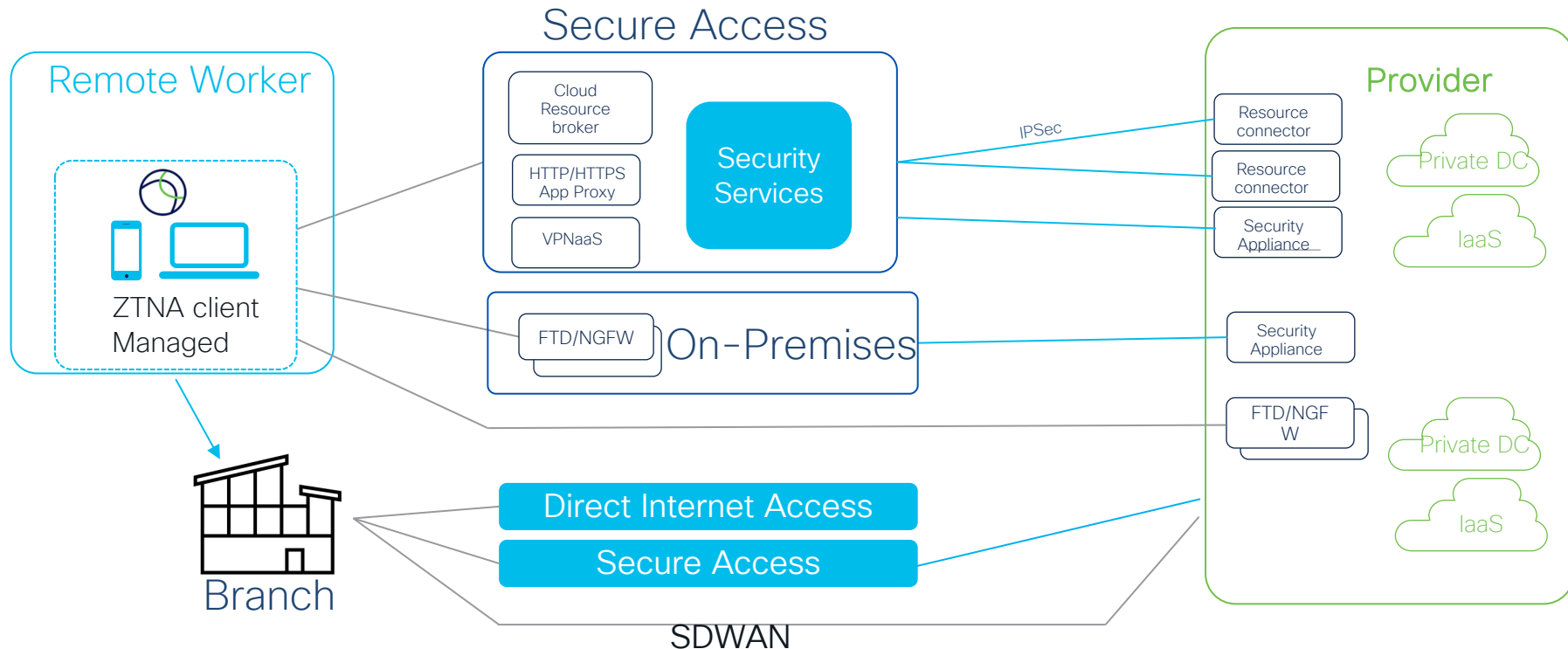
ZTNA: Remote Worker to Private Apps



ISPM=Identity Security Posture Management, ITDR=Identity Threat Detection Management

Hybrid ZTNA Architecture Options

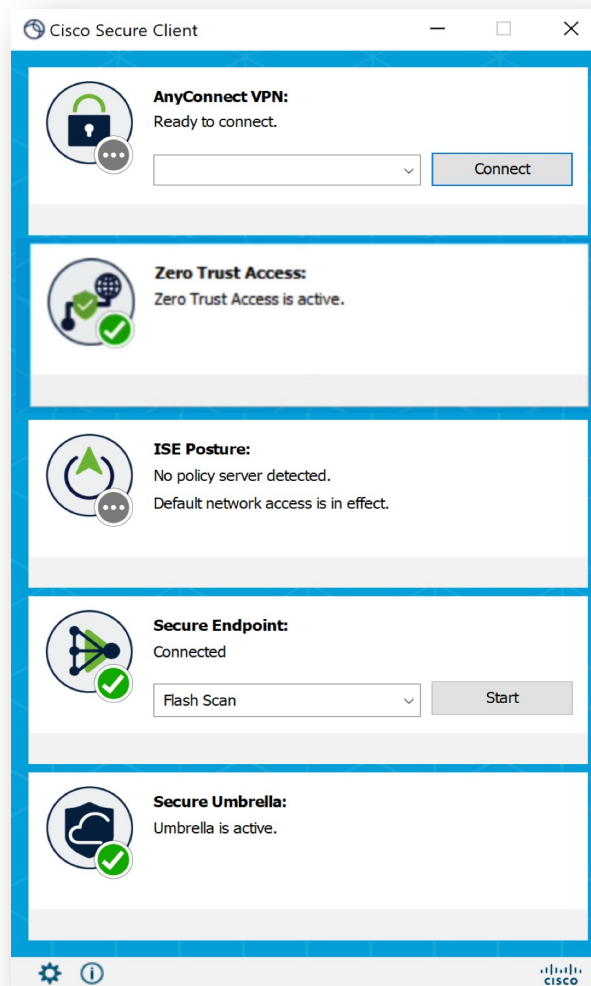
Cisco Secure Access



Cisco Secure Client Unified security services



- Cisco Secure Client = (rebranded) AnyConnect 5.x + (rebranded) Secure Endpoint 8.x
 - New combined client is more efficient than standalones
 - Cloud managed by Cisco XDR
 - Device Insights provides comprehensive inventory
-
- ✓ Simple migration
 - ✓ If you could do it in AnyConnect 4.x, you can do it in CSC 5.x
 - ✓ If you could do it with Secure Endpoint 7.x, you can do it with CSC 5.x



Unified ZTNA Client

Transparently secures the connections needed

Unified Agent or Clientless



Step 1. User Authentication and Device Trust
Step 2. Transport method is auto selected



