



# Cisco Security Architecture

Zero Trust Architecture done right

Jatin Sachdeva [jasachde@cisco.com](mailto:jasachde@cisco.com)  
Principal Security Architect - Worldwide

Cisco Global Security Architecture Team (GSAT)

# One Cisco portfolio delivers customer outcomes



AI-Ready Data Centers



Future-Proofed Workplaces

← Secure Global Connectivity →



Digital Resilience



Accelerated by Cisco AI




# 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



Identity



Network



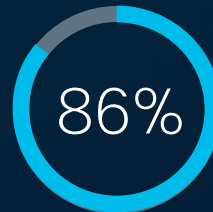
Devices



Apps/Workload

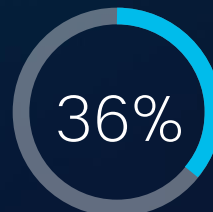


Data



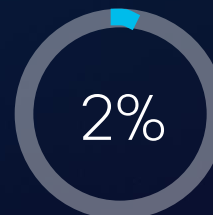
Nearly all organizations have started on some aspect of zero trust (at least one pillar)

“We know we need to do it”



Have reached maturity in at least one pillar

“Our focus is on XYZ pillar”



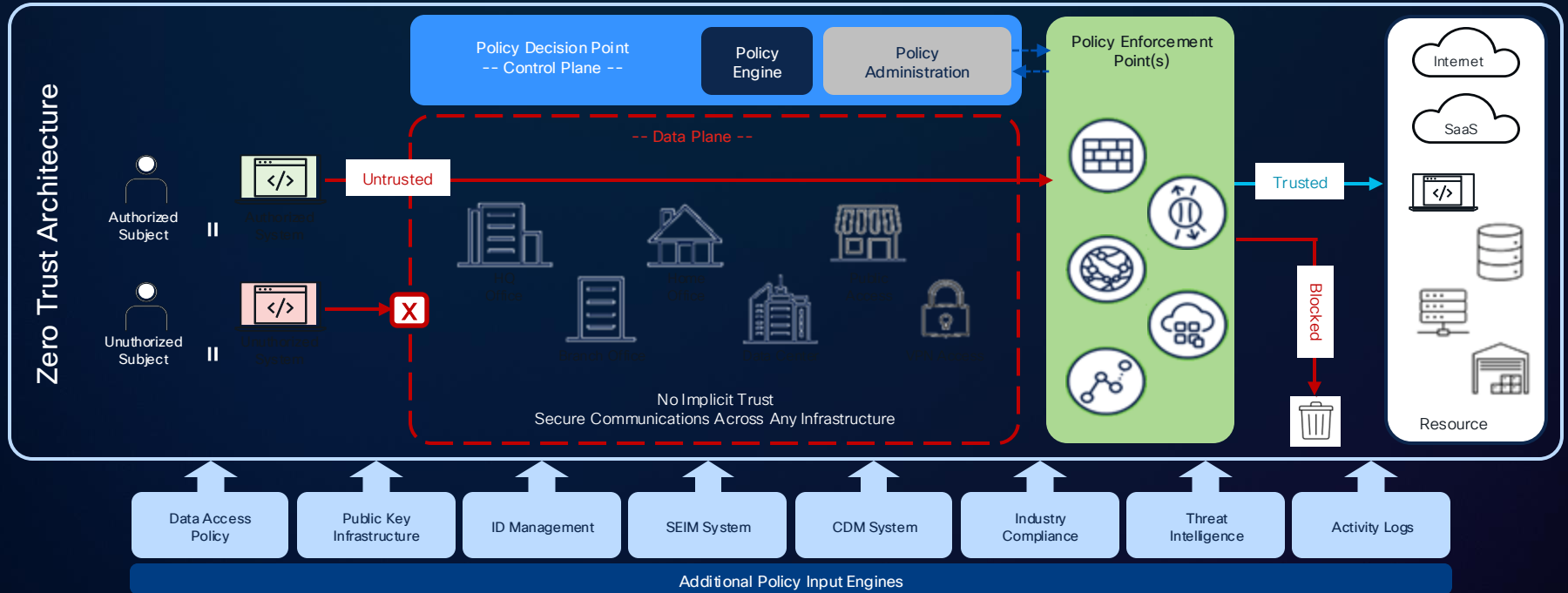
Have reached maturity across all pillars which means that 98% have not.

“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

SDA & SD-WAN

SSE

Perimeter & Cloud  
Edge Firewalls

DC/Cloud/K8  
Infra

Workload  
Inventory &  
Posture

Workload Security



Threat Intelligence & SOC

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

# Zero Trust Platform

Cloud Management (Security Cloud Control)

Universal ZTNA

Hybrid Mesh Firewall

Access Control

AI Access

North South  
Segmentation

AI Model  
Protection

East West Macro/  
Microsegmentation

Distributed  
Exploit  
Protection

SDA & SD-WAN  
(Catalyst,  
Meraki, FTD)



SSE  
(Secure Access)



FTD & Multicloud  
Defense, 3<sup>rd</sup> Party  
Firewall



Hypershield  
(Smart Switch)



Secure  
Workload

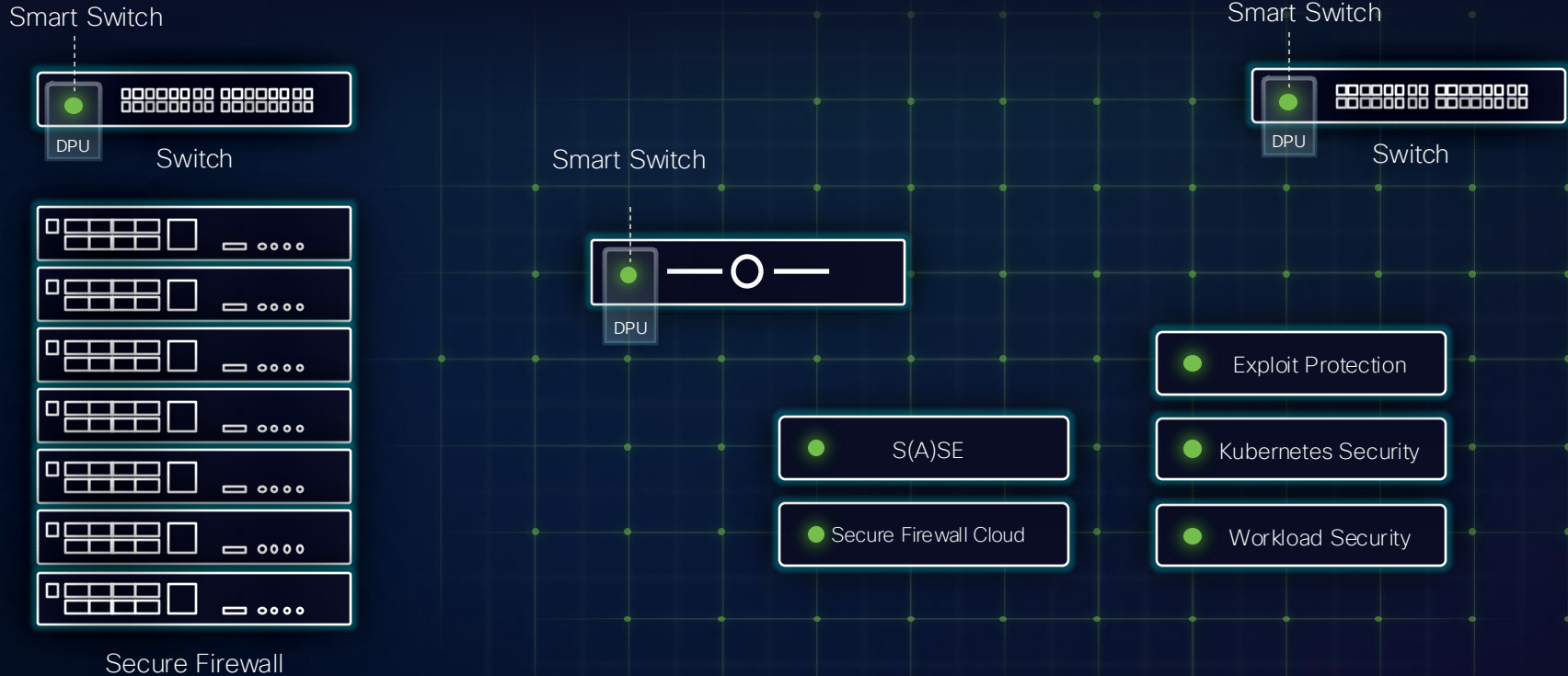


Hypershield  
(Isovalent Agent)



