The bridge to possible

Securing Tomorrow

Zero Trust Design Strategy for Modern Networks

Anthony Sabella, Principal Architect
www.linkedin.com/in/anthony-sabella
BRKSEC-2153

cisco Live!

#CiscoLive

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2153

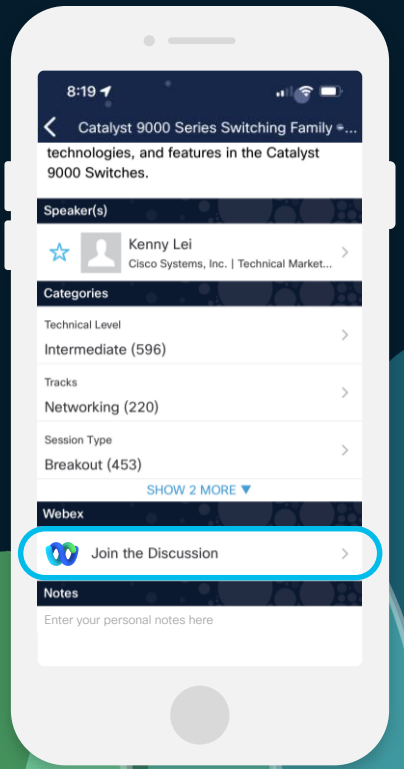
Questions?

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

How

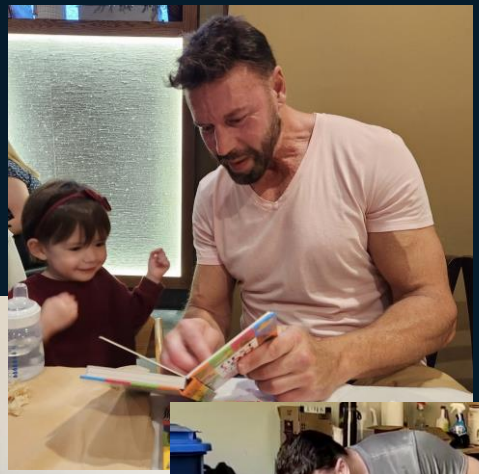
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.



About the Presenter

- Principal Architect for Cisco Systems - Enterprise Office of the CTO
- Specialize in combining the latest technology with cybersecurity
- Authored several white papers & books including “Orchestrating and Automating Security for the Internet of Things”
- Sports, fitness, car/motorcycle performance, daughter-everything



ANSABELL@CISCO.COM

Agenda

- Zero Trust Introduction
- Zero Trust Strategy / Roadmap
  - Defining Business Objectives
  - Assess / Plan
  - Evaluate / Pilot
  - Create Policies
  - Govern & Manage
- Cisco's Latest Advancements/Acquisitions for ZT Maturity

- **Housekeeping**: Q/A in Webex app & after session

Challenge

- Many leaders struggle to understand zero trust and how best to incorporate the concepts across their existing IT diameter.
- Evolution from a perimeter-based security approach to an "**never trust - always verify**" approach is inevitable to better address the current threat landscape.
- Creating a **Zero Trust Architecture** can be very challenging when you don't have a proper plan.

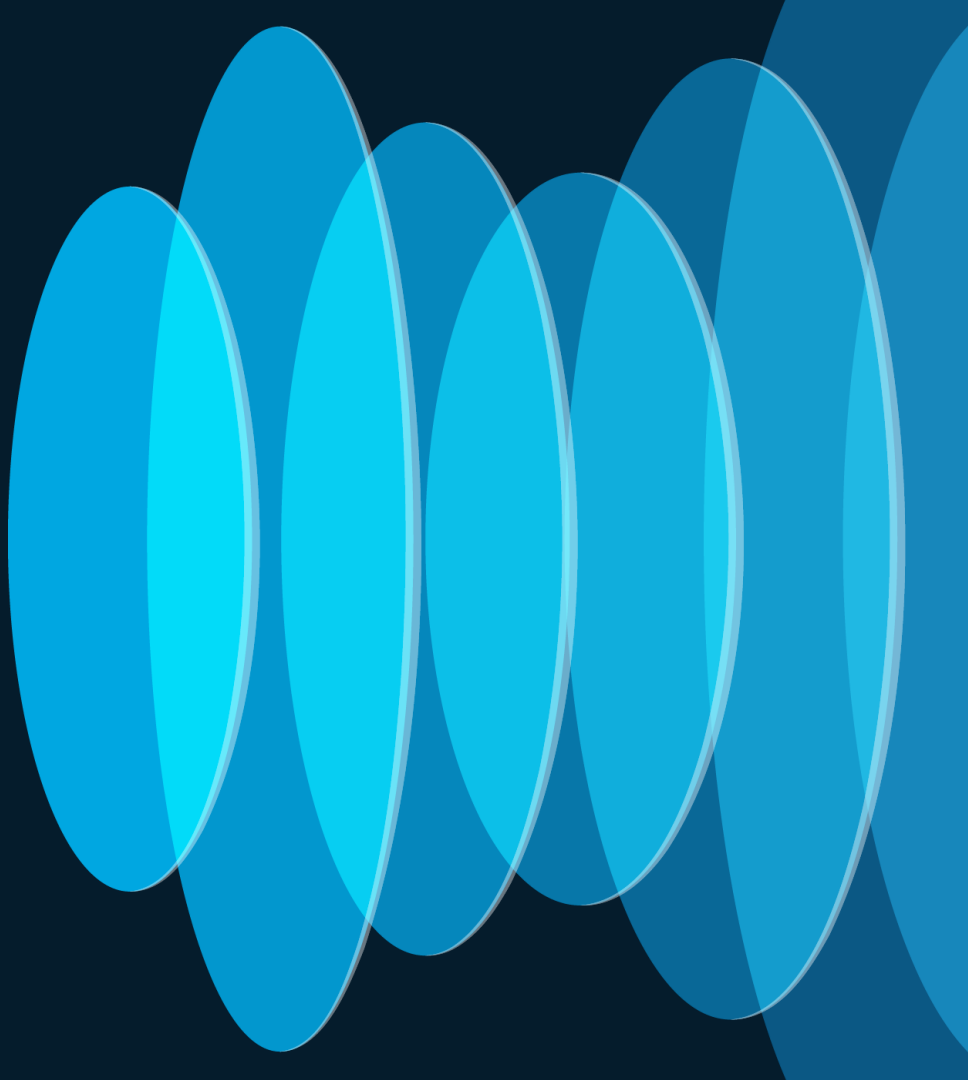
Zero Trust Roadmap

Every organization should consider a Zero Trust Roadmap for design, strategy, implementation, and governance

ZT Roadmap Methodology

	Define Business Objectives	Assess / Plan	Solution Evaluation	Create policies	Manage / Govern
Phases	• Define business objectives • CxO Alignment	• Identify DaaS areas • Assess “as-is” capabilities & define “to-be” ZT state • Identify / prioritize gaps • Align tasks with stakeholders	• Determine candidate solutions • Test/Pilot	• Create policies for functional ZT areas	• Establish metrics • Monitor and detect • Iterate for maturity
Objectives	Align C-suite & overall business objectives with ZT initiative	Capability assessment, gap analysis, & stakeholder alignment	Evaluation of potential solutions	Establish method for creating ZT policies	Establish metrics to measure progress, continual improvement of security posture

Zero Trust Primer



cisco Live!

Zero Trust Principles

Always Verify

Authenticate based on all data points/pillars

Least Privilege Access

Limit access using Just-in-time (JIT) & Just-enough-access (JEA)

Assume Breach

End to end encryption, limit blast radius

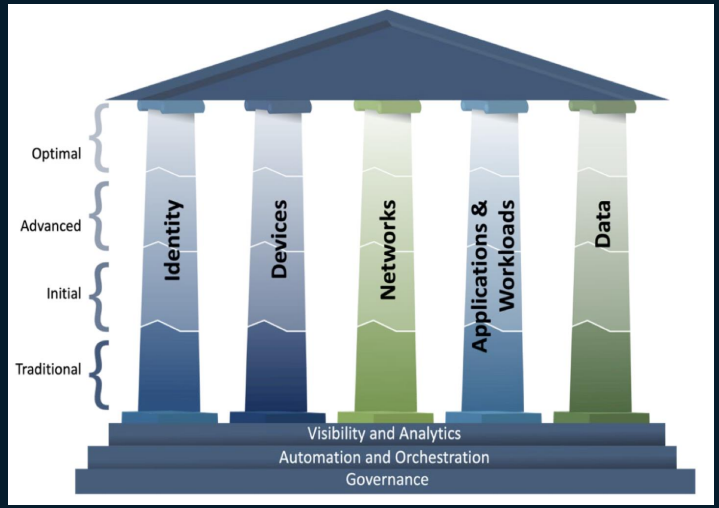
Zero Trust Architecture

- ZTA is a design and cybersecurity plan
- Based on ZT principles
- Designed to prevent data breaches and limit internal lateral movement
- Encompasses component relationships, workflow planning, and access policies Privileged Identities

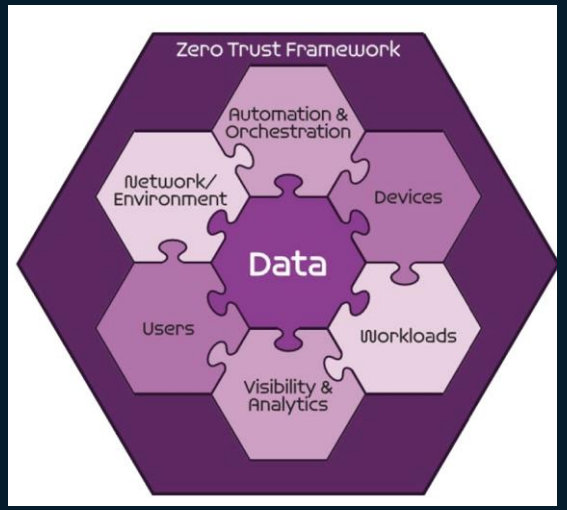
ZT Frameworks

Forrester

CISA



DoD



Zero Trust

Common Functional Pillars

The Concept of ZT Maturity

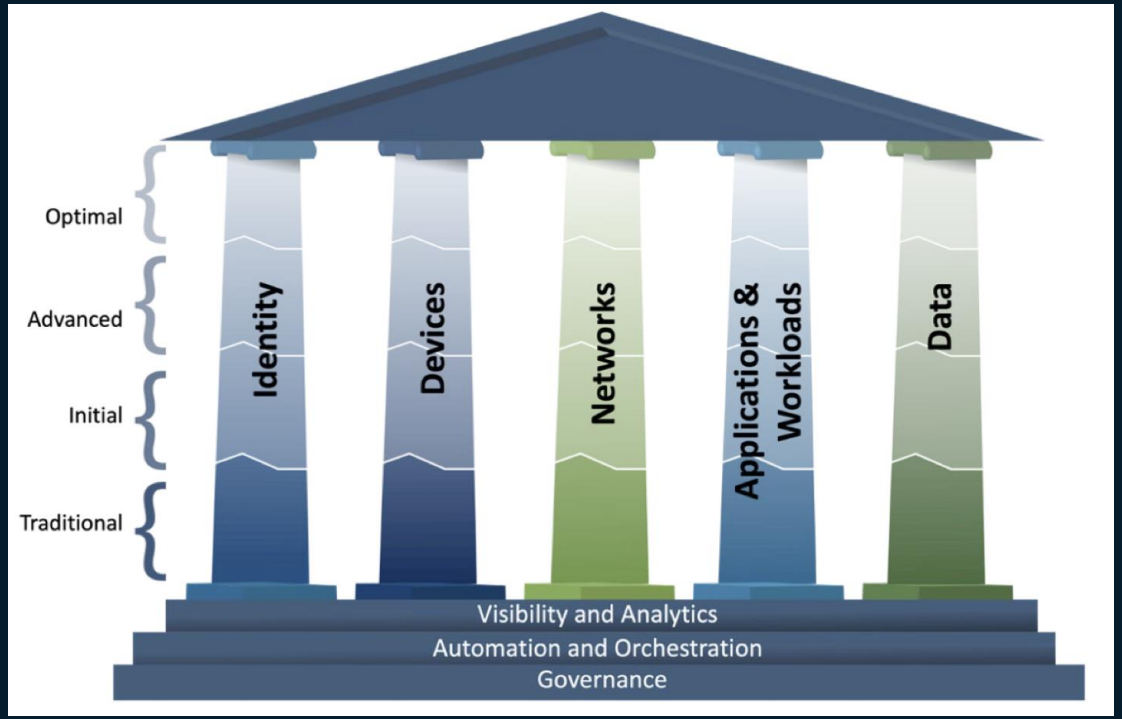
Cybersecurity Infrastructure & Security Agency (CISA)

Optimal = fully automated, JIT lifecycles, dynamic policies based on triggers, dynamic least priv, complete situational awareness across pillars

Advanced = automated assignment of attributes and config, centralized identify/visibility/control

Initial = starting automation of attribute assignment & configuration

Traditional = manually config'd lifecycles



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

CISA ZT Maturity Model

	Traditional	Initial	Advanced	Optimal
Identity	• Passwords or MFA • On-prem identity store • Limited identity risk assessment • Permanent access periodic review	• MFA with passwords • Self-managed & hosted identity stores • Manual identity risk assess • Access expires w/automated review	• Phishing-resistant MFA • Consolidated identity stores • Automated identity risk assessment • Session-based access	• Consistent validation & risk analysis • Ent wide identity integration • Tailored, as-needed automated access
Devices	• Manual tracking device inv • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• All physical assets tracked • Limited device-based access control & compliance • Some protections via automation	• Most physical & virtual assets tracked • Enforced compliance with integrated threat protection • Resource access based on device posture	• Continuous physical & virtual asset analysis with integrated threat protection • Resource access depends on real-time device risk analytics
Networks	• Large perimeter/macro seg • Limited resilience, manually managed rulesets & configs • Minimal traffic encryption, ad hoc key mgmt	• Initial isolation of critical workloads • Network manages demand • Dynamic configs for some network devices • Encrypt more traffic & formalize key mgmt. process	• Expanded isolation & resilience mechanisms • Configs adapt via automated risk-aware app profile assessment • Encrypt network traffic & manages key issuance/rotation	• Distributed micro-perimeters with JIT and JEA access control • Configs evolve to meet app profile needs • Integrated best practice cryptography
App/ Workload	• Mission critical apps via private networks • Protections have minimal workflow integration • Ad hoc dev, testing, prod	• Some mission critical workflows accessible via public • Formal CI/CD security tactics • SAST & DAST prior to deployment	• Most mission critical apps available over public networks • App workflow protection with context-based app controls • Team coordination for dev, sec, & ops	• Apps available over public networks with continuous authorized access • All workflows have protection • Immutable workloads with sec testing integrated in lifecycle
Data	• Manual inventory & data categorization • On-prem data stores • Static access controls • Minimum encrypt of data at rest and data in transit with adhoc key mgmt	• Limited automation inventory data & control process • Begin data categorization • Some highly avail data stores • Encrypt data in transit • Initial centralized key mgmt. policies	• Automated data inv with tracking • Consistent tiered categorization and labeling • Redundant highly available data stores • Automated context-based access • Encrypt data at rest	• Continuous data inventorying • Automated data categorization & labeling enterprise-wide • DLP exfil blocking • Dynamic access controls • Encrypt data in use

Identity Categories

Authentication

FROM - password use

TO- phishing resistant MFA beyond initial access grant

Identity Stores

FROM = on-prem identity store

TO- full integration of all identity stores (on-prem + cloud

Risk Assessments

FROM - limited determination of risk

TO- identity risk in real-time based on continuous analysis

Access Mgmt

FROM - permanent access of privileged / un-privileged accounts

TO- use of automation to provide tailored JIT/JEA

Identities (Tactical Examples)

- **Federate** on-premises identity systems with cloud identity systems (centralized identity management)
- Combine self-service password reset and MFA capabilities in a single workflow
- **Conditional access policies** to gate application access with remediation activities
- Risk-based policies to access/protect identified assets
- Password protection capabilities to block weak passwords
- **Password-less capabilities** to reduce the risk of phishing, password attacks, and ultimately streamline workflows
- SIEM / SOAR to persist and **analyze logs to improve visibility** for authentication, authorization, and provisioning.
- SIEM / SOAR to **integrate threat signals** from other security solutions to improve detection, protection, and response.

Privileged Identities

- Privileged access to protect **administrative** user accounts.
- **Privileged Identity Management (PIM)** for a time-bound, just-in-time approval process for the use of **privileged** user accounts.