Internet

Redirected transparently to SSE cloud



SaaS apps

CASB/DLP protections inline and via API. App bypass also supported



Private modern apps

ZTNA gives controlled access to selected applications



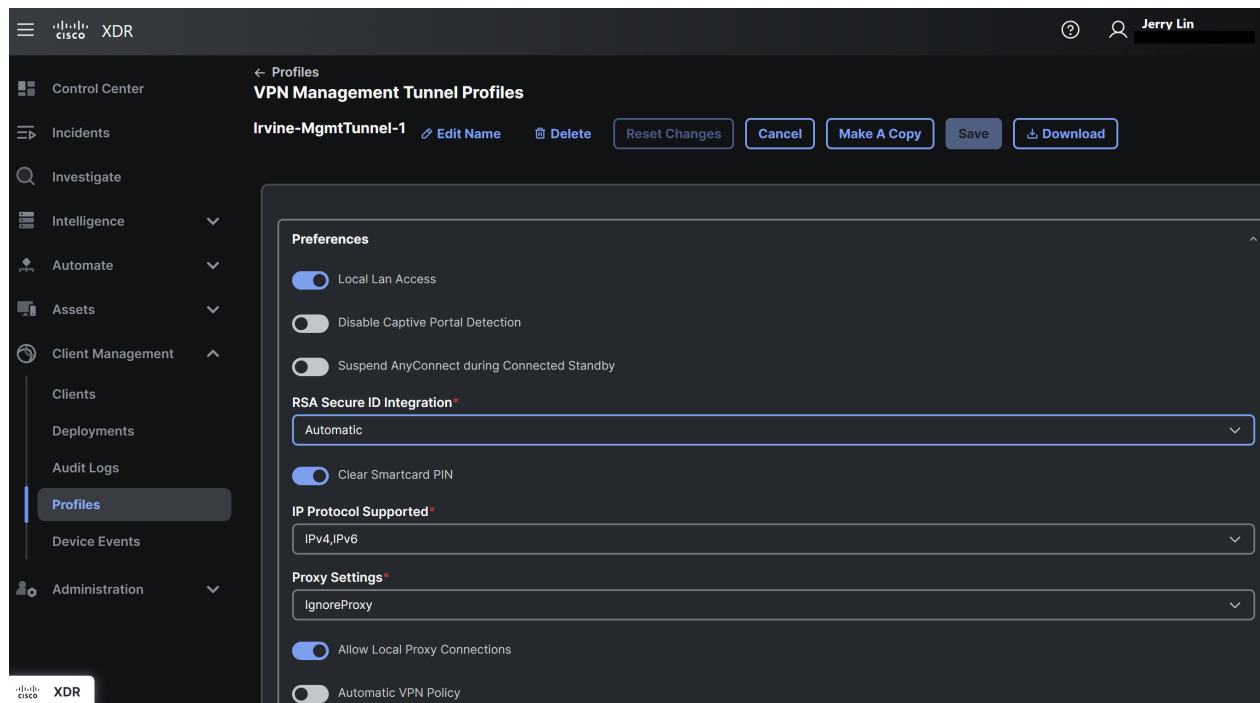
Private Traditional apps

RA-VPN gives full network access for existing applications

Managed from Cisco XDR Cloud UI

Deployments

- Groups of endpoints to get specific modules + configs
- “Groups” are coming in future version & can assign entire groups to a Deployment



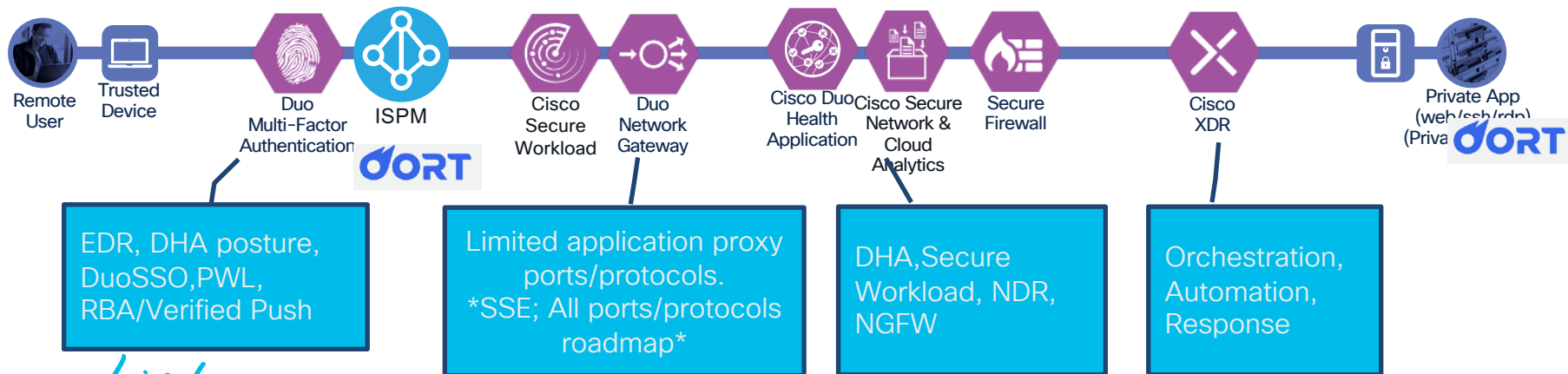
ZTNA: Remote Worker to Private App

Recommendations

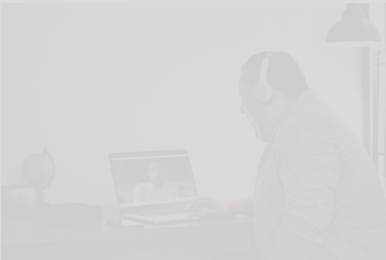
Establish &
Continuous
ly Verify
Trust

Enforce
Trust-
Based
Access

Respond to
Change in
Trust



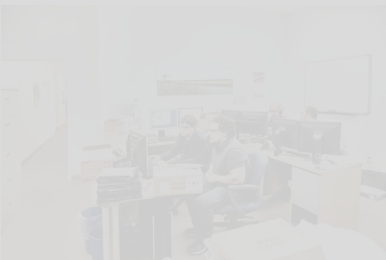
Zero Trust Use Cases



Remote
User



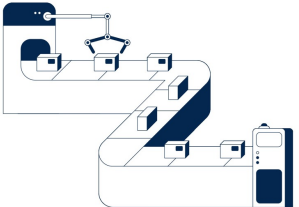
- ZT access to public SaaS
- ZTNA to private apps
- Client-based VPN private app access
- Secure Connect (VPNaaS)
- *Unified ZTNA client (roadmap)



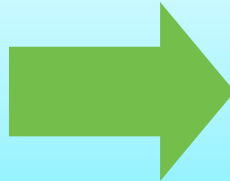
On-
Premises
User &
IOT



- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps



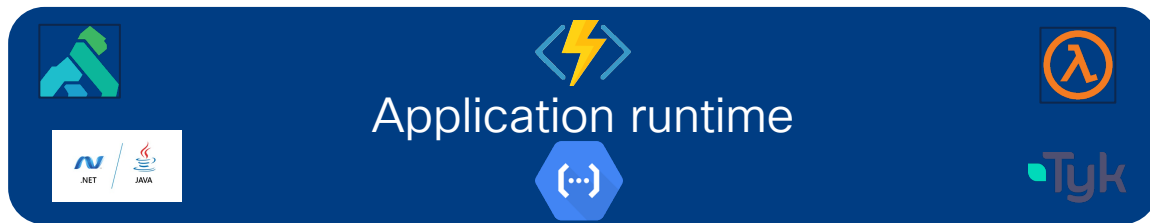
App-to-
App



- App-to-App across multi-cloud

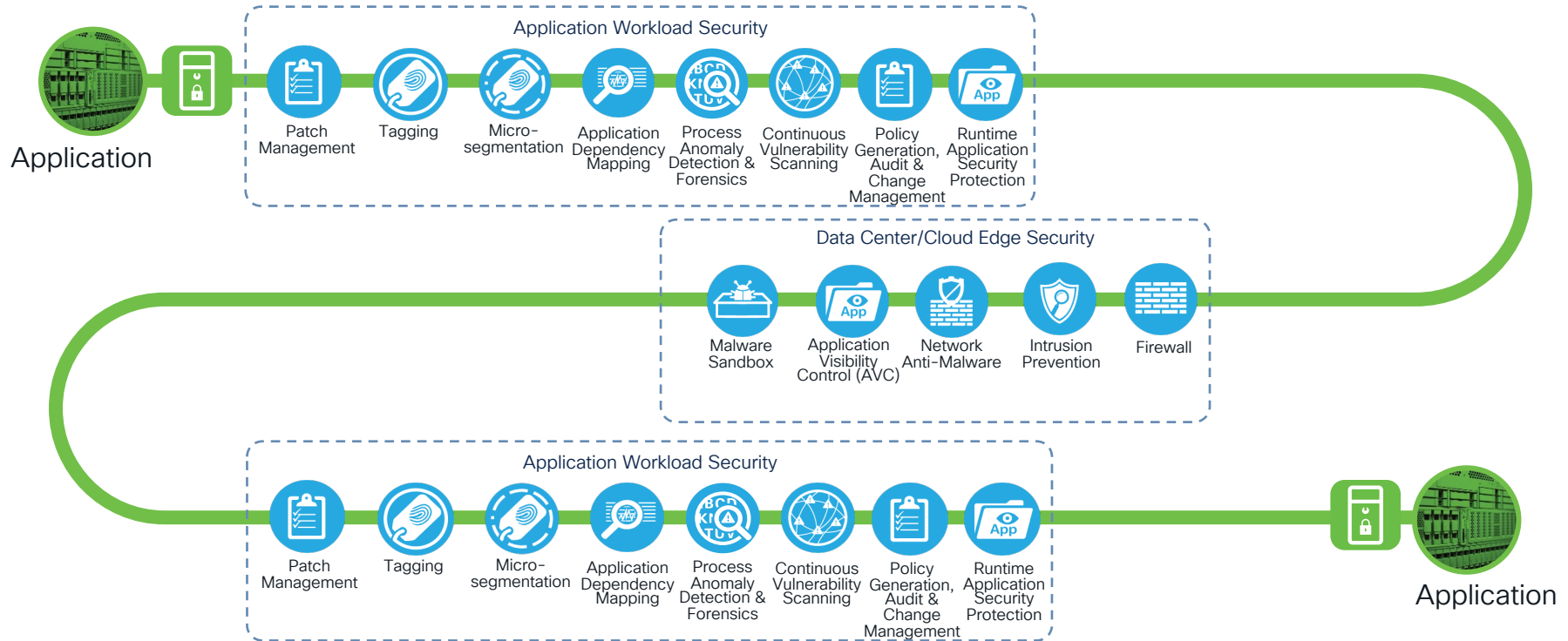
Securing private application across multi-cloud

