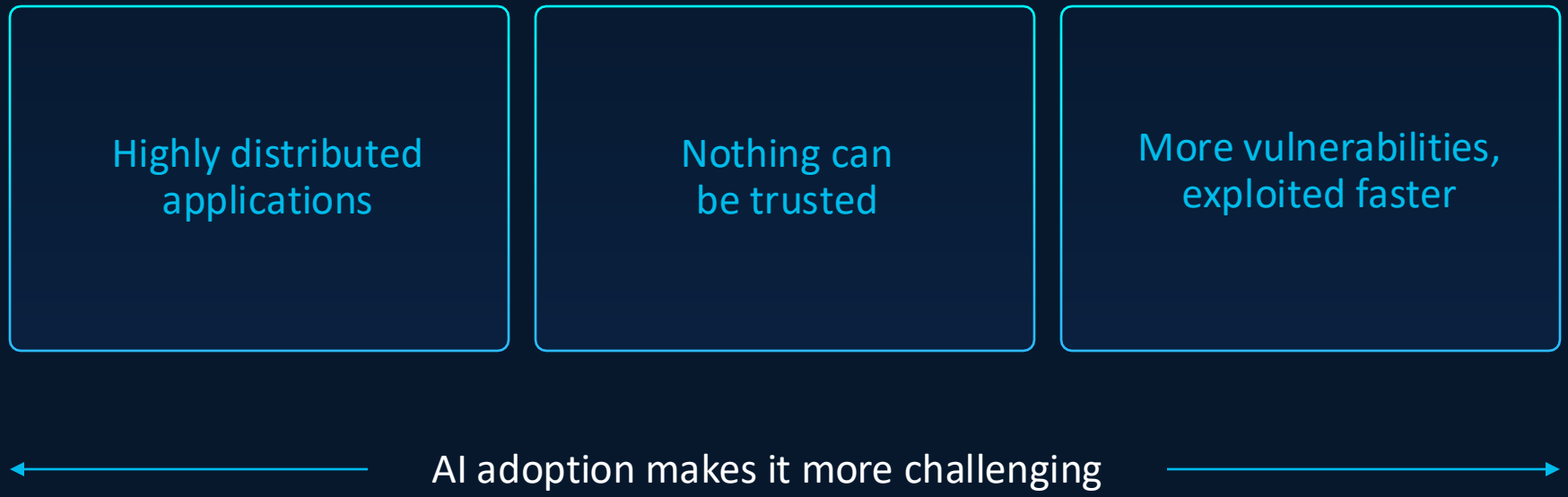
Cisco **Security**

Dynamic Defense: Hybrid Mesh Firewalls & Unified Security Management

Product Innovation

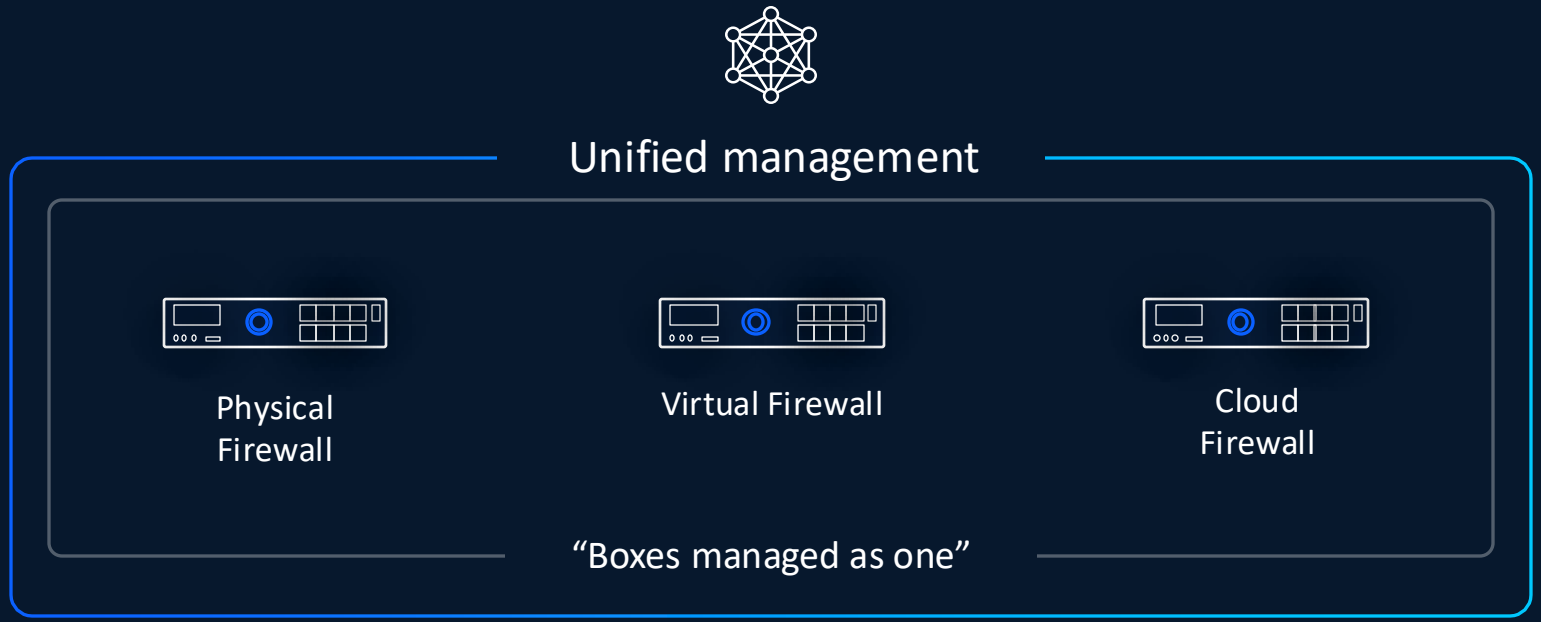
Securing the enterprise is increasingly challenging