Cisco TALOS, Cisco XDR & Splunk

# Security Cloud Control



Enforcement points change, rules don't

# Cisco Security Cloud Control



# 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

The screenshot displays the Cisco Security Cloud Control interface with a new navigation structure. The interface is divided into several sections:

- Top Nav:** Includes a search bar (Type 'Ctrl' + '/' to search), user profile (Carter Briggs), and a notification bell.
- Organization Switcher:** Shows the current organization as 'Stark Enterprises - North America'.
- Home:** Displays 'Top insights & alerts' with 10 new insights. Three alerts are visible:
  - Elephant flow spike observed:** Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues. (Last 24h)
  - Risky users accessing privileged apps:** Implement zero trust access to limit access to only required user groups, and protect your applications from risky users. (Last 24h)
  - 1% Decrypted traffic towards internet:** Failure to decrypt a significant portion of traffic poses a severe security risk, potentially concealing malicious activities, leaving your network vulnerable to threats. (Last 24h)
- Micro App 1:** A placeholder for a micro application.
- Micro App 2:** Displays 'Asset connectivity status' with a donut chart showing 15% disconnected assets (up 8% since yesterday). A table lists disconnected assets by source:

Source	Count	24hr Δ
Firewall devices	250	↗ 11%
Universal ZTNA Firewall devices	45	↗ 5%
Network tunnel groups	36	—
Resource connectors	8	—
Cloud accounts	1	—
Tesseract security agents	12,942	↗ 4%
Workload agents	19	—
- Side Nav:** A new left navigation menu with categories:
  - Organization: Stark Enterprises - North America
  - Home
  - Products: AI Defense, Firewall, Hypershield, Multicloud Defense, Secure Access, Secure Workload
  - Platform services: Favorites, Security Devices, Shared Objects, Platform Management

