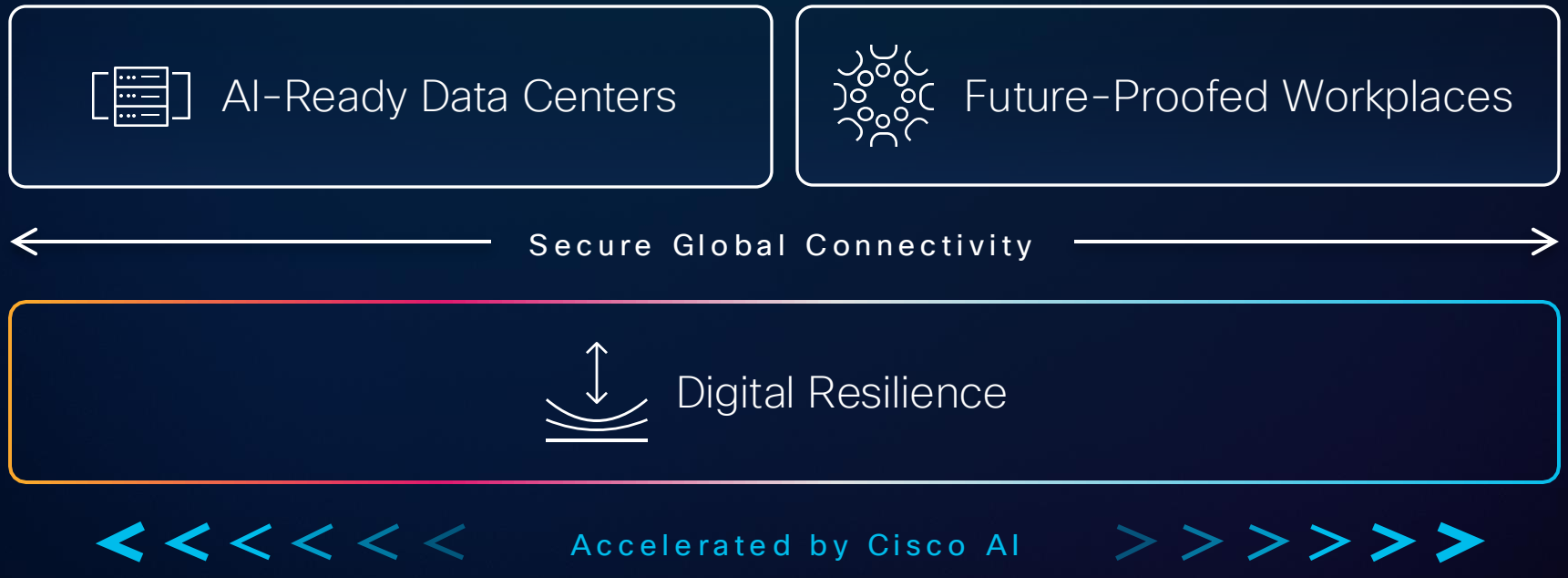
Cisco Security Architecture

Zero Trust Architecture done right

Jatin Sachdeva jasachde@cisco.com
Principal Security Architect - Worldwide

Cisco Global Security Architecture Team (GSAT)

One Cisco portfolio delivers customer outcomes



Proposed Agenda

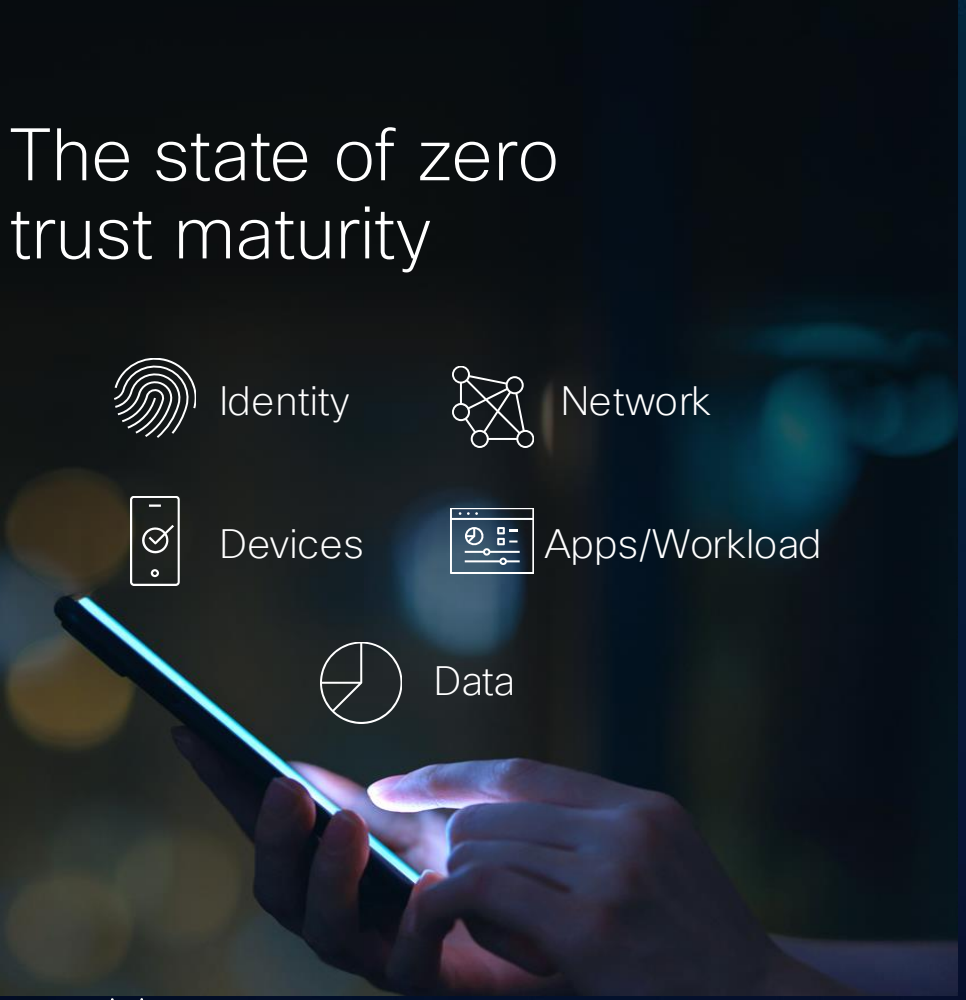
- Security Reference Architecture
- Zero Trust via Hybrid Mesh Platform
  - User and Device Security
  - Hybrid DC/Cloud Security
  - SOC of the future
- Summary

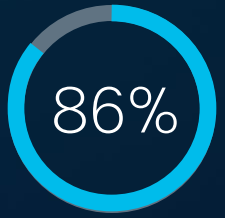
Security Reference Architecture


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 via Hybrid Mesh Platform

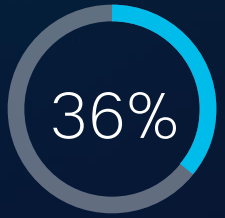
The state of zero trust maturity





Nearly all organizations have started on some aspect of zero trust (at least one pillar)

"We know we need to do it"



Have reached maturity in at least one pillar

"Our focus is on XYZ pillar"

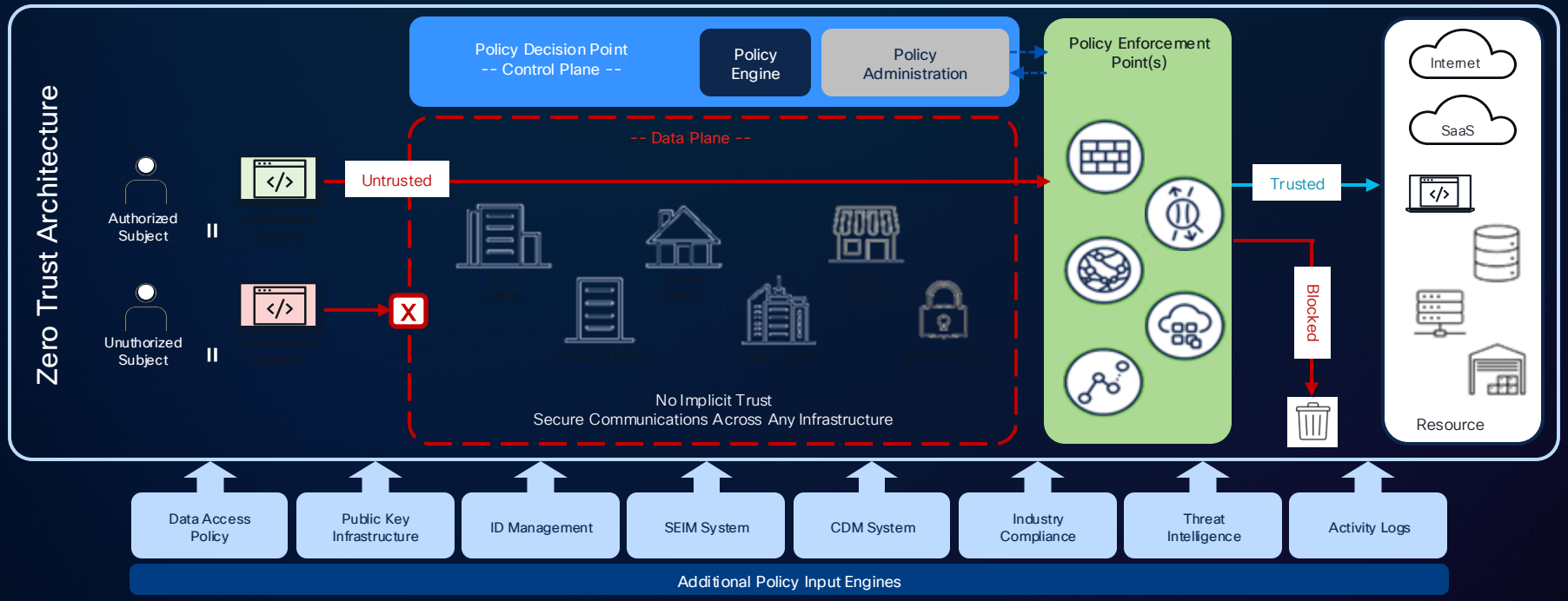
Have reached maturity across all pillars which means that 98% have not.