Application Security – Critical to Zero Trust

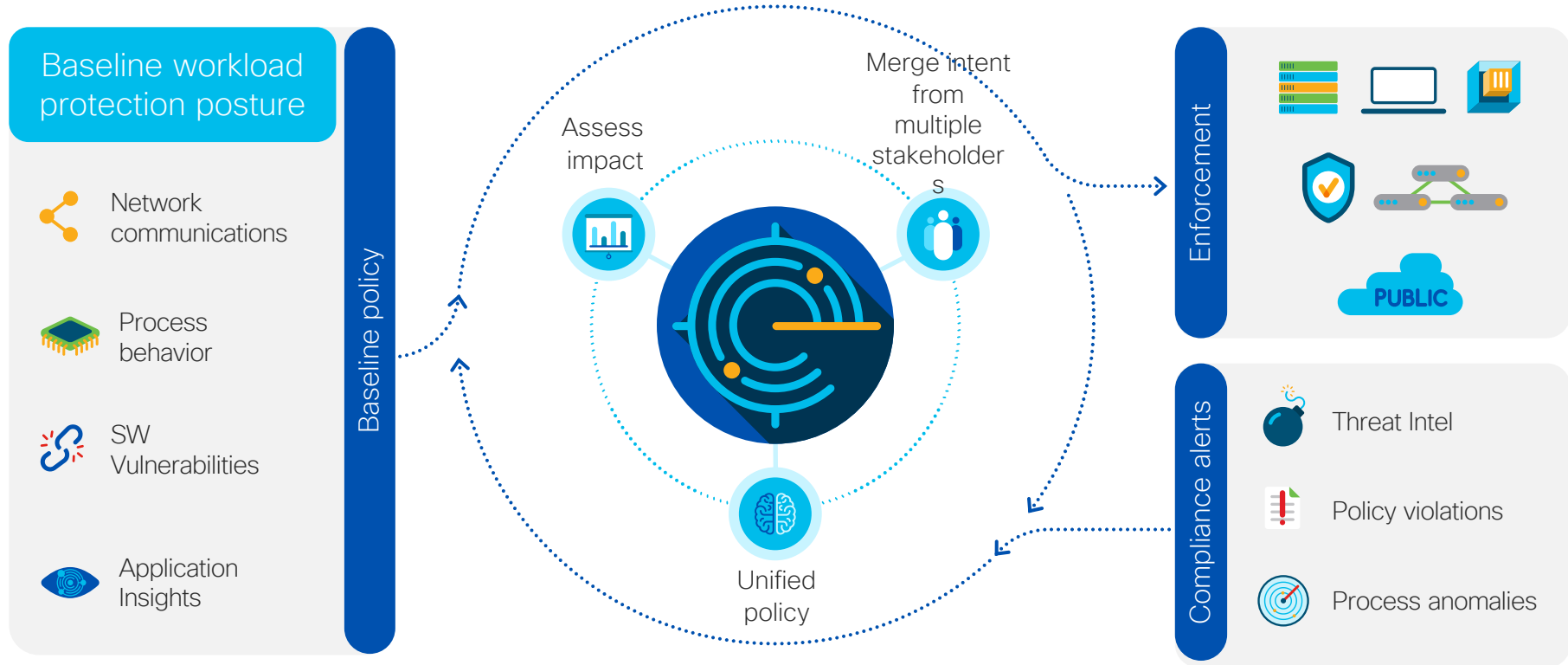


- Application code (SAST, DAST, SCA)
- Application runtime (Java, .Net, Container, API, Serverless)
- CI/CD, pod standards, image registry, Service Mesh
- App aware micro segmentation at host, macrosegmentation in cloud, advanced threat protection in firewalls