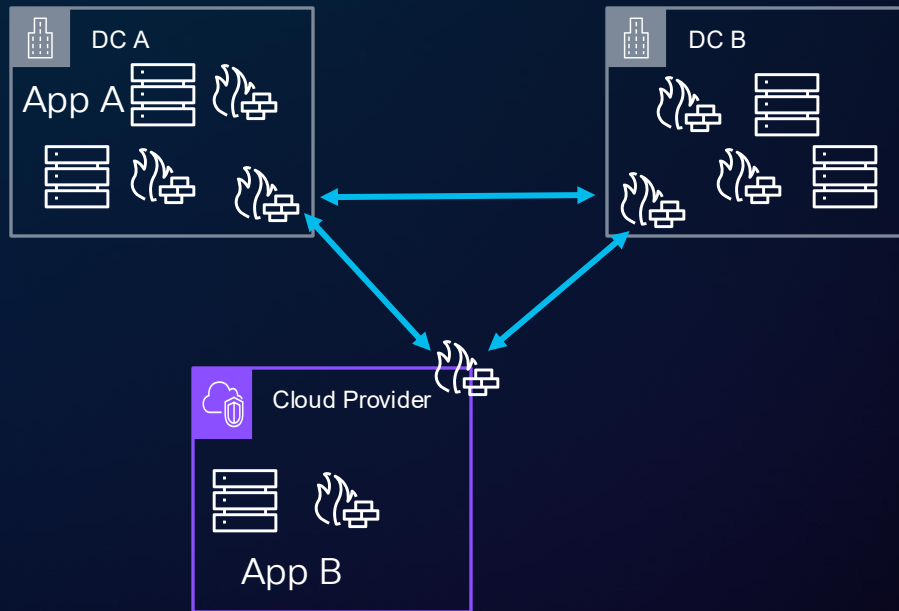
# Shift to outcome-based policy

## 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

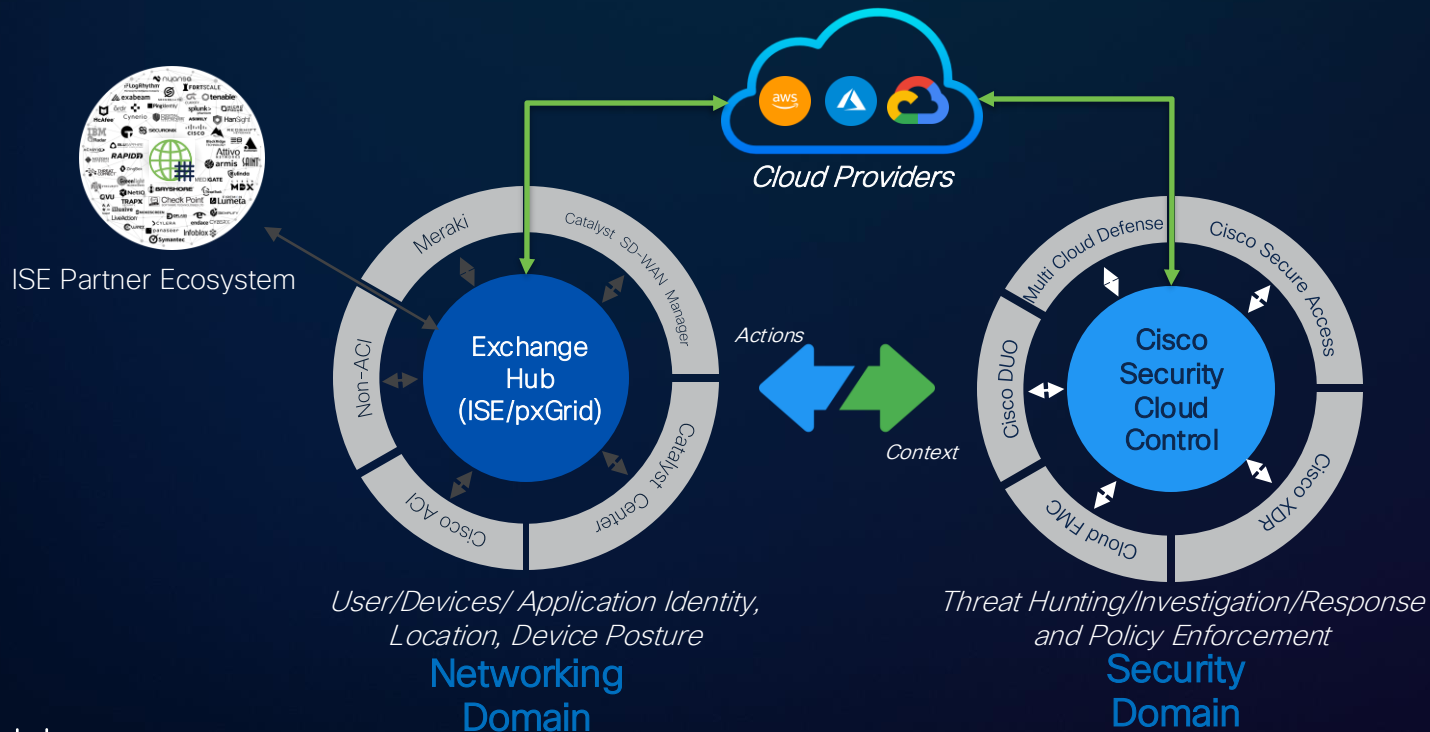
## What it isn't

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



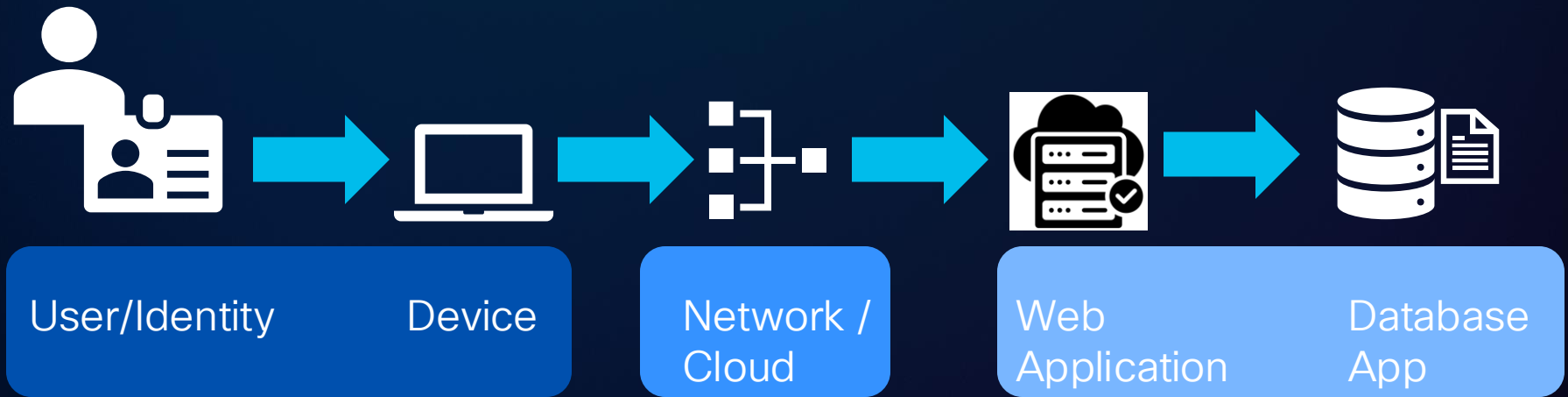
# Extending Segmentation into Campus, Branch, DC & Cloud