"We've still got a long way to go"

Source: Cisco's Security Outcomes for Zero Trust Report, 2024

Zero Trust Architecture

NIST Special Publication 800-207 Zero Trust Architecture



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

Zero Trust Policy Decision Points (PDP) & Policy Enforcement Points (PEP)

Zero Trust Platform

Single Policy Decision Point (PDP)

Mesh of Policy Enforcement Points (PEPs)

User to Application			App to App		
Access Control	AI Access	North South Segmentation	AI Model Protection	East West Macro/ Microsegmentation	Distributed Exploit Protection

Threat Intelligence & SOC

Zero Trust Policy Decision Points (PDP) & Policy Enforcement Points (PEP)

Zero Trust Platform

Cloud Management (Security Cloud Control)

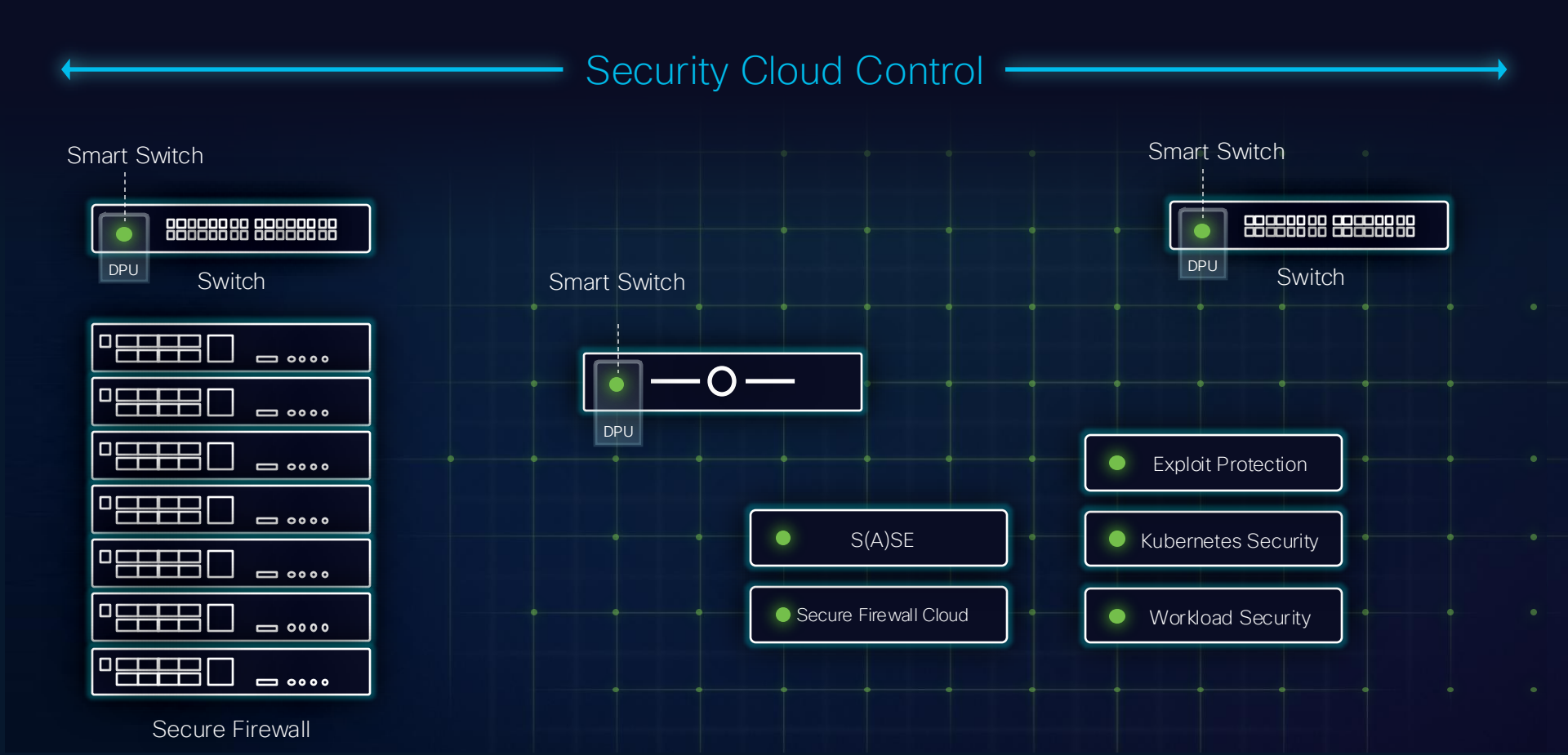
Universal ZTNA

- Access Control
- AI Access
- North South Segmentation

Hybrid Mesh Firewall

- AI Model Protection
- East West Macro/ Microsegmentation
- Distributed Exploit Protection

Cisco TALOS, Cisco XDR & Splunk



Enforcement points change, rules don’t

Cisco Security Cloud Control

Global Search

Common Dashboard

AI Assistant

Centralized Notifications

MSP Mode

Common Access Control

Common Provisioning

AIOps

Common Posture/Identity

Alerting & Notification Service

Common Objects

Policy & Intra-Product Communication

Secure Workload | Firewall | Multicloud Defense

Secure Access | AI Defense | Hypershield

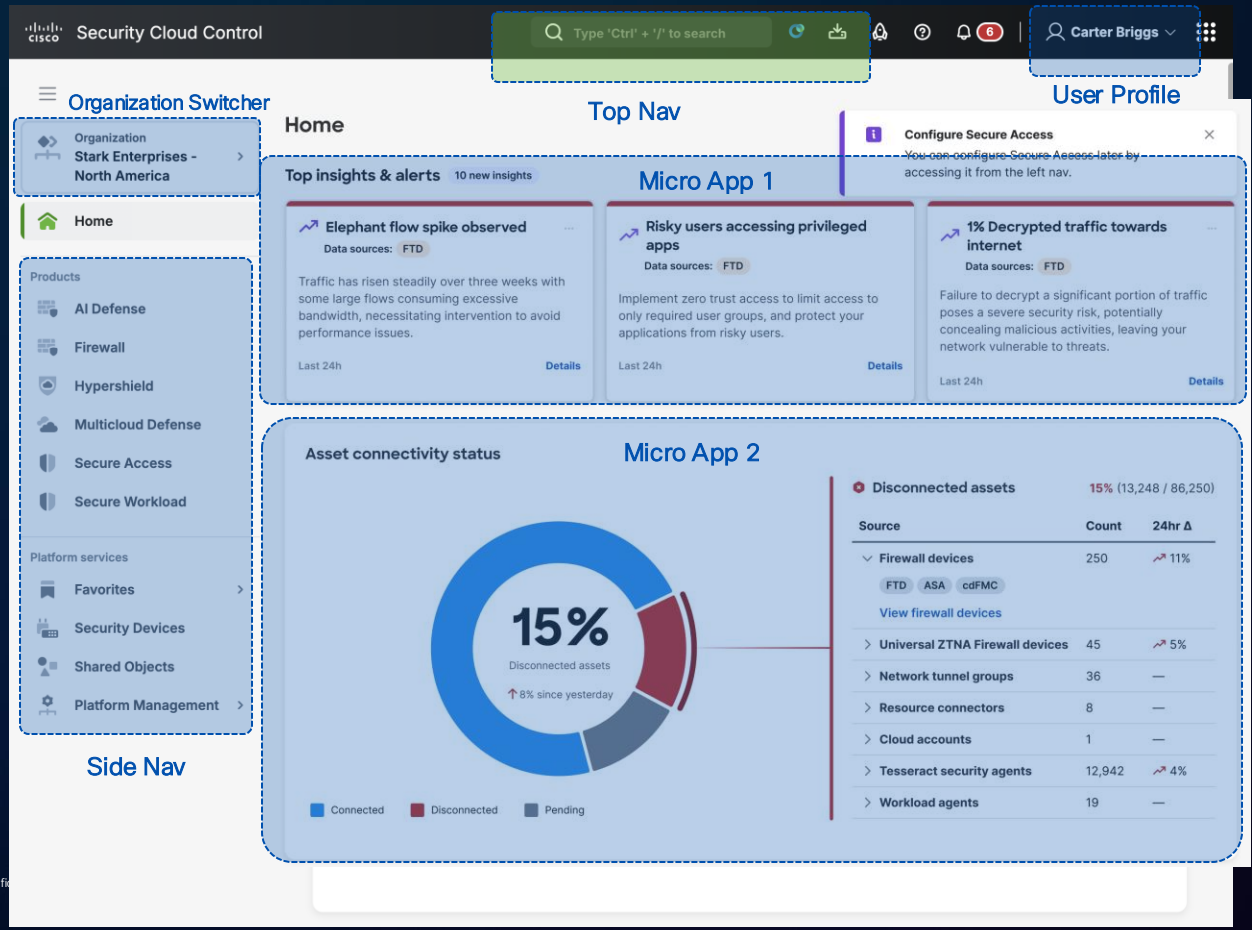
Endpoint | XDR | Splunk

Vulnerability Management | ISE | Network Analytics

Vision Delivered

Capabilities

- New left navigation integrates product menus from across the portfolio
- Shown only when products are activated and users have access
- Services like search, AI Assistant, notifications, and help expressed globally
- Organizations isolate data and contain multiple products
- View entire organization from a single admin's standpoint
- Complete RBAC control – central management, group mapping, custom roles, audit



Shift to outcome-based policy

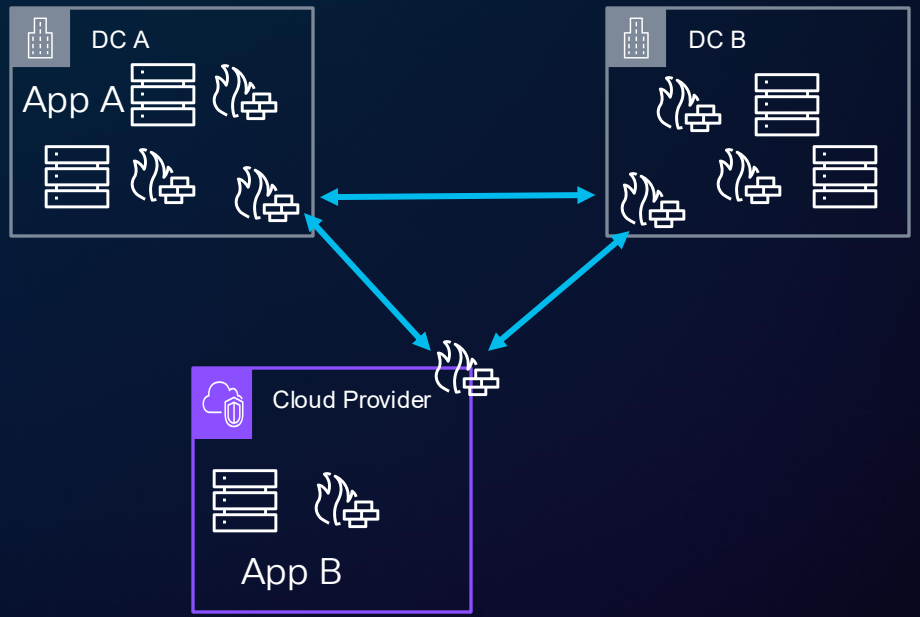
NEW

What it is

- Topology-aware, vendor-agnostic, outcome-based L3/L4 policy orchestration
- Intelligently places the most effective policy on the relevant enforcement points
- Accessible through Cisco Security Cloud Control
- Charged per non-Cisco enforcement device