Device Categories (CISA)

Policy Enforcement

FROM – limited visibility into behavior/compliance

TO- integrate device mgmt, software approval, config, & vuln mgmt (continuous insight for compliance enforcement)

Asset/risk Mgmt

FROM - limited tracking of physical &virtual assets

TO- real-time view of all assets across vendors

Resource Access

FROM – not using device visibility to access resources

TO- considers real-time risk analytics to access resources

Threat Protection

FROM – manual deployment of threat protect capabilities

TO- centralized solution with unified approach for threat protection, policy enforcement, compliance monitoring

Devices (Tactical Examples)

- Integrate current **device mgmt** solutions to cloud iAM
- **Compliance policies** (min security reqs) for resource access (trusted endpoint policies)
- Integrate **endpoint security (EDR)** with iAM to better assess risk level
- Conditional access policies (adding **endpoint risk** to equation) for corporate and BYOD endpoints
- Remediation notification/rules (self-guided remediation) attached to conditional access policies
- DLP – control behavior after data access (restrict copy/paste, saving to untrusted locations, etc.
- SIEM / SOAR to persist and analyze logs to improve visibility for authentication, authorization.
- SIEM / SOAR to integrate threat signals from other security solutions to improve detection, protection, and response.
- **Integrate** device mgmt, software approval, config, & vuln mgmt solutions across physical and virtual devices (continuous insight for **compliance enforcement**)

Network Categories (CISA)

Segmentation	Network Traffic Mgmt	Traffic Encryption	Network Resilience
FROM – large perimeter-based macro segmentation	**FROM =** static rules/configs to manage traffic	**FROM –** encrypts minimal traffic	**FROM –** manual configs to match individual app availability demands with limited resilience measures
TO- fully distributed ingress/egress micro-seg based on app profiles with JIT/JEA	**TO-** dynamic rules/configs that evolve based on app	**TO-** encrypts all internal & external traffic enforcing least-privilege access	**TO-** auto-scaling / auto-healing capabilities to meet network and availability demands for all workloads

Network (Tactical)

Example tactical tasks include:

- Require **encryption** for all traffic connections, including between IaaS components and between on-premises users and apps.
- Limit access to critical data and applications by policy (user/device identity) and/or **traffic filtering.**
- Deploy **on-premises network segmentation** with ingress and egress traffic controls with micro-perimeters and micro-segmentation
- Deploy **cloud network segmentation** with ingress and egress traffic controls with micro-perimeters and micro-segmentation.
- Establish **application profiles/SLAs** with distinct traffic mgmt features, and map applications to profiles
- Implement dynamic network rules/configs based on risk-aware traffic

Application Categories (CISA)

App Access

FROM – access based on local authorization

TO- access via user/device trust, context, & real-time risk analysis to grant access

App Threat Protection

FROM - minimal threat protection within workflow

TO- advanced threat protection in all workflows

Accessible App

FROM – some apps available only via private network/VPN

TO- all critical workloads available via public networks

Secure SDLC

FROM – ad hoc dev, testing, prod environments with elementary code deployment capabilities

TO- immutable workloads where feasible with security integrated within CI/CD

App/Workload (Tactical Examples)

Example tactical tasks include:

- All workloads should be assigned an **identity** (policies can require adding tags upon creation).
- Implement **app access policies** based on user/device trust, context, and risk analysis
- Ensure apps support **modern auth'C** protocols such as Oauth/OIDC, SAML, and SSO
- **Secure SDLC** and **CI/CD** with IaC scanning capabilities
- Deploy cloud workload visibility/protection including **risk assessment** capability (scan SBOM / CVE assessment) & **posture** for credential exposure + iAM permissions.
- Deploy runtime security capabilities including **securing API communications** for both internal and 3rd party APIs

Data Categories (CISA)

Inventory Mgmt

FROM – manually identify & inventory some data

TO- automated data/inventory enterprise-wide with continuous update capabilities w/dynamic DLP

Classification / labeling

FROM - limited ad-hoc data categorization capabilities

TO- automated data categorization enterprise-wide, structured formats, & abilities to handle all data types

Data Access

FROM – static access controls to govern access to read, write, copy, etc.

TO- automated data access control based on user/device trust, risk, data category, etc. – and providing JIT/JEA

Data Security

FROM – encrypts minimal data at rest

TO- encrypts all data at rest and data in use where appropriate, enforcing least-privilege access

Data (Tactical)

Learn data

- Determine data sensitivity level and develop classification schema
- Discover and classify sensitive data

Protect data

- Determine use of sensitivity labels
- Discover/label/protect sensitive data in both on-prem and cloud environments

Prevent data loss

- Establish DLP policies
- Add protection to specific labels (encryption, etc.) for cloud environments

Extend data protection

- Extend labels/protection to both data in transit & data-at-rest (begin with sensitive data then extend to all data)

Zero Trust Roadmap

Business Objectives

Assess / Plan

Solution Evaluation

Create Policies

Govern / Manage

- CxO Buy-In
- Define business objectives

CxO Buy-in SD-WAN benefits

Buy-in across C-Suite

Resources & assets under multiple organizations requiring buy-in across C-Suite

Gaining Alignment

Begins with identifying leadership & meeting to learn their goals

Support Needed

ZT is shared responsibility. CISO may lead discussion, but support needed across C-Suite

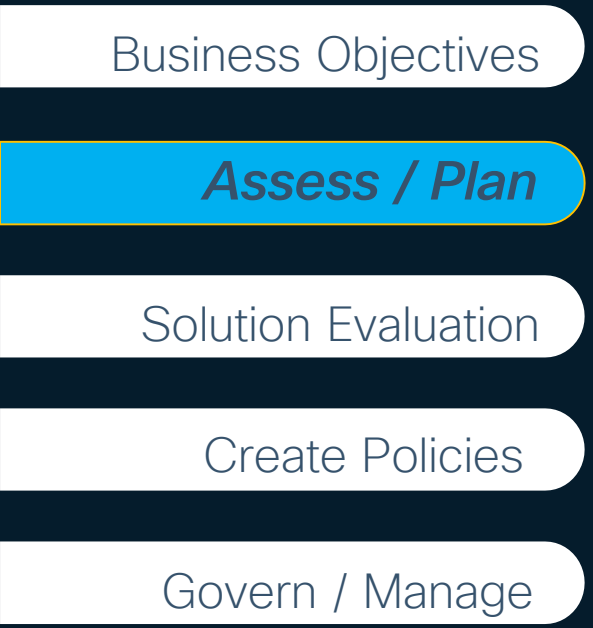
CxO Alignment / Investment into ZT Initiative

- **Chief Executive Officer (CEO):** Empowering the business to achieve its strategic goals and objectives (inclusive of the security strategy) in a quantifiable way that enables evaluation of risks and costs, so that returns to the shareholders could be maximized.
- **Chief Information Officer (CIO):** Helping the company evolve technology and processes to better align to overall business objectives. Security should be a measurable outcome and aligned with IT strategy.
- **Chief Information Security Officer (CISO):** A remote or hybrid work environment creates a larger surface area for security breaches. Modernizing and evolving the security posture, policies, and procedures to improve risk-based and defensive strategies to comply with security and data protection requirements.
- **Chief Technology Officer (CTO):** Technologies that facilitate both remote work and the adoption of cloud services in a secure manner should be evaluated. Creating and adopting an overall technology framework that can address business objectives more efficiently and effectively.
- **Chief Financial Officer (CFO):** Fixed datacenter investment and buildings are moving to cloud applications and users working from home (hence spending priorities are shifting from fixed to agile models). Overall **alignment of budget** allocation and spending to business Objectives
- **Chief Marketing Officer (CMO):** How business is perceived internally and externally, where breach readiness and incident response strategy are critical to managing overall perception.

Aligning ZT to Business Objectives

- Identify a clear zero trust strategy with a set of principles
- Ensure a clear statement of **benefits** resulting from said strategy
- Establish a clear **link** between the strategy and the organization's IT and business goals
- Identify **ownership and responsibilities** for the continued development of said strategy
- Establish **metrics** to be measured and reported in a systematic manner

Zero Trust Roadmap



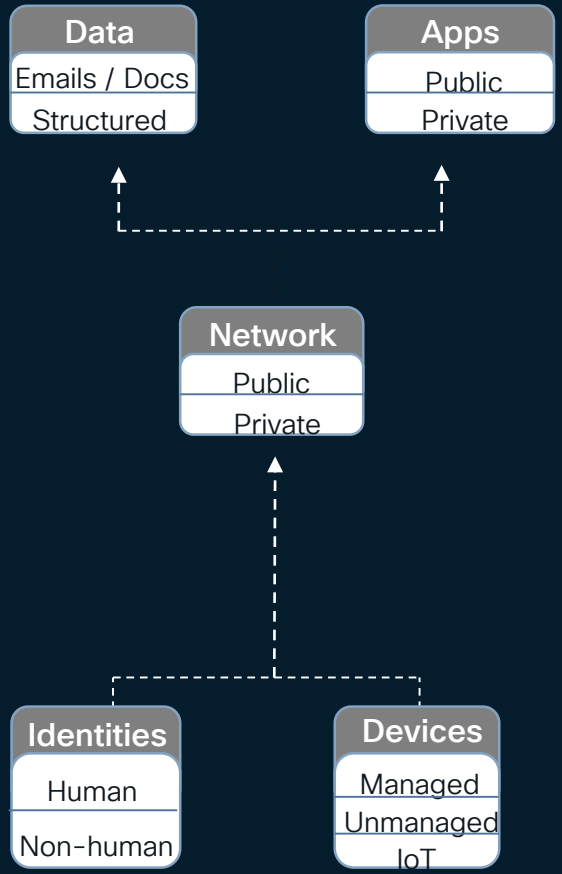
- Identify DaaS areas & create Zero Trust Architecture (ZTA)
- Assess “as-is” capabilities & define “to-be” ZT state
- Identify / prioritize gaps between “as-is” and ”to-be”
- Align gaps/tasks with stakeholders

Identify DaaS Areas

Helping to form Zero Trust Architecture (ZTA)

Identify DaaS as well as access and authorization existing across the IT diameter

- **Data** – can be PII, PCI, etc and be either data at rest or data in transit
- **Assets** – often used to access and store data including hardware, software, servers, printers, IoT devices, etc
- **Applications** – often used to access the data which execute in both private & cloud environments
- **Services** – used to obtain/use data (ex AD, SSO, etc)

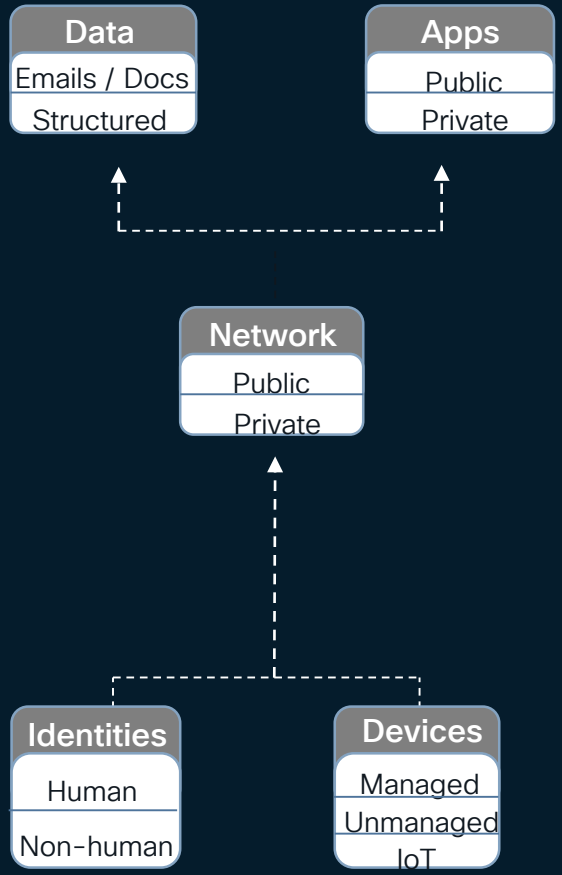


Bolstering “As-Is” Documentation with **Use Cases**

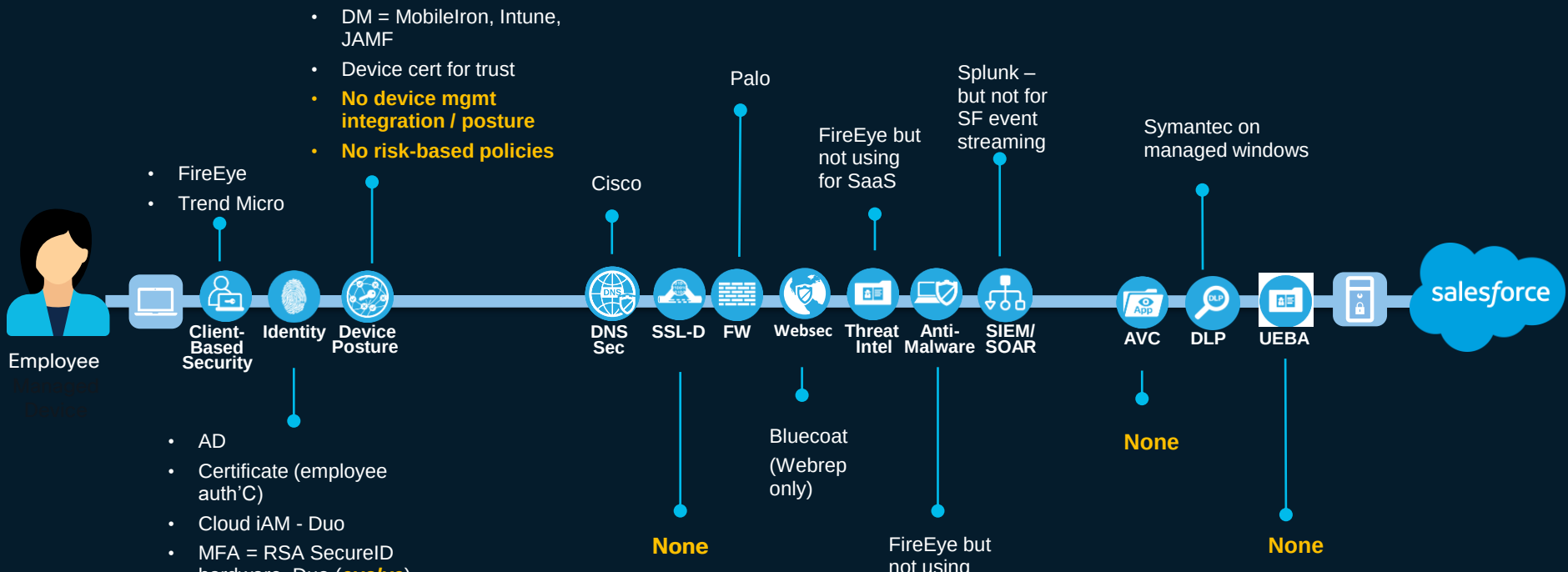
Consumer = source or consumer of data

Provider = provider of data/service

1. User to Application/Service
   - Ex. Consumer to INET/SaaS or private application
2. Machine to Application/Service
   - Ex. IoT device to private cloud service
3. App-App / Service-Service
   - Microservice in AWS VPC A to a microservice in AWS VPC B



Documenting capabilities/processes per use case
(Ex. employee managed device – SaaS)



1. Security capabilities
2. Zero Trust principles
3. Tool / process used

Using Checklist as "to-be" to Identify Gaps

CISA example

	Traditional	Initial	Advanced	Optimal
Identity	• Passwords or MFA • On-prem identity store • Limited identity risk assessment • Permanent access periodic review	• MFA with passwords • Self-managed & hosted identity stores • Manual identity risk assess • Access expires w/automated review	• Phishing-resistant MFA • Consolidated identity stores • Automated identity risk assessment • Session-based access	• Consistent validation & risk analysis • Ent wide identity integration • Tailored, as-needed automated access
Devices	• Manual tracking device inv • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• All physical assets tracked • Limited device-based access control & compliance • Some protections via automation	• Most physical & virtual assets tracked • Enforced compliance with integrated threat protection • Resource access based on device posture	• Continuous physical & virtual asset analysis with integrated threat protection • Resource access depends on real-time device risk analytics
Networks	• Large perimeter/macro seg • Limited resilience, manually managed rulesets & configs • Minimal traffic encryption, ad hoc key mgmt	• Initial isolation of critical workloads • Network manages demand • Dynamic configs for some network devices • Encrypt more traffic & formalize key mgmt. process	• Expanded isolation & resilience mechanisms • Configs adapt via automated risk-aware app profile assessment • Encrypt network traffic & manages key issuance/rotation	• Distributed micro-perimeters with JIT and JEA access control • Configs evolve to meet app profile needs • Integrated best practice cryptography
App/ Workload	• Mission critical apps via private networks • Protections have minimal workflow integration • Ad hoc dev, testing, prod	• Some mission critical workflows accessible via public • Formal CI/CD security tactics • SAST & DAST prior to deployment	• Most mission critical apps available over public networks • App workflow protection with context-based app controls • Team coordination for dev, sec, & ops	• Apps available over public networks with continuous authorized access • All workflows have protection • Immutable workloads with sec testing integrated in lifecycle
Data	• Manual inventory & data categorization • On-prem data stores • Static access controls • Minimum encrypt of data at rest and data in transit with adhoc key mgmt	• Limited automation inventory data & control process • Begin data categorization • Some highly avail data stores • Encrypt data in transit • Initial centralized key mgmt. policies	• Automated data inv with tracking • Consistent tiered categorization and labeling • Redundant highly available data stores • Automated context-based access • Encrypt data at rest	• Continuous data inventorying • Automated data categorization & labeling enterprise-wide • DLP exfil blocking • Dynamic access controls • Encrypt data in use

Using Checklist as "to-be" to Identify Gaps

CISA example

Current state

	Traditional	Initial	Advanced	Optimal
Identity	• Passwords or MFA • On-prem identity store • Limited identity risk assessment • Permanent access periodic review	• MFA with passwords • Self-managed & hosted identity stores • Manual identity risk assess • Access expires w/automated review	• Phishing-resistant MFA • Consolidated identity stores • Automated identity risk assessment • Session-based access	• Consistent validation & risk analysis • Ent wide identity integration • Tailored, as-needed automated access
Devices	• Manual tracking device inv • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• All physical assets tracked • Limited device-based access control & compliance • Some protections via automation	• Most physical & virtual assets tracked • Enforced compliance with integrated threat protection • Resource access based on device posture	• Continuous physical & virtual asset analysis with integrated threat protection • Resource access depends on real-time device risk analytics
Networks	• Large perimeter/macro seg • Limited resilience, manually managed rulesets & configs • Minimal traffic encryption, ad hoc key mgmt	• Initial isolation of critical workloads • Network manages demand • Dynamic configs for some network devices • Encrypt more traffic & formalize key mgmt. process	• Expanded isolation & resilience mechanisms • Configs adapt via automated risk-aware app profile assessment • Encrypt network traffic & manages key issuance/rotation	• Distributed micro-perimeters with JIT and JEA access control • Configs evolve to meet app profile needs • Integrated best practice cryptography
App/ Workload	• Mission critical apps via private networks • Protections have minimal workflow integration • Ad hoc dev, testing, prod	• Some mission critical workflows accessible via public • Formal CI/CD security tactics • SAST & DAST prior to deployment	• Most mission critical apps available over public networks • App workflow protection with context-based app controls • Team coordination for dev, sec, & ops	• Apps available over public networks with continuous authorized access • All workflows have protection • Immutable workloads with sec testing integrated in lifecycle
Data	• Manual inventory & data categorization • On-prem data stores • Static access controls • Minimum encrypt of data at rest and data in transit with adhoc key mgmt	• Limited automation inventory data & control process • Begin data categorization • Some highly avail data stores • Encrypt data in transit • Initial centralized key mgmt. policies	• Automated data inv with tracking • Consistent tiered categorization and labeling • Redundant highly available data stores • Automated context-based access • Encrypt data at rest	• Continuous data inventorying • Automated data categorization & labeling enterprise-wide • DLP exfil blocking • Dynamic access controls • Encrypt data in use

Security gaps organized into phases

Graduated approach ensuring proper ZT maturity

P1 – strong auth'c	P2 – devices in DM	P3 – app access	P4 – monitor/mature
• **Federate on-prem identity systems** with iDP (centralized identity) • Secure each identity with **strong auth'N** (eg. MFA) • **Federate SaaS apps** with iDP (SSO)	• ***Integrate*** device management solutions with iDP (trusted device) • Establish a **trusted device** policy • Establish **compliance policies** (min sec reqs) for resource access (MFA for low-risk, block non-supporting clients, etc) • Gain visibility & control into **Shadow IT apps**	• ***Expand*** Trusted Device to larger group/audience • Configure **conditional access policies** (only allowing compliant devices to access resources) • Create remediation notification/rules (self-guided remediation) for **conditional access** • Integrate MFA and self-service password reset workflows	• Implement **password-less** authentication (Phishing resistant) • Configure SIEM/SOAR to persist and analyze logs to **improve visibility** for authentication, authorization, and provisioning • Configure SIEM/SOAR to **integrate threat signals** from other security solutions and begin tying actionable responses to behavior.