Normalizing and sharing context across domains



# Zero Trust End to End

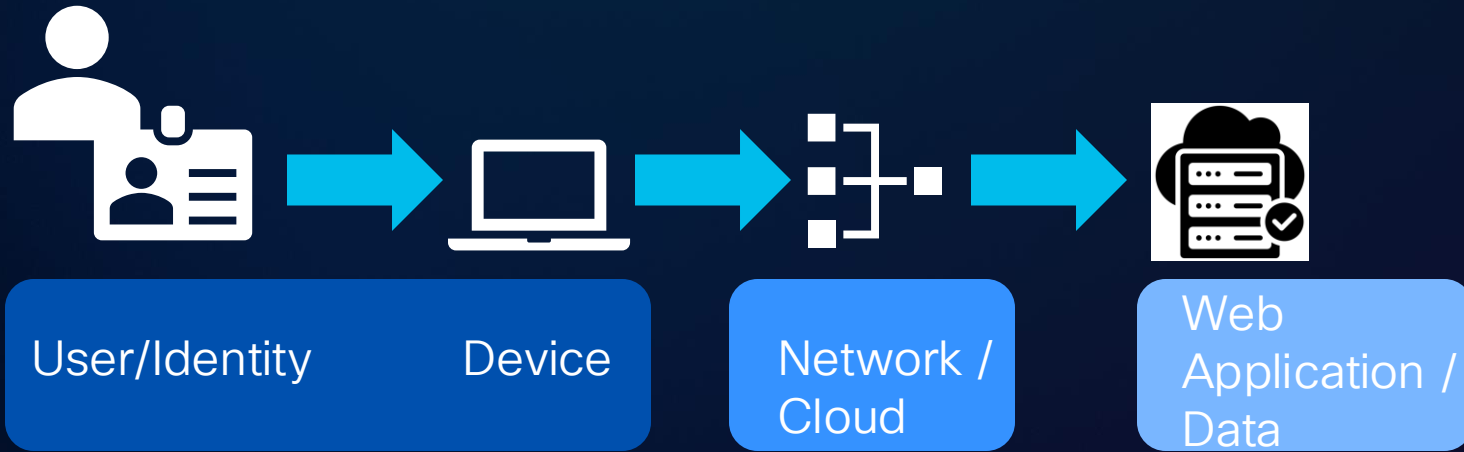
## User to App, App to App



# Addressing User to App with **Universal ZTNA and Identity**

# Zero Trust User to Application/Service

## Domains



# Universal ZTNA from CISCO

People



Managed



Unmanaged



Things



Modern private apps



SaaS apps



Internet apps



Traditional apps



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

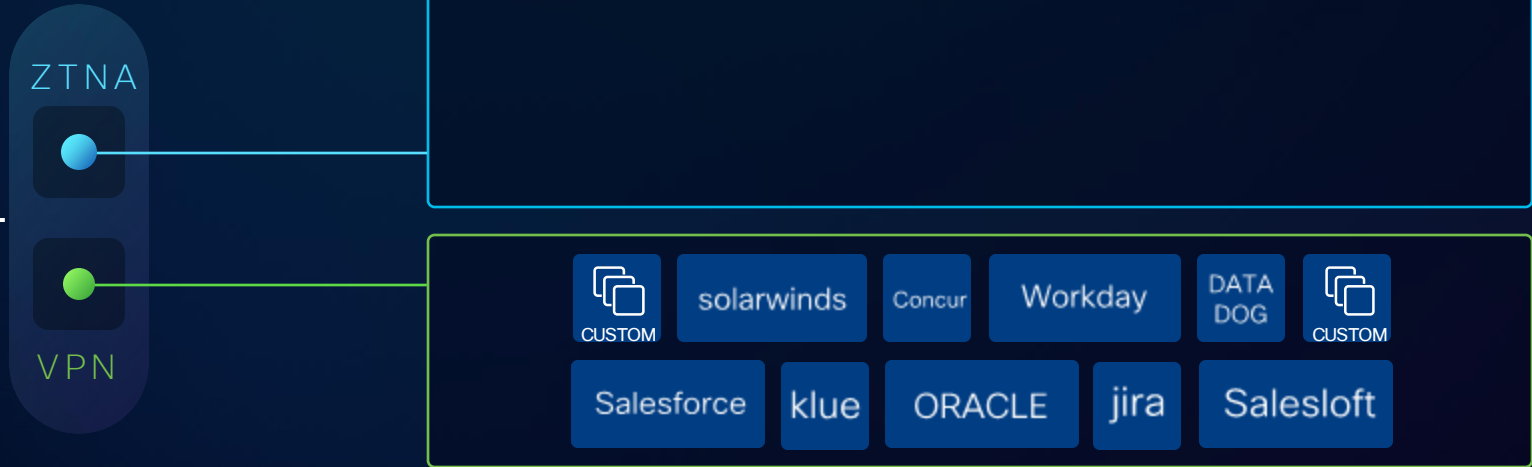
Internet Apps

Traditional Apps

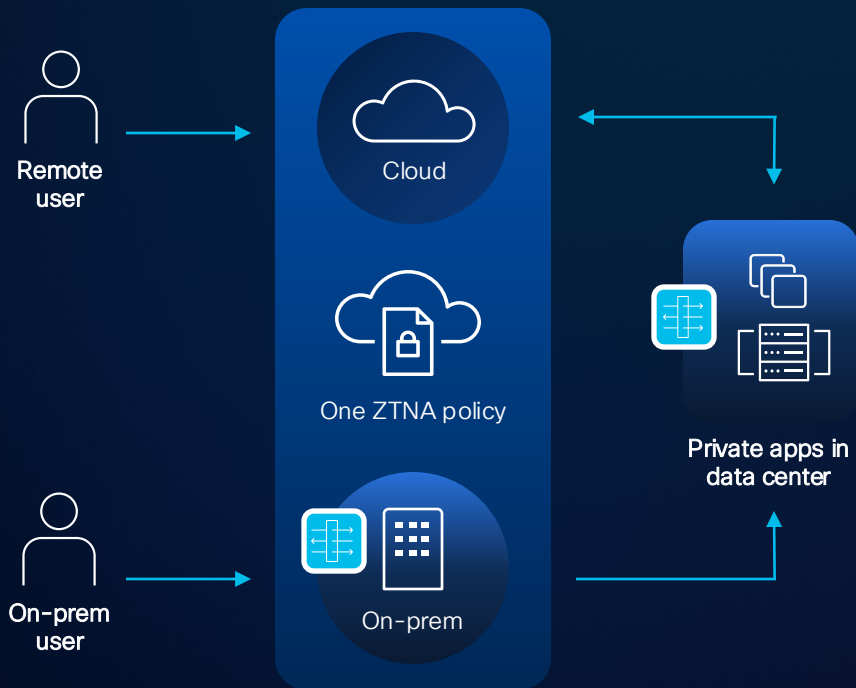
SaaS Apps

# Seamless Experience

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



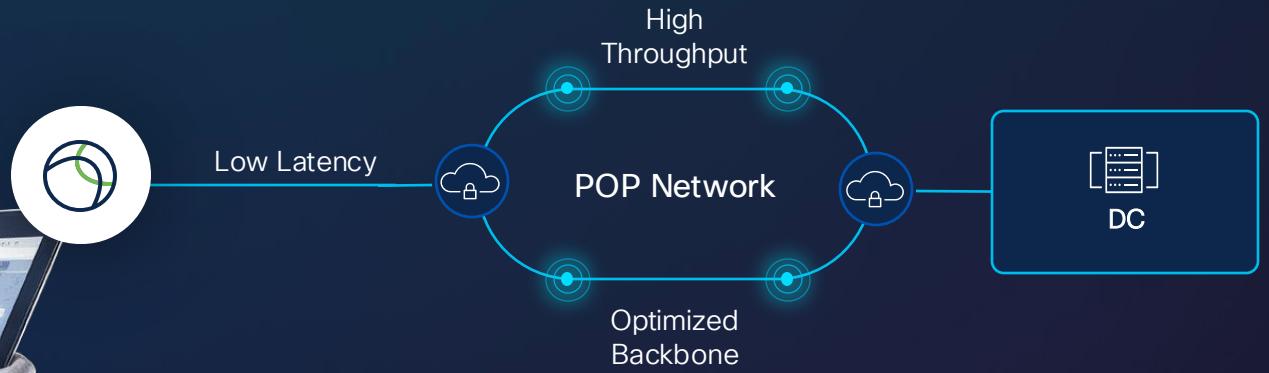
# Extending ZTNA with Cisco Secure Firewall



- 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

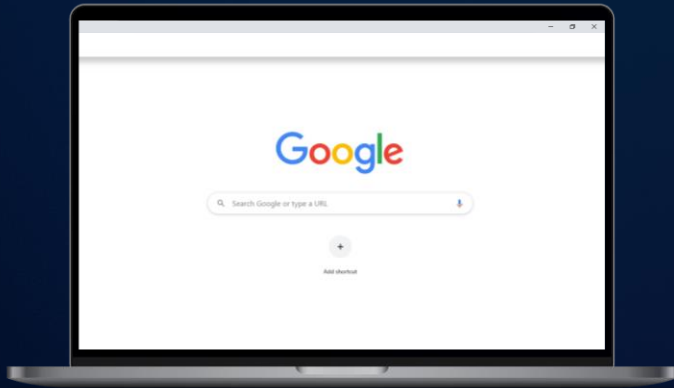
# Cisco's modern PoP architecture

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



# Native Device Support

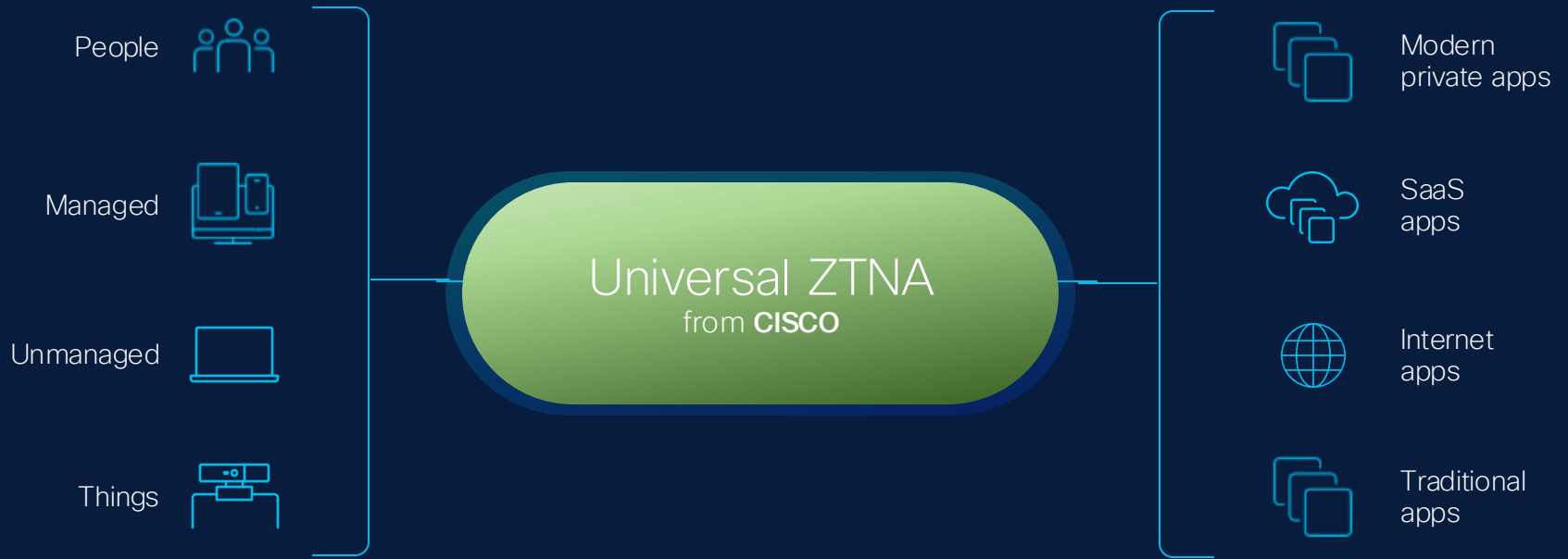
BYOD via enterprise managed Google Chrome  
Advanced protocol support for Apple, Samsung



Chrome Enterprise Browser



Native OS Integration



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

SailPoint

Dragos

CrowdStrike

Salesforce

Okta

PingIdentity

Cisco ISE

Auth0

Cyberark

Microsoft

Google

Amazon

# Cisco Identity Intelligence



USERS



MACHINES



SERVICES



HRIS



DATA



APPS



PLATFORMS



SailPoint

Dragos

CrowdStrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon



# User trust timeline

The screenshot displays the Cisco Identity Intelligence interface for a user named Brian Hayes. The user's profile includes a summary of attributes such as 'Inconsistent, Non Employee', 'N/A', 'Cort', 'US', and 'MFA Configured'. A prominent 'Trust Score' section indicates the user is 'Untrusted' as of September 18, 2024, with a list of reasons including an MFA flood attack, a resurrected account, and unmanaged devices. A notification banner at the top suggests linking other users with similar usernames or employee IDs.

**Identity Intelligence** Search Jeffrey Groesbeck genie

Users > **brian.hayes@simubiz.com**

**Brian Hayes** **US** **Active** Overview Activity Networks Devices Applications Groups Checks 8 Actions

We identified other users with a similar username or the same employee ID as **brian.hayes@simubiz.com**. Do you want to link them? Dismiss Review

**Summary**

- Inconsistent, Non Employee
- N/A
- N/A
- Cort
- US
- MFA Configured
- Sep 18, 2024 03:59:00 UTC (20 hours ago)
- N/A

Created Jul 18, 2010

**Trust Score** Last Updated: Sep 18, 2024 04:50:14 UTC  
**Untrusted**

Special account engaged in MFA flood attack  
New country for tenant and special account.  
New country for tenant, special account, resurrected account, and unmanaged device.

**Additional details**

- Special Account
- Resurrected Account  
Failing Checks: [Access From Dormant Account](#)
- MFA Flood  
Failing Checks: [Telecom MFA Limit Reached](#)
- New Country for Tenant  
Failing Checks: [New Country for Tenant](#)
- Unmanaged Device  
Failing Checks: [Unmanaged Devices Access](#)

5 events matching score View in Activity Tab View all activities with a score

Last Login Attempt View more data

# User Trust Score

The screenshot shows the Cisco Identity Intelligence interface for user Brian Hayes. The user's status is 'Active'. A notification banner at the top asks if the user wants to link other accounts with similar usernames or employee IDs. The main section displays the 'Trust Score' as 'Untrusted', last updated on Sep 18, 2024. Below this, a 'Summary' list includes attributes like 'Inconsistent, Non Employee', 'N/A', 'Oort', 'US', and 'MFA Configured'. A detailed 'Trust Score' section lists several security events: 'Special account engaged in MFA flood attack', 'New country for tenant and special account', 'Resurrected Account', 'MFA Flood', and 'Unmanaged Device'. Each event includes a 'Falling Checks' link to more details. At the bottom, there are links to 'View all activities with a score' and 'View in Activity Tab'.