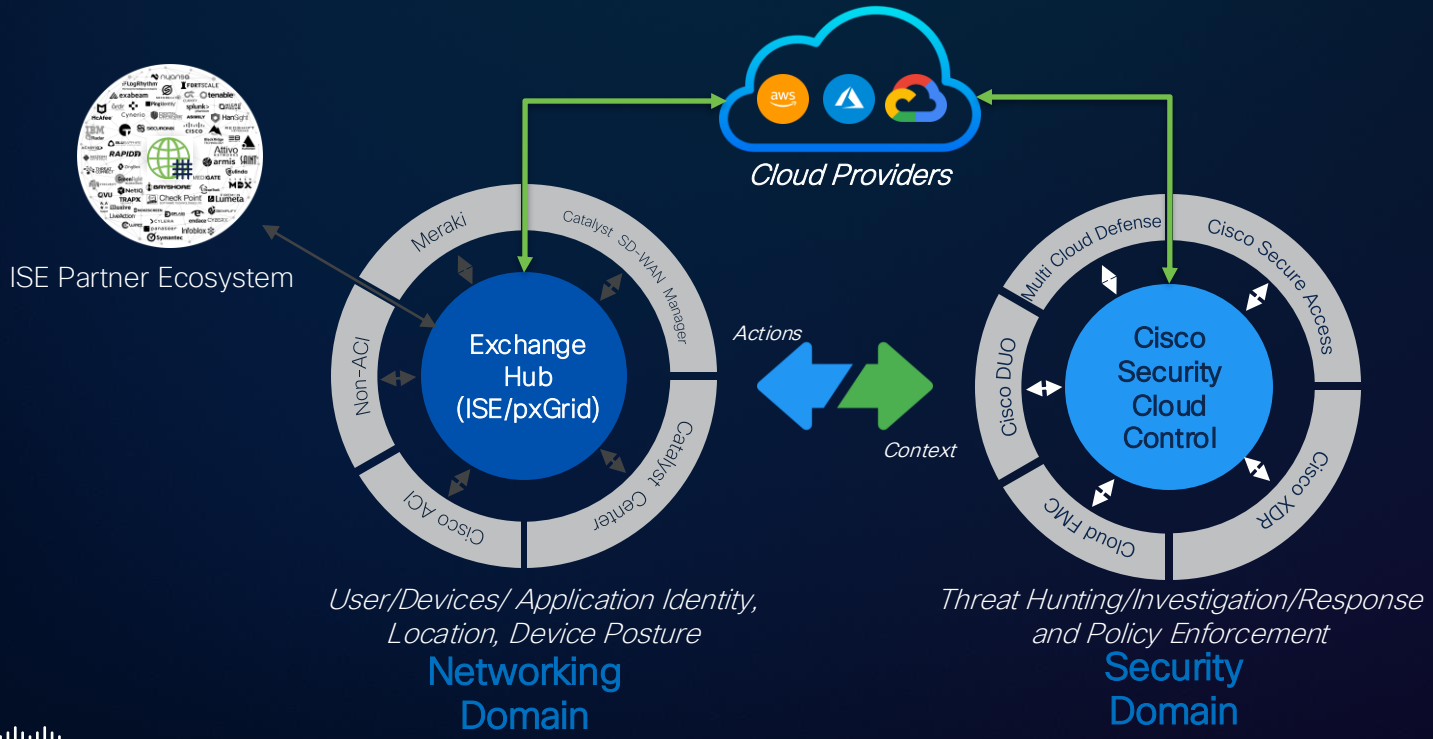
What it isn't

- Device manager – use the native manager for device configuration like upgrades
- A policy converter – use Cisco Secure Firewall Migration Tool



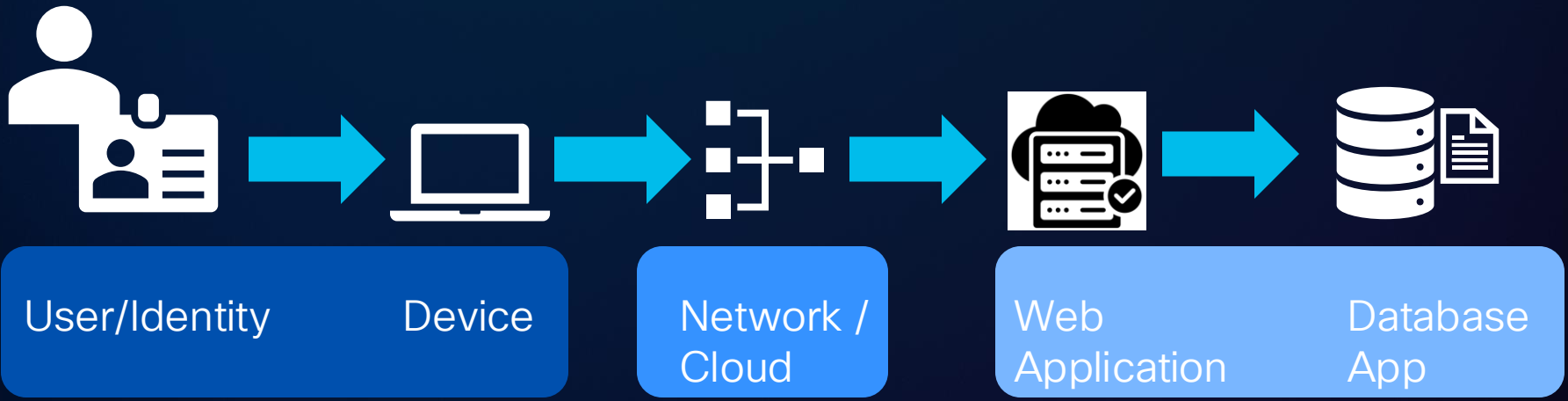
Extending Segmentation into Campus, Branch, DC & Cloud

Normalizing and sharing context across domains



Zero Trust End to End

User to App, App to App



Addressing User to App with Universal ZTNA and Identity

Zero Trust User to Application/Service

Domains

Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | ...

Single client, multiple functions

Single client, multiple functions

Seamless Access

We handle the plumbing

Go to work

Private Apps

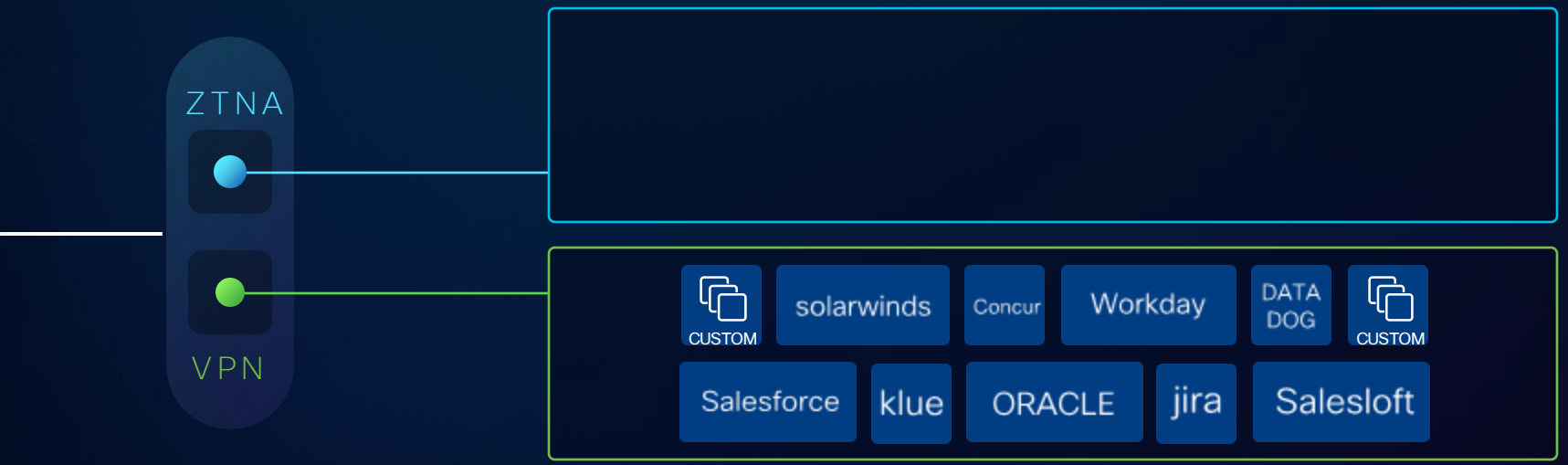
Internet Apps

Traditional Apps

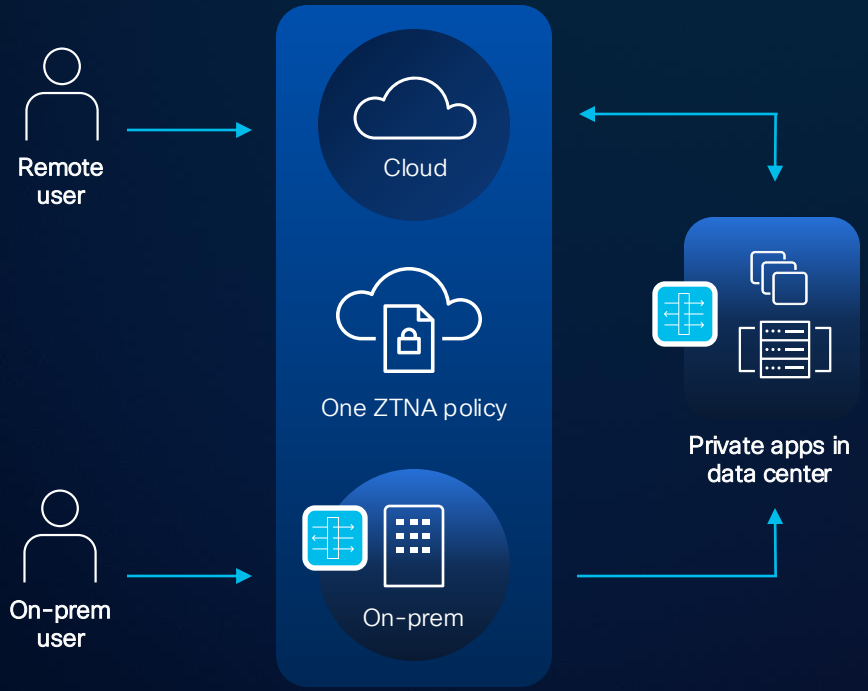
SaaS Apps

Seamless Experience

VPN-as-a-Service simplifies ZTNA roll-out



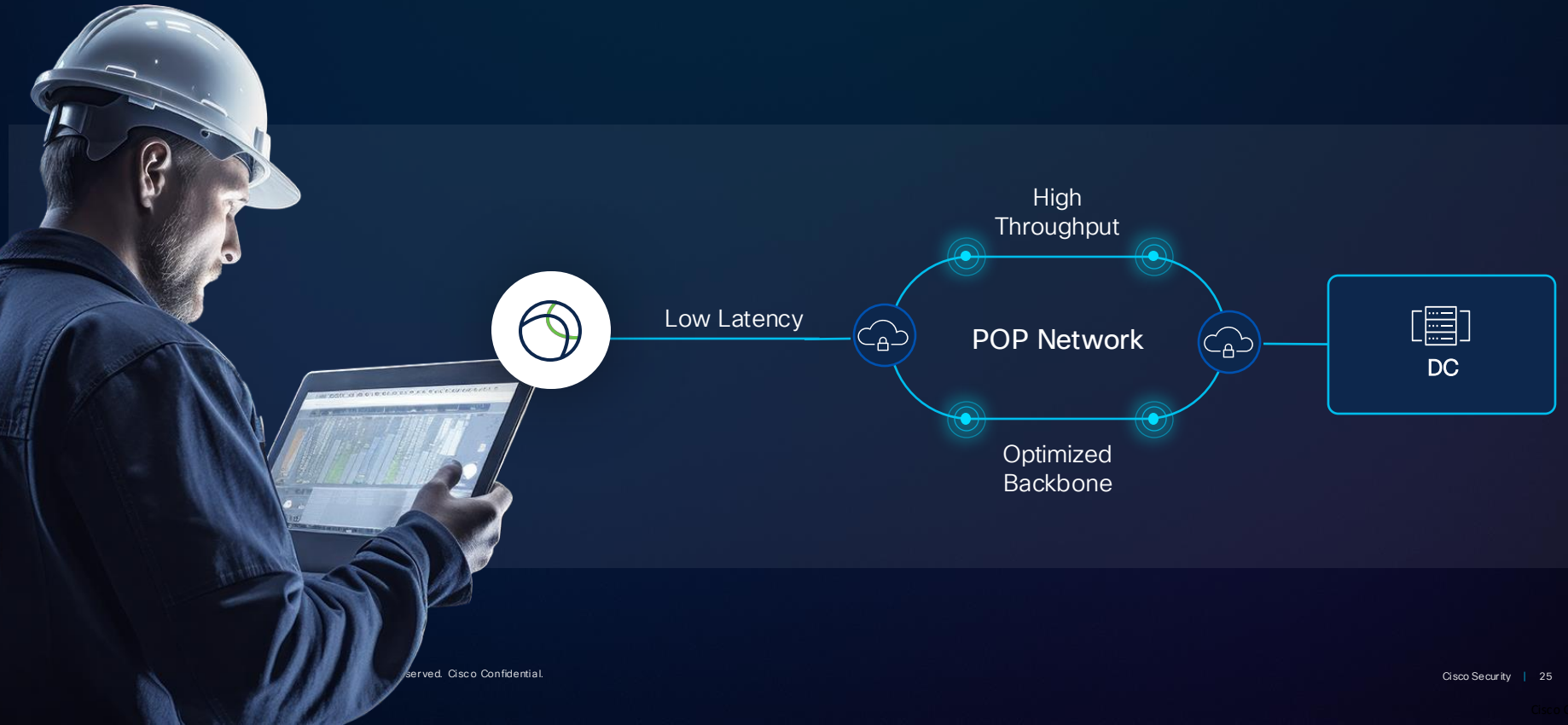
Extending ZTNA with Cisco Secure Firewall