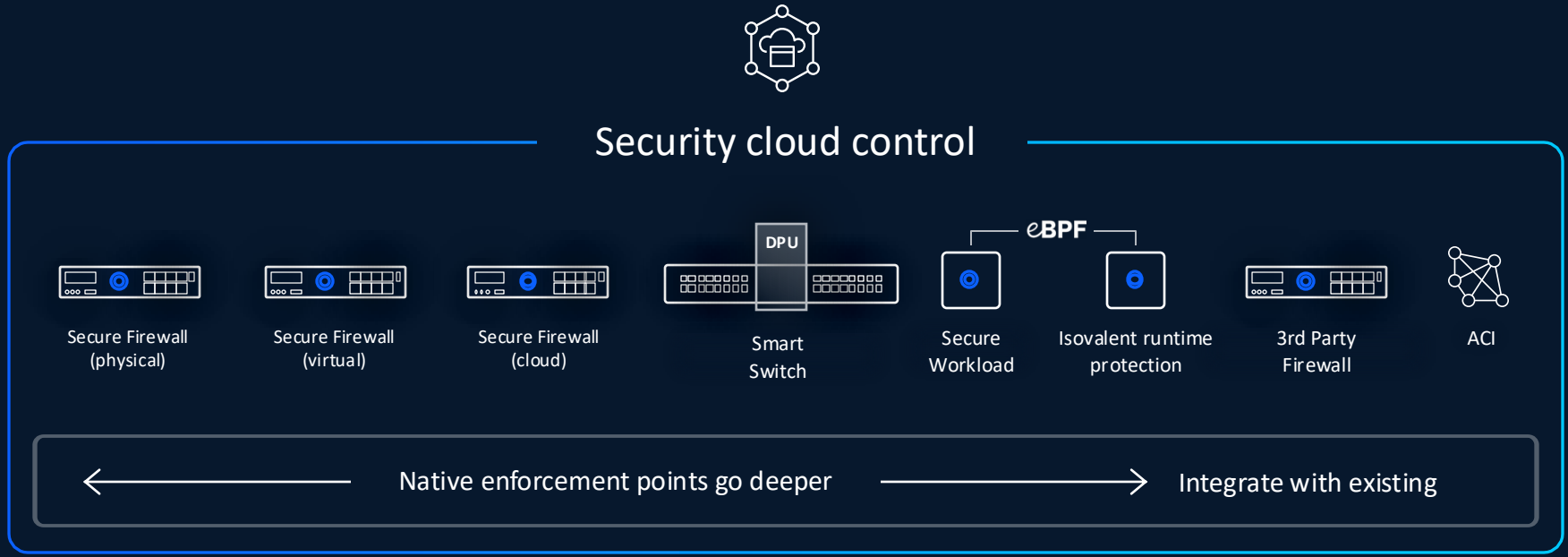
From Firewall to Firewalling

	Stateful Firewall	Next generation Firewall	Hybrid Mesh Firewall
	1990-2007	2008-2024	2025
Drivers	Growing internet access Basic attacks Need perimeter control	Rise of SaaS/cloud apps Mobile users App layer threats	Increasingly distributed apps Rise of AI Zero trust imperative
Needs	Tracks connection state Filters by IP/port Basic traffic control	App & user aware Integrated threat prevention SSL/TLS decrypt	Hyper-distribution Integrated AI protection AI-powered management

Competitor definition of Hybrid Mesh Firewall is limited



Cisco Hybrid Mesh Firewall goes broader and deeper



Write policy once, enforce across the mesh

NEW

Security Cloud Control

Industry’s first multi-vendor intent-based policy

Absorb and optimize existing rules

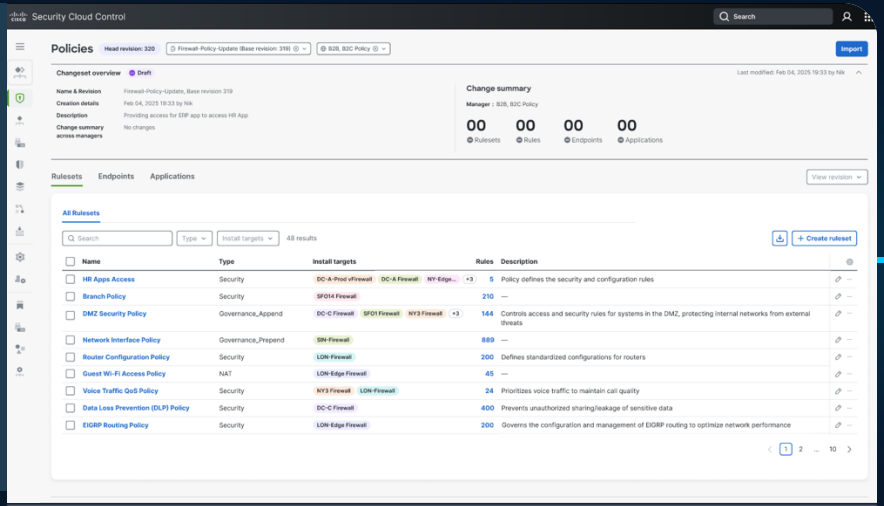
Change enforcement points, not policy

No rip and replace

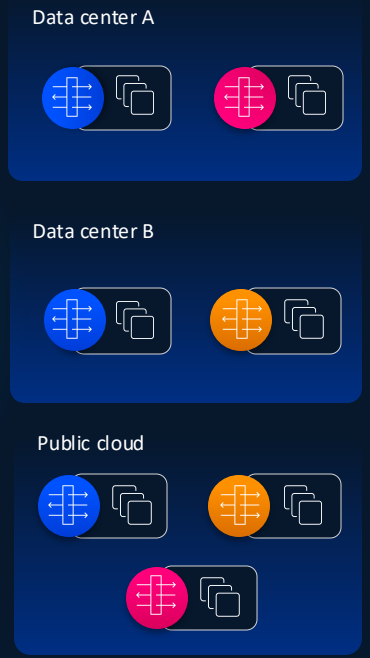
Introducing Mesh Policy Engine

Cisco is the only enterprise firewall vendor that extends policy to non-Cisco enterprise firewalls

- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy **and** the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors



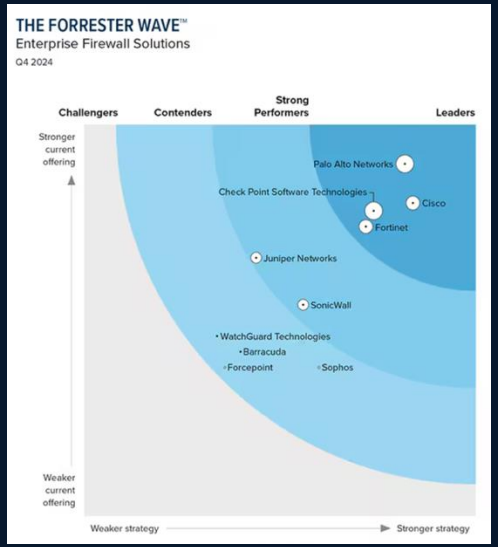
Cisco Security Cloud Control



FORRESTER®

2024 Forrester Wave: Enterprise Firewall Solutions

LEADER



IDC

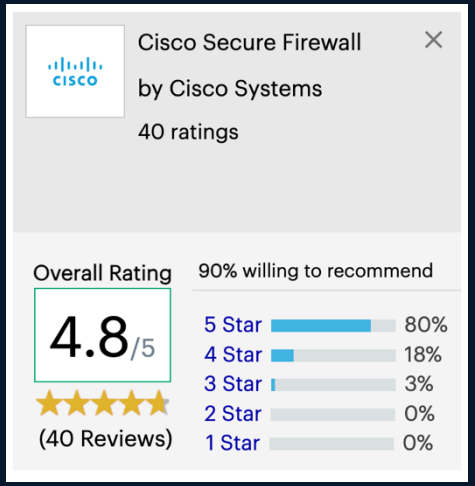
2025 IDC MarketScape: Worldwide Enterprise Hybrid Firewall

LEADER

Gartner Peer Insights™

Network Firewalls

SCORE LEADER*



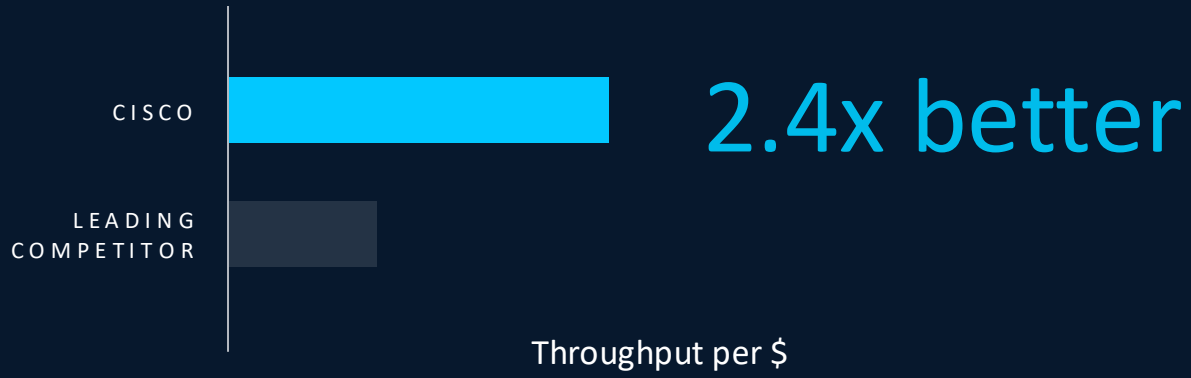
* Vs Palo Alto Networks 4.6, Fortinet 4.7. All scores for last 12 months as of Aug 19, 2025.