Application: API calls between microservices across Multiple Cloud Providers

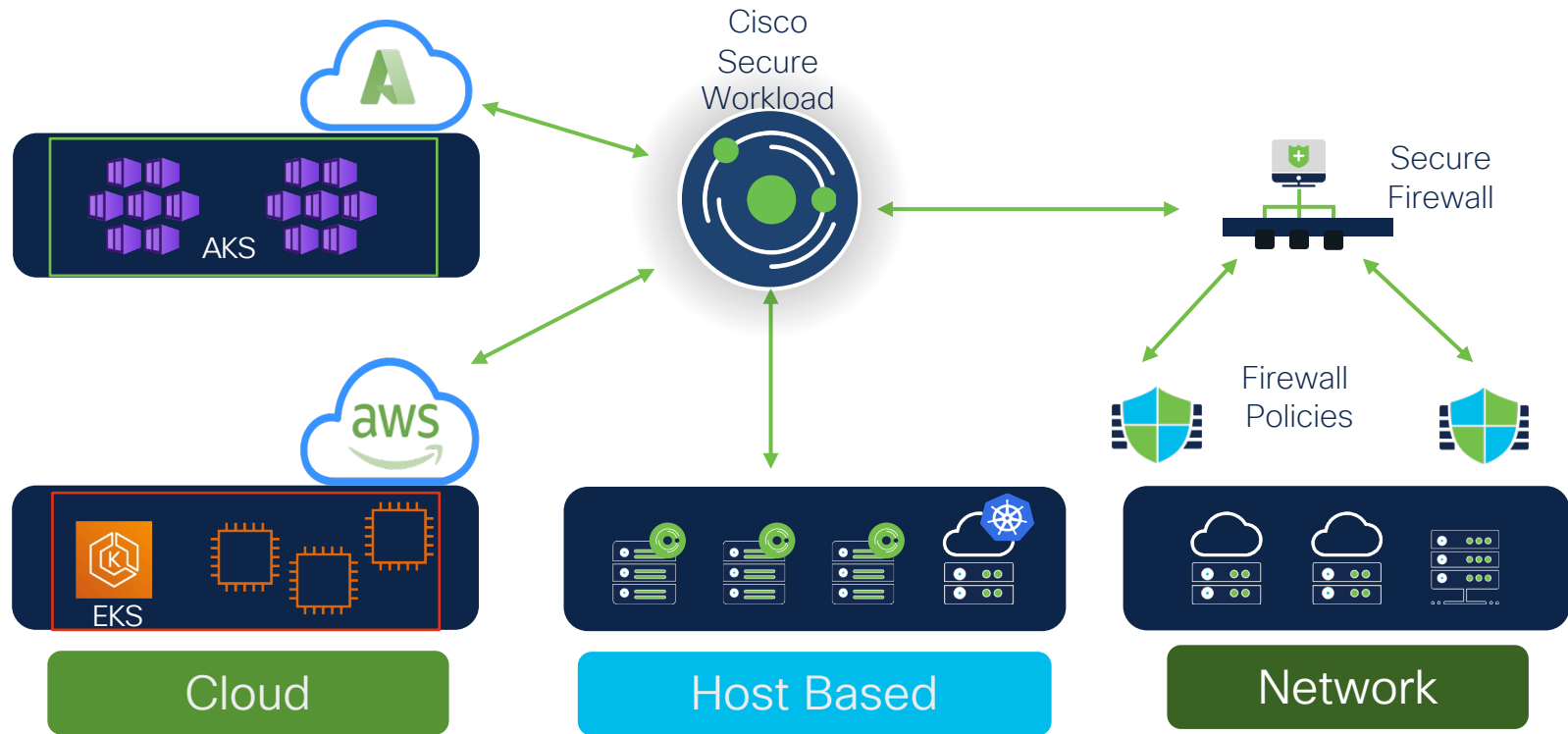


Achieving ZT framework with Cisco Secure Workload



Enforce Trust with Cisco Secure Workload

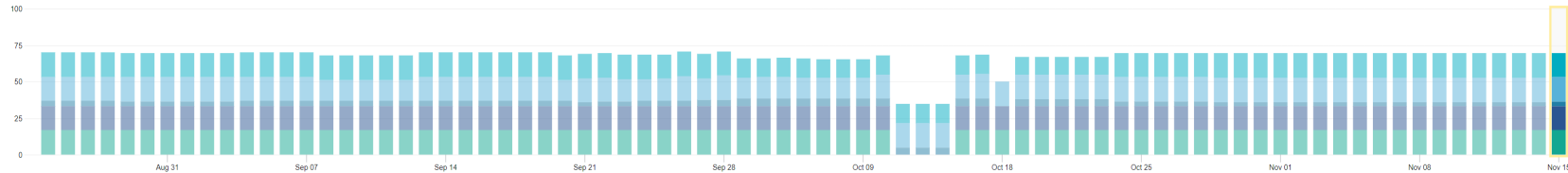
Unified Policy across Host, Network and Cloud





Security Dashboard

SCOPE SECURITY SCORE November 15, 2023 Irvine : JerryLin-Lab

[Filter Workloads](#) [Adjust Weights](#)

SCORE BREAKDOWN



N/A

Segmentation Compliance Score

Workload Score Distribution

8 total



Workloads ↓	Score ↑
Jerry-AC2	100
JumpPC4-W10	100

Vulnerability Score

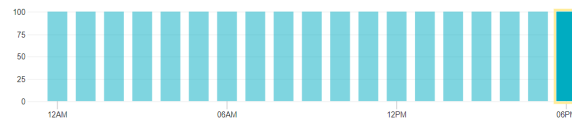
Nov 15 6:00pm

Irvine : JerryLin-Lab

Average score, 2 workloads (6 N/A)



Hourly scores - November 15, 2023

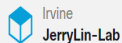


Child Scope Scores

JerryLin-Lab has no applicable descendant scopes

Scopes and Inventory

No Draft Changes



Primary Workspace

DC-Access-PCI Compliance (NEW)

Query

Address = 10.2.2.0/24 or Address = 10.3.3.0/24 or Address = 10.10.1.0/24 or * ISE_state = POSTURED or Address = 172.16.0.0/16 or Address = 10.11.11.0/24 or * orchestrator_system/virtual_network_id = vpc-04ae4072760e59d34

Delete

Edit

Ac

Filter Scopes...

12 Scopes

Irvine
3 / 11 Children Inventory: 47
Uncategorized: 14

Appledreams Corp
1 / 6 Children Inventory: 14

JerryLin-Lab
1 / 2 Children Inventory: 15
Uncategorized: 15

us-west-1
1 / 1 Children Inventory: 0

ToWinbur-Lab
0 Children Inventory: 4

All Inventory 15

Uncategorized Inventory 15

Overlapping Scopes 0

Suggested Child Scopes

Usages

Enter attributes...

Workloads 8

IP Addresses 7

8 of 8 inventory

Orchestrator Type ↑↓	Hostname ↑	Address ↑↓	OS ↑↓
	Jerry-AC2	10.2.2.13	MSWindows10Pro
	JumpPC1	10.2.2.40	MSWindows10Pro
	JumpPC4-W10	10.2.2.41	MSWindows10Enterprise
	ubuntu2-vm	10.3.3.112	Ubuntu
	VM1-jelin	172.16.10.4	Ubuntu
	W2016-AuthProxy	10.2.2.110	MSServer2016Standard
	Win2016-VM3	10.3.3.110	MSServer2016Standard
	Win2016-VM4	10.3.3.111	MSServer2016Standard

Rows per page 20

- Overview
- Organize
- Defend
- Segmentation
- Enforcement Status
- Policy Templates
- Forensic Rules
- Investigate

Workspaces

DC-Access-PCI Compliance (NEW)

PRIMARY

Version 1

View Version History

Matching Inventories 42

Policies 6

Filters 0

Conversations

Provided Services

Policy Analysis

Enforcement Status

Enforcement

Filter Policies ...

Run Quick Analysis

Add Policy

Absolute and Default Policies 5

Catch All ALLOW

Grouped 1

Ungrouped

DENY and policies for ANY protocol have different behavior in Windows firewalls when compared to Linux. See User Guide for more details.

	Rank [1]	Priority [1]	Action [1]	Consumer [1]	Provider [1]	Protocols And Ports [1]	
	Default	50	DENY	Kill_Switch	Finance Servers	Any	
	Default	90	DENY	CVE-2021-34480	PCI	Any	
	Default	90	DENY	Irvine : JerryLin-Lab	CVE 2022-30190	ICMP ...1 more	
	Default	92	ALLOW	JumpPC1-non-PCI	non-PCI server	ICMP	