- Single ZTNA policy created and automatically applied from Security Cloud Control
- Cloud and on-prem firewall enforcement, including on-prem inspection for sensitive apps
- Reduced cost and latency when on-prem users access on-prem apps
- No additional infrastructure or purchase to implement

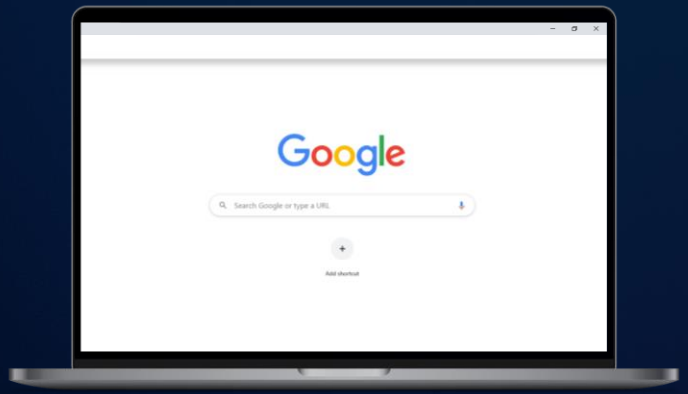
Cisco’s modern PoP architecture

Leverages MASQUE/QUIC, Vector Packet Processing (VPP), and a global peering



Native Device Support

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



Chrome Enterprise Browser

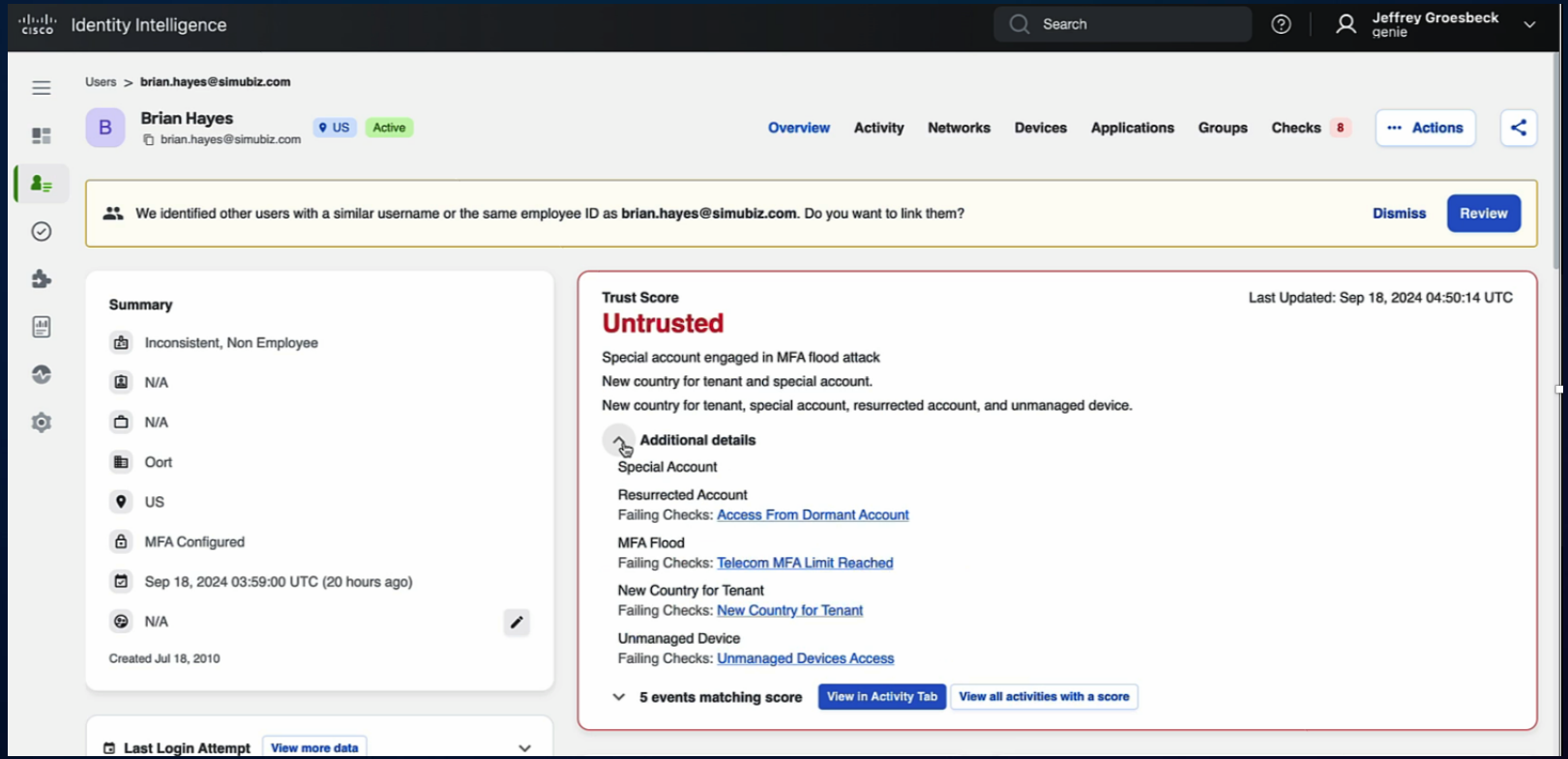
Native OS Integration

There is no universal zero trust
without ubiquitous, shared identity across the enterprise

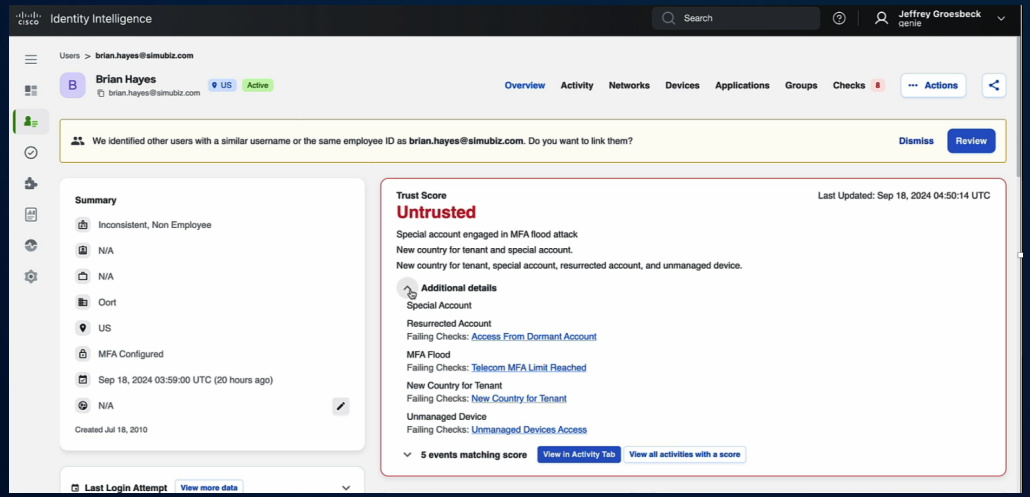
Cisco Identity Intelligence

SailPoint
Dragos
Crowdstrike
Salesforce
Cisco ISE
Okta
PingIdentity
Auth0
Microsoft
Google
Cyberark
Amazon

User trust timeline



User Trust Score



User Trust Score

Identity Intelligence will be providing a user trust score for integrating solutions to leverage. Will be a single score, determined by a user's behaviors, actions and posture

Easy Workflows

After assessment, seamlessly take response action from the console.

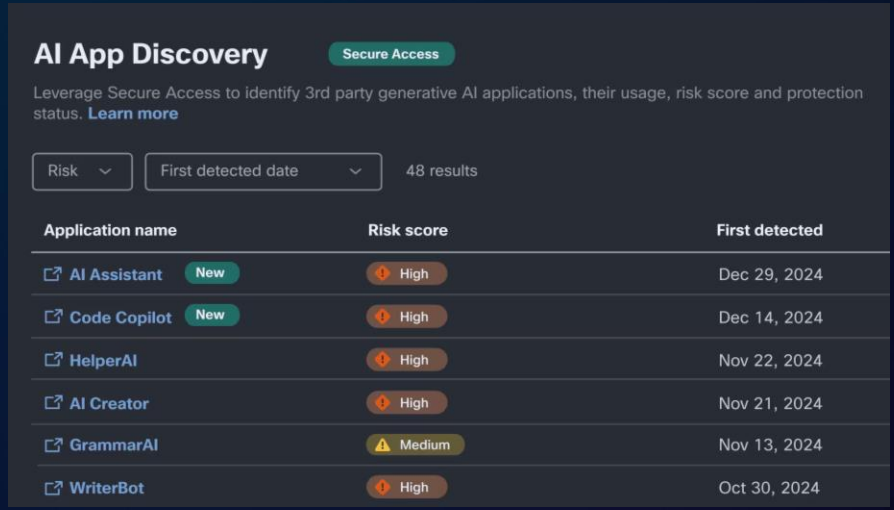
Key Scores

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown

Shadow AI Security

Superior visibility & control

- Discover Shadow AI; define acceptable use
- Granular control
  - Sensitive documents
  - Source code
- Machine learning finds unstructured data
  - Patent applications
  - M&A
  - Financial statements and more



1200+
AI Apps Protected

100%
Guardrails for top AI Apps

1
Unified Security Framework

Enforce zero trust using on-prem context

Leverage security group tags for granular access policy

----- = Future

Universal Zero Trust Network Access

Cloud Management (Security Cloud Control)