Cisco changes the economics of decryption

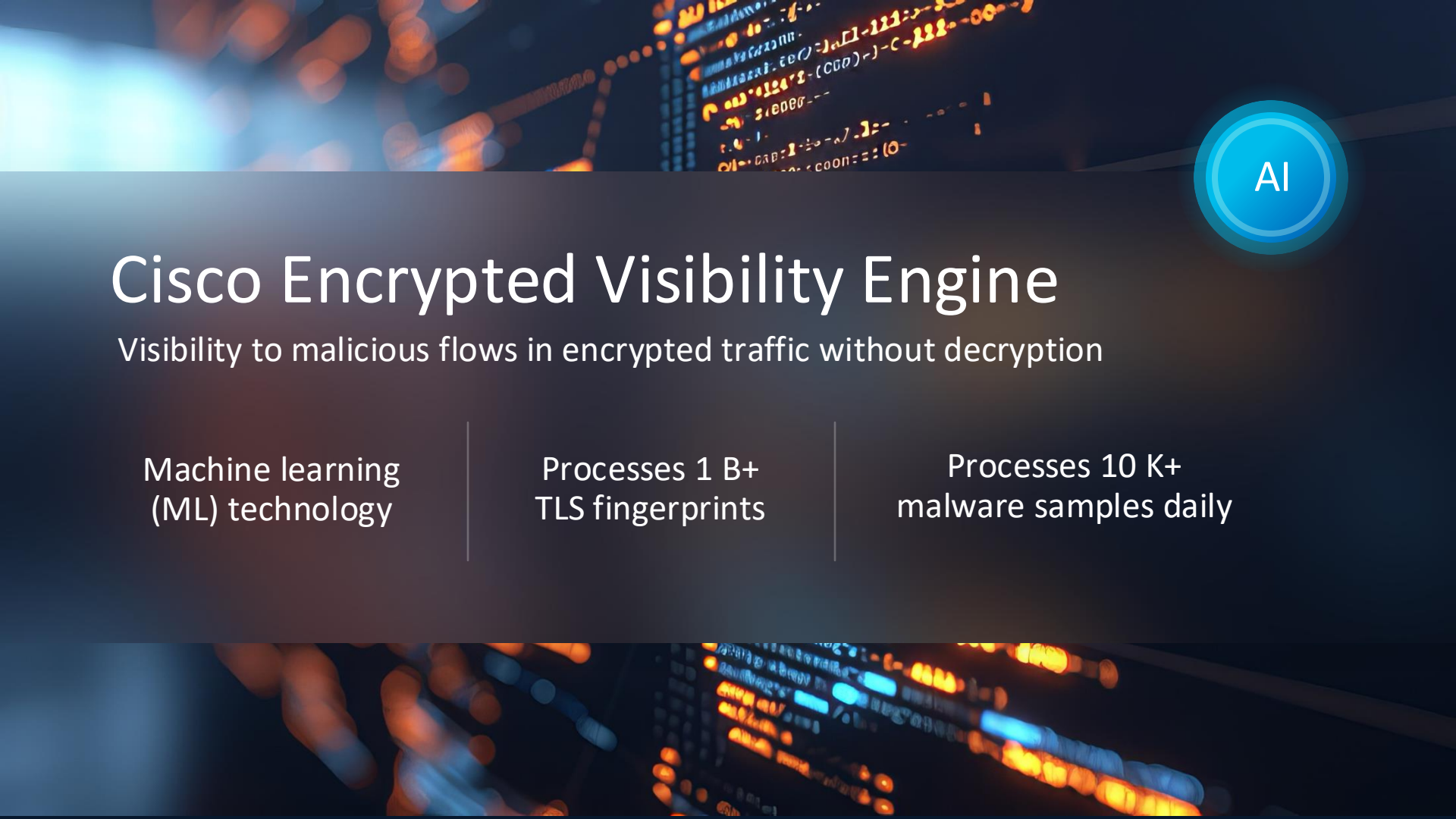
High-performance hardware offload architecture delivers price-performance leadership

NetSecOPEN

Testing validates Cisco's decryption advantage



1 Table 2: Performance specifications and feature details, Cisco Firewall 3100 Series Data Sheet
2 Table 11: HTTPS Throughput, NetSecOPEN Certification Report, Fortinet
Price from https://www.cdw.com/search/?key=cisco%203105
and https://www.cdw.com/product/fortinet-fortigate-601f-security-appliance/7122512?pfm=srh



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

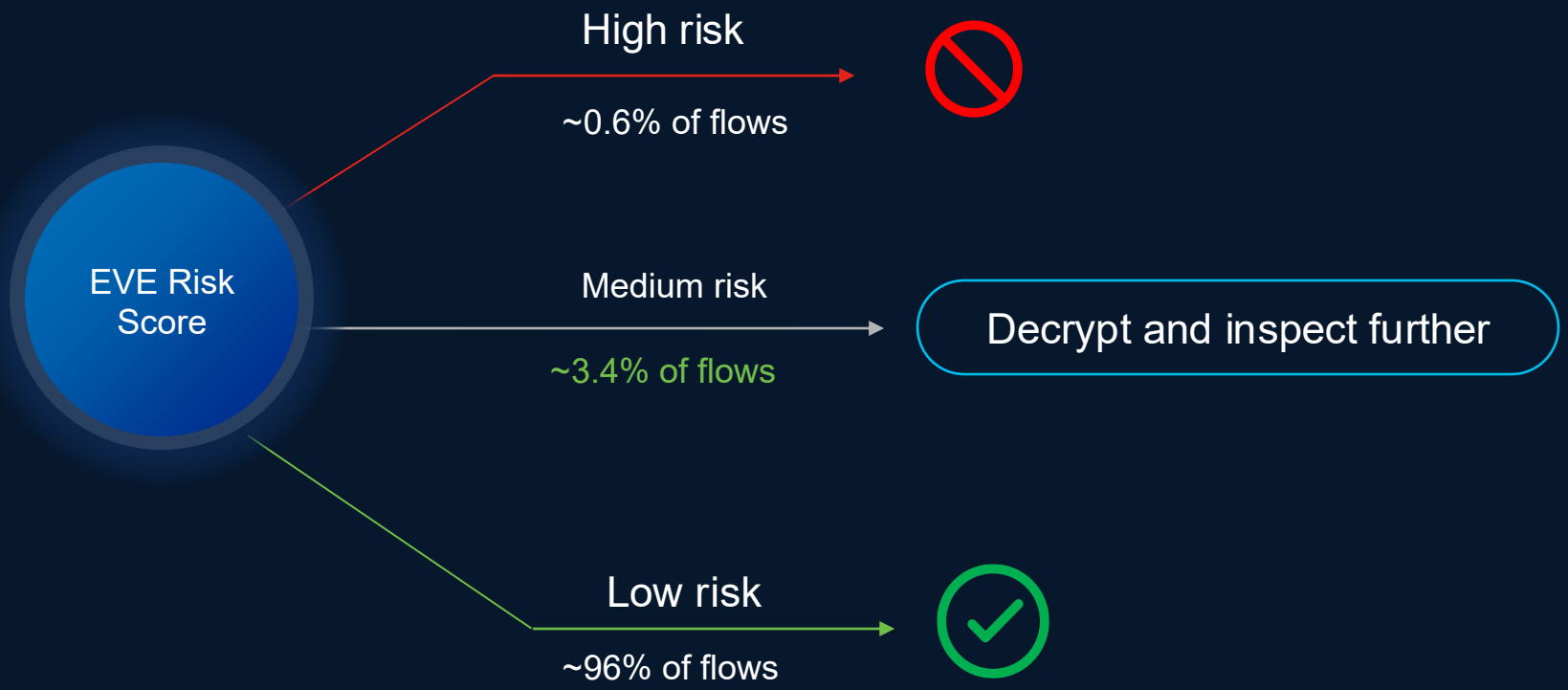
Machine learning (ML) technology

Processes 1 B+ TLS fingerprints

Processes 10 K+ malware samples daily

Eve changes the game on decryption

Risk-based intelligent decryption, powered by Cisco Encrypted Visibility Engine (EVE)