Align Stakeholders

Sponsor
Name

Strategy, management coordination, escalation, approvals, business alignment

Project Lead
Name

Manage collective engagement, resources, timeline and schedule, communications, etc.

CISO
Name

Security and governance of identities, devices, and apps; risk and policy determination, tracking and reporting

Arch Lead
Name

Tech requirements, architecture, reviews, decisions, and prioritization

Identity architect
Name

Identifies required controls to address tech and architecture requirements; implements these

IT Compliance Manager
Name

Identifies required controls to address compliance and protection requirements

Device management architect
Name

Executes the strategy for protecting organization data on devices, including managing devices

App management lead
Name

Tech requirements, and prioritization of app investments – bringing apps up to standards with modern authentication and coordinating apps with conditional access rules

SaaS admins
Name

Tenant/environment, preparation, configuration, testing

Information Protection Manager
Name

Data classification and sensitive data identification, controls and remediation

Quick Tech Explanation

Identity

Password-less

Device Management

Integration

Identity Example of Evolving to ZT Maturity

IDENTITY	L1 Password	L2 Password	L3 Password	Password less
Authentication	password	SMS	Authenticator push	FIDO2 methods Apple Touch/Face ID
	qwerty	Voice	Software token (OTP)	FIDO2 Security key
	123456		Hardware token (OTP)	

Password-less Authentication

What

- Verifying a person's identity without relying on a password (more user-friendly)

How

- Traditional MFA = something you have + something you know (*ex. password*)
- Password-less = **Replaces** something you know with something you are (*ex. biometric*)
- Uses two factors like MFA, but can happen in **single** gesture (*ex. biometric*)

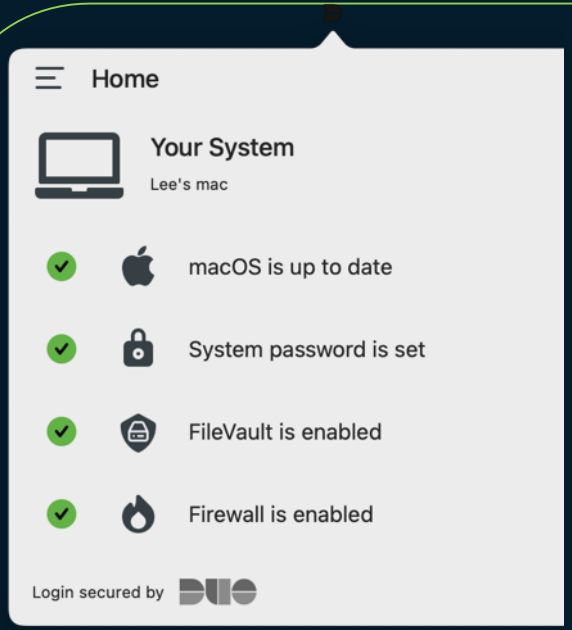
Device Example of Evolving to ZT Maturity

DEVICES **Policy enforcement & compliance monitoring**	IDP + Device Health	IDP + Device Health + Device Management	IDP + Device Health + Device Management + EDR/XDR

DM Integration - Trusted Device Standard

DM platform responsibilities (communicating with iAM solution @ reg intervals)

Duo Health App

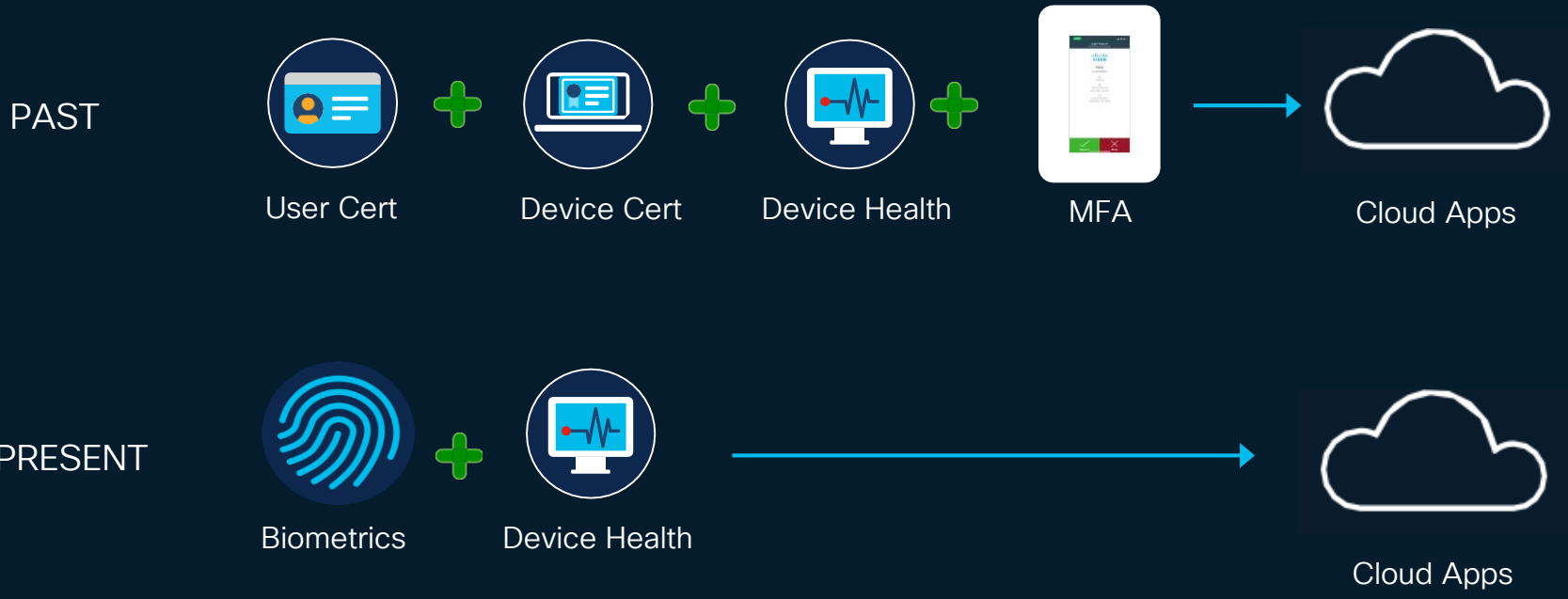


Duo Mobile

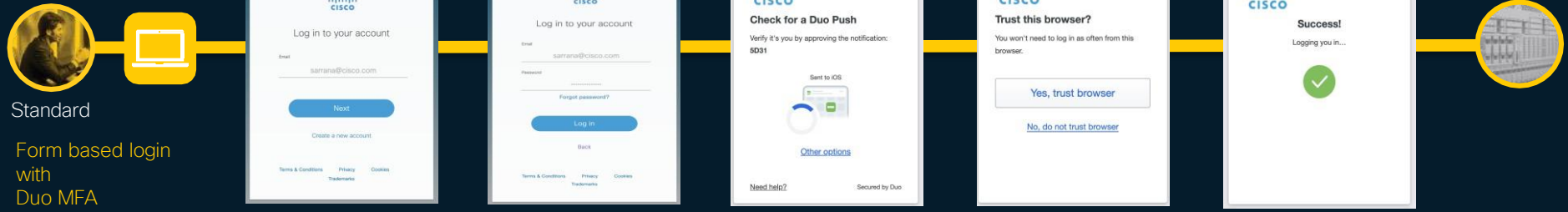
DM Integration

- Anti-Malware
- Data Encrypttion
- Minimum OS
- Software Patching
- Rooted Device Detection
- Remote Wipe (company data)
- Password/Screen-lock Enforcement
- Hardware/Software Inventory
- Hardware TPM Support

Zero Trust flow – Evolution



Login Flows for Single Sign-On apps



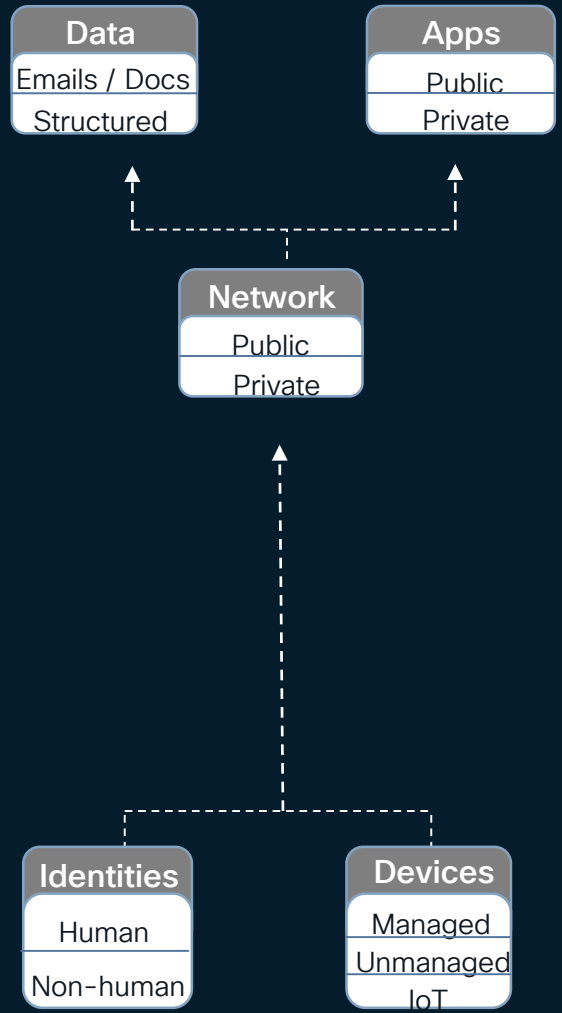
Standard

Form based login with Duo MFA

Duo PasswordLess Biometrics based login

Zero Trust Architecture

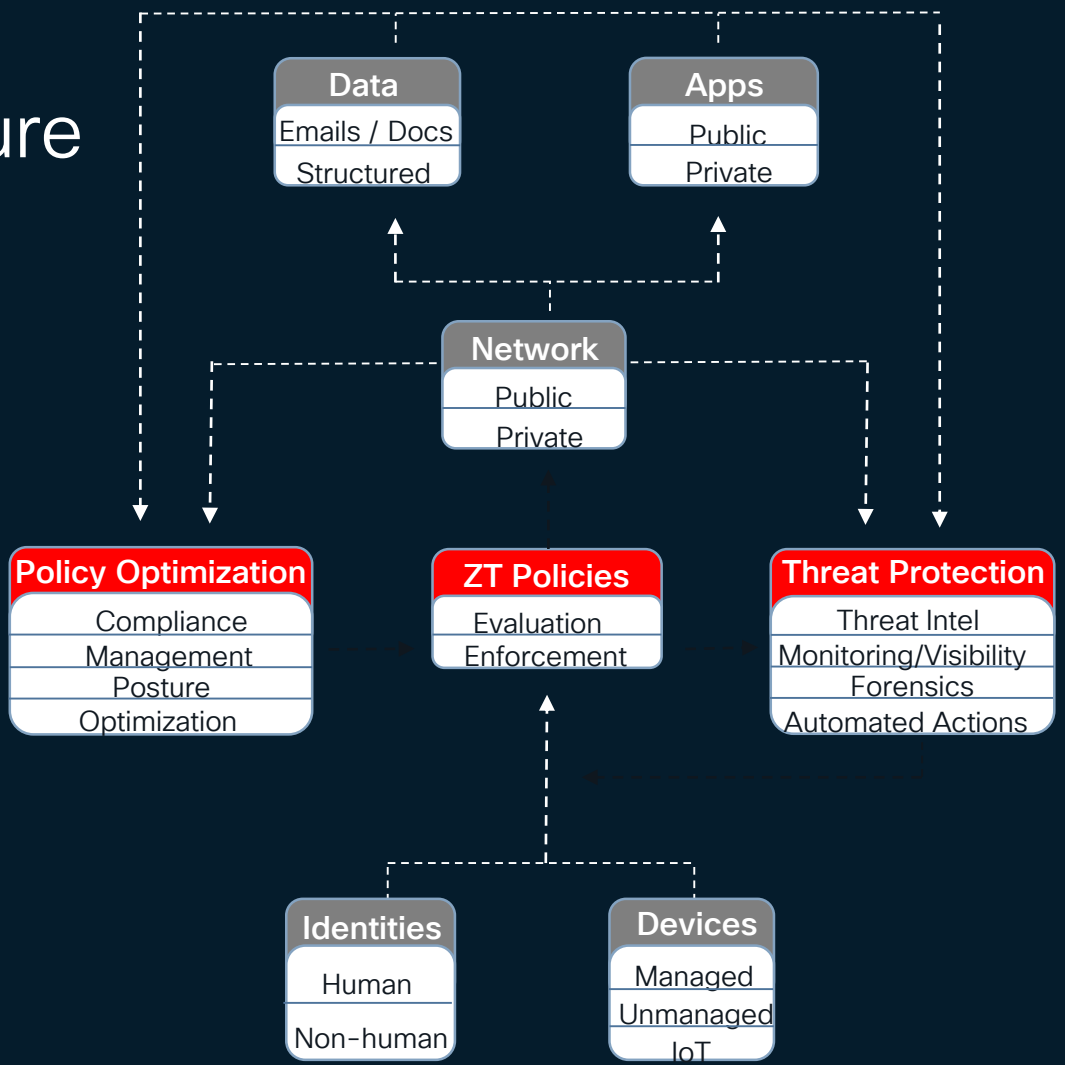
Zero Trust Architecture Foundation



Zero Trust Architecture Foundation

Protection and security are integrated across all DaaS/pillars via **ZT Policies** & **Policy Optimization**

Threat protection aggregates telemetry across the ZT pillars in real-time, where actionable responses can be tied to behavior to improve incident response & MTTR.



Zero Trust Roadmap

Business Objectives

Assess / Plan

Solution Evaluation

Create Policies

Govern / Manage

- Determine candidate solutions
- Test / pilot

Solution Evaluation (risks)

Evaluate

- Determine **resources** to evaluate risks
- Determine evaluation **method** (can be executed via several different methods include ISO standards and/or table-top exercises)
- Determine **stakeholder participation**, and review chosen methods to determine viability

Pilot

- If using **tabletop** method – execute a selected scenario with the smaller stakeholder team, review results, and determine viability.
- If you're using **ISO standards** method, select a portion of the standard to narrow the scope to a manageable level, review results and viability, and proceed to the next portion.

ISO/IEC 27001:2002

- **Specifies the requirements** for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
- Includes requirements for the assessment and treatment of information security risks tailored to the needs of an organization (requirements are generic and can apply to any organization.
- Provide a **structured and comprehensive method** to **identify/gauge risks** that apply to the organization, as well as mitigation strategy.
  - Information security management systems
  - Infosec, cybersecurity, privacy protect
  - Requirements/guidelines

Tabletop Exercises – (e.g. Malware Infection)

Risk scenarios evaluating state of preparedness

Scenario

An employee within your organization used the company's digital camera for business purposes. In the course of doing so, they took a scenic photograph that they then loaded onto their personal computer by inserting the SD card. The SD card was infected with malware while connected to the employee's personal computer. When re-inserted into a company machine, it infected the organization's system with the same malware.

Questions

- Who within the organization would you need to notify?
- How would your organization identify and respond to malware infecting your system through this vector?
- What other devices could present similar threats?
- How can you prevent this from occurring again?
- Does your organization have training and policies in place to prevent this?