Extend Identity Context

- Identity Intelligence/MFA
- ISE & SD-WAN integration

Modernize Application Access

- Secure Internet Access
- Secure Private Access

Build Operational Resilience

- Digital Experience Monitoring
- Policy Assurance

SD-WAN

Firewall/Network Infrastructure

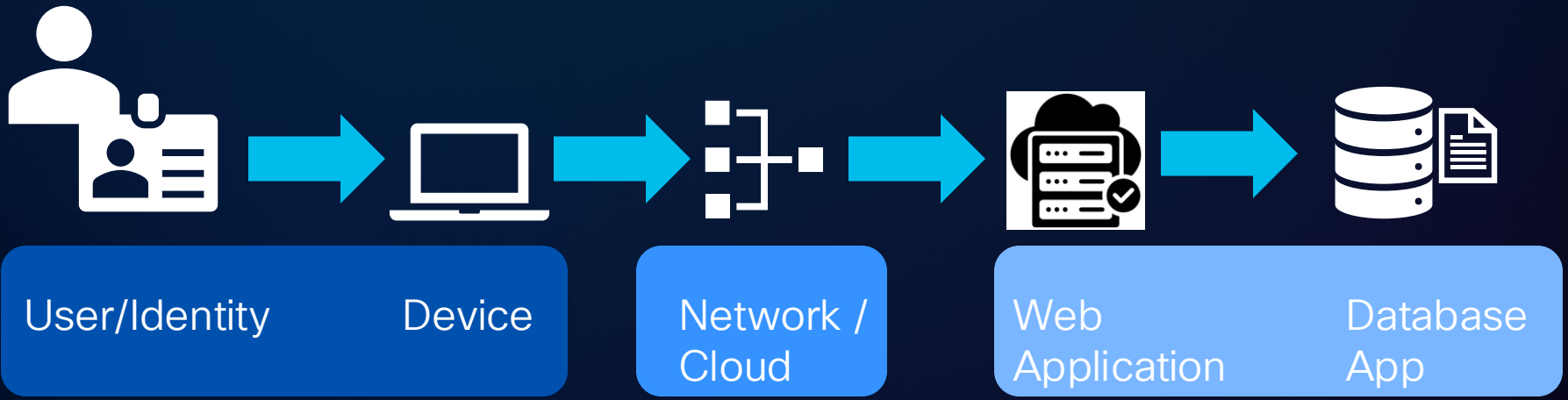
Splunk Cisco XDR

Telemetry

Addressing Application Security

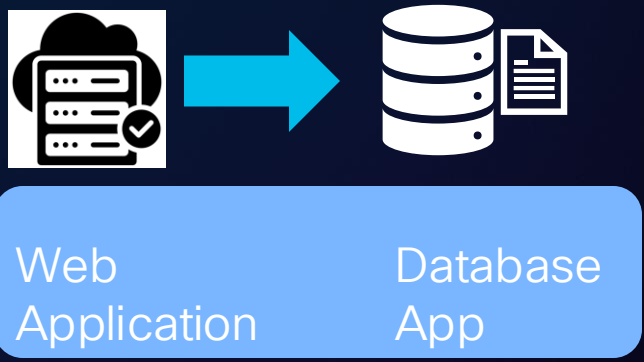
Zero Trust End to End

- User to App, App to App

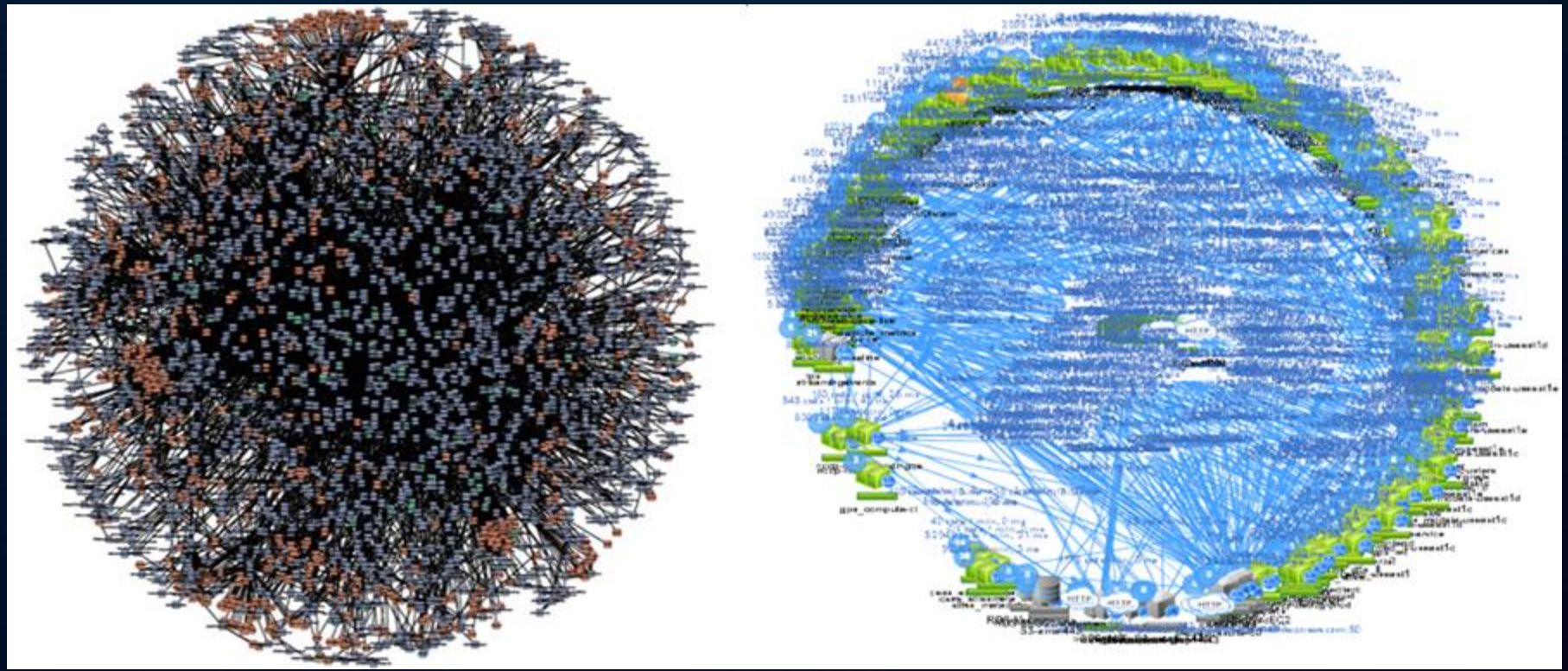


Zero Trust App to App/Service

- Is it this Simple?



The Reality – One Day



Extending Segmentation into Applications

Edge Firewall


Secure Firewall


Multicloud Defense

Macro-Segmentation


ACI


Secure Firewall

aws

Azure


Secure Workload

Google Cloud

Micro-Segmentation


Secure Workload

Hypershield

Unified Segmentation

Perimeter Defense

- Ingress & Egress Security
- Threat inspection at the data center or cloud edge.

Zones

- Segment zones within your data center and cloud.
- Agentless coverage for cloud, on-prem and legacy workloads

App Segmentation

- Automated policy discovery and compliance
- Zero trust micro-segmentation enforcement at the workload (L3-L7, system calls)

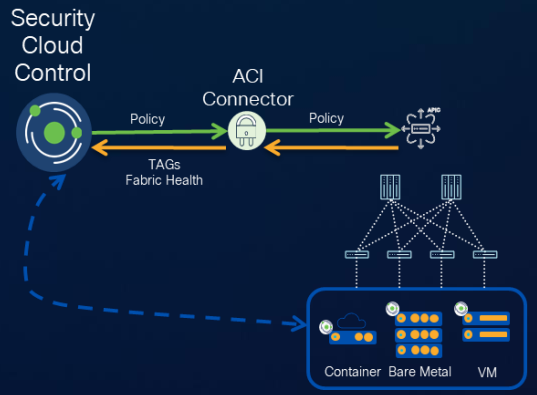
Agentless visibility & enforcement everywhere

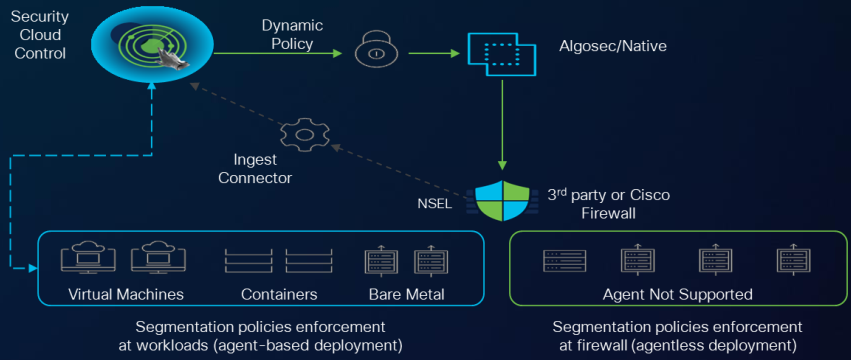
Public Cloud

- Centralized cloud-onboarding & cloud connectors
- Visibility with real-time discovery of workloads and labels & Flow telemetry via VPC/VNets flow-logs
- Enforcement using Security Groups (AWS), Network Security Groups (Azure), Firewall (GCP)

On-prem with ACI

- Realize ACI vision of App Centric deployment
- Automated Policy Lifecycle management





With Firewalls

- Topology aware policy enforcement
- Support access control policy and dynamic object

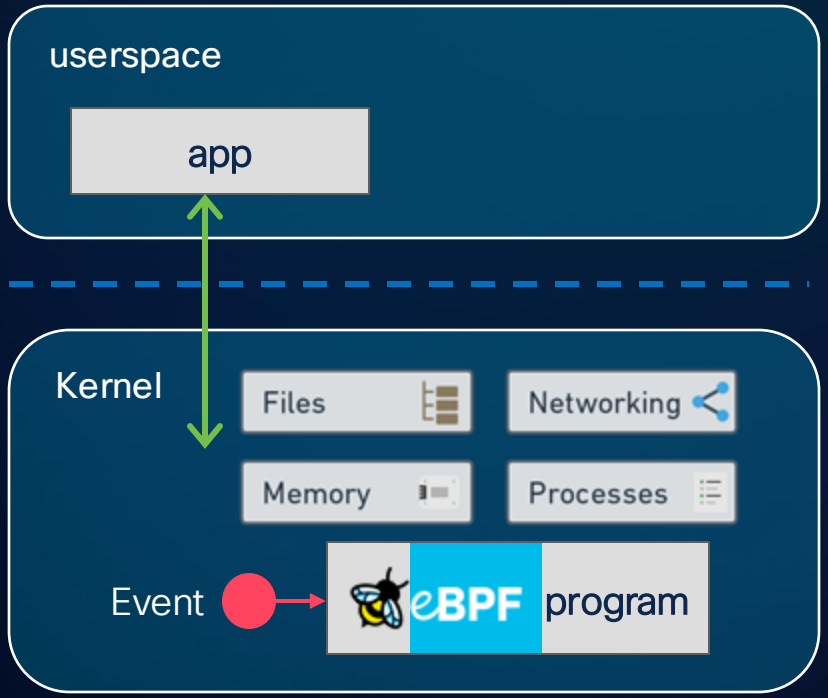
Extending Firewalling to the cloud, *natively*