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

Flexibility to swap components

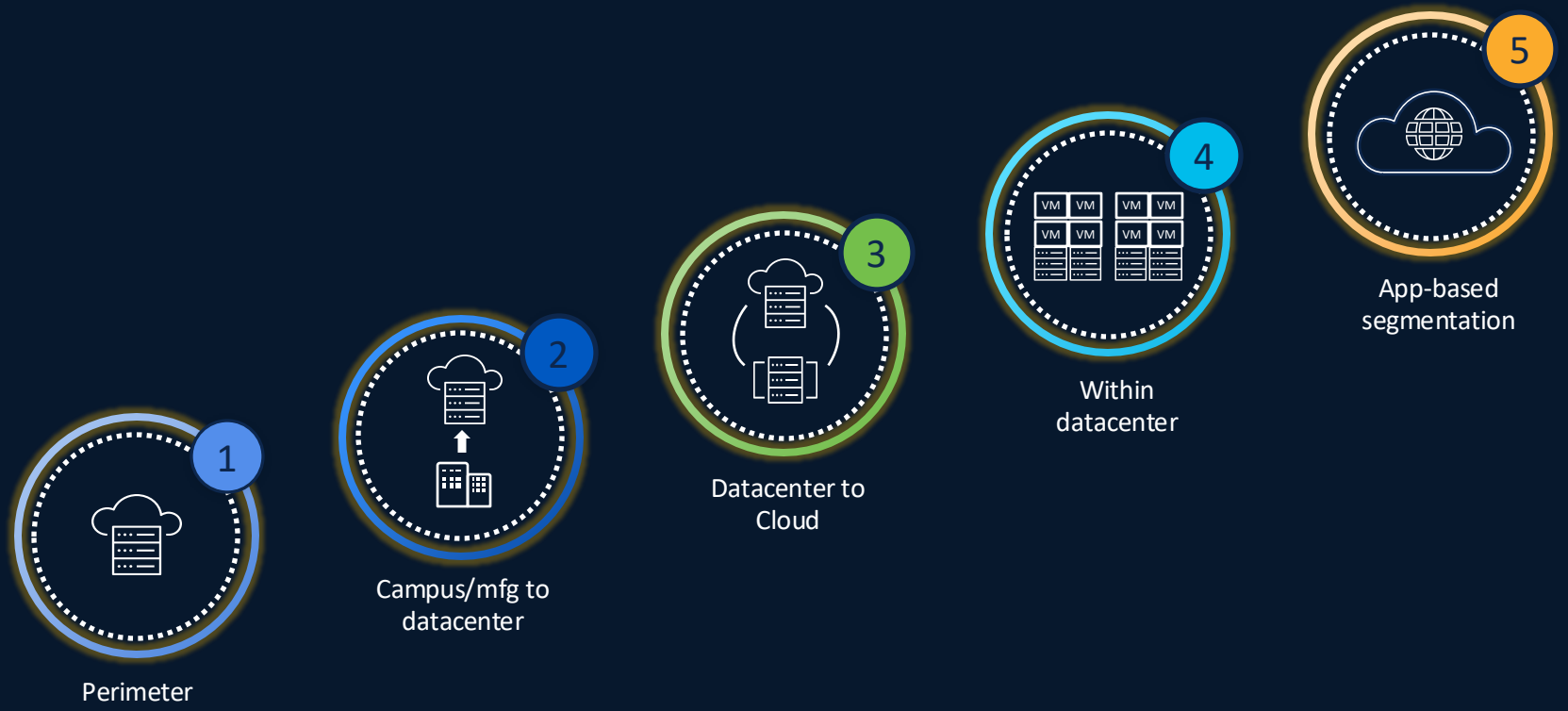
Cloud Protection Suite license

Gateways

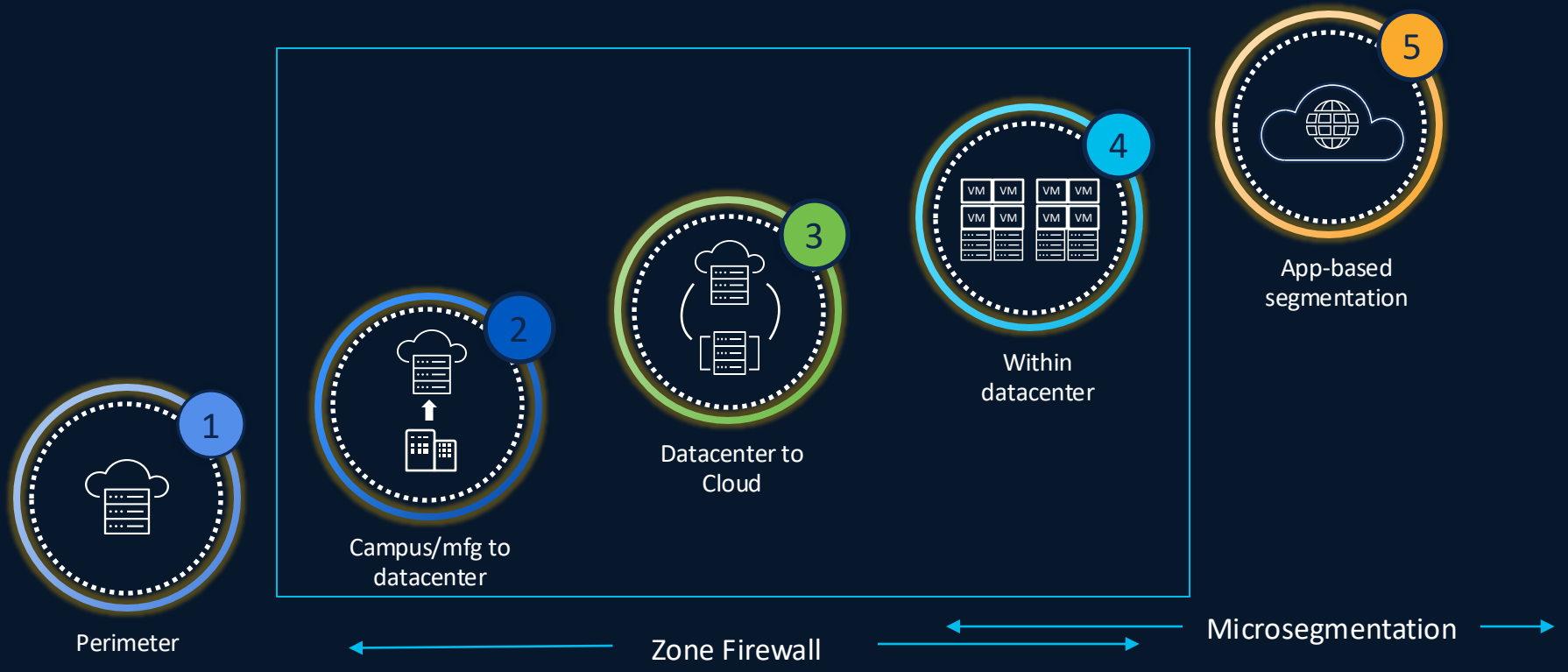
Workloads

Secure Firewall	Multicloud Defense	Secure Workload	Isovalent Enterprise	Hypershield