## 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

**AI App Discovery** Secure Access

Leverage Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. [Learn more](#)

Risk  First detected date  48 results

Application name	Risk score	First detected
<a href="#">AI Assistant</a> <span>New</span>	<span>High</span>	Dec 29, 2024
<a href="#">Code Copilot</a> <span>New</span>	<span>High</span>	Dec 14, 2024
<a href="#">HelperAI</a>	<span>High</span>	Nov 22, 2024
<a href="#">AI Creator</a>	<span>High</span>	Nov 21, 2024
<a href="#">GrammarAI</a>	<span>Medium</span>	Nov 13, 2024
<a href="#">WriterBot</a>	<span>High</span>	Oct 30, 2024

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



# 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

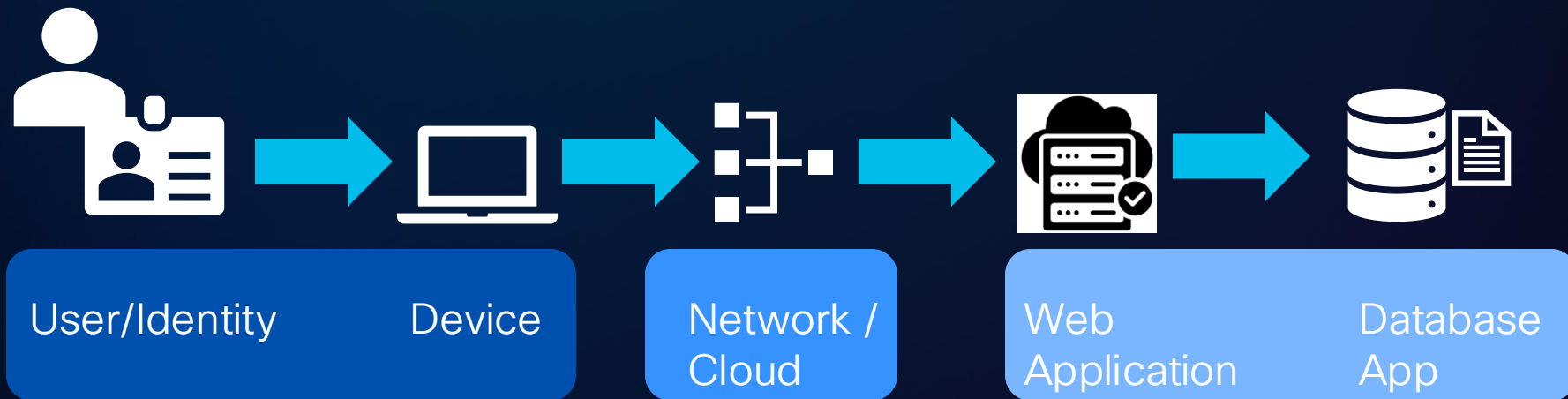


Telemetry

# Addressing Application Security

# Zero Trust End to End

- User to App, App to App



# Zero Trust App to App/Service

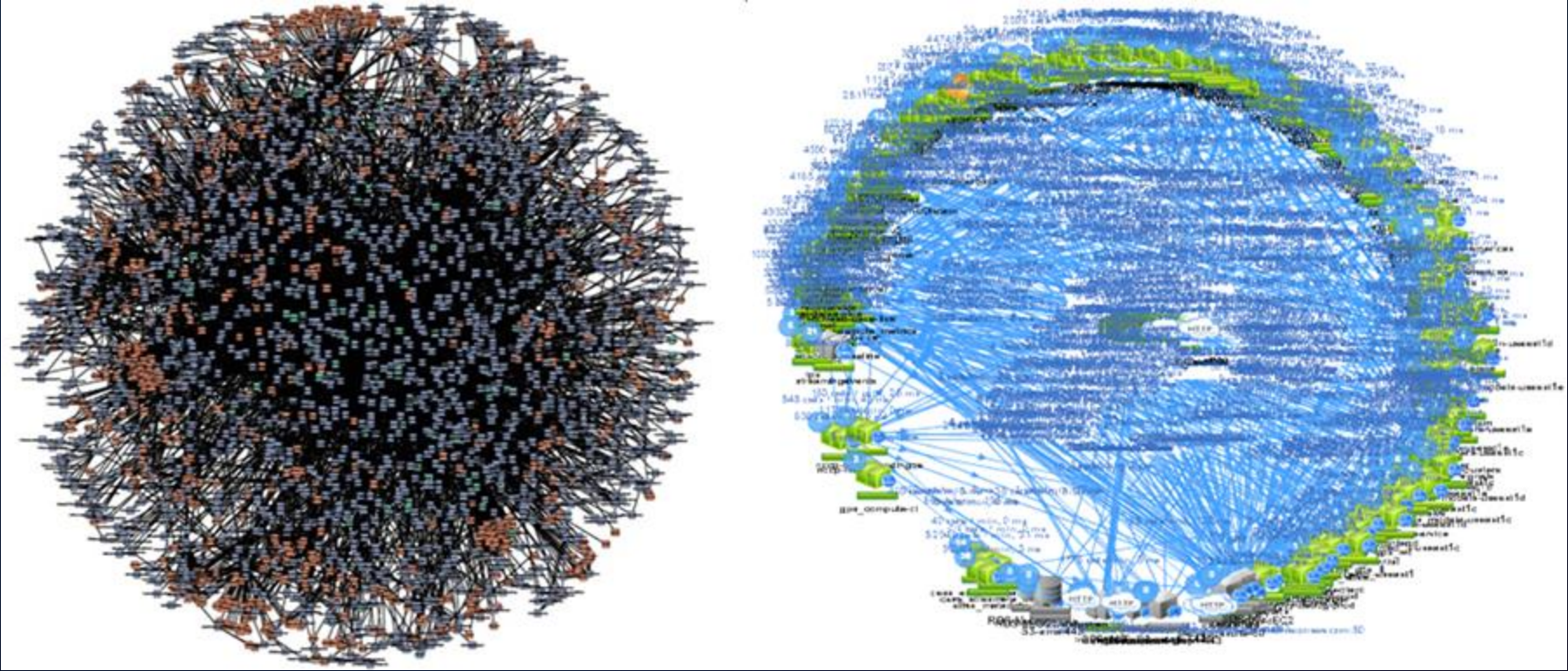
- Is it this Simple?



Web  
Application

Database  
App

# The Reality – One Day



# Extending Segmentation into Applications

## Edge Firewall



Secure Firewall



Multicloud Defense

## Macro-Segmentation



ACI



Secure Firewall



Secure Workload



## Micro-Segmentation



Secure Workload



tetragon

Hypershield



cilium

## 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

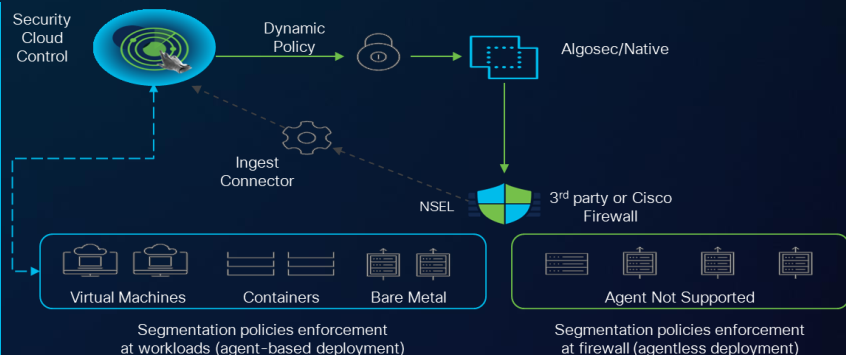
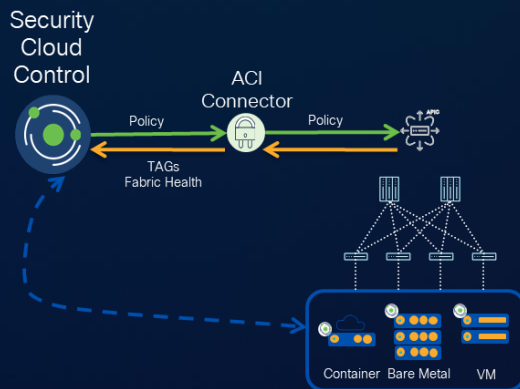