Filter

CVE 2022-30190

Filter Actions

Query

Package CVE = 2022-30190

Scope

Irvine:JerryLin-Lab

Restricted

No

Provides Service

No

View Filter Details

servers identified with CVE 2022-30190

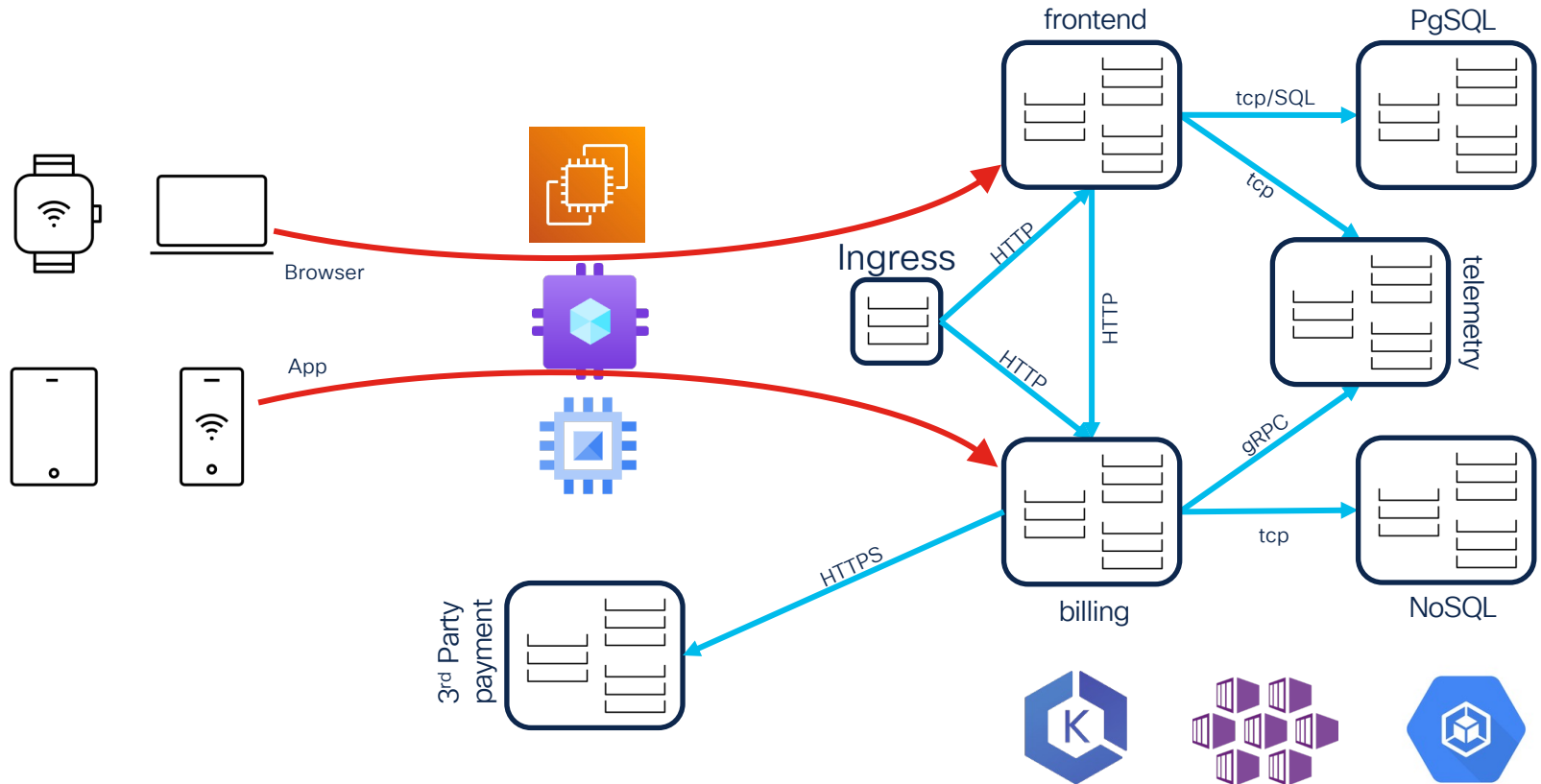
Workloads 4

Address	Hostname	OS
10.3.3.111	Win2016-VM4	MSServer2016Standard
192.168.1.241	TomHomeLabDC	MSServer2019Standard
10.2.2.110	W2016-AuthProxy	MSServer2016Standard
10.3.3.110	Win2016-VM3	MSServer2016Standard

IP Addresses 0

Achieving ZT within Cloud Native Apps

Application Architectures have evolved



OVERVIEW K8SHIELD

All clusters

Tour
 Refresh
 Generate Report

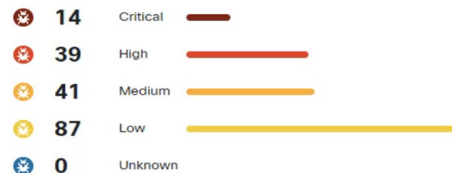
Top security risks

PODS APIS SERVERLESS

nginx	HIGH
front-end	HIGH
payment	HIGH
queue-master	HIGH
session-db	HIGH

Vulnerabilities

PODS SERVERLESS



Permissions (RBAC)

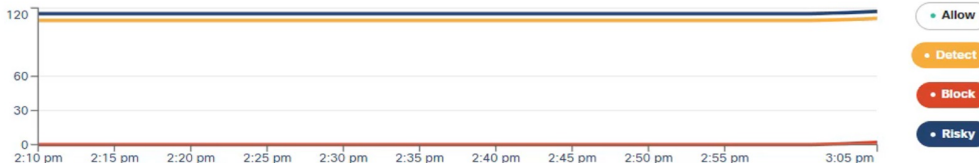
Show system roles ☐



Events

EVENTS CONNECTIONS PODS

Runtime view
 Policy
 Last hour



9 Protected Namespaces



24 Protected Pods



1 Expansions

Panoptica; MITRE ATT&CK Framework

DASHBOARD

OVERVIEW **K8SHIELD**

LAST UPDATE: Jan 27th 2023, 24:12

5 CLUSTER: All clusters

16/16 COMPROMISED NAMESPACES: Finance/finance +15 All

Generate Report

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIALS ACCESS	DISCOVERY	LATERAL MOVEMENT	IMPACT
✓ PUBLIC FACING PRIVILEGED WORKLOAD	△ CONTAINER SERVICE	△ WRITABLE HOSTPATH MOUNT	△ PRIVILEGED PODS/ ROOT PODS	△ CLEAR CONTAINER LOGS	△ EXPOSE KUBERNETES SECRETS	✓ EXPOSED KUBERNETES DASHBOARD	△ CLUSTER INTERNAL NETWORKING	△ DATA DESTRUCTION
✓ EXPOSED KUBERNETES DASHBOARD	△ DEPLOY CONTAINER	△ KUBERNETES CRONJOB CREATION	△ PRIVILEGES ESCALATION ENABLED	△ DEPLOY CONTAINER	△ SERVICEACCOUNT ACCESS	△ CONTAINER RESOURCE DISCOVERY	✓ ACCESS TILLER ENDPOINT (HELM 2)	
△ VULNERABLE WORKLOADS	△ SSH SERVER RUNNING INSIDE CONTAINER		△ RESTRICT ADMIN BINDING ABILITY	△ DELETE KUBERNETES EVENTS			✓ EXPOSED KUBERNETES DASHBOARD	
△ UNAUTHORISED REGISTRIES USAGE			△ MULTIPLE CLUSTER ADMINS				△ CORE DNS POISONING	
△ SUSPICIOUS DEPLOYMENT			△ ACCESS THE KUBERNETES API SERVER					
△ COMPROMISED IMAGES IN REGISTRY			△ WRITABLE HOSTPATH MOUNT					

Continuous Integration Risk Visibility

The screenshot displays the Cisco Panoptica CI/CD interface. The left sidebar contains navigation options: Dashboard, Navigator, CI/CD (highlighted), Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment, and an ADMINISTRATION section with K8s Controllers, Audit, and System. The main content area is titled 'Images' and shows details for a Docker image: `docker.io/broadcaststorm/vulnerable-openssl`. Below this, a table lists vulnerabilities. Two high-severity (7.5) CVEs are shown: CVE-2022-3602 and CVE-2022-3786, both with a 'Fix available' status. The table columns are FINDINGS, NAME, FIX AVAILABILITY, and DESCRIPTION. The interface also includes filters for 'Active only' and 'Acknowledged only', and a pagination bar at the bottom showing page 1 of 1.

CI/CD

< Images

docker.io/broadcaststorm/vulnerable-openssl

Image Hash: 0199701686707c1621120c49393d0ce9ac34e8b3824001e7107b00722007
Image Tags: ubuntu-20221003

VULNERABILITIES IMAGE LAYERS CIS BENCHMARK PACKAGES & LICENSES

Active only ☐ Acknowledged only ☐

Image layer: Select... Fixable only: No

Acknowledge Refresh Columns

FINDINGS	NAME	FIX AVAILABILITY	DESCRIPTION
☐ 7.5 high	CVE-2022-3602	Fix available	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).
☐ 7.5 high	CVE-2022-3786	Fix available	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the '.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