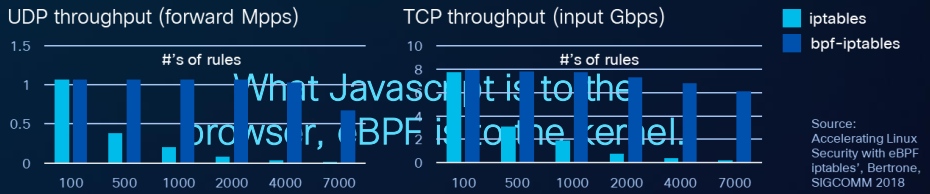
NEW

- Cloud-agnostic automation and orchestration
- Comprehensive visibility of clouds, assets, and their risks
- Automatically deploy, scale, and heal, from Security Cloud Control
- Hourly price; unlike other offers based on size and bandwidth

eBPF – Extended Berkely Packet Filter

- Makes the kernel programmable in a secure and efficient way



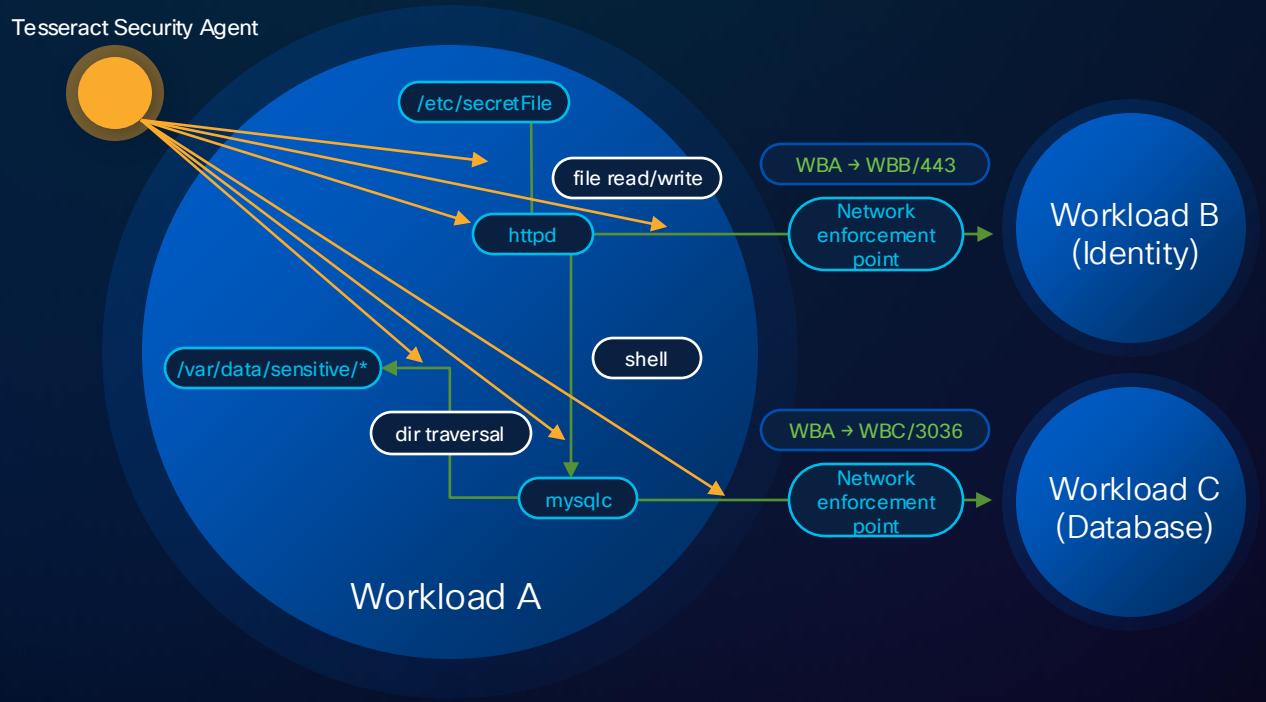


- eBPF runs in a restricted execution environment
- Before eBPF script is compiled:
  - Verifier ensures things such as memory safety
  - Hardening process (program execution protection, mitigation against spectre, constant blinding, ...)
- eBPF can only access pre-approved kernel functions and data structures

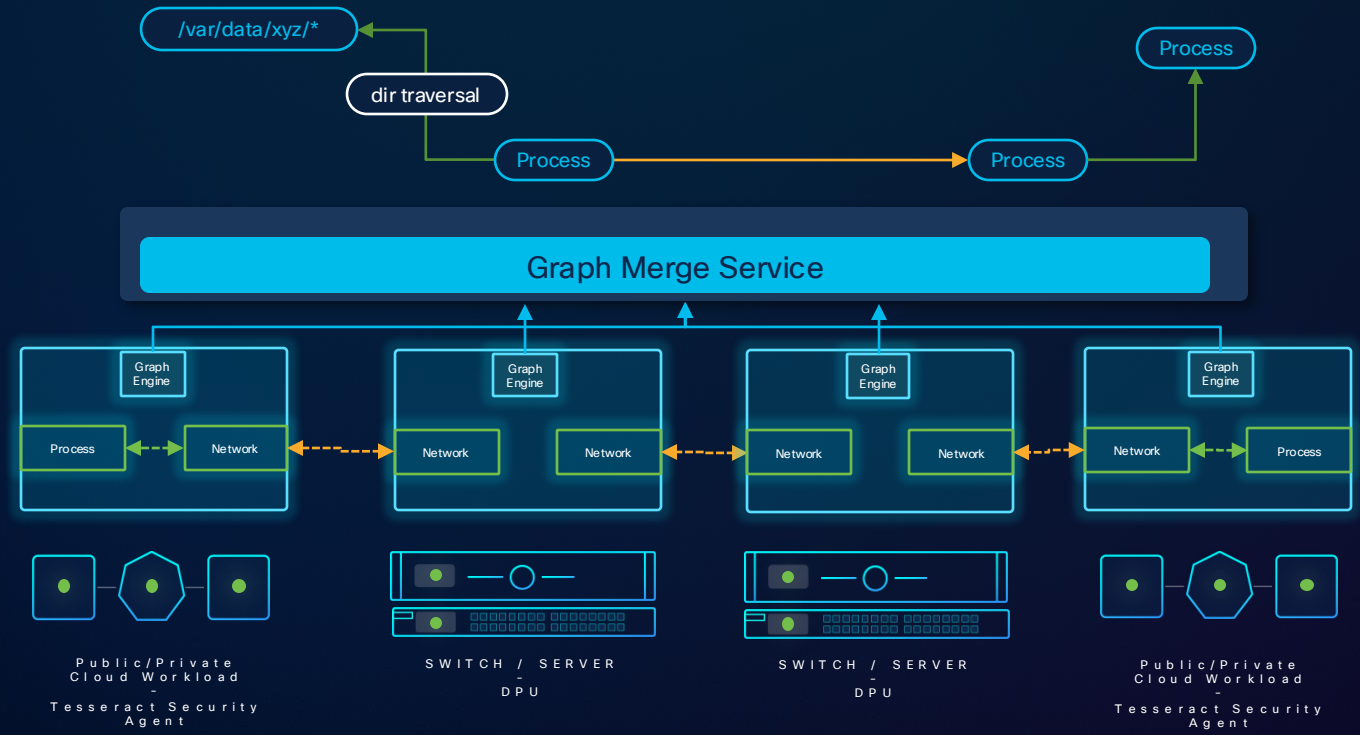
eBPF based visibility & controls in network & workload

Tesseract Security Agent provides deep **visibility** and **enforcement** within workload

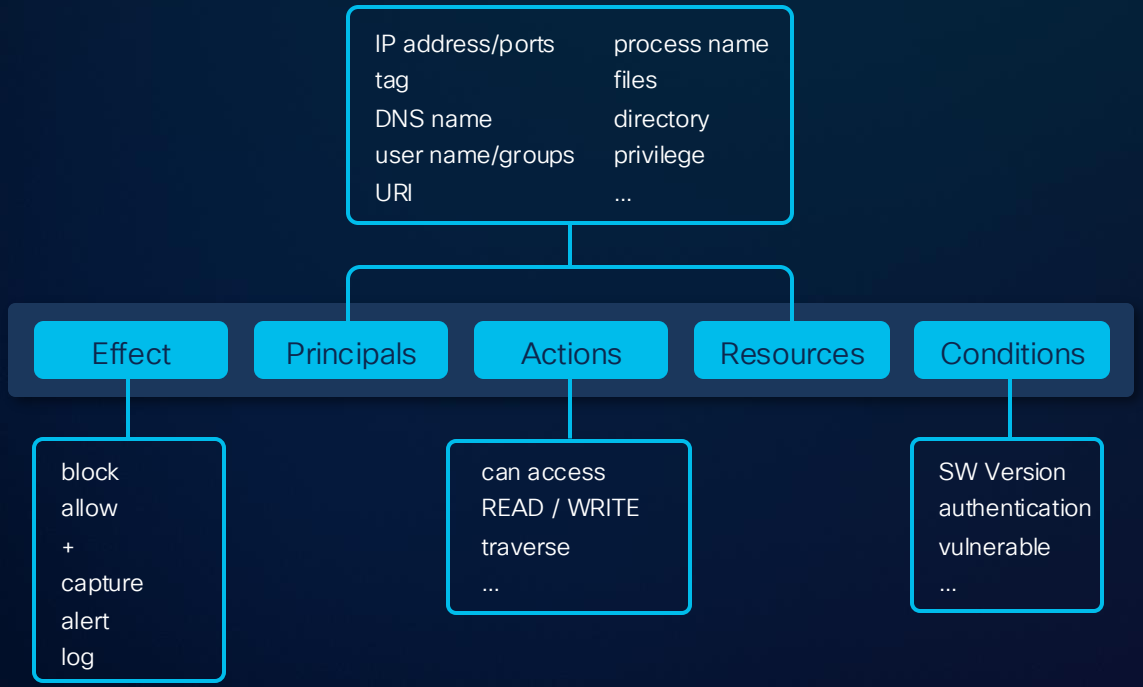
- Network
- File read/write
- Directory traversals
- Privilege escalations



Distributed AI Graph Engine



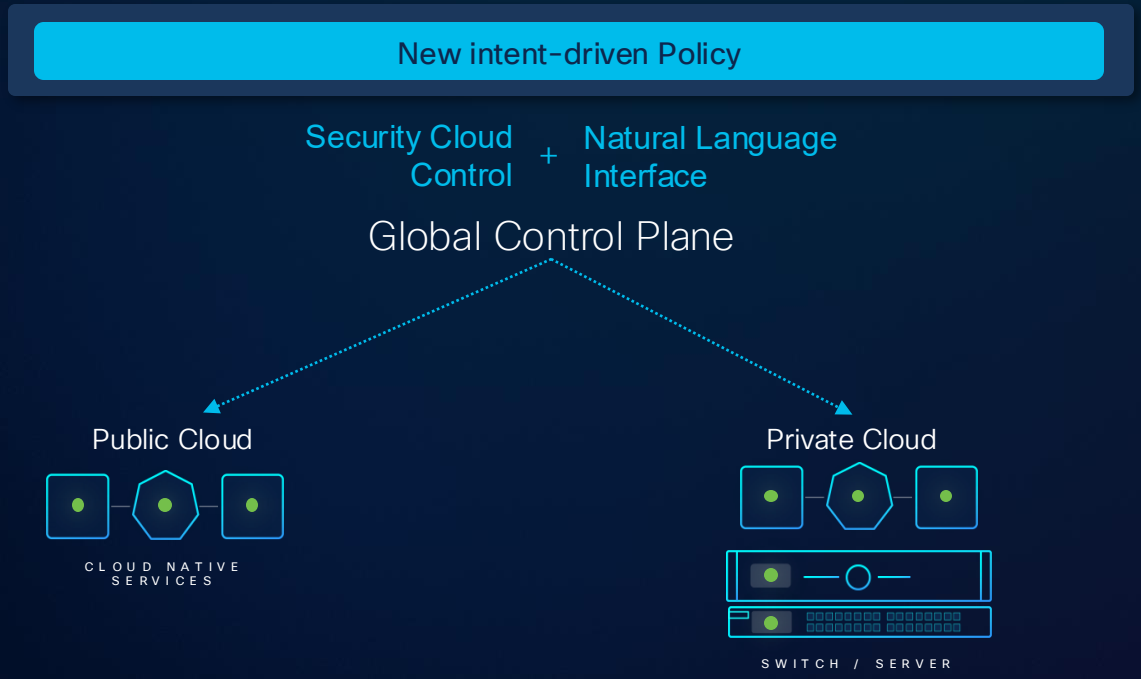
Intent-driven policy covering network and workload



Hypershield Policy Construct

- AWS Cedar inspired/adapted
- Intent based
- Order independent
- Auto-compiled to rule

Manage globally, enforce locally



Includes

Unified management

Single global policy

Unified policy (PARC) compiled to platform specific rule sets for variety of enforcement points

Intelligent placement of rules

Integrations with cloud/app/infra metadata

AI recommended policies with approval workflows

Environments

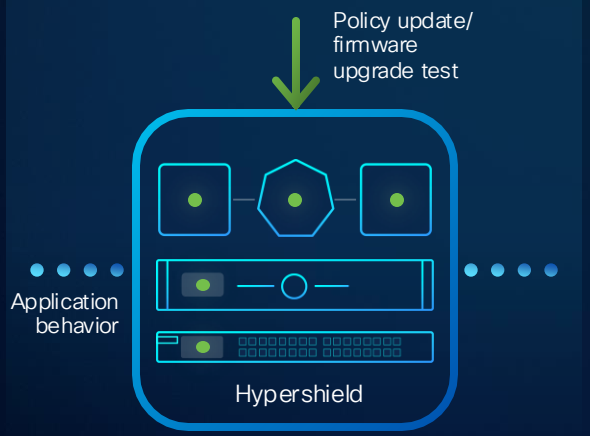
Kubernetes

Cloud – Private/Public

On-prem

Policy Lifecycle management

- Self-qualifying firmware and policy updates



1) Technical design — AI-approved
2) Security review — AI-approved
3) Change request — AI-approved
4) Business approval — Approval needed

The application affected by these changes is the **Finance app.**
The app owner's approval is needed due to the high risk of the affected application.