Process/audience/impact

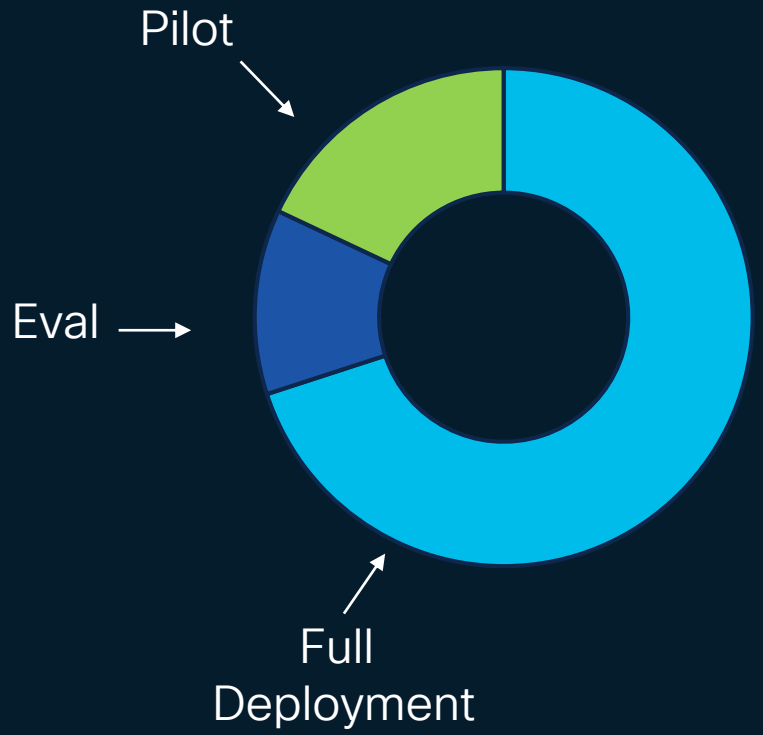
- **Processes tested**: User awareness / Detection capabilities
- **Threat actor**: Insider
- **Asset impacted**: Network integrity
- **Applicable controls**: Malware Defenses, limitation & control of network ports/protocols/services, boundary defense

Source: https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team

Solution Evaluation (Test/Pilot)

Phase	Method
Evaluate	Identify 25 endpoints for testing
Pilot	Determine next 50 endpoints or a particular VLAN/group in production
Deployment	Begin iterative deployment across IT diameter using chosen strategy

** *User training* *Educate employees on new measures*



Zero Trust Roadmap

Business Objectives

Assess / Plan

Solution Evaluation

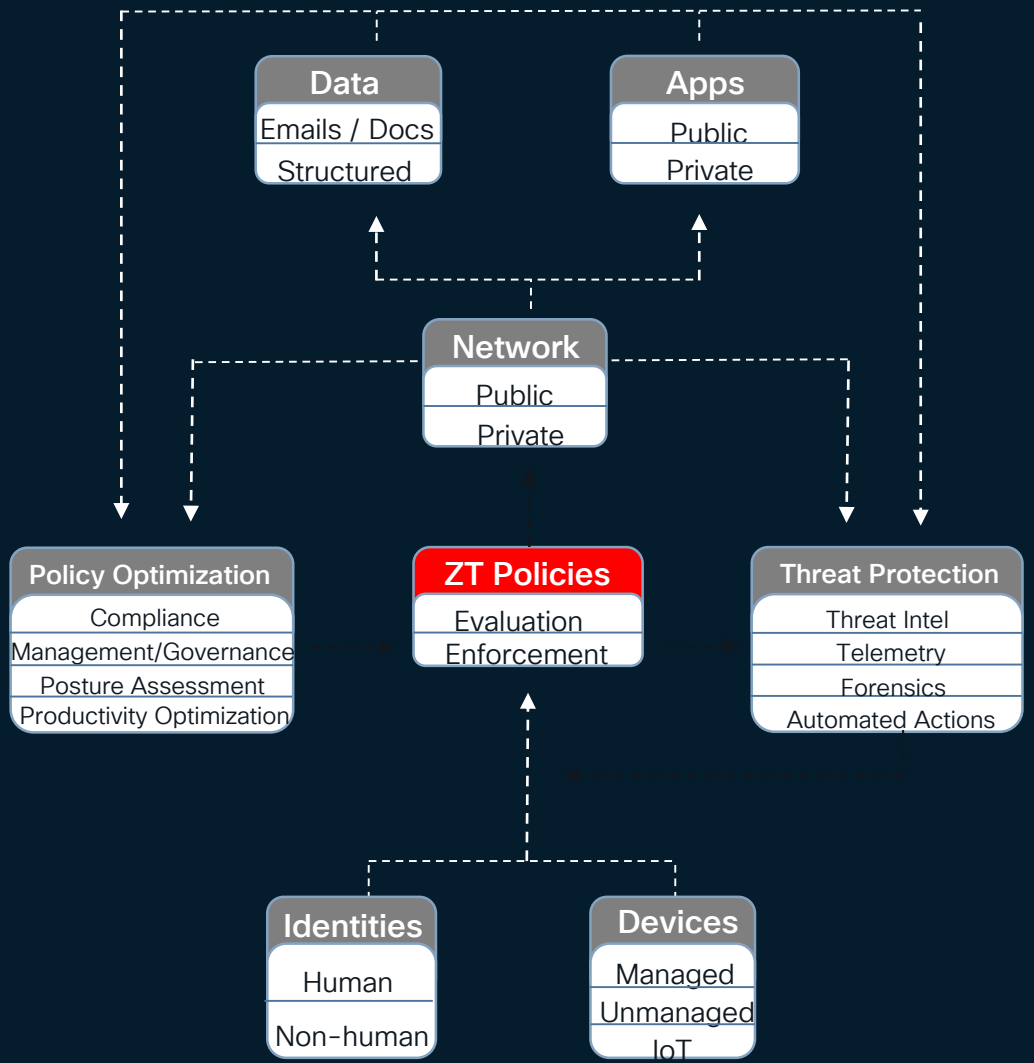
Create Policies

Govern / Manage

- Create polices for functional ZT areas

Zero Trust Policies

- Kipling method
- Minimum security requirements for Resource access



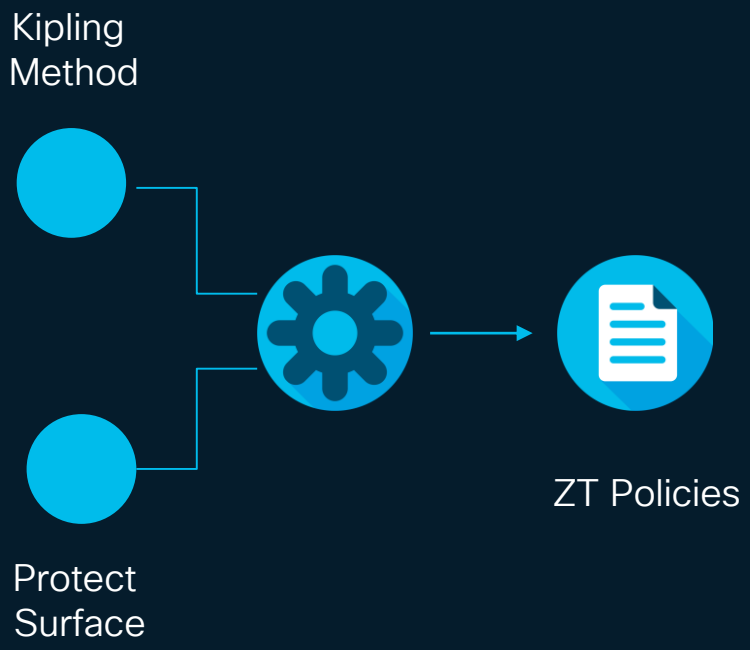
Kipling Method

I keep six honest men

They taught me all I knew

Their names are WHAT, WHY, and WHEN

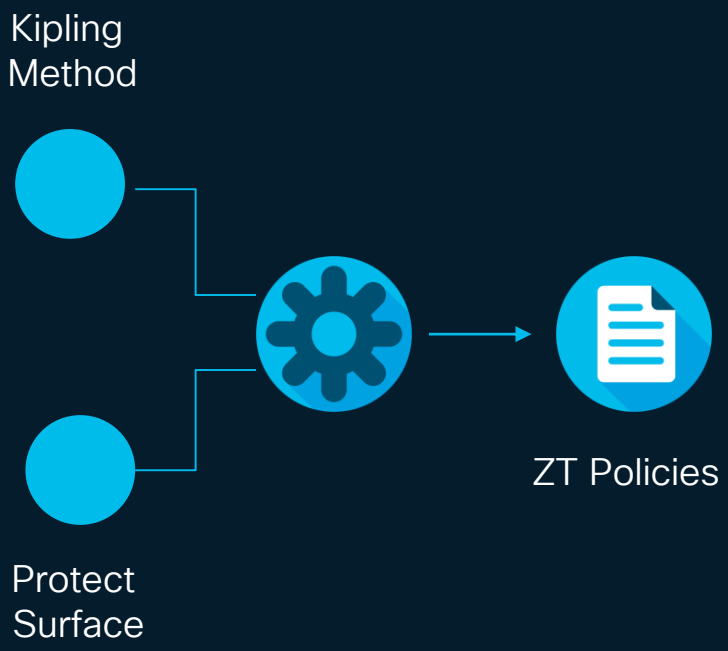
And HOW, WHERE, and WHO



Kipling Method

ZT Policy Creation Mirrors Essence of Kipling's Poetic Wisdom

- Who: Who can access the asset
- What: What asset is the consumer trying to access
- When: When does permitted access begin and end (timing is important)
- Where: Where is the consumer, and where is the provider? (could be more friction for regulation/compliancy)
- Why: Why does a consumer need access to specific asset. Job function?
- **How**: Are there limitations on how asset is accessed? Is it only via VPN? Is posture assessed?



Modify common policy models method

Unmanaged Policy

Application Types	Authenticators / App Policies	Device Trust Features
• New employee onboarding • Helpdesk • etc	• Require one of the following methods • Password + Push Notification • Password / WebAuthN • WebAuthN (no pin/bio required) • Session duration: re-auth @ each sign-on	• Not applicable

Bronze Policy

Application Types

- Essential, low risk apps

Authenticators / App Policies

- Require one of the following methods (two if risks detected)
- Password + Hardware / software-based OTP
- WebAuthN (no pin/bio required)
- Session duration: re-challenge @ 12-hour

Device Trust Features

- Managed: Corp
- Trusted endpoints: (UEM/MDM integration)

Platinum Policy

Application Types

- Most sensitive apps
- Apps with PCI, PII, etc

Authenticators / App Policies

- Requires combo of:
- Phishing resistant + biometric required
- WebAuthN + pin or biometric required
- Session duration: re-auth @ each sign-on

Device Trust Features

- Managed: Corp
- Trusted endpoints: (UEM/MDM integration)
- ** Endpoint risk score (e.g.. Cisco security risk score < = X, Crowdstrike ZTA < = X)
- Behavior Detection

Zero Trust Roadmap

- Monitor and detect
- Define metrics
- Iterate for ZT maturity

Monitoring and Measuring Progress

Monitoring

- A comprehensive monitoring and analytics program is critical to evolve ZT
- Monitoring user/device behavior, app behavior, network traffic, and security telemetry is key.
- Establish KPIs, monitor/evaluate, and creating an environment for continuous improvement.

Incident response (IR) and remediation

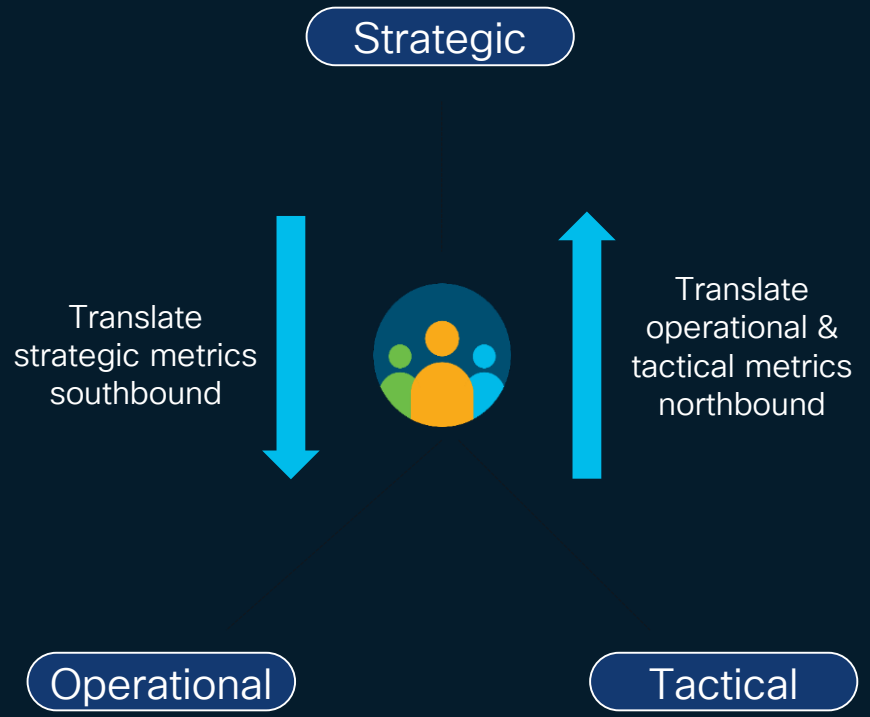
- A comprehensive IR plan that aligns with the Zero Trust principles is a key factor.
- Having **defined roles** responsibilities, and **clear escalation paths** is important.
- Goal = implement IR mechanisms where possible (tying actionable responses to behavior and IoCs), regularly update/test toward ZT maturity.

Metrics and Accountability

- Clear metrics and accountability mechanisms implemented to measure the ZT progress
- Define **strategic and tactical KPIs** that align with the organization's goals
- Hold individuals and **stakeholder teams accountable** for their assigned tasks.

Metrics

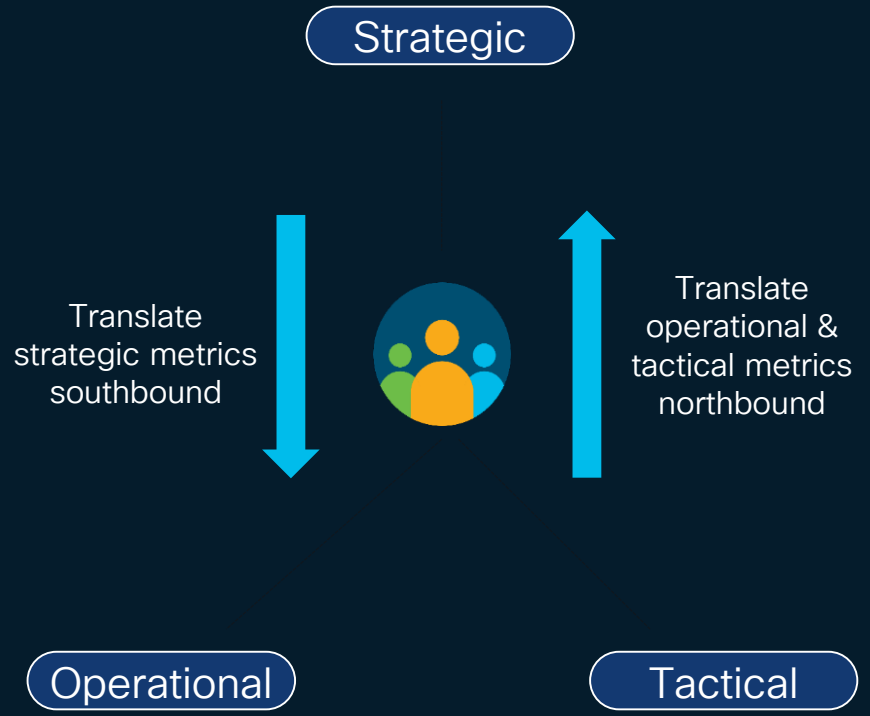
Metric Type	Meaning
Strategic	• **Target audience**: CxO and heads of business • **Use**: impact on brand reputation, customer loyalty
Operational	• **Target audience**: Business unit and technology leads • **Use:** How well the teams are supporting ZT protection
Tactical	• **Target audience**: security staff • **Use**: provide data on prioritizing efforts and time on tasks



Metrics Examples (Strategic)

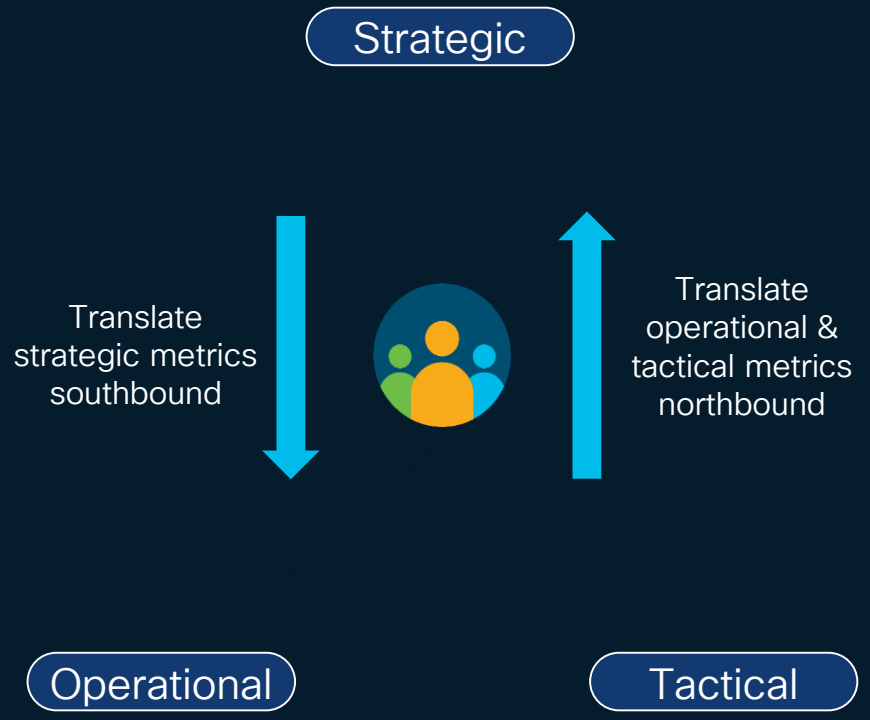
Impact on performance, market perception, brand, customer loyalty