Segmentation that meets you where you are



Segmentation that meets you where you are



Know who is accessing what, and how apps are interacting

Segmentation

Network Segmentation

Microsegmenation

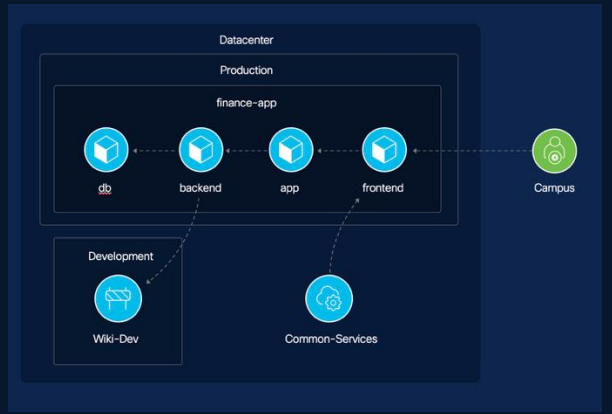
Kubernetes

Automated Application Policy Discovery

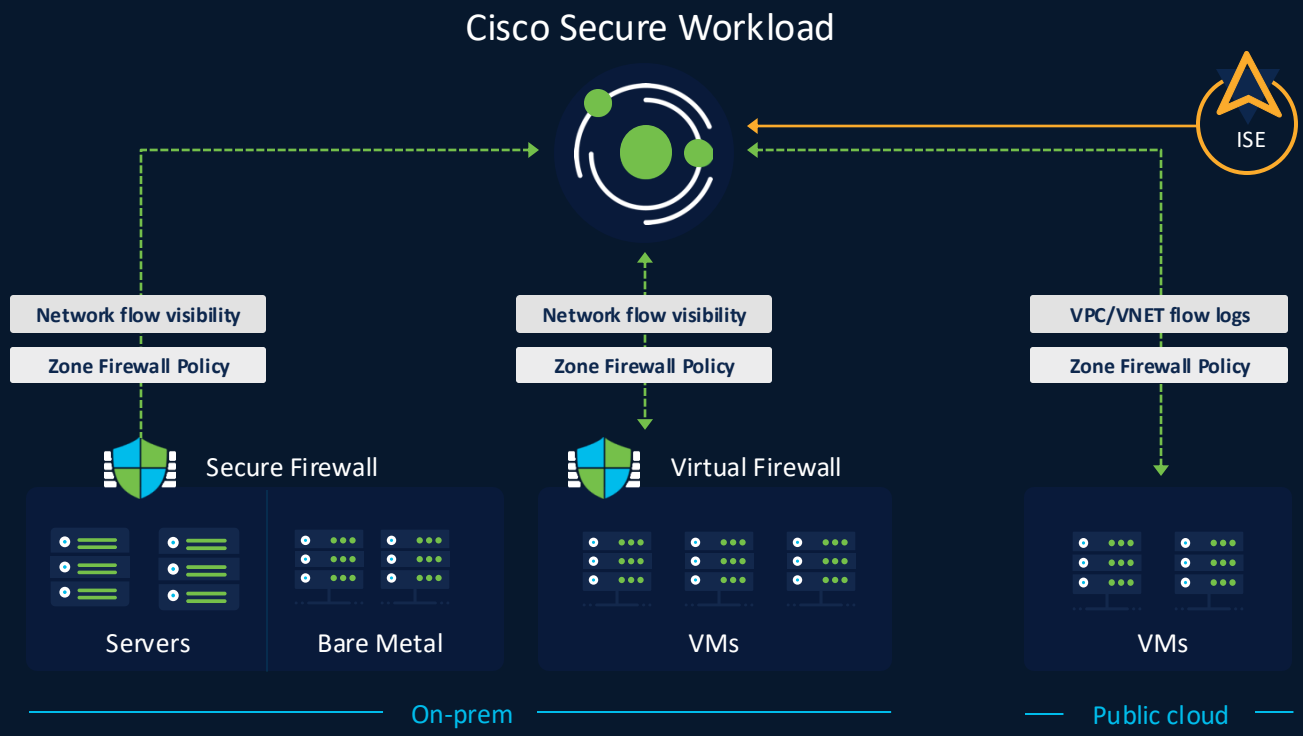
Baseline workload protection posture

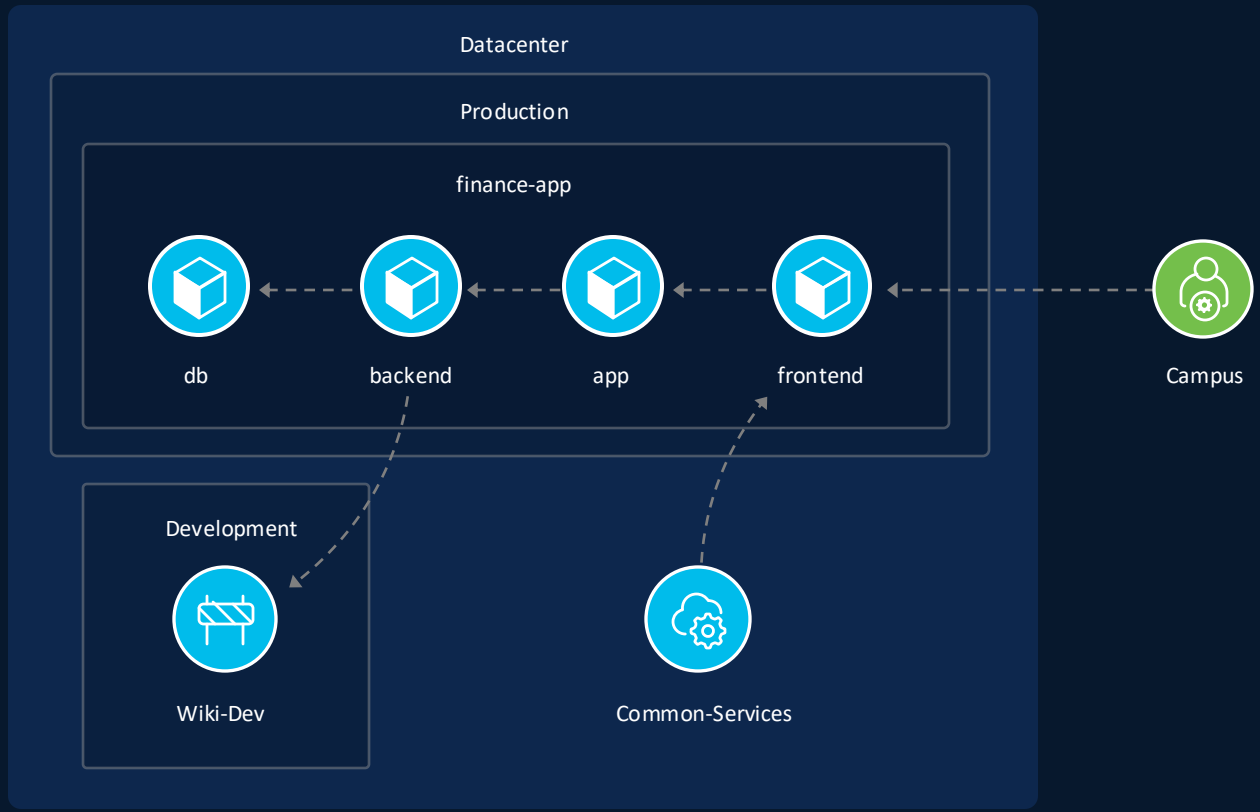
- Network communications
- Process behavior
- Labels
- SGT tags (ISE)