Drew has been identified as the app owner of Finance app.

Test

Using a digital twin, firmware and policy changes are validated against customer environment

Review

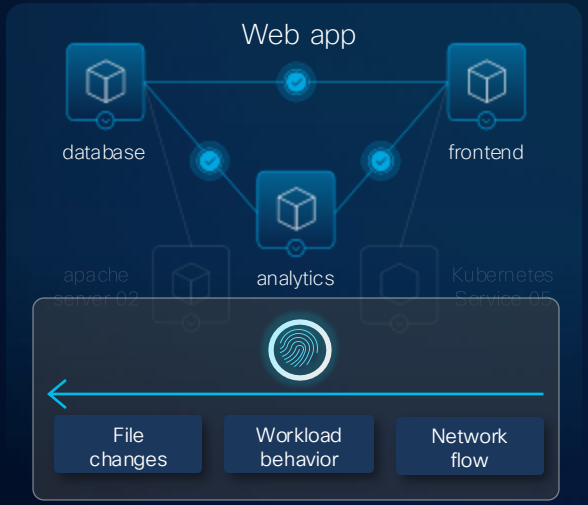
AI system evaluates change. Admin controls promotion

Deploy

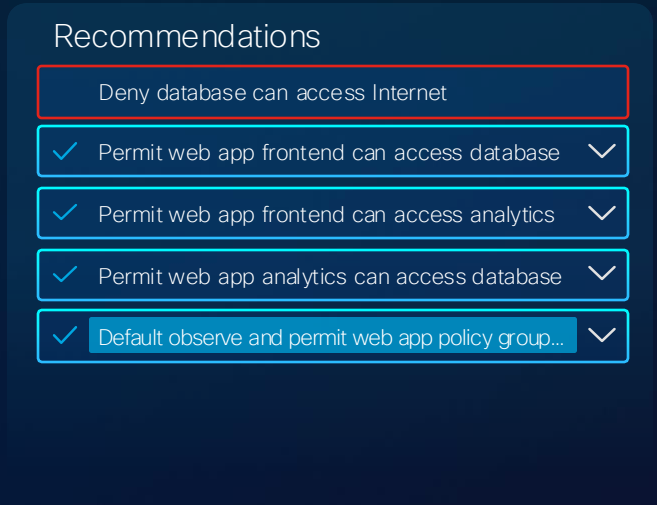
Hitless deployment with single click, enabling teams to move fast with confidence

Note: Images are not an exact product UI representation

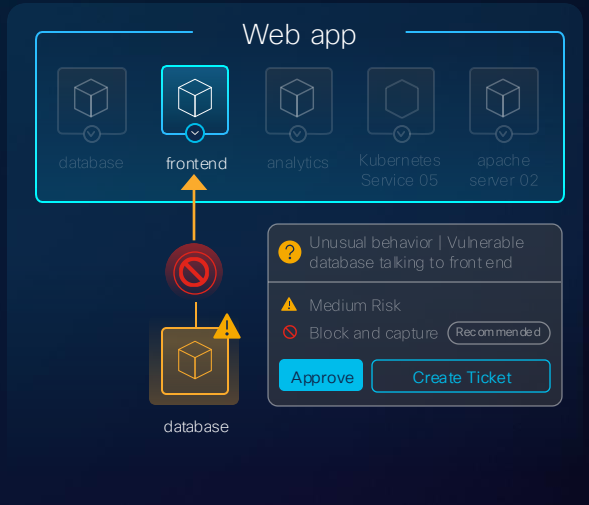
Segmentation that is effective and keeps up with changing applications



Complete understanding of changing app behavior from network to workload to pre-prod



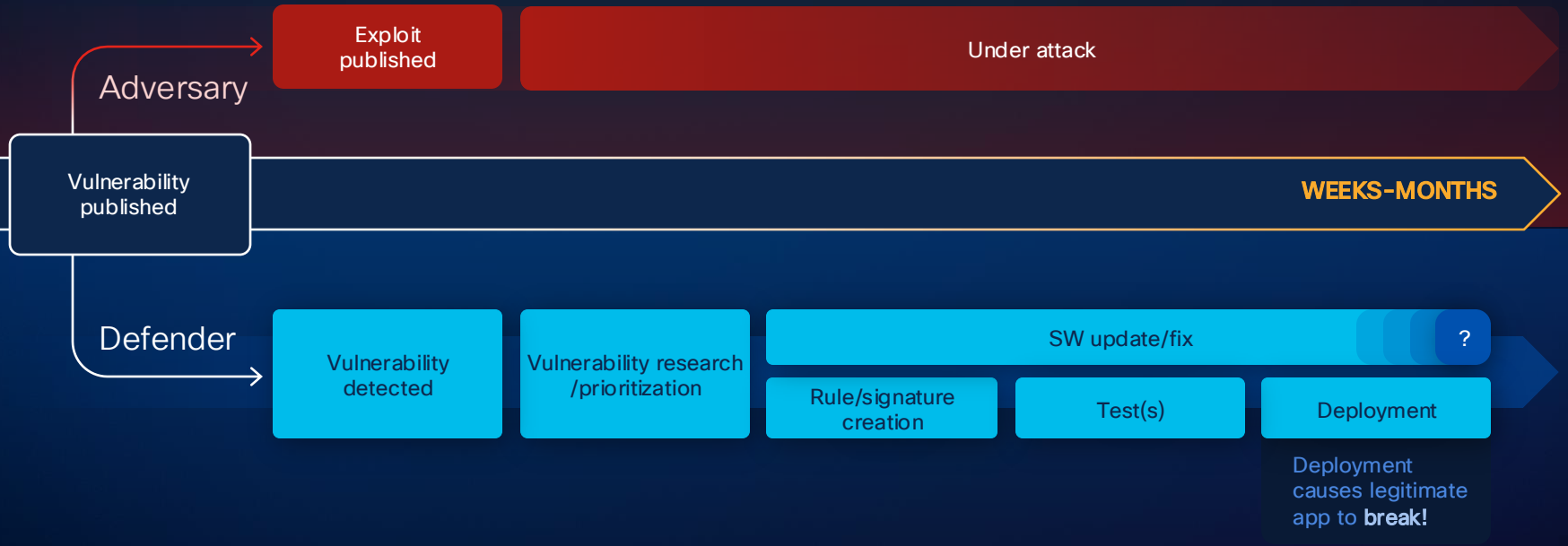
Flexible segmentation rules that help avoid app fragility



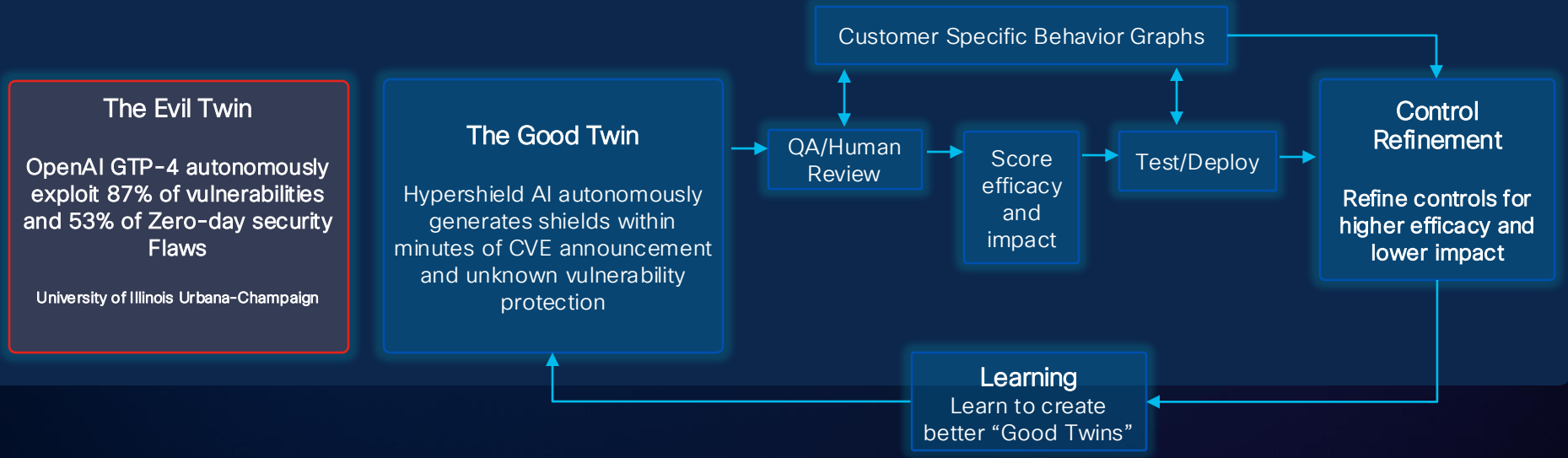
Policies updated to stricter rules in response to suspicious events

Note: Images are not an exact product UI representation

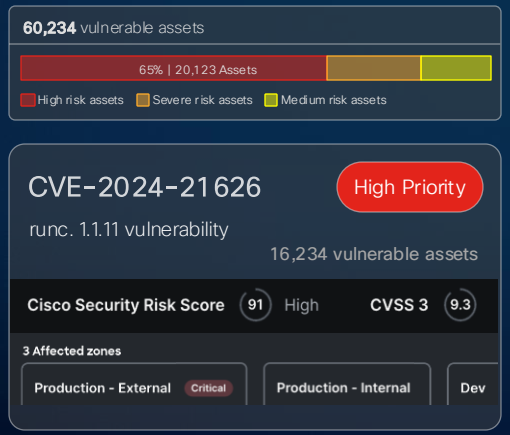
Vulnerability management is a race against time



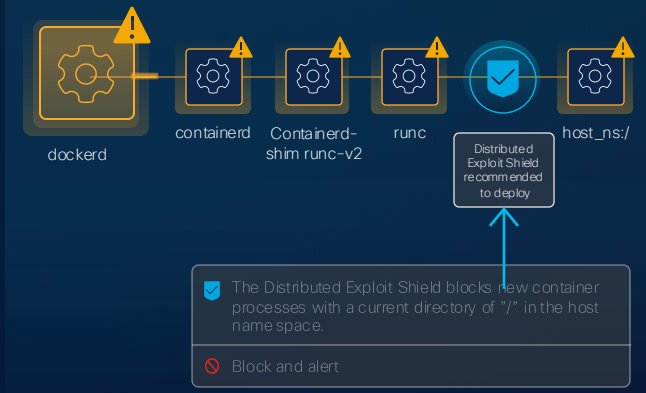
AI and Compensating Control Creation



Close the exploit gap against growing vulnerabilities with automated workflows Speed vs resilience