Metric	Meaning
Maximize business performance	• Revenue loss due to IP theft • Organization security rating (cybersec insurance)
Increase / maintain customer base	• Number of breaches requiring notification (sensitive info – PCI, PII, etc), as this could damage company reputation • Customer experience index
Recruit, retain, & enable employees	• Retention rate for security employees • Employee Experience Index



Metrics Examples (Tactical)

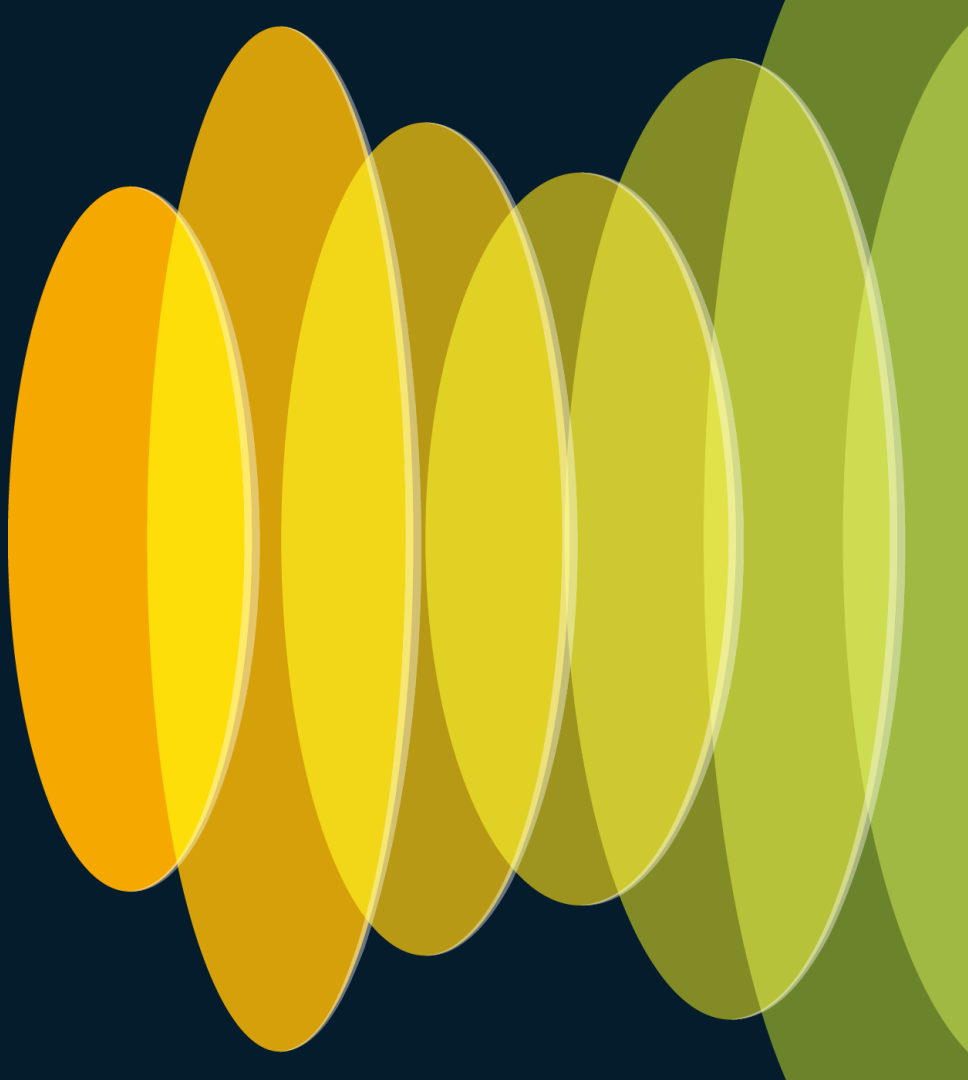
Metric	Meaning
iAM	• % employees adopting MFA • % employees covered by PIM • % employees with password-less
Device	• % of devices used with trusted endpoint • % of devices using conditional access policy • % of devices with integrated threat protection
Network	• % of internal traffic encrypted • % of external traffic encrypted • % of traffic mapped to app profiles
App	• % of SSO enabled • % of apps with conditional access policies • % of apps with formal CI/CD sec tactics
Data	• % of data classified & labeled • % of data protected using DLP policies



Iterate for Maturity – Suggestions

- **User lifecycle:** Update, evolve, automate lifecycle management of users as they enter, use, and exit the organization.
- **Admin access:** Create process to approve admin access when required (as opposed to standing admin access).
- **Device lifecycle**: Update, evolve, automate the lifecycle management of devices.
- **New App criteria:** Update the release criteria for new apps to be sure these are included in the scope of Conditional Access policies
- **Legacy systems**: Assess landscape for additional legacy systems that can be negated
- **Reassess risk:** Continually reassess risks and cyberthreat landscape and evolve SecOps procedures, responsibilities, policies, & priorities.

Cisco’s latest advancements for ZT maturity

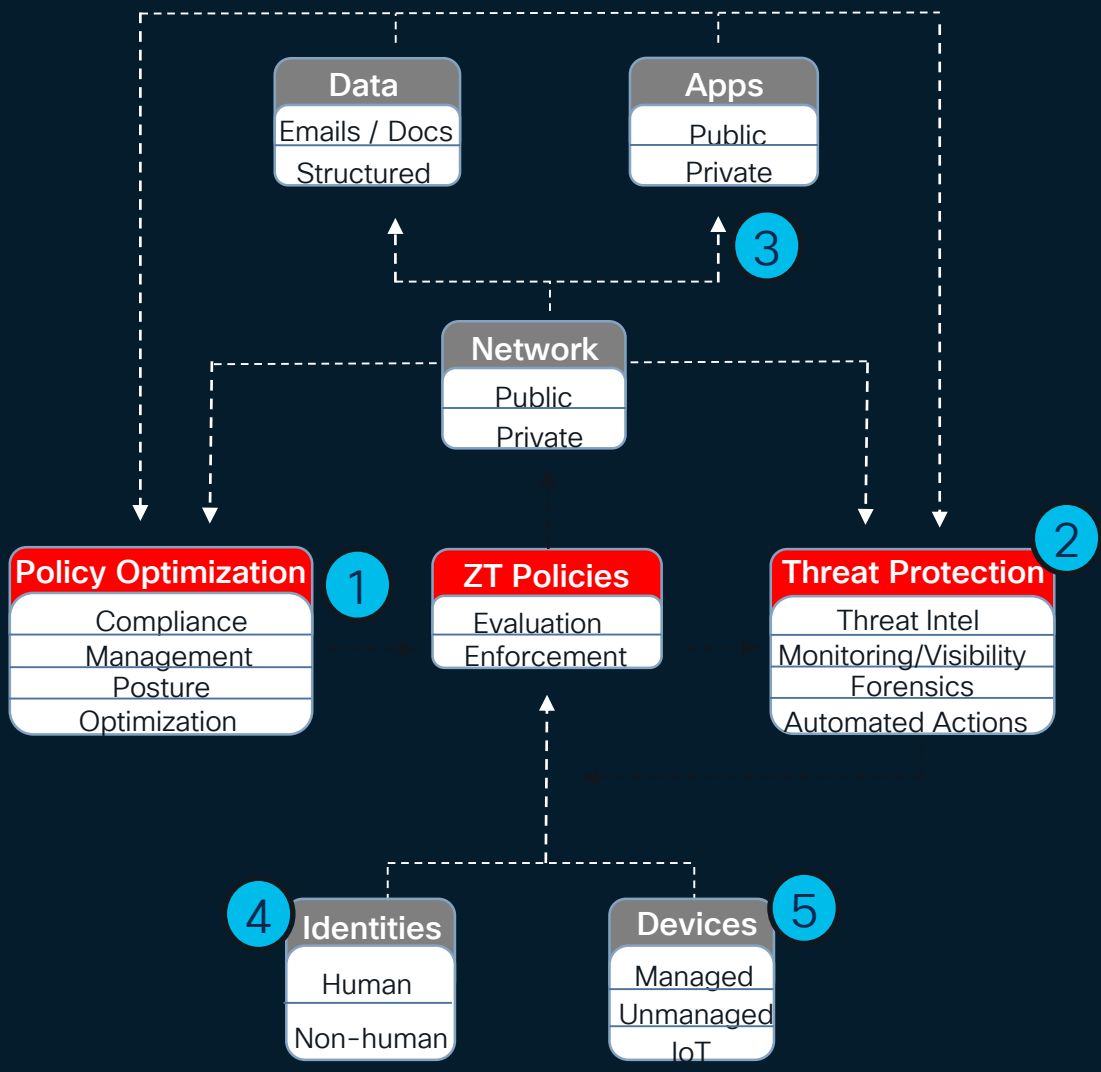


cisco Live!

Zero Trust Advancements

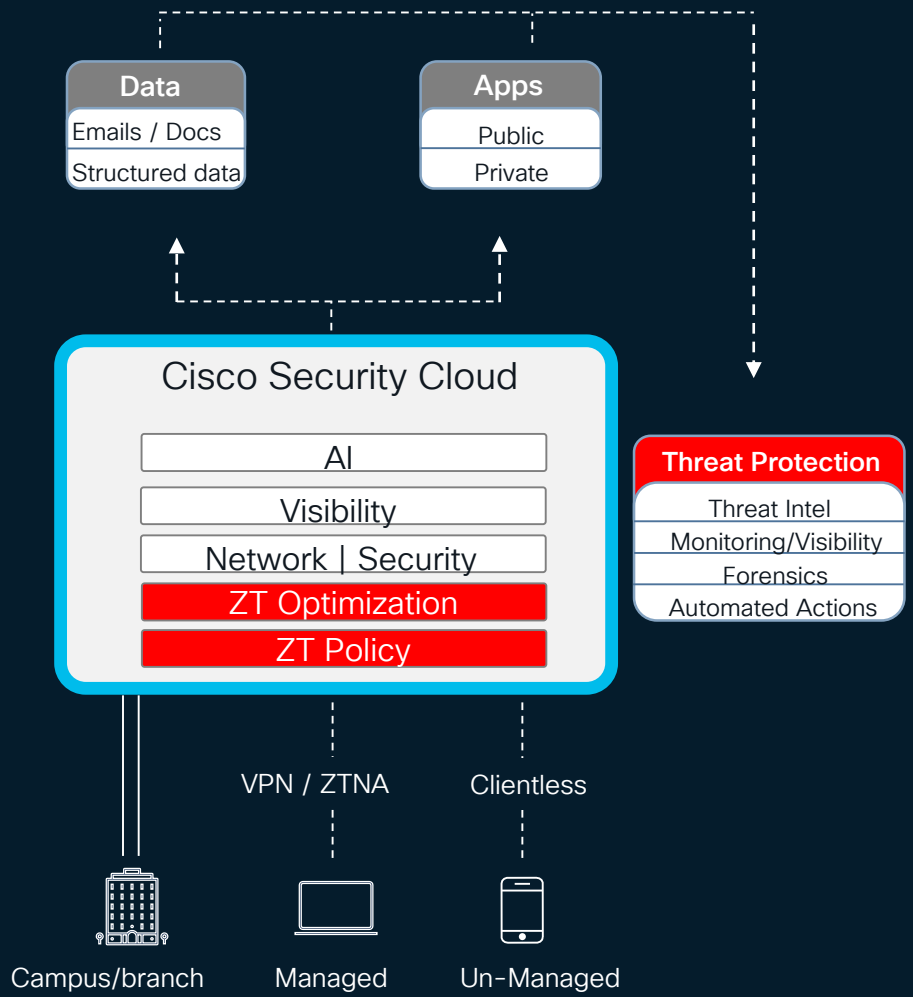
1. Security Cloud - Secure Access
2. Splunk
3. Hypershield
4. Identity Intelligence
5. Secure Client

*** Integration & Automation keys to ZT Maturity*



Secure Access
Consolidates ZT Policy/Optimization

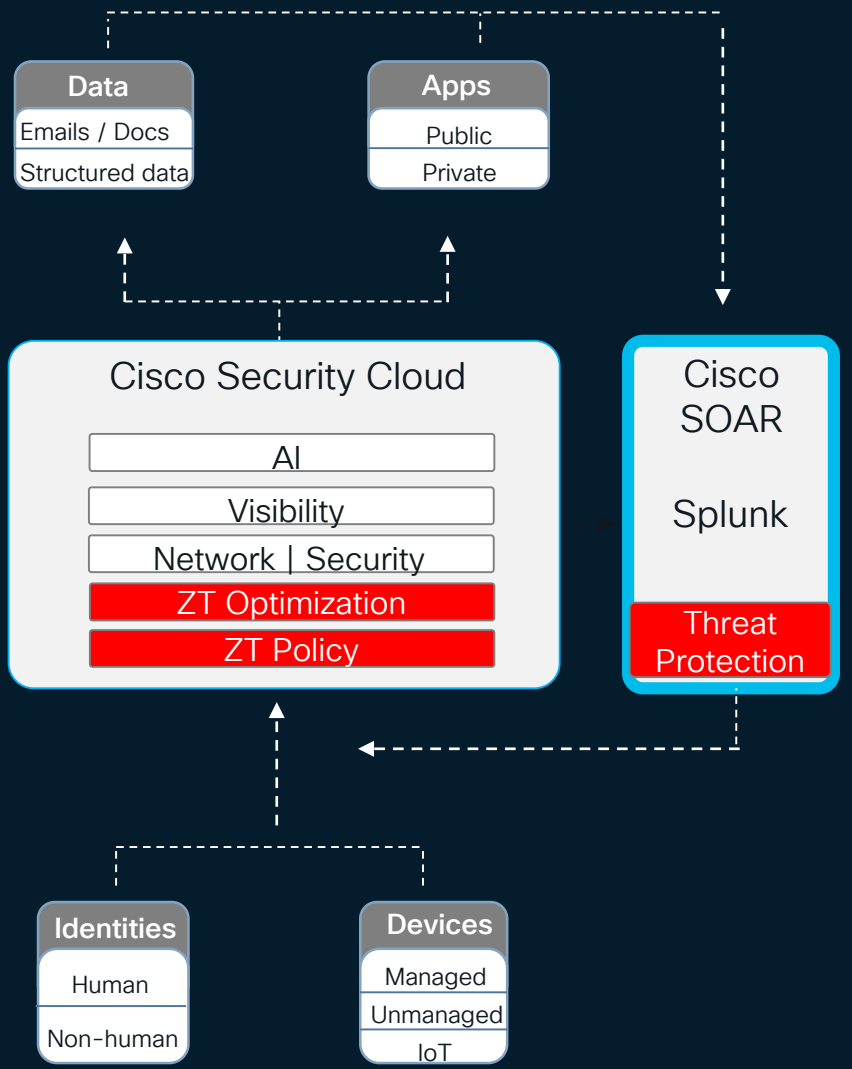
- Security SaaS
- ZT Policy – centralized brain for ZT policy/optimization including **user identity** and **device posture** controls under single UI
- Network - Consolidate connections for all on-premesis and remote user connections
- Security – Consolidates/integrates security capabilities FW, IPS, SWG, CASB, DLP, RBI



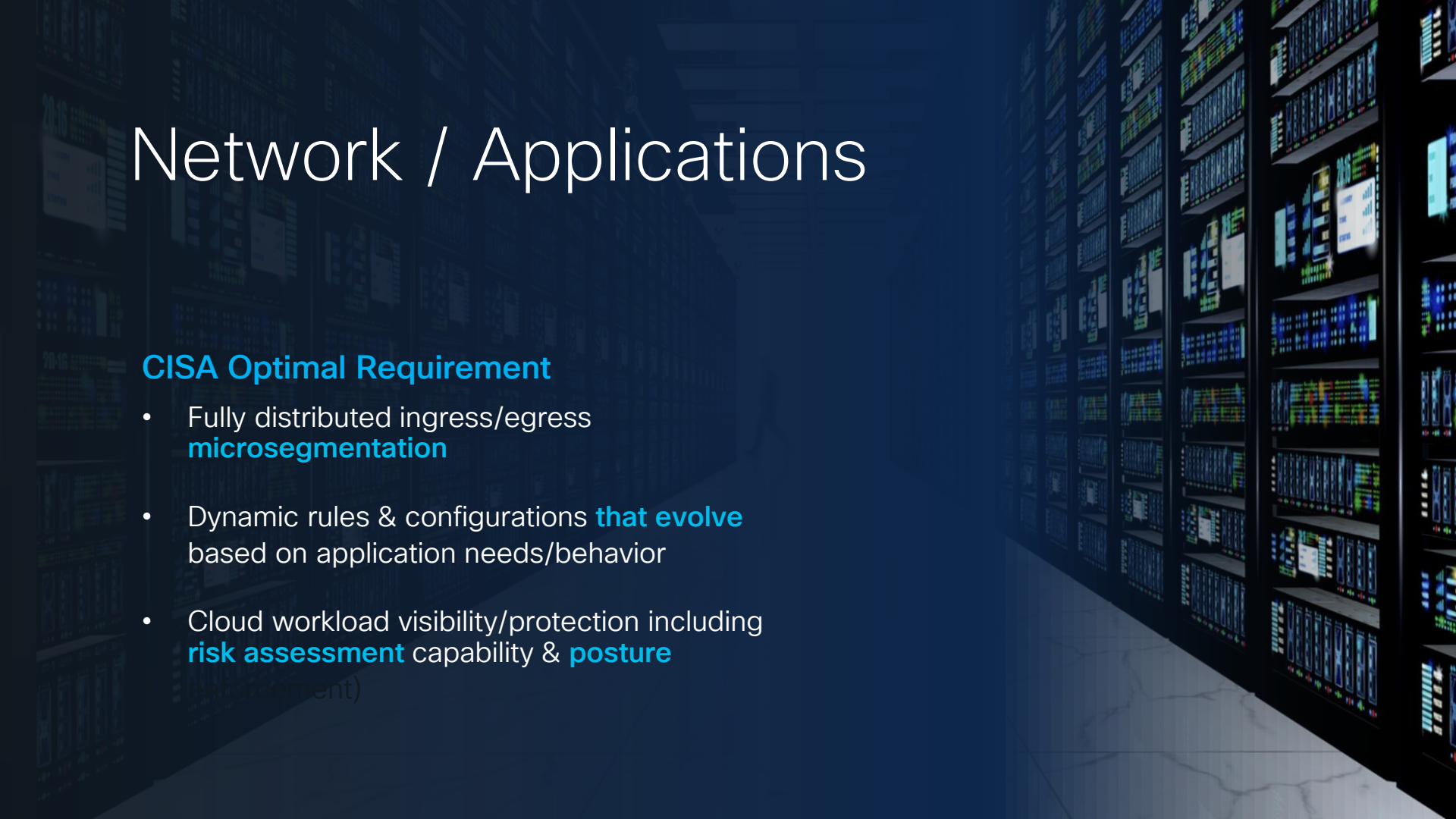
Splunk

Consolidates telemetry for ZT threat protection

- SIEM / SOAR
- Embrace **federated data access** for comprehensive visibility
- **Unified threat detection**, investigation, and response dramatically improving MTTD and MTTR.
- Deploy **full-scale automation** across threat analysis, containment, response and recovery actions increasing security team's productivity and efficiency.
- **Leverage AI** for enhanced security operations to help increase efficiency and effectiveness of the security team