## Public Cloud

- 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

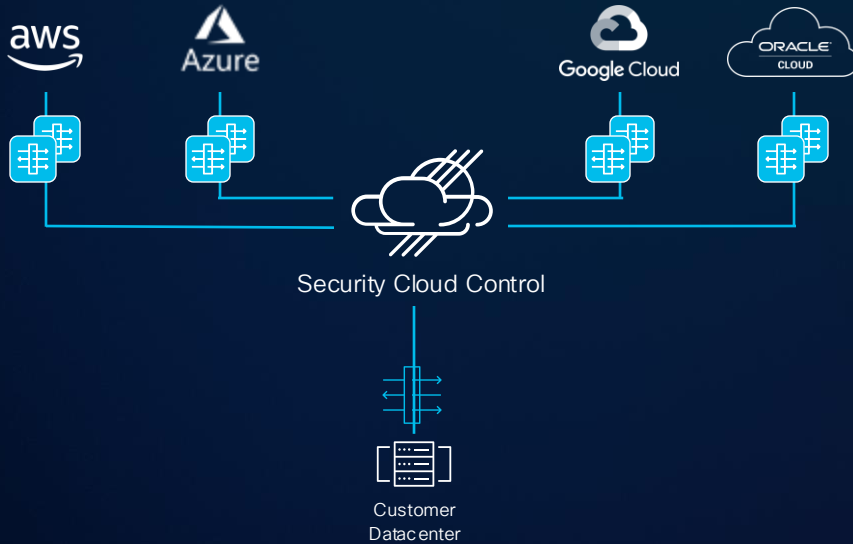


## With Firewalls

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



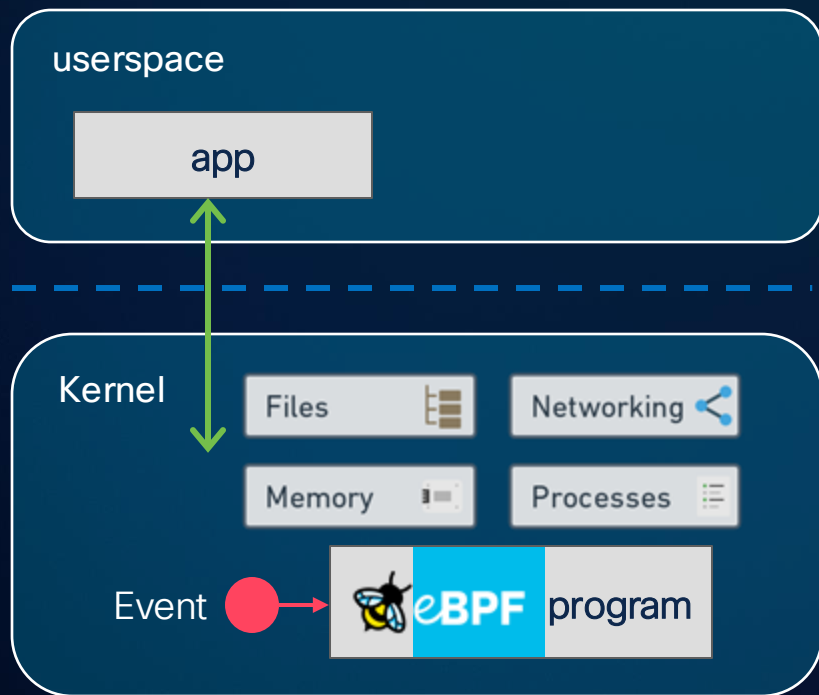
# Extending Firewalling to the cloud, *natively*



- 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

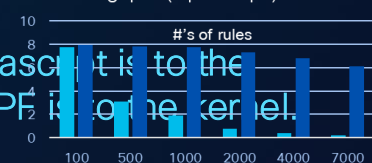
- Makes the kernel programmable in a secure and efficient way



UDP throughput (forward Mpps)



TCP throughput (input Gbps)



■ iptables  
■ bpf-iptables

Source:  
Accelerating Linux  
Security with eBPF  
iptables', Bertrone,  
SIGCOMM 2018

## System calls

- 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

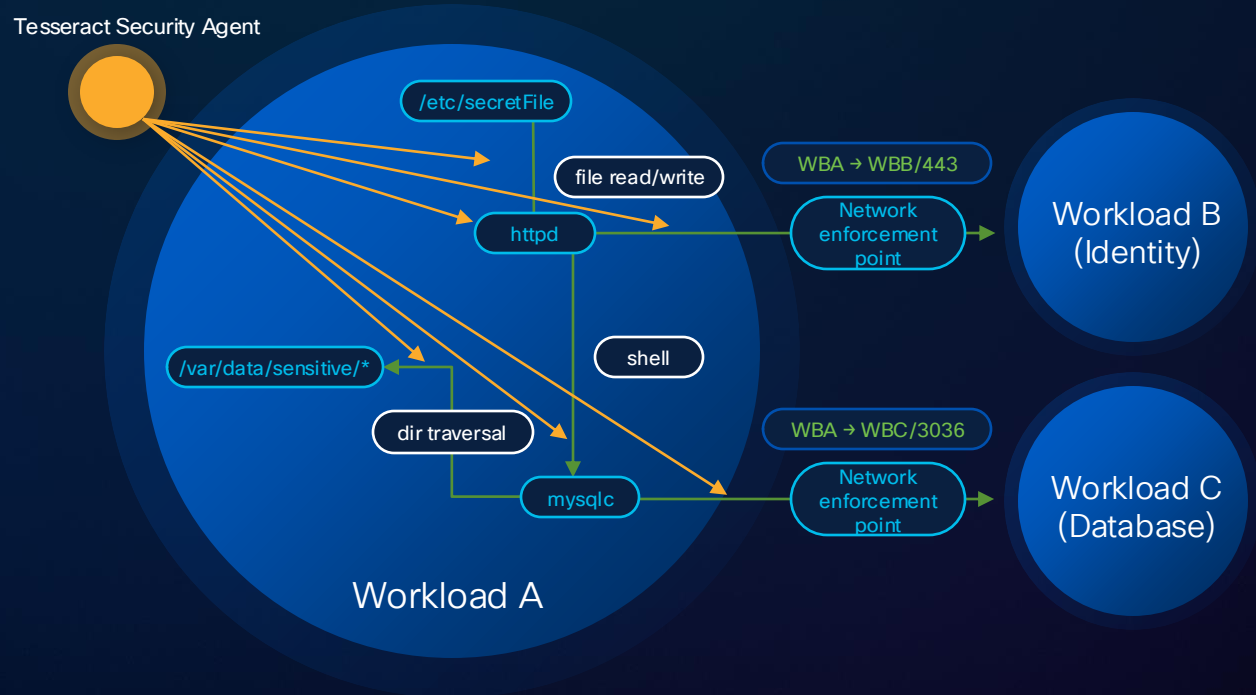
Tesseract Security Agent provides deep **visibility** and **enforcement** within workload