PAGE 1

50 100 200 PER PAGE

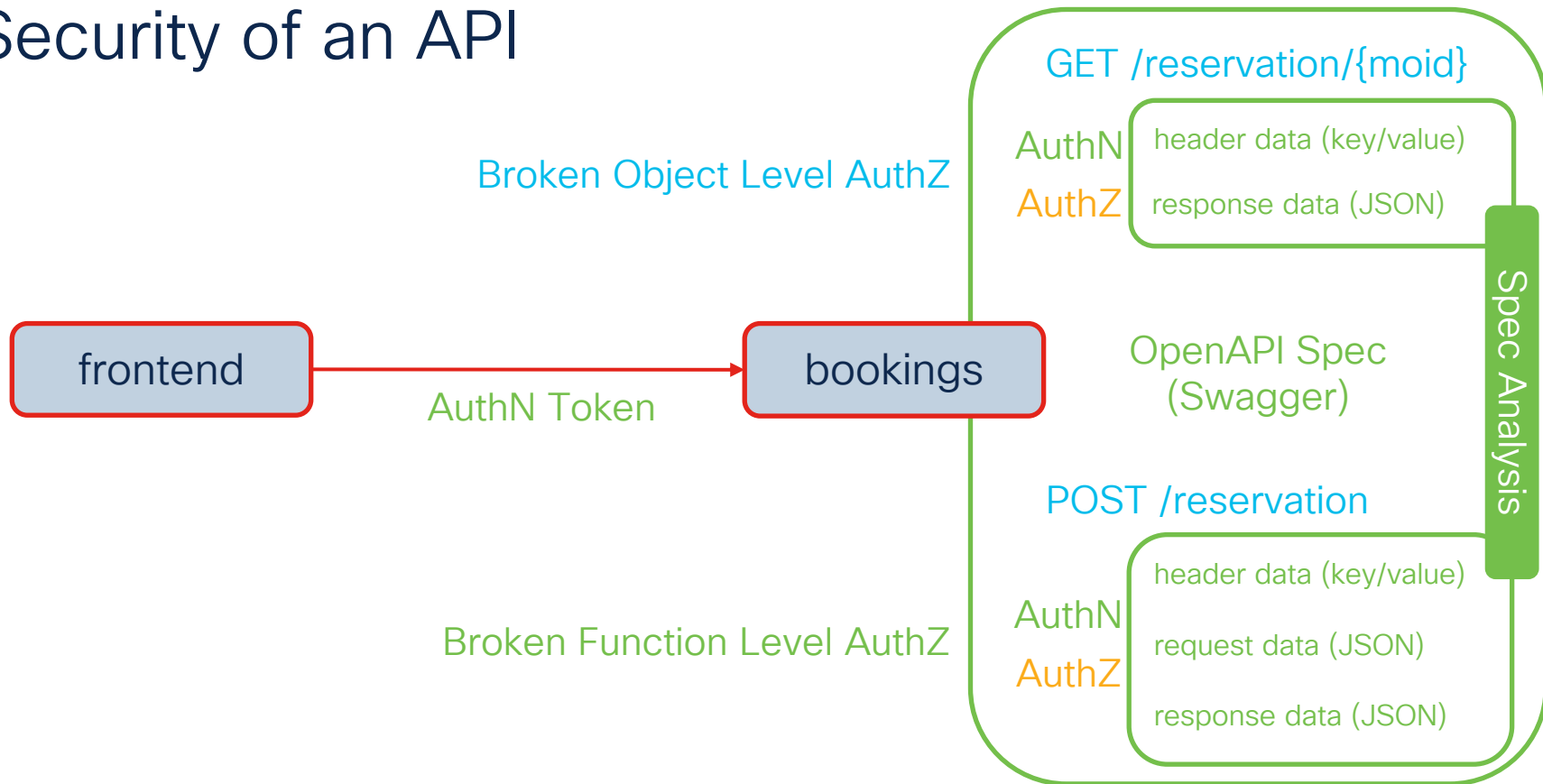
Serverless Comprehensive Risk Findings

The screenshot displays the Cisco Panoptica Serverless interface. On the left, a dark blue sidebar contains navigation links: Dashboard, Navigator, CI/CD, Runtime, APIs, **Serverless** (highlighted with an orange box and a red '1'), Deployments, Policies, Risk Assessment, and an ADMINISTRATION section with K8s Controllers, Audit, and System. The main header is dark blue with the 'SERVERLESS' title, a help icon, 'API', 'DEMO USER', and a user profile for 'James Miller' (Global Administrator). The main content area is titled '< Functions' and shows a function named 'billing' (highlighted with an orange box and a red '2'). Below the function name are four tabs: **DETAILS & RISKS** (highlighted with an orange box), VULNERABILITIES, ROLE POLICIES, and SECRETS. Under the 'DETAILS & RISKS' tab, a green box indicates 'Function risk: High'. Below this, a green-bordered box contains two findings: 'The function has a vulnerability of severity HIGH or CRITICAL' and 'Environment variable with the name: PASSWORD should be defined as secret'. To the right, the 'Function details' section shows the ARN 'arn:aws:lambda:us-east-1:872186993740:function:billing'. Below this is a table with two rows: one for 'CLOUD PROVIDER' (AWS), 'REGION' (eu-south-1), and 'CLOUD ACCOUNT NAME' (Production); and another for 'RULE NAME' (Default rule) and 'RULE ACTION' (Allow).

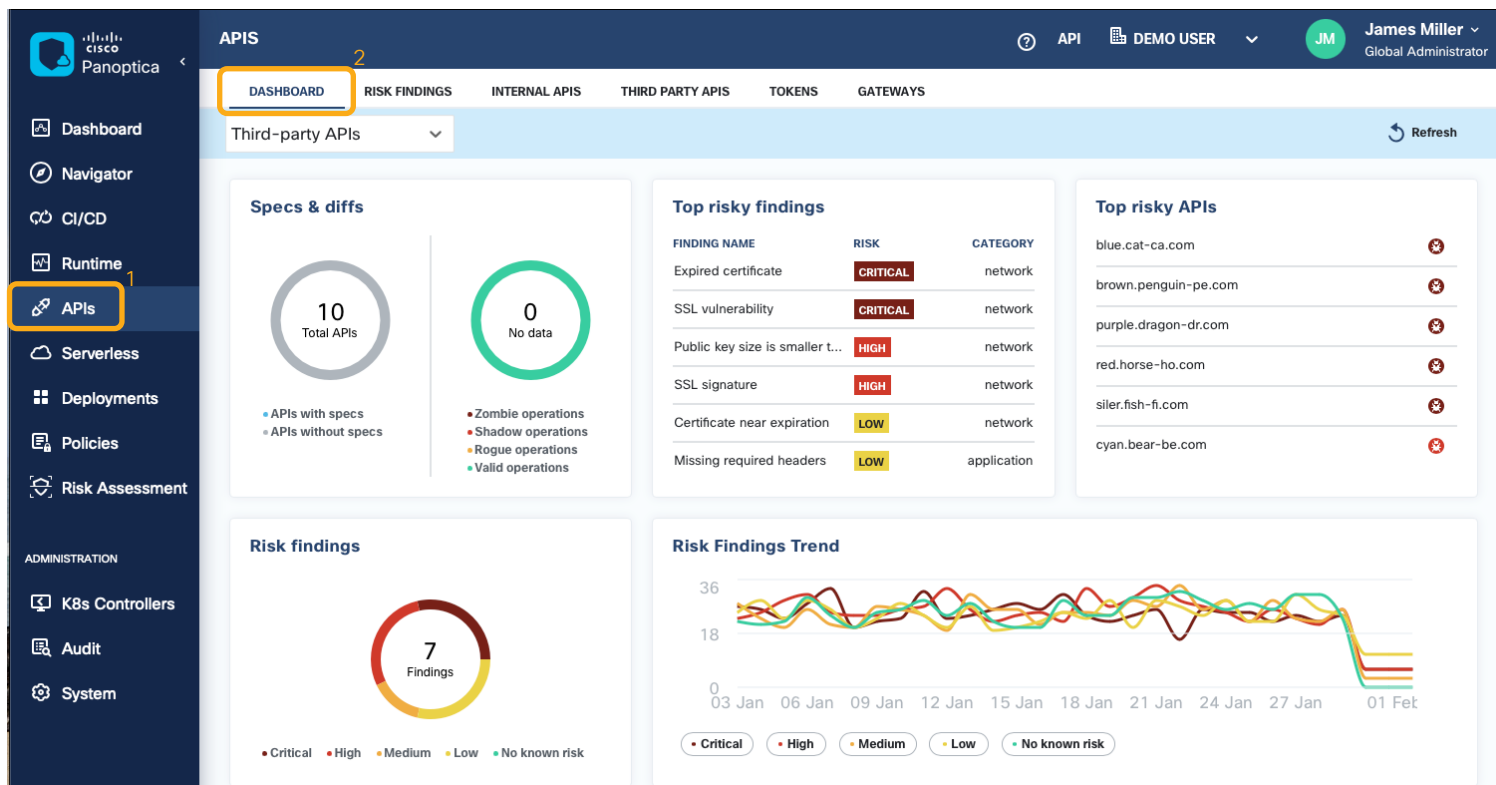
CLOUD PROVIDER	REGION	CLOUD ACCOUNT NAME
AWS	eu-south-1	Production