Network / Applications



CISA Optimal Requirement

- Fully distributed ingress/egress **microsegmentation**
- Dynamic rules & configurations **that evolve** based on application needs/behavior
- Cloud workload visibility/protection including **risk assessment** capability & **posture** enforcement)

Cisco Hypershield

Foundational Elements

EBPF

- Hyper-distributed L7 capabilities
- Runs sandboxed programs in Linux Kernal w/o changing source code
- Network filtering (in/egress)
- Observability identify process flows
- Security identify process & behavior to trigger policies at Kernal level

Hardware Acceleration

- Accelerate repetitive tasks
- Inside servers, routers, switches
- No routing to security engines, bring engines to source

AI

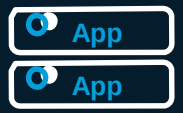
- AI built inside product
- Use of AI to automate patch testing & deployment


ISOVALENT

Where to consume

Public Cloud

VM's K8 Clusters



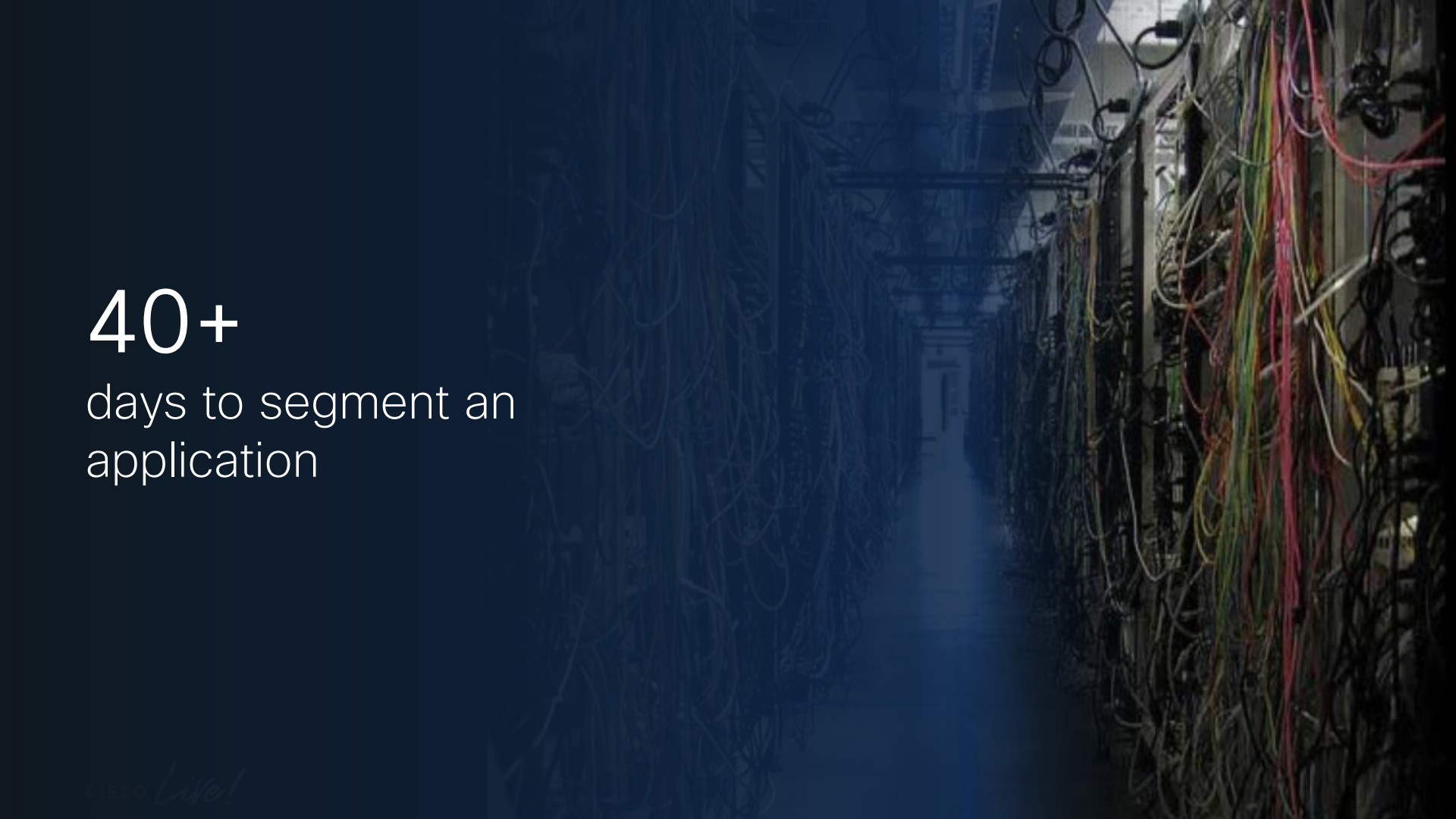
Private Cloud

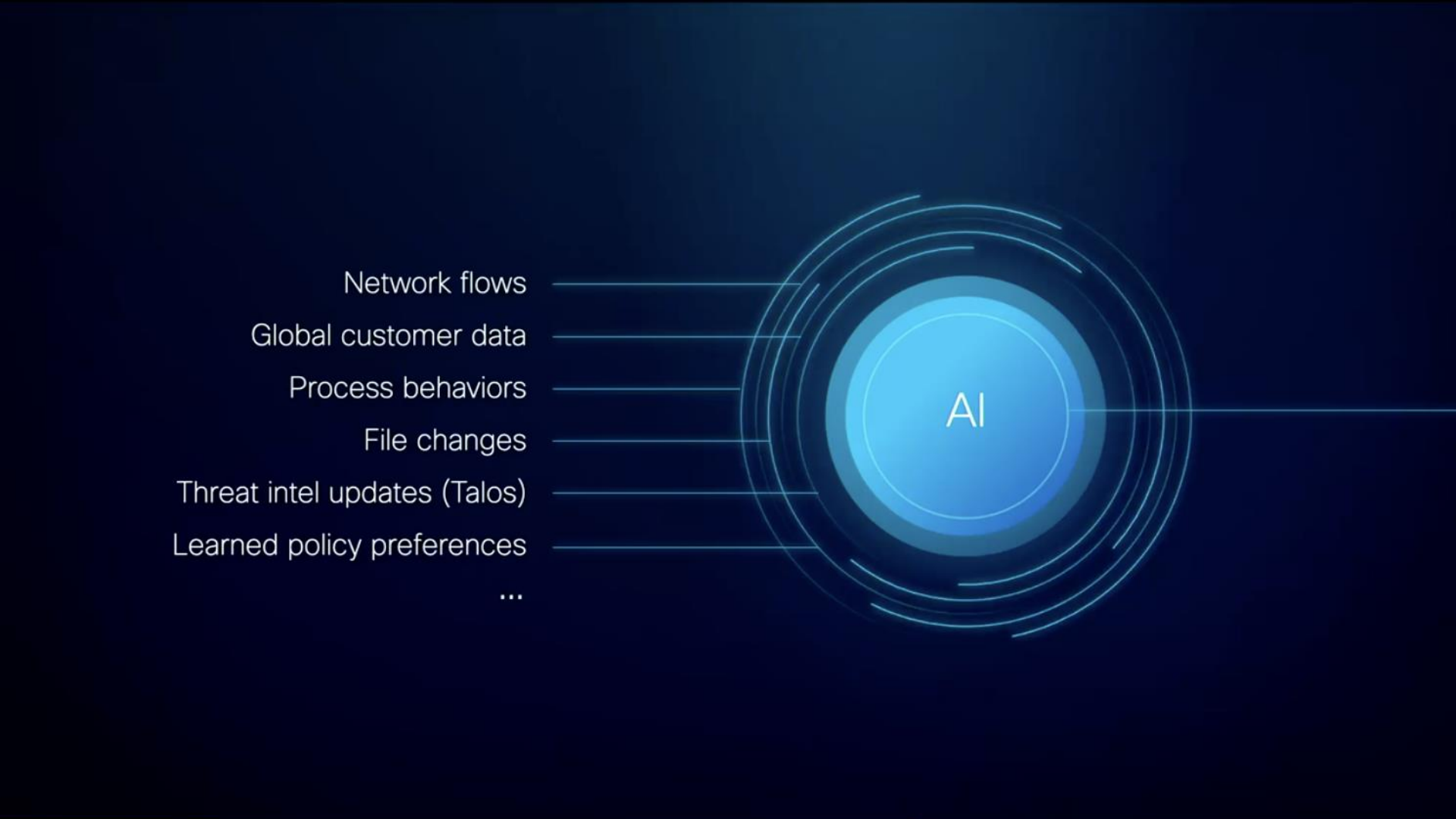
Can run in **server** at Kernal level (between Kernal & physical) – or- on **network devices**

IoT

Can put in **DPUs** in the switch that IoT device connects to for security closest to source

Segmentation
is Challenging


40+
days to segment an
application

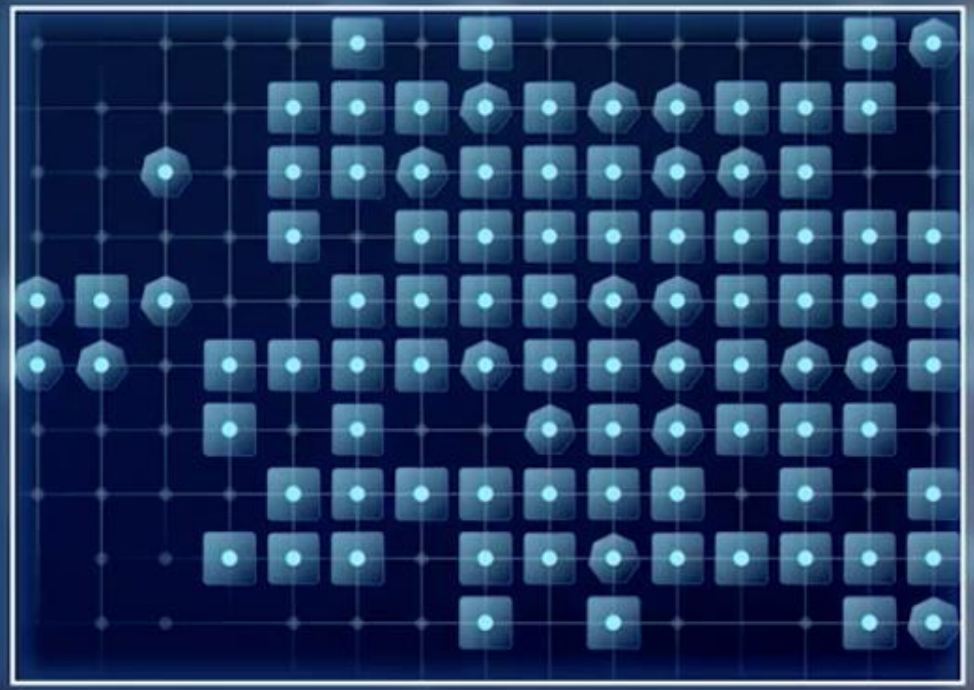

Network flows
Global customer data
Process behaviors
File changes
Threat intel updates (Talos)
Learned policy preferences
...
AI

APPLICATION DISCOVERY

CONFIDENCE

Listening

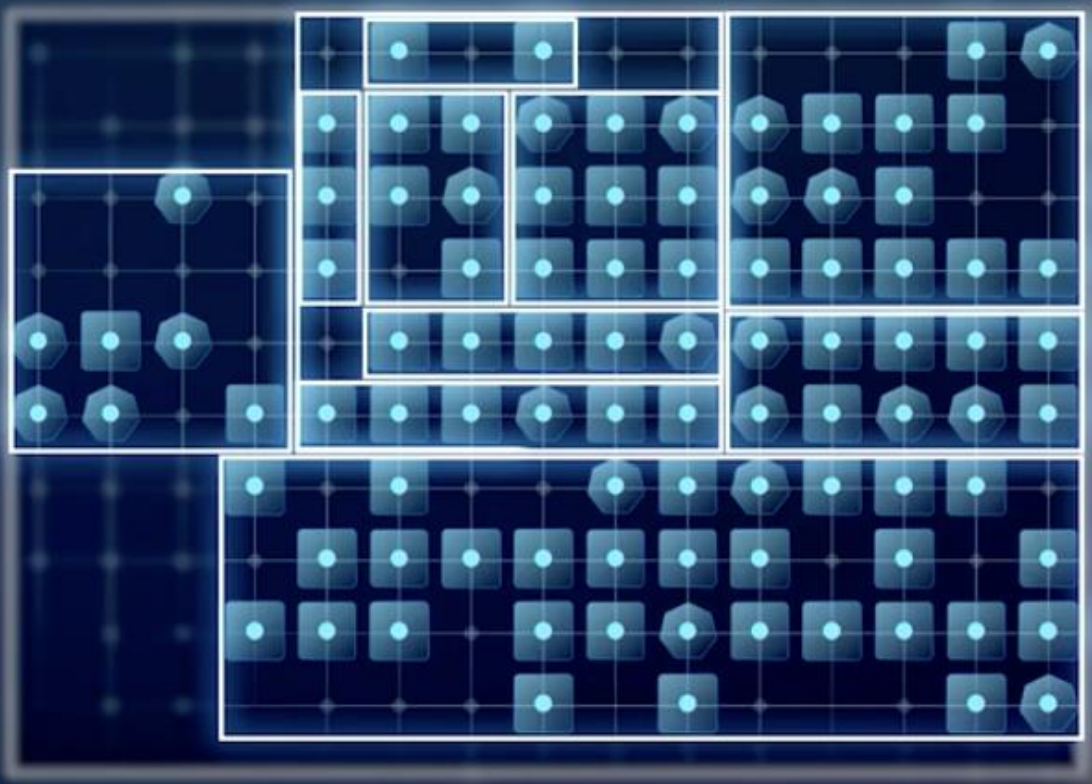
Carving out portions based on what we learn