Network

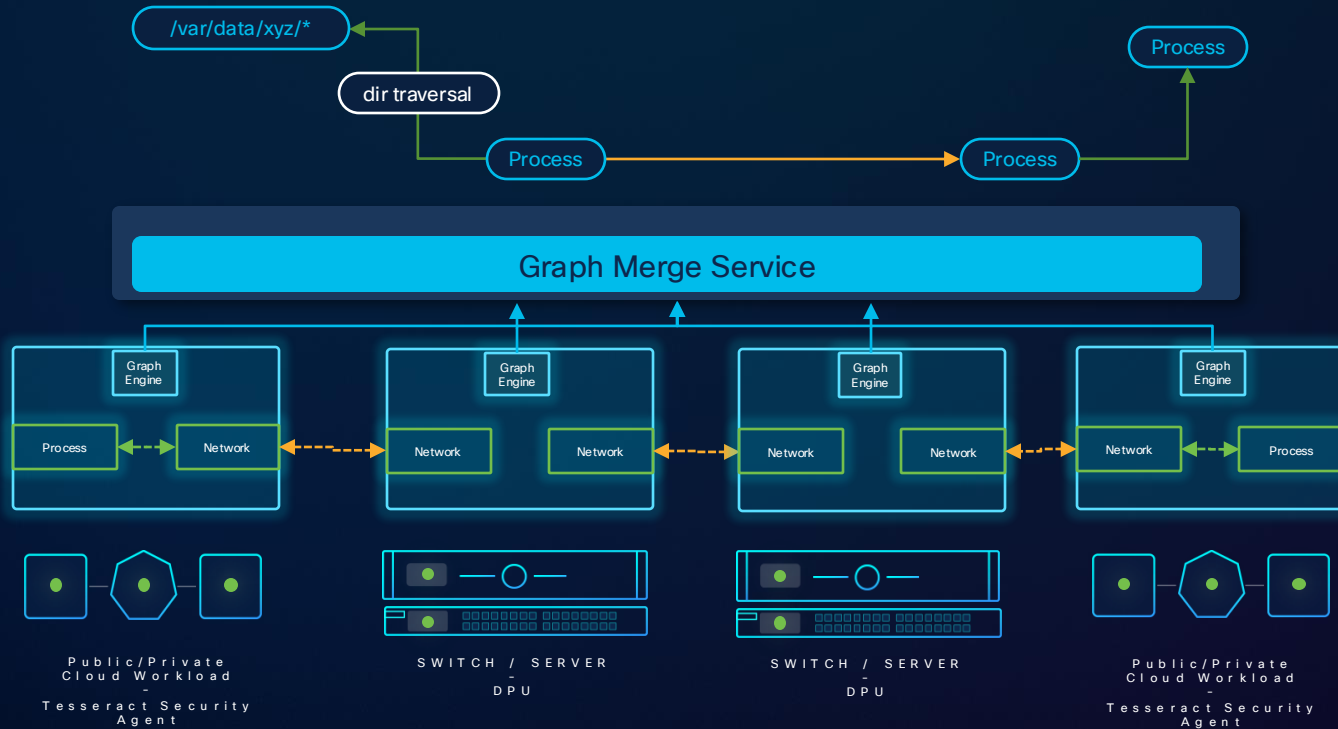
File read/write

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

New intent-driven Policy

Security Cloud Control + Natural Language Interface

Global Control Plane

Public Cloud



CLOUD NATIVE SERVICES

Private Cloud



SWITCH / SERVER

● Enforcement point



## 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

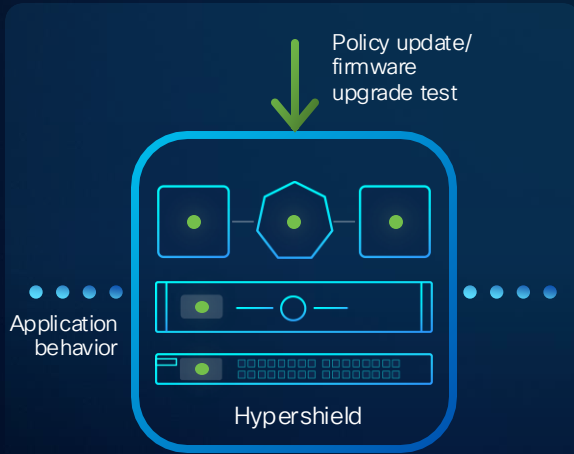
Kubernetes

Cloud – Private/Public

On-prem

# Policy Lifecycle management

- Self-qualifying firmware and policy updates



## Test

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

- 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.

## Review

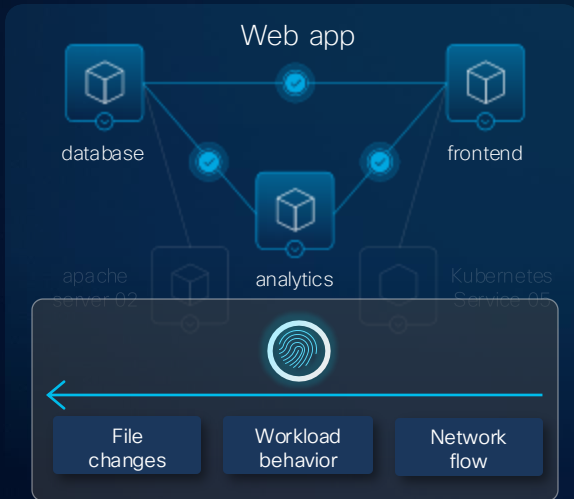
AI system evaluates change.  
Admin controls promotion



## Deploy

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

# Segmentation that is effective and keeps up with changing applications

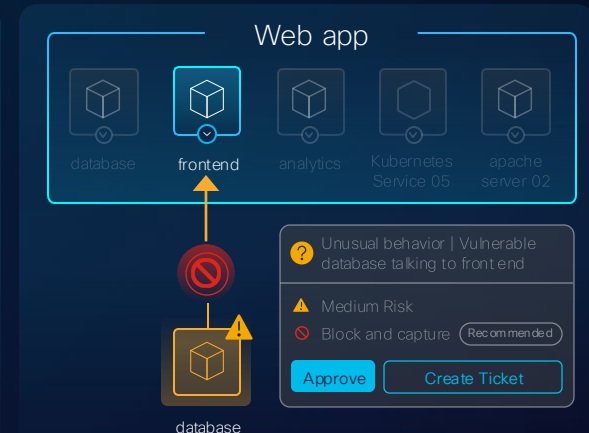


Complete understanding of changing app behavior from network to workload to pre-prod

## Recommendations

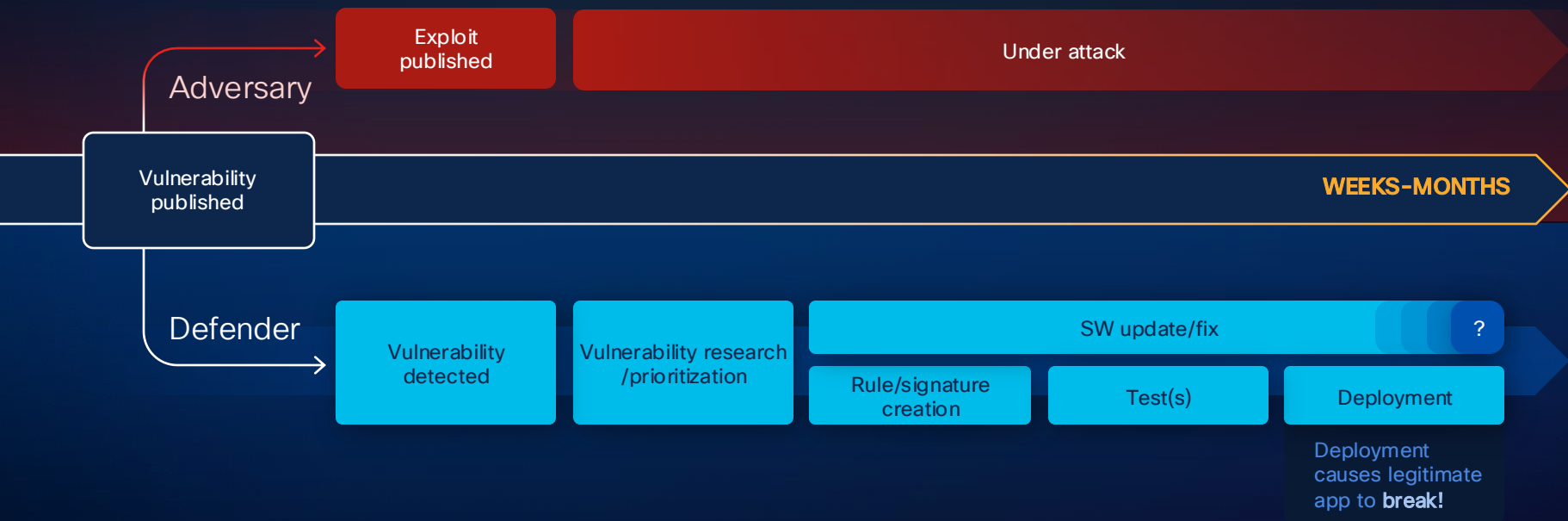
- Deny database can access Internet
- ✓ Permit web app frontend can access database
- ✓ Permit web app frontend can access analytics
- ✓ Permit web app analytics can access database
- ✓ Default observe and permit web app policy group...