Complete view of the vulnerabilities, prioritized by severity and critical business flows



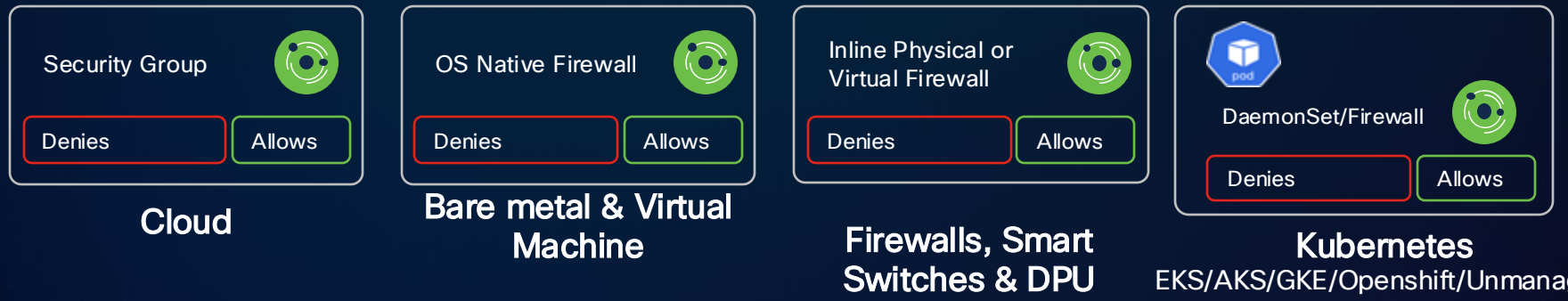
Surgical mitigating control in the path of the process that keeps application running

Tested against live production traffic to earn trust and increase confidence

Note: Images are not an exact product UI representation

Coverage for non-eBPF capable workloads?

- Security Cloud Control renders security rules using native capabilities



- Agentless in Public Cloud (AWS, Azure, GCP) with cloud native groups
- IP Tables on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Inline Firewalls. Load Balancers, Smart Switches, DPUs
- IP Tables on Kubernetes

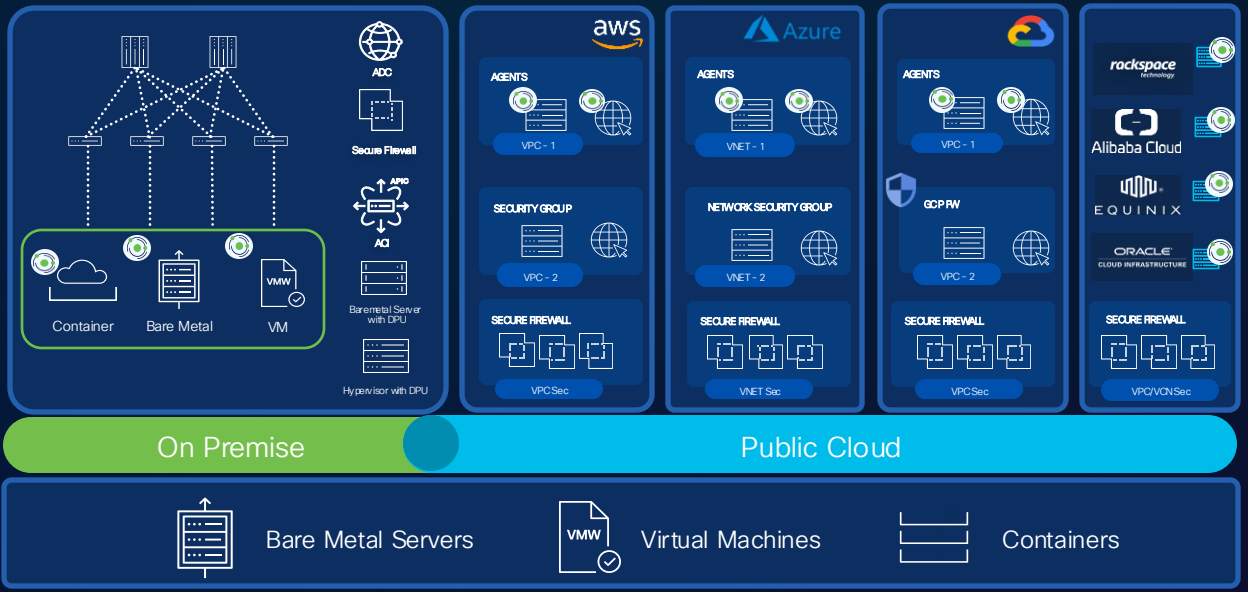
Full coverage micro segmentation from on-premises to cloud

Agent

Cisco Security Cloud Control with Hybrid Mesh Firewall

Agentless

- Anywhere
- Windows Desktop
- Windows Server
- IBM AIX
- Oracle Solaris
- Oracle Linux
- Centos, Rocky, Alma Linux
- Ubuntu, Debian
- SUSE Linux
- RedHat Linux
- Amazon Linux
- OpenShift
- Kubernetes



On Premise

Public Cloud

Bare Metal Servers

Virtual Machines

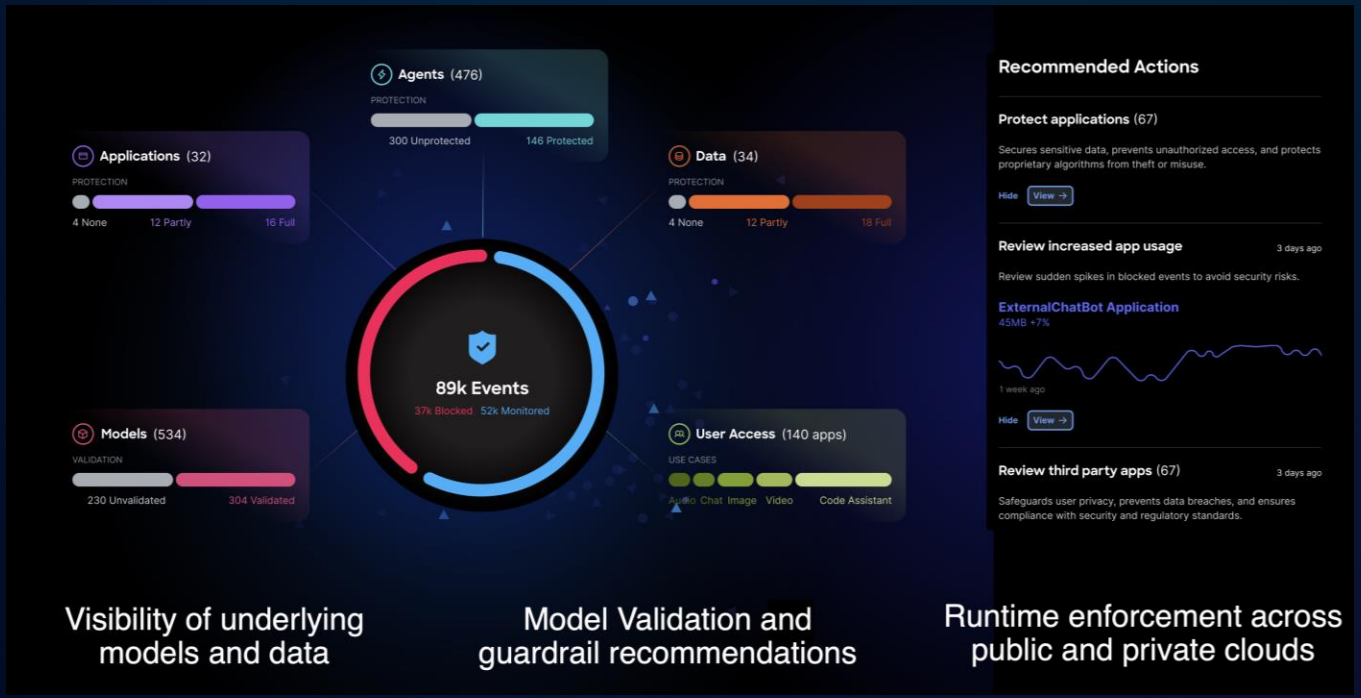
Containers

- On-Prem
- Loadbalancer (ADC)
- Firewalls
- Data Center Fabric (SDN)
- ACI
- AWS, GCP, Azure
- Security Group
- Network Security Group
- Cloud Network Firewall
- Multicloud Defense*
- NVIDIA Smart NIC (DPU)

User Identity | Tags and Labels | Vulnerability

Threat Feed | Application Encryption | Domain/FQDN | Cisco Security Risk Score

AI Defense delivered via the Hybrid Mesh Platform



Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Cisco Security Cloud Enforcement Points

- Hypershield
- Secure Access
- Cloud Firewalls
- On-prem Firewalls

SOC of the Future

NEW

Security Insight, on Us

Free Cisco firewall logs to Splunk*

AVAILABLE AUGUST 2025

New detections | Automated response

*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

Cisco XDR – fastest, easiest path to TDIR

Cisco has a network-led, open XDR solution

XDR Strategy

Converge EDR, NDR, CDR, MDR into one risk-based solution, integrating a specific set of third-party capabilities and leveraging a focused GTM to deliver customers the fastest incident detection and the most comprehensive / effective response

Key Tenets of the Strategy

1. Network & Cloud centric in one
2. Choice of multiple integrated EDRs
3. Turnkey and curated outcomes
4. Response focused
5. Open and extensible platform
6. Product and managed service offers

Cisco XDR + Splunk

- *The combination of XDR + Splunk delivers the most complete TDIR solution available on the market today*
- XDR provides an extremely rich *'Analyst Experience'* which obfuscates the operational complexity of the Splunk platform, leveraging the out of box detections that eliminates the need for detection engineering
- Splunk cloud adds dashboarding, integrations, investigations/search (using SPL if necessary), and federated search wherever the data resides, for longer-term investigations/eradication, etc.

How it Works: Architecture (XDR + Splunk)

- Splunk Cloud has native support for the Wild West of 3rd-Party tools, plus XDR, and most Cisco Tools
- *Analyst Experience: XDR gets the data, creates the detection, and then enriches that detection with data from Splunk adding additional context – hiding the operational complexity of the Splunk platform*
- *XDR can ingest its own and add Splunk data for all alerts to enhance its ingestion pipeline, drive correlation, investigation and take quick action on all events.*

Summary


Threat Intelligence
Extended Detection and Response
ZERO TRUST
SASE
User / Device Security
Cloud Edge Network
On Premises Network
Workload, Application, and Data
Platform

Security Reference Architecture

cisco.com/go/sra

TALOS THREAT INTELLIGENCE — Actionable threat intelligence | Collective responses | Comprehensive visibility | Signal identification | Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics
XDR | Secure Client | Talos Incident Response

SERVICES

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

CAPABILITIES

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

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed
- VPN
- Telemetry Visibility
- Endpoint detection & response
- DNS-layer security
- Secure web
- Anti-virus Anti-malware
- Query
- Host FW
- Mobile device management
- Risk-based MFA
- Password-less
- Device trust
- Continuous Trust
- Email, Phishing, SPAM, BEC,DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Connect | Umbrella

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

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela

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

In the Office/Managed Location

Catalyst | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

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

Industrial Threat Defense

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

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

Workload, Application, and Data Security

ACI | Attack Surface Management | Hypershield | Radware | Secure Application | Secure Endpoint| Secure Firewall |Multicloud Defense | Secure Workload

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

SECURITY CLOUD — CLOUD-BASED | MULTICLOUD | UNIFIED MANAGEMENT & POLICY | AI / ML DRIVEN | OPEN & EXTENSIBLE

THANK YOU