APPLICATION DISCOVERY

CONFIDENCE

As you learn segmentation becomes more granular



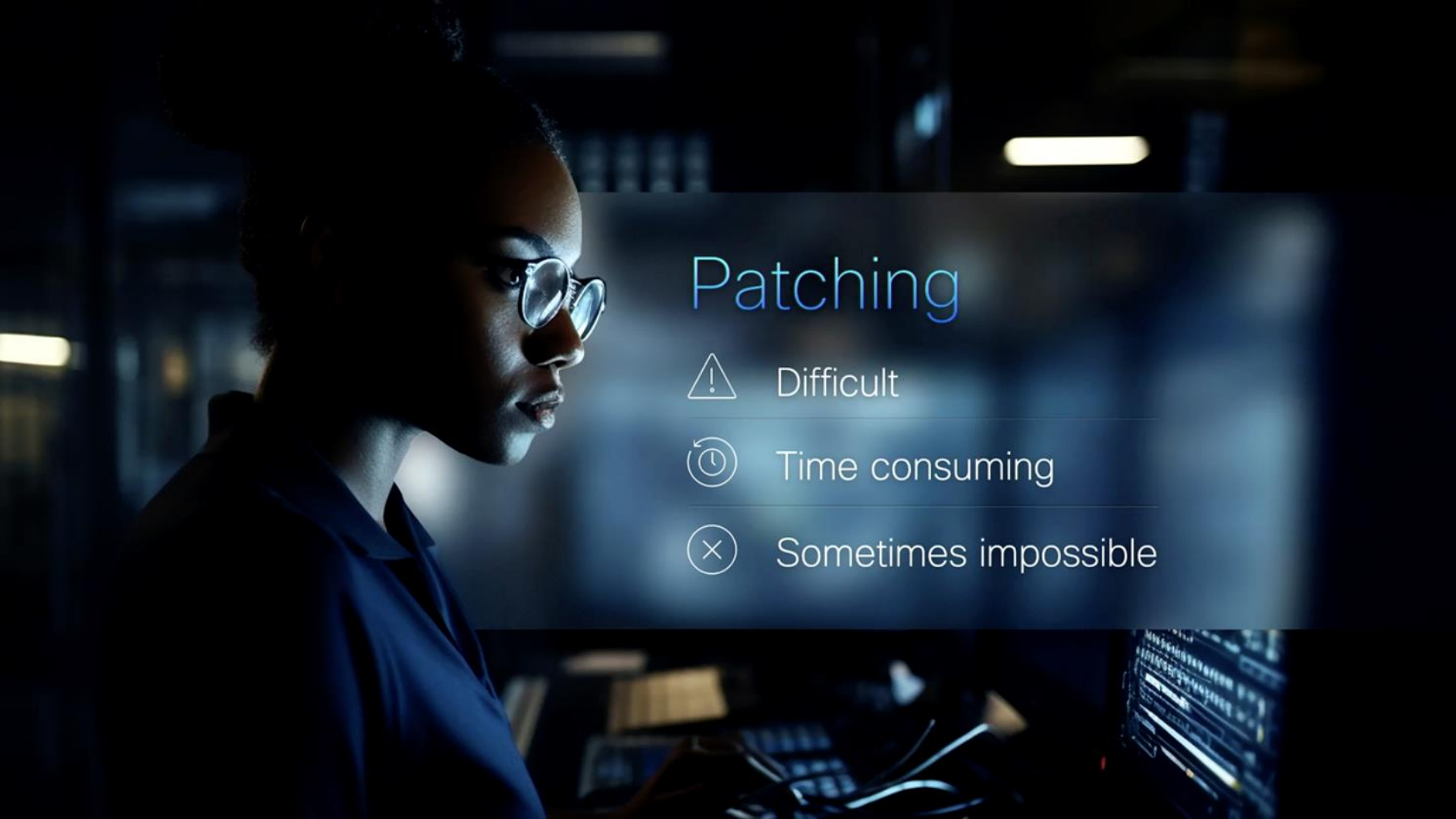
APPLICATION DISCOVERY

CONFIDENCE

Change – policy relaxes, learns, & re-applies

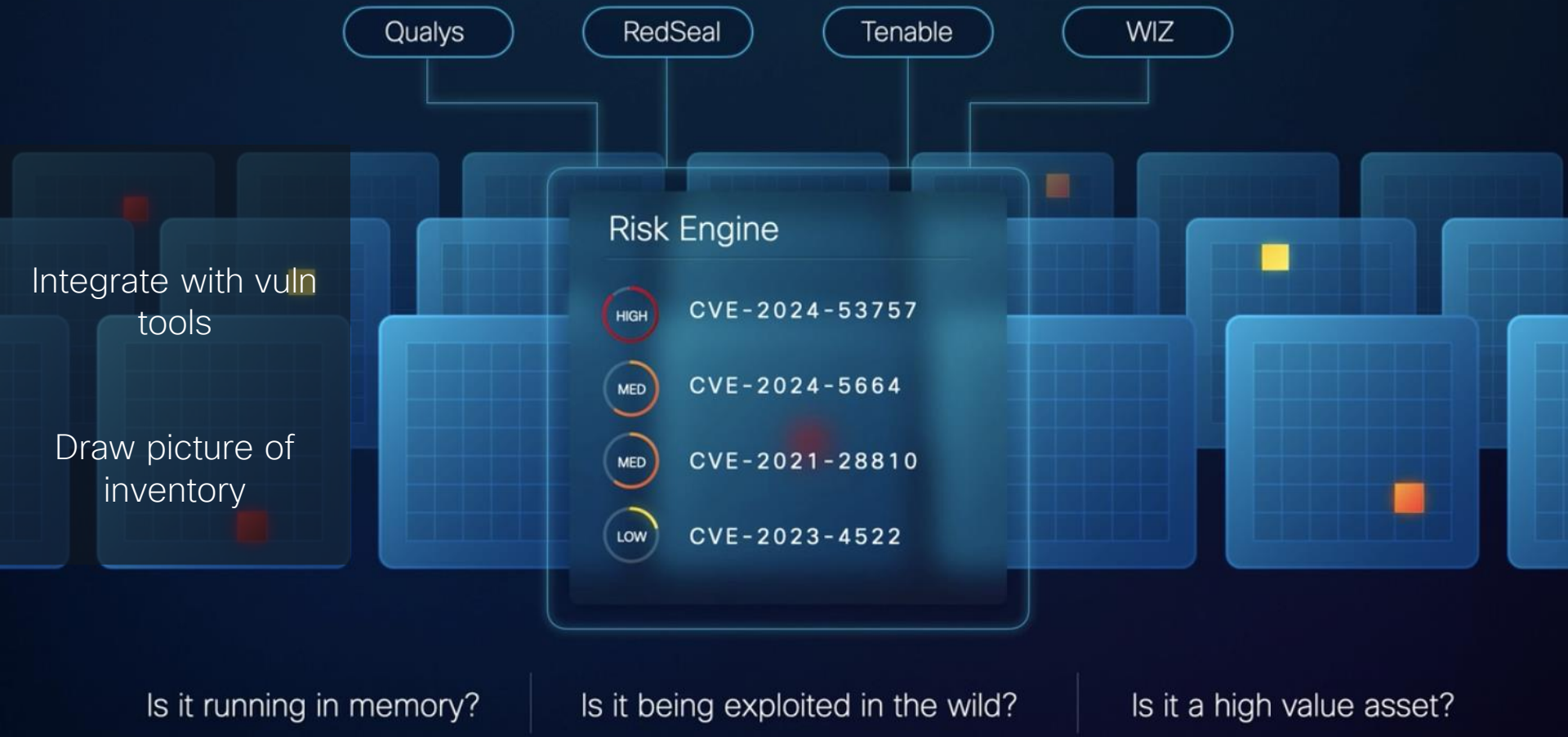
Segmentation at any scale

FB, Google, MS, Netflix

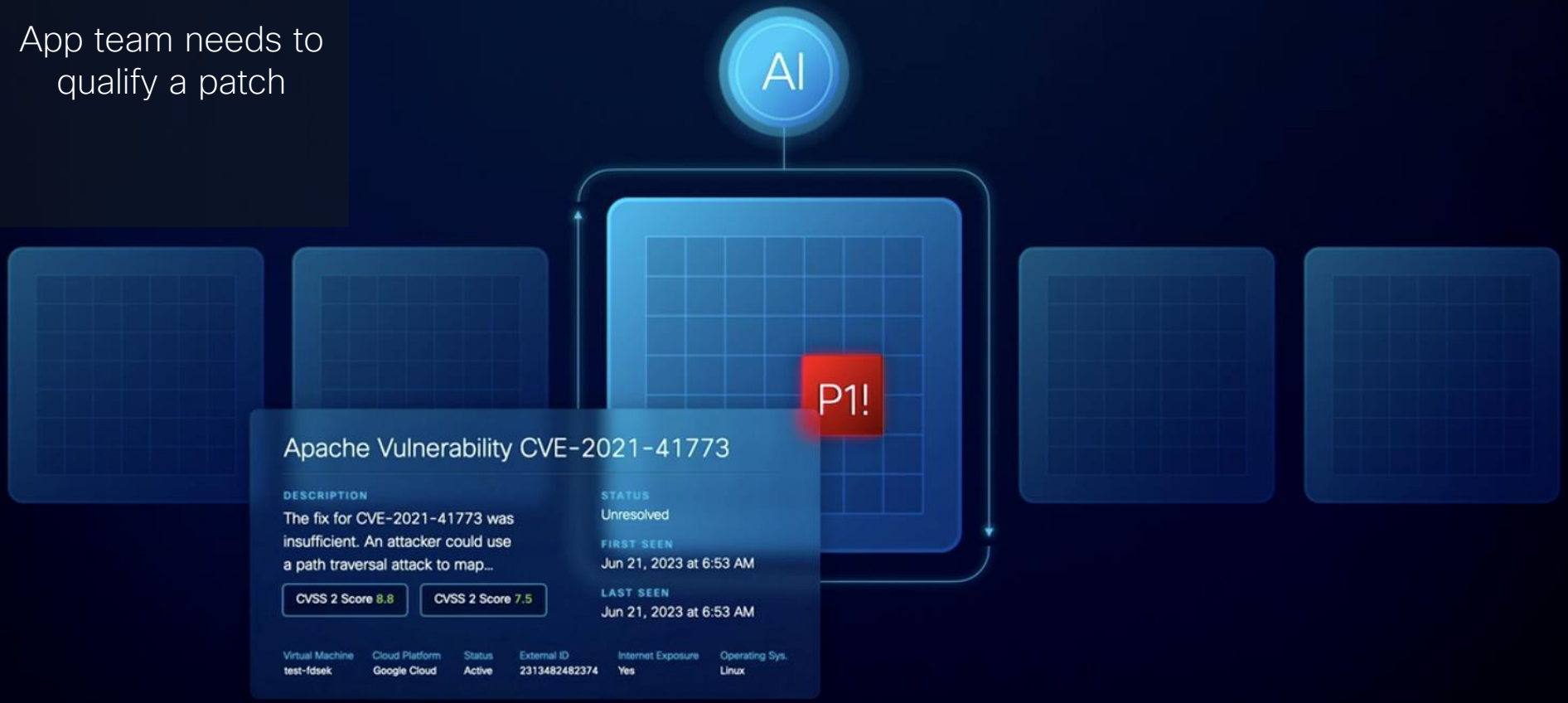

Patching
Difficult
Time consuming
Sometimes impossible

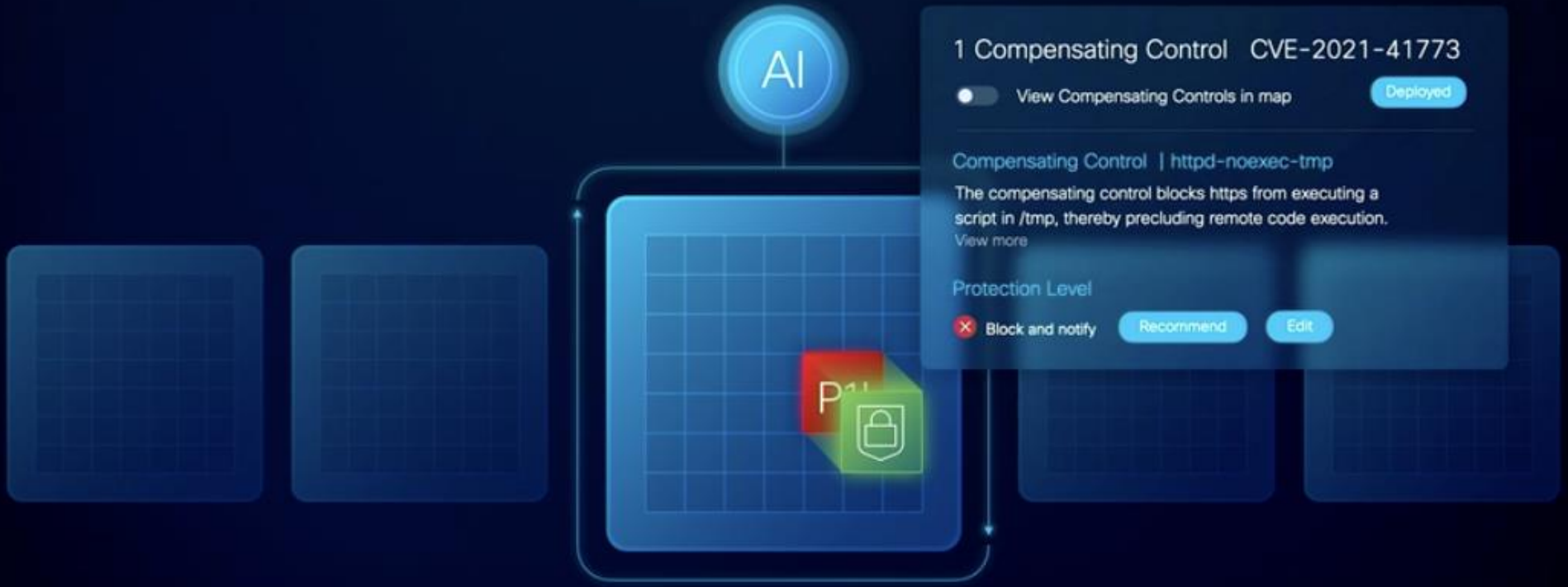
Timeframe for vulnerability being known to being exploited is shrinking quickly

Average time for a patch = 25-49 days

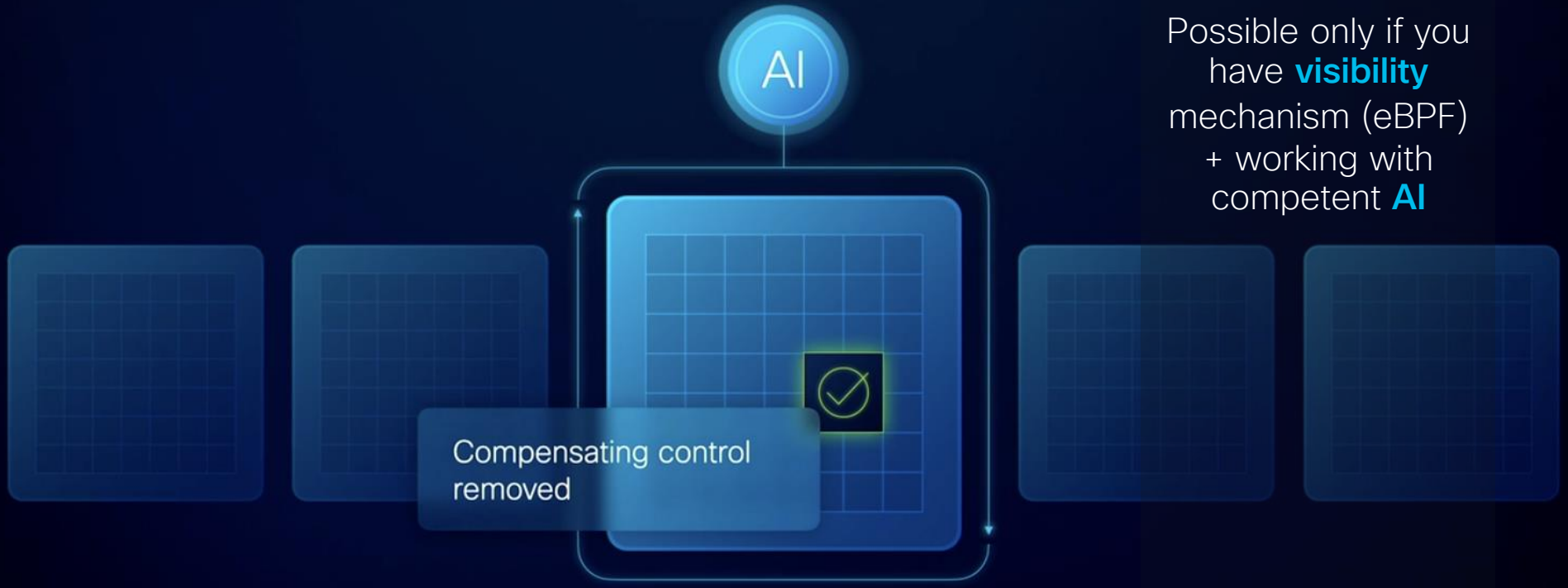

Qualys
RedSeal
Tenable
WIZ
Integrate with vuln tools
Draw picture of inventory
Risk Engine
HIGH
CVE-2024-53757
MED
CVE-2024-5664
MED
CVE-2021-28810
LOW
CVE-2023-4522
Is it running in memory?
Is it being exploited in the wild?
Is it a high value asset?

App team needs to qualify a patch





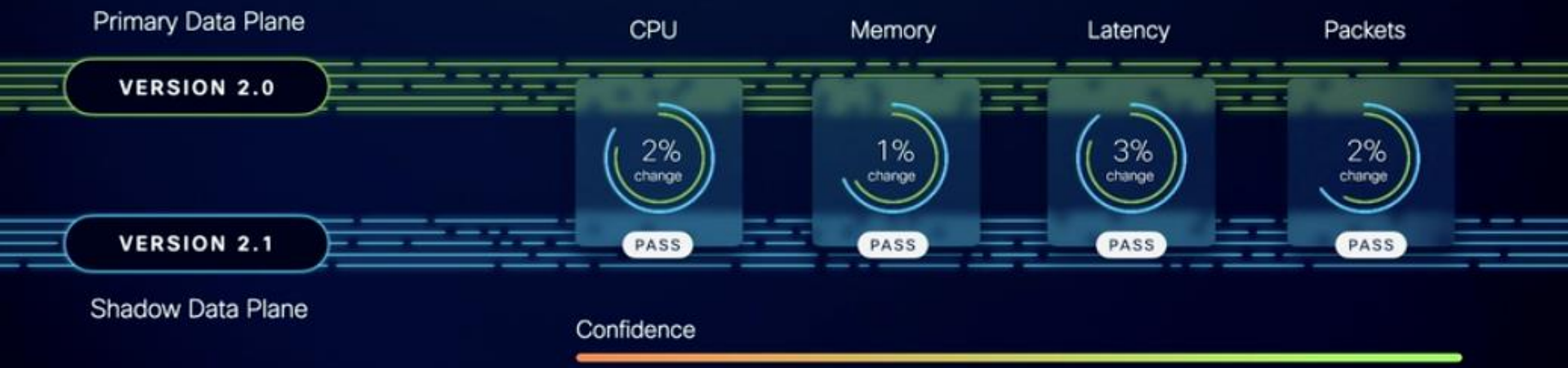
Perfect fit | Tested against real world traffic | Optimal placement



Possible only if you have **visibility** mechanism (eBPF) + working with competent **AI**