Flexible segmentation rules that help avoid app fragility

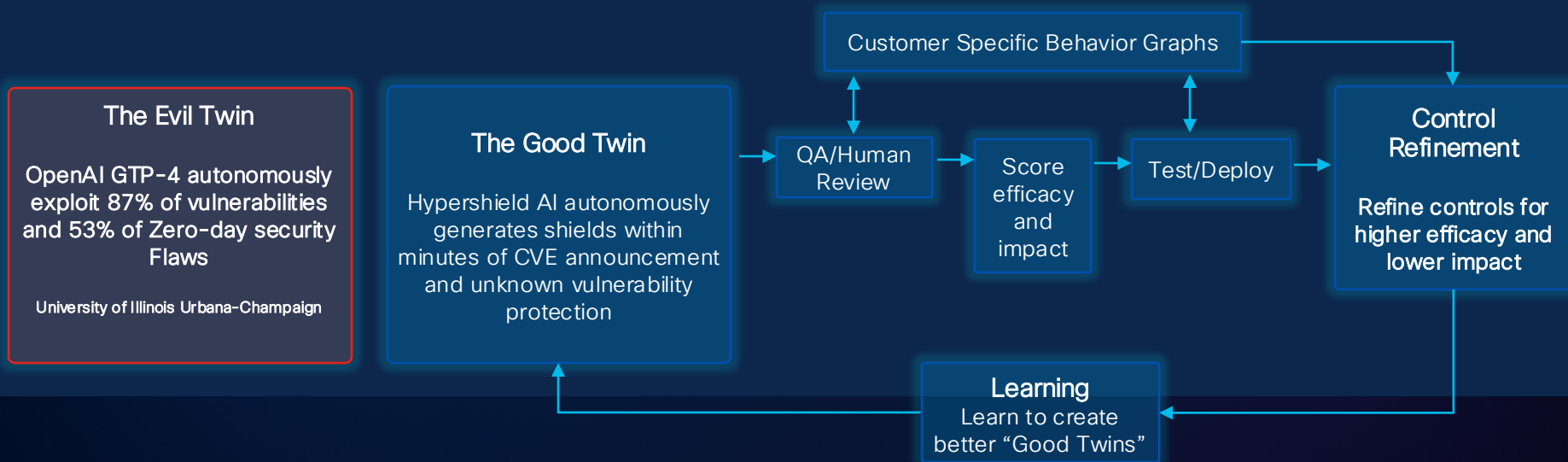


Policies updated to stricter rules in response to suspicious events

# 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



**CVE-2024-21626** High Priority

runc. 1.1.11 vulnerability

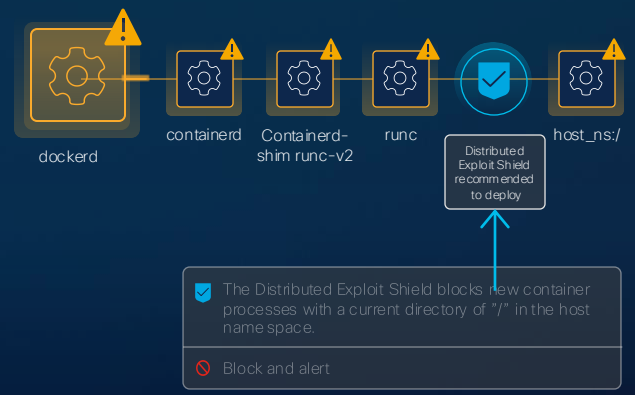
16,234 vulnerable assets

**Cisco Security Risk Score** 91 High **CVSS 3** 9.3

3 Affected zones

Production - External Critical Production - Internal Dev

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



The Distributed Exploit Shield was already tested in your environment

Tested against live production traffic to earn trust and increase confidence

# Coverage for non-eBPF capable workloads?

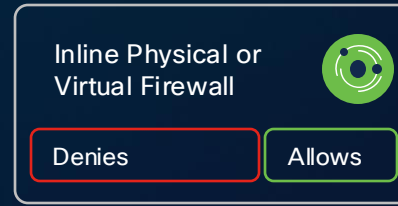
- Security Cloud Control renders security rules using native capabilities



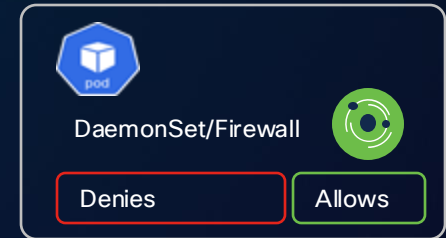
**Cloud**



**Bare metal & Virtual  
Machine**



**Firewalls, Smart  
Switches & DPU**



**Kubernetes**  
EKS/AKS/GKE/OpenShift/Unmanaged

- 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

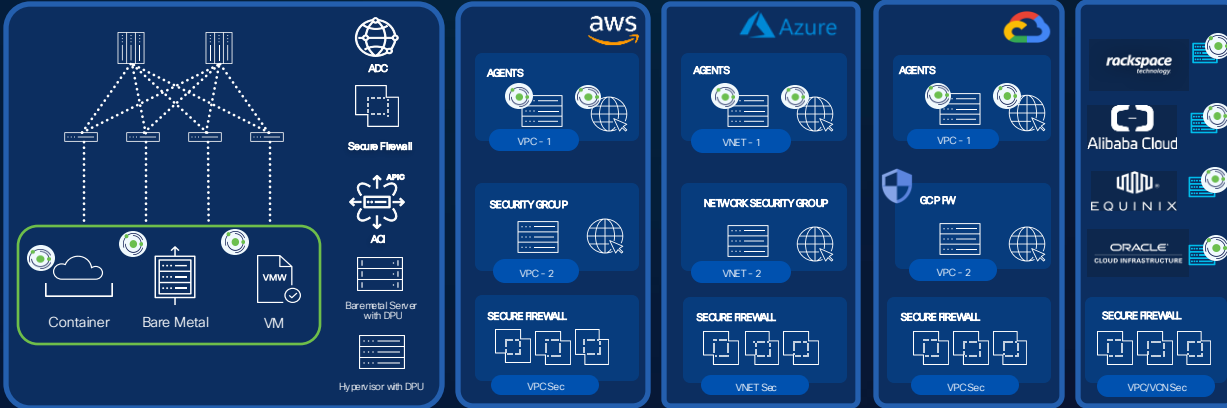
SUSE Linux

RedHat Linux

Amazon Linux

OpenShift

Kubernetes



On Premise

Public Cloud



Bare Metal Servers



Virtual Machines



Containers

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

## Recommended Actions

### Protect applications (67)

Secures sensitive data, prevents unauthorized access, and protects proprietary algorithms from theft or misuse.

Hide [View →](#)

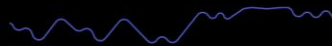
### Review increased app usage

3 days ago

Review sudden spikes in blocked events to avoid security risks.

#### ExternalChatBot Application

45MB +7%



Hide [View →](#)

### Review third party apps (67)

3 days ago

Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.



Cisco Security Cloud Enforcement Points

Hypershield

Secure Access

Cloud Firewalls

On-prem Firewalls

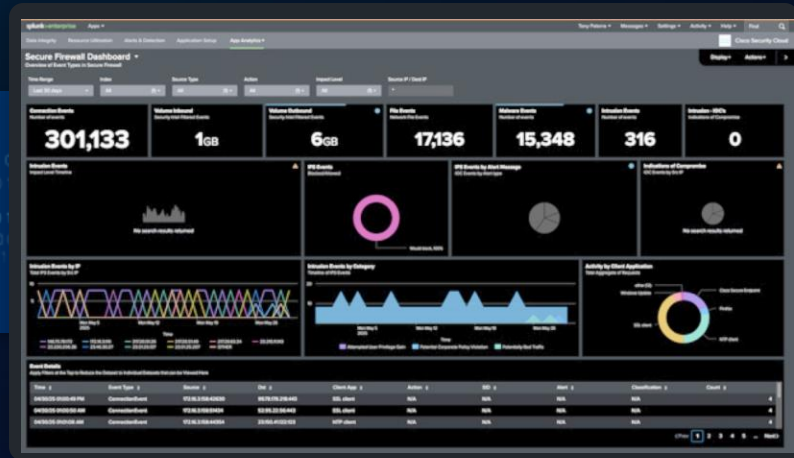
SOC of the Future

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 3<sup>rd</sup>-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



TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

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 & 3<sup>rd</sup> party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility incident response & threat hunting

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

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
- Identity / posture
- Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes

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

In the Office/Managed Location

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

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

Industrial Threat Defense

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

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

Workload, Application, and Data Security

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

# THANK YOU