RULE NAME	RULE ACTION
Default rule	✓ Allow

Security of an API



API Security Dashboard – Third party APIs



API Risk Findings

APIS

RISK FINDINGS INTERNAL APIS EXTERNAL APIS TOKENS GATEWAYS

Finding name Risk Category Sources Affected element

Detected findings only ☐

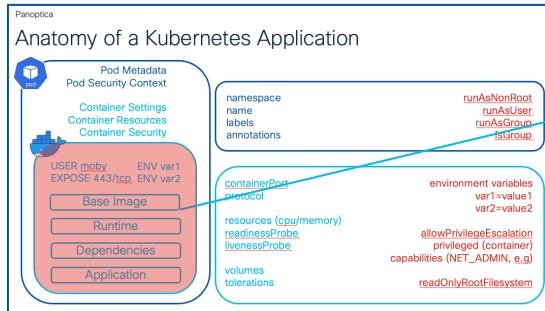
FINDING NAME	RISK	AFFECTED ELEMENTS	CATEGORY	SOURCE	DESCRIPTION	MITIGATION
SSL vulnerability	CRITICAL	blue.cat-ca.com pink.snake-sn.com ...3 more	network	shodan	SSL is vulnerable to a CVE.	Review the CVE and perform the recommended action(s) for fixing the issue.
Expired certificate	CRITICAL	orange.dog-do.com pink.snake-sn.com ...1 more	network	shodan	This certificate has expired. While the traffic to the host is still encrypted, it may be vulnerable to new attacks such as man-in-the-middle attacks. Individual are also vulnerable to fraud and identity theft.	Obtain and install an updated certificate from an industry certificate authority as soon as possible.
Missing security scheme both in operation and globally	CRITICAL	carts catalogue ...3 more	api-specification	oas_analyser	Spec analyzer detected that the spec does not define neither a global nor a operation specific security scheme. It is highly recommended that all API operations support a security scheme, which means supporting proper authentication and authorization. In principle this can be achieved without a global security scheme, by specifying a security scheme for each API operation. However it is a good practice to have a global one instead of individual ones. This makes maintenance easy and avoids that new API operations are added without any security scheme association.	Make sure all API operations have a security scheme associated and as a good practice add a global security scheme.
SSL signature	HIGH	blue.cat-ca.com red.horse-ho.com ...1 more	network	shodan	The weak signature algorithm is known to be cryptographically weak and vulnerable to collision attacks. Attackers can observe the encrypted traffic between your website and its visitors by leveraging the use of this vulnerability.	Obtain and install an updated certificate using SHA-2 from an industry certificate authority as soon as possible.

PAGE 1

50 100 200 PER PAGE

Deployment Policy

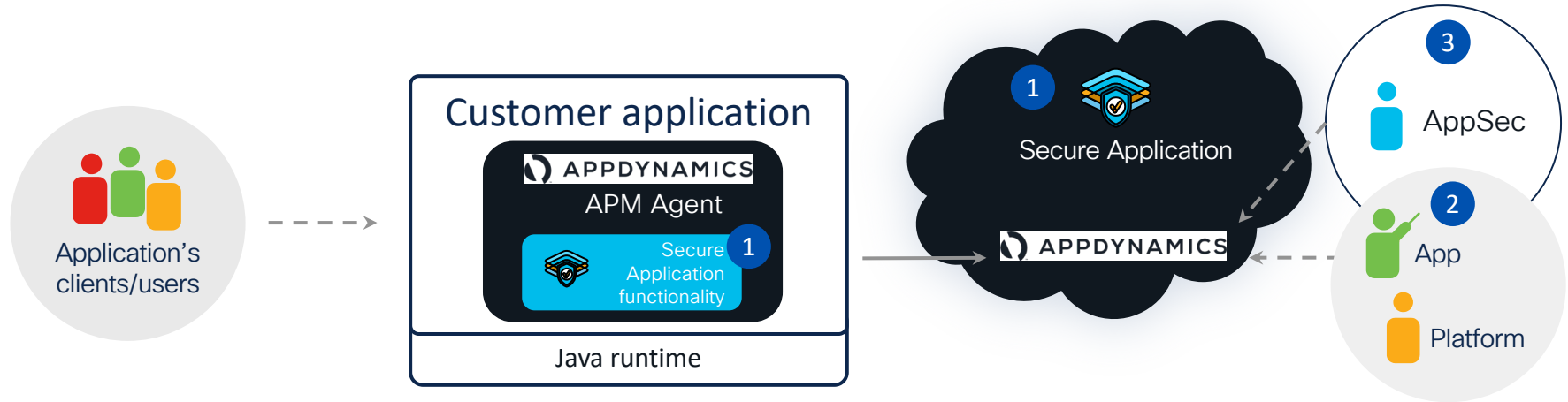
- Prevent Risky Workloads
- If an image is determined to be risky from our vulnerability assessments, Panoptica can block the deployment to any or all cluster environments.



The screenshot shows the 'New Deployment Rule' configuration page in the Cisco Panoptica interface. The page is divided into two main sections: 'STEP 1 Rule Properties' and 'STEP 2 Workloads'. In the 'STEP 2 Workloads' section, the 'Vulnerability Level' is set to 'High' and the 'On Violation Action' is set to 'Block'. A red box highlights the 'Vulnerability Level' and 'On Violation Action' fields. The 'Vulnerability Level' field has a red warning icon and the text 'High'. The 'On Violation Action' field has a dropdown menu with 'Block' selected. The 'Pod Security Standards Profile' and 'API Policy Profile' fields are also visible, both set to 'Select'. The 'Allowed Sidecars' field is set to 'Allow all'.

Bringing ZT into the Application Runtime

AppDynamics with Cisco Secure Application



1
New security functionality
In and through AppDynamics
“Check-box” integration

2
New security insights and action for
App/Platform teams
Context specific to application

3
New collaboration with AppSec teams
Policies and vulnerability/breach in context

Deeper dive & demo - <https://www.ciscolive.com/on-demand/on-demand-library.html?search=jatin#/session/16360602950640017TdP>

Continually Verify Trust with Cisco Secure App

Attack info tied to application context

The screenshot displays the AppDynamics web interface for an attack named "PoliteJavelin". The interface includes a top navigation bar with links for Home, Applications, Libraries, Vulnerabilities, Attacks (selected), Observations, and Policies. On the right, there are icons for Log4Shell-CVE, a search icon, and a help icon.

The main content area is divided into several sections:

- Attack Details:** ID: PoliteJavelin, Source: Internal, Outcome: Blocked, Attack Type (Events): API (1), U, Application: Log4Shell, Tier (Nodes): Log4Shell, Lifespan: 1 Second, Status: Open.
- Stack Trace:** A list of Java stack frames, with the following frames highlighted in blue:
 - org.apache.logging.log4j.core.lookup.JndiLookup.lookup(JndiLookup.java:56)
 - org.apache.logging.log4j.core.lookup.StrSubstitutor.resolveVariable(StrSubstitutor.java:1110)
 - org.apache.logging.log4j.core.lookup.StrSubstitutor.substitute(StrSubstitutor.java:1033)
 - org.apache.logging.log4j.core.lookup.StrSubstitutor.substitute(StrSubstitutor.java:912)
 - org.apache.logging.log4j.core.lookup.StrSubstitutor.replace(StrSubstitutor.java:467)
 - org.apache.logging.log4j.core.pattern.MessagePatternConverter.format(MessagePatternConverter.java:132)
 - org.apache.logging.log4j.core.pattern.PatternFormatter.format(PatternFormatter.java:38)
 - org.apache.logging.log4j.core.layout.PatternLayout.toSerializable(PatternLayout.java:344)
 - org.apache.logging.log4j.core.layout.PatternLayout.toText(PatternLayout.java:244)
 - org.apache.logging.log4j.core.layout.PatternLayout.encode(PatternLayout.java:229)
 - org.apache.logging.log4j.core.layout.PatternLayout.encode(PatternLayout.java:59)
 - org.apache.logging.log4j.core.appender.AbstractOutputStreamAppender.directEncodeEvent(AbstractOutputStreamAppender.java:197)
 - org.apache.logging.log4j.core.appender.AbstractOutputStreamAppender.tryAppend(AbstractOutputStreamAppender.java:190)
 - org.apache.logging.log4j.core.appender.AbstractOutputStreamAppender.append(AbstractOutputStreamAppender.java:181)
 - org.apache.logging.log4j.core.config.AppenderControl.tryCallAppender(AppenderControl.java:156)
- EVENTS (3):** A table showing the sequence of events:

Outcome	Event Type
UNAUTHENTICATED_ACCESS	
Blocked	SOCKET_RESOLVE
CLEAR_TEXT_HTTP	

Detailed insight for risk prioritization

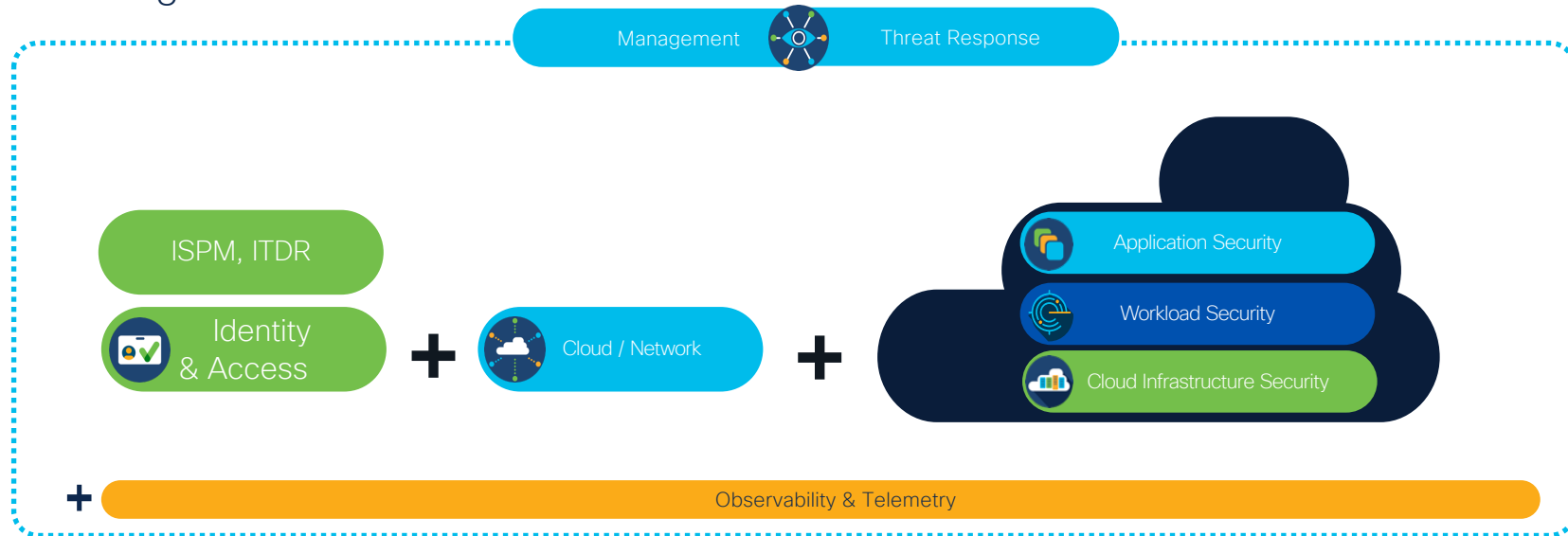
- Timeline of events to assess scope and methodology of attack
- Attack Source
- App Correlation App/Tier/Node/BT



Bringing it all together

Securing the User, Device & Application Transitions

The Big Picture



Zero Trust Capabilities to SECURE THE CLOUD ACCESS

- **User/Device** – Adaptive MFA, ITDR, ISPM, Remote Access VPN, Reverse Proxy, SAML/SSO Gateway, EDR
- **Network/Cloud** – SD-WAN, SIG

Zero Trust Capabilities to SECURE THE APP TRANSITION

- **Cloud Infra** – Visibility & Segmentation, NGFWv,
- **Workloads** – Workload based μ seg and app visibility
- **Applications** – Runtime Security of microservices and containers, FaaS Visibility, NGFWc

Take Aways

Establish &
Continuous
ly Verify
Trust

Enforce
Trust-
Based
Access

Respond to
Change in
Trust

- Follow our Zero Trust use cases
 - Draw out your Zero Trust use cases and workflows
 - Identify any potential gaps
 - Communicate risks involved
- Zero Trust policy should be end-to-end
 - User-Applications
 - Applications-to-Applications



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

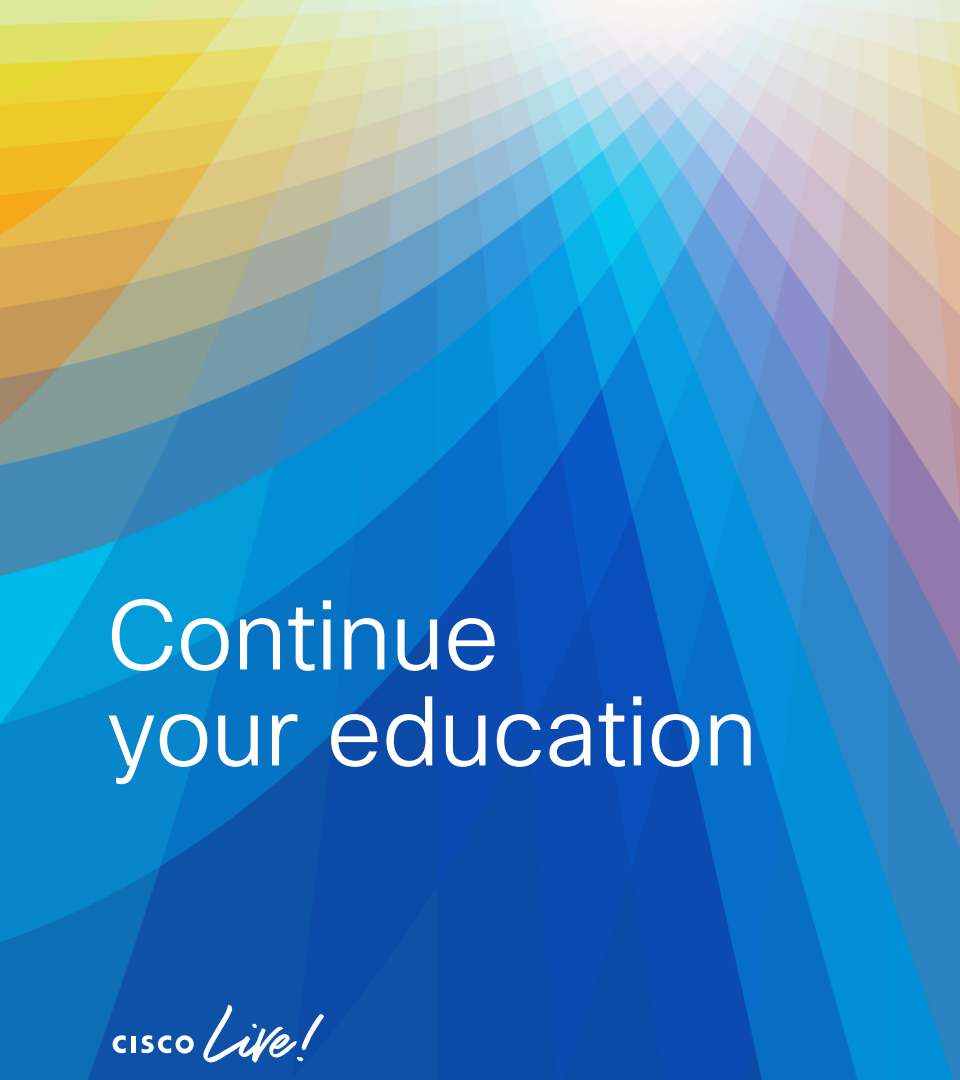
We would love to know your feedback on this session!

- Complete a minimum of four session and the overall event surveys to claim a Cisco Live merchandise.



Score = 5(excellent)





Continue your education

CISCO *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, triangular rays of color in a radial pattern, also following the rainbow spectrum. The overall effect is energetic and celebratory.

cisco *Live!*

Let's go

#CiscoLiveAPJC