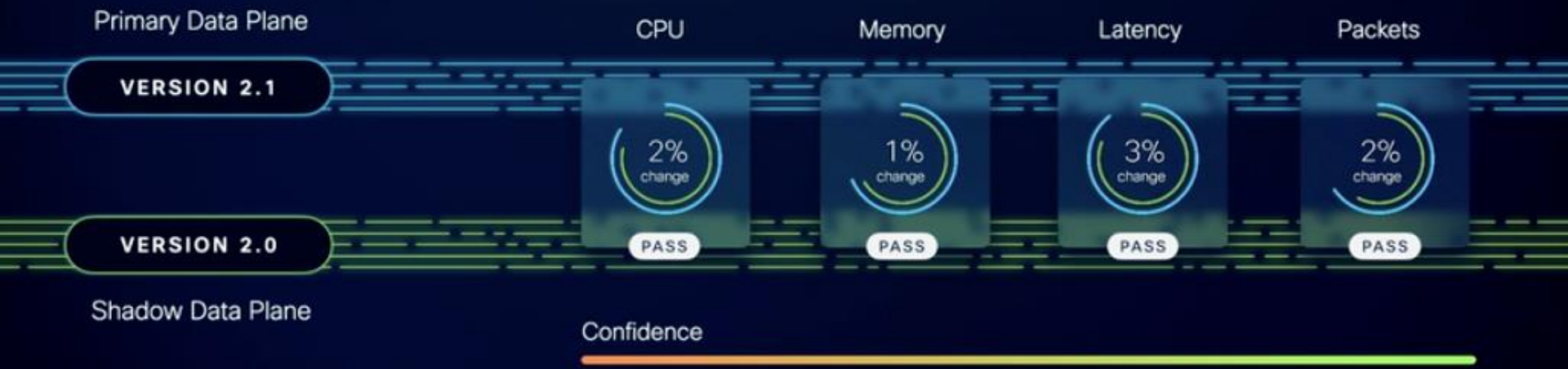
Dual Data Plane: Upgrades

Dual Data Plane: Upgrades



Using AI
compare performance of
current version vs new version

Dual Data Plane: Upgrades



Using AI
Move 1 flow at a time from
shadow to primary DP

Dual Data Plane: Upgrades

Over time – gain confidence in upgrading capabilities

Upgrades will become predictable

General Availability

August

Pricing

Per workload / per port for network-based enforcement

Packaging

SaaS , hardware a-la-carte

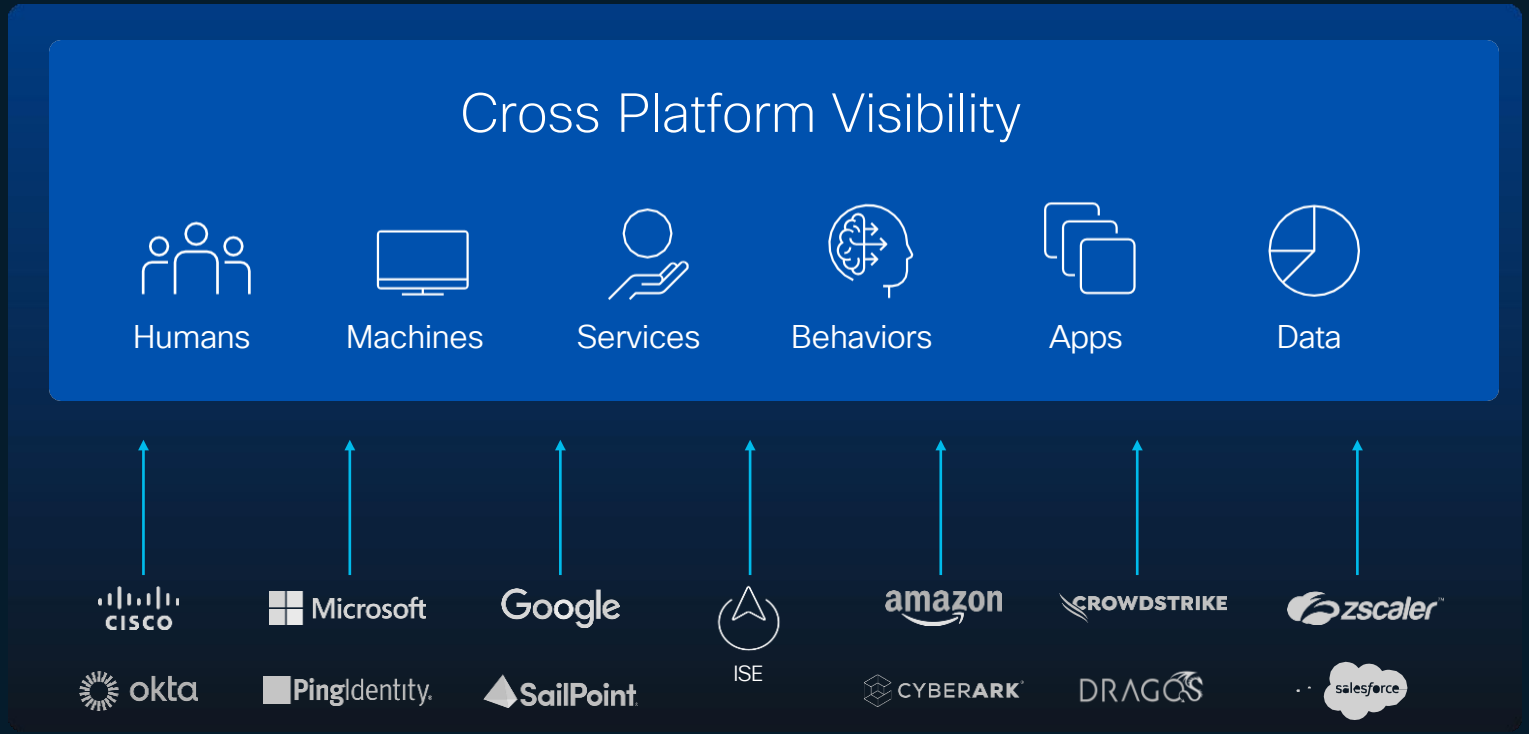
Identity

CISA Optimal Requirement

- Consistent validation & risk analysis
- Enterprise-wide identity store integration

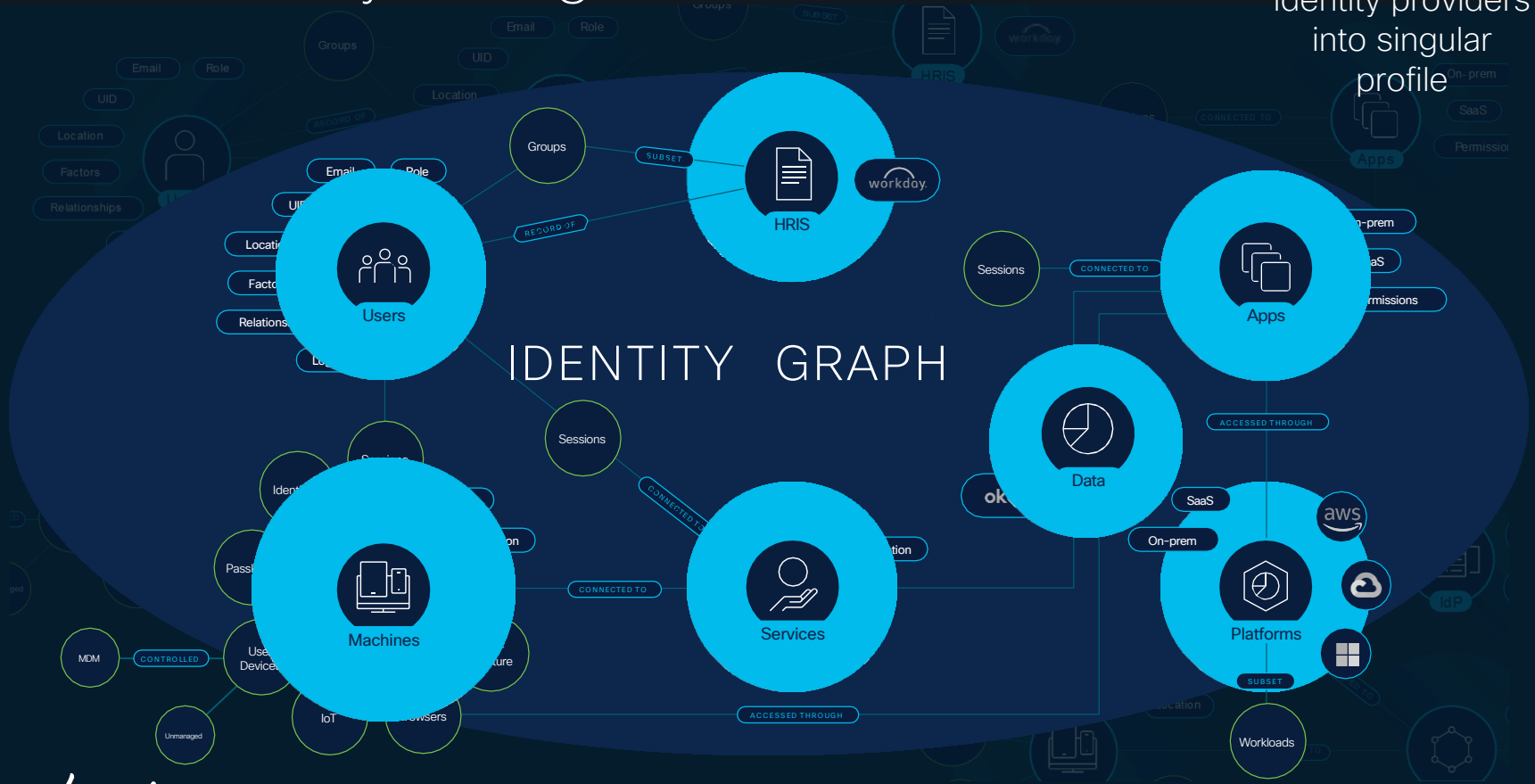
Cisco Identity Intelligence

Correlate intel – user, device, HR info, apps

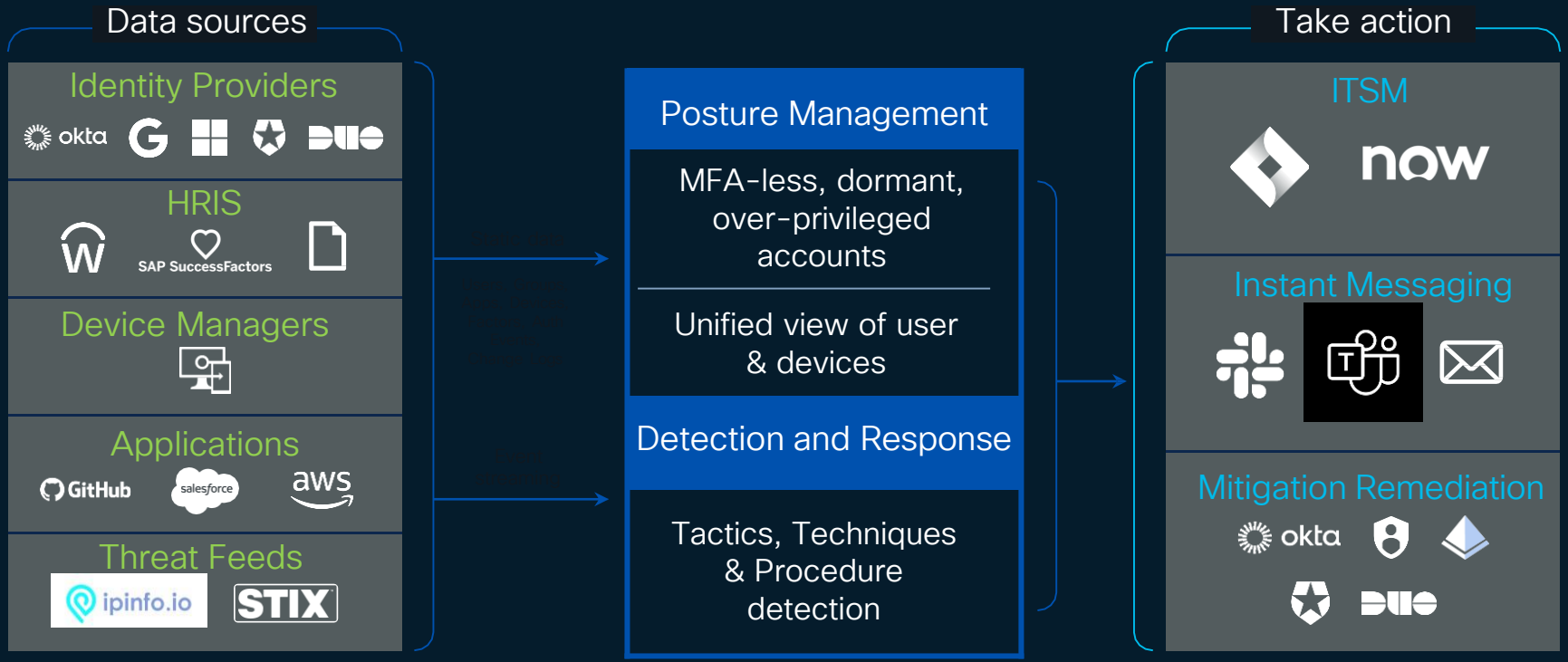


Cisco Identity Intelligence

Consolidates data from diverse identity providers into singular profile



Enhanced visibility across your identities & apps



Cisco Identity Intelligence

Available July 2024

Smart Authentication

with Cisco Duo

Smart Access

with Cisco Secure Access

Smart Threat Detection

with Cisco XDR

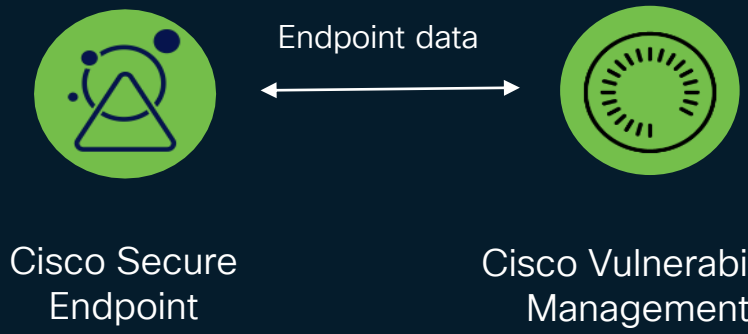
Devices

CISA Optimal Requirement

- Integrate device mgmt, software approval, config, & vuln mgmt solutions (continuous insight for compliance
- Resource access depends on real-time device risk analytics
- enforcement)

Secure Endpoint & Vulnerability Management

Risk-based vulnerability management for endpoints



- Detect and understand vulnerabilities on endpoints
- Comprehensive view of risk across Secure Endpoint & other vulnerability data sources
- Prioritize vulnerabilities based on risk & asset context
- Report on risk posture and remediation progress

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

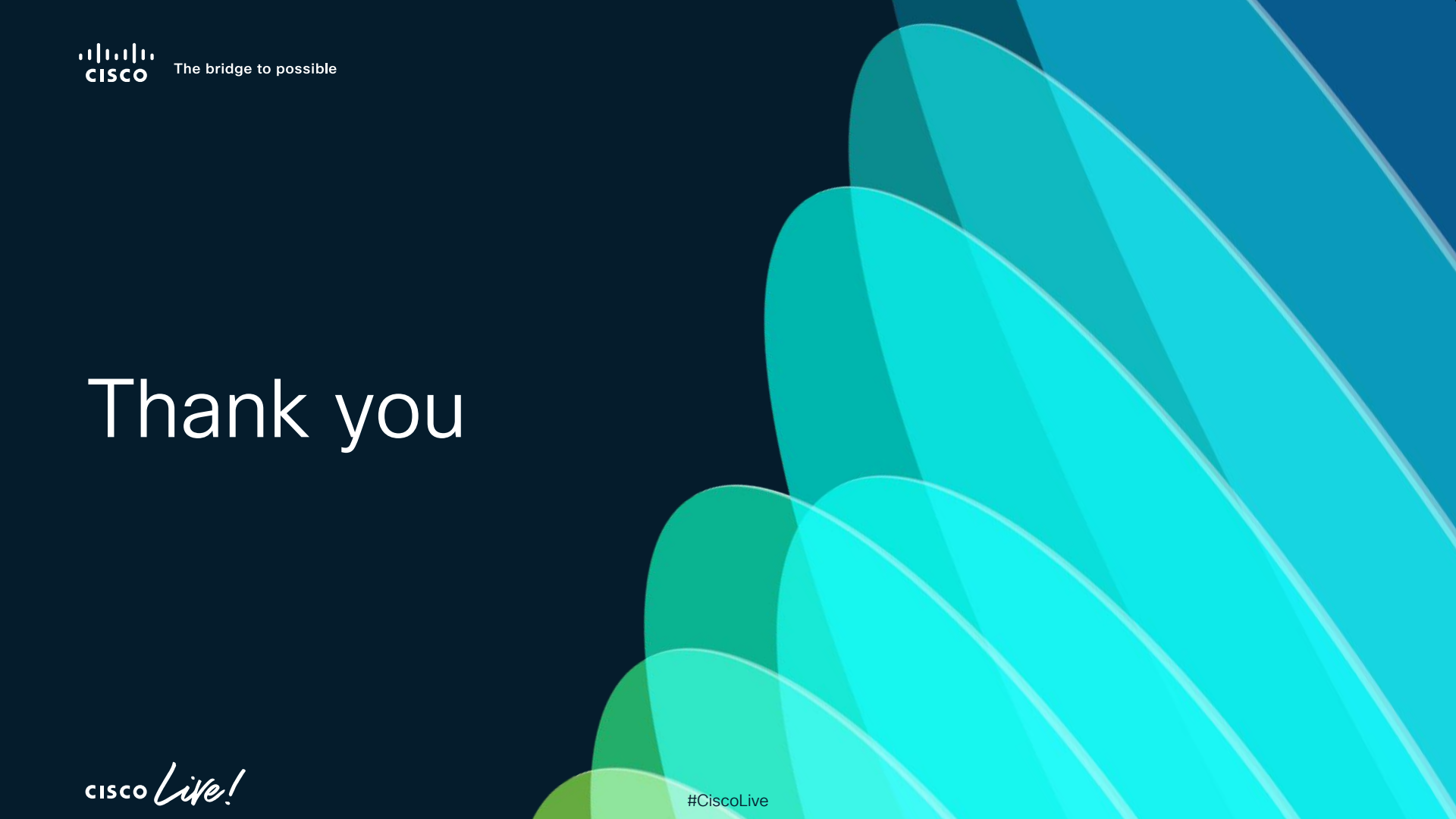
Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

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

Contact me at: ansabell@cisco.com


The bridge to possible
Thank you
cisco Live!
#CiscoLive