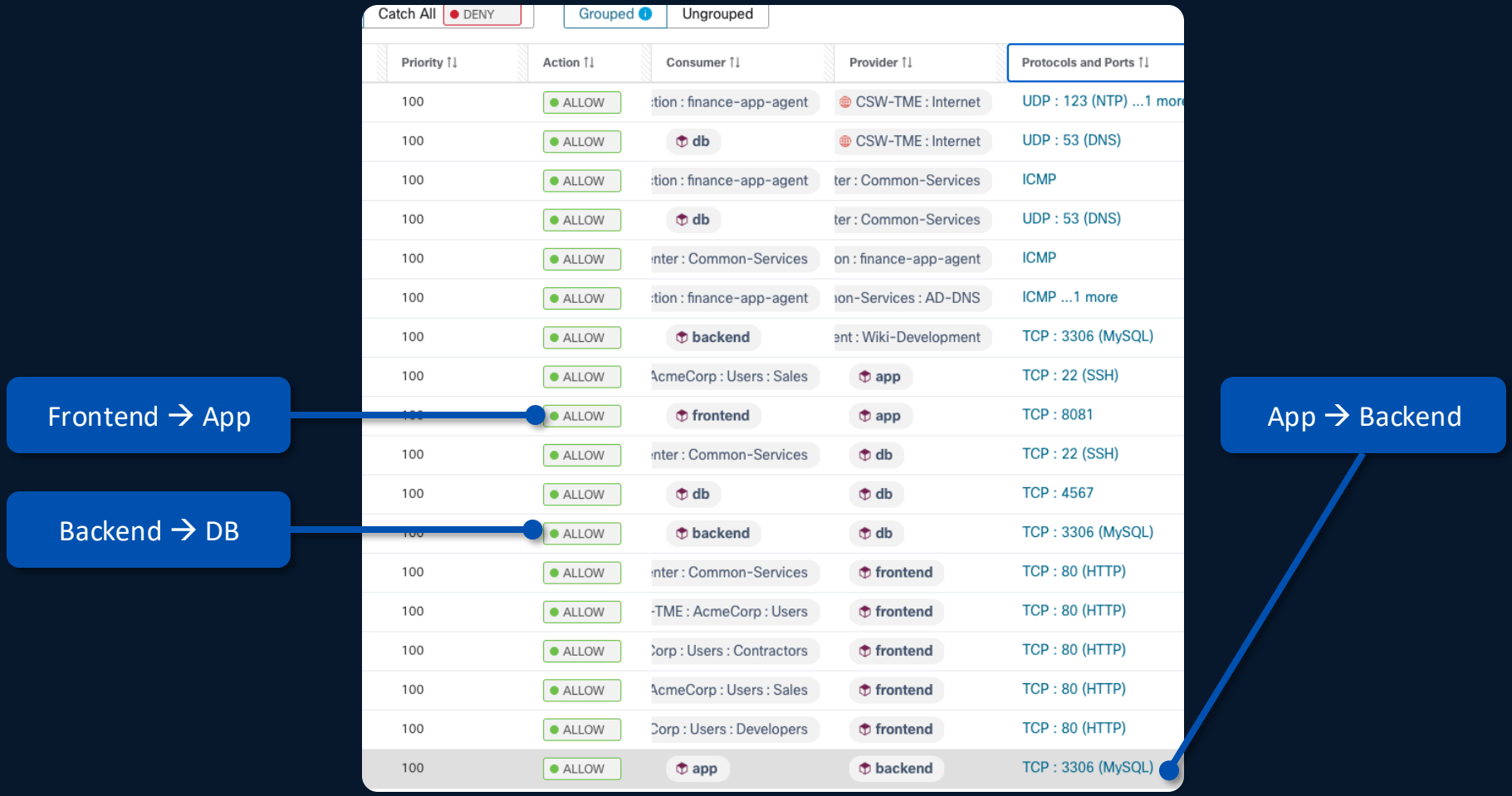
Secure Workload



Agentless policy discovery and enforcement



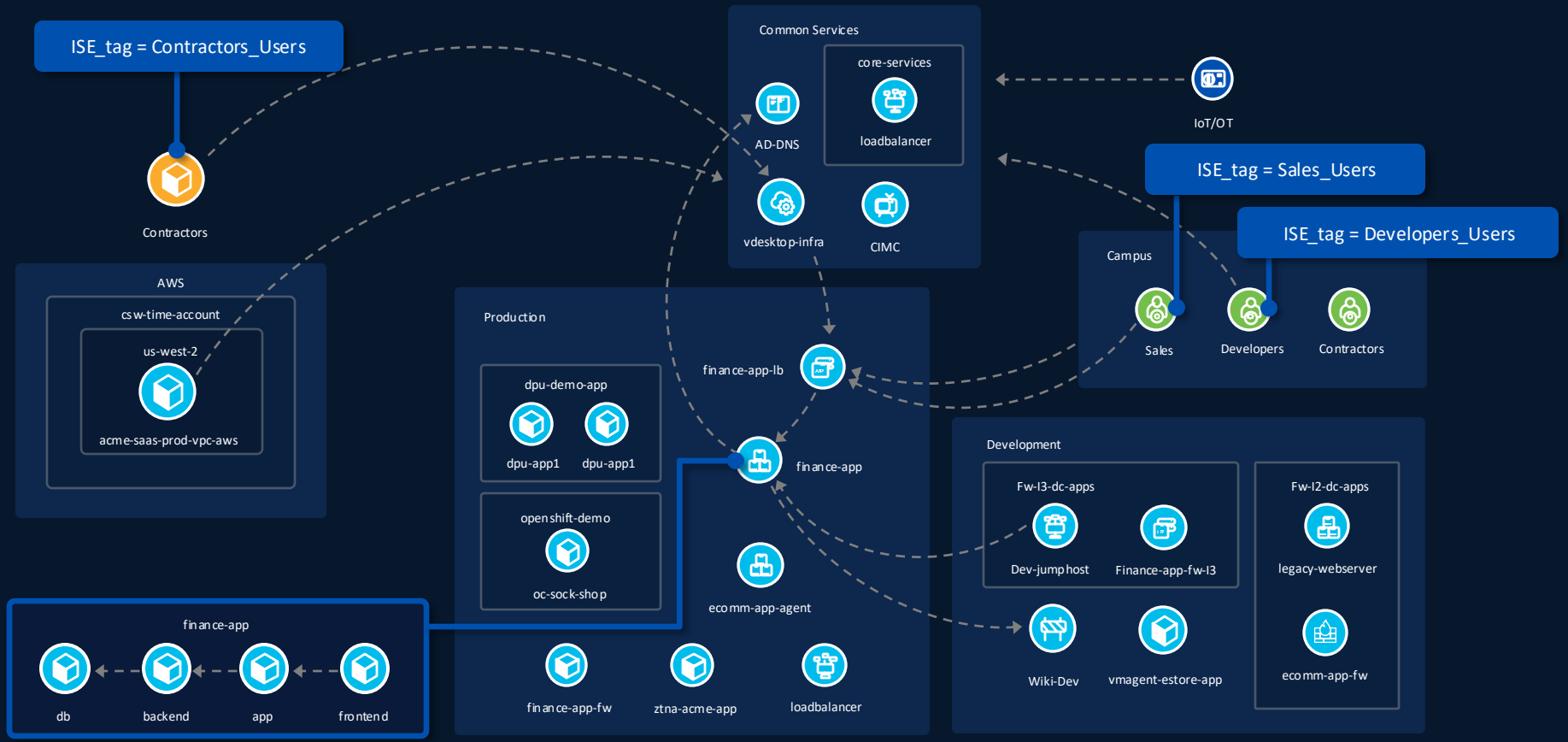

Datacenter
Production
finance-app
db
backend
app
frontend
Campus
Development
Wiki-Dev
Common-Services


Frontend → App
Backend → DB
App → Backend
Catch All
DENY
Grouped
Ungrouped
Priority
Action
Consumer
Provider
Protocols and Ports
100 ALLOW tion : finance-app-agent CSW-TME : Internet UDP : 123 (NTP) ...1 more
100 ALLOW db CSW-TME : Internet UDP : 53 (DNS)
100 ALLOW tion : finance-app-agent ter : Common-Services ICMP
100 ALLOW db ter : Common-Services UDP : 53 (DNS)
100 ALLOW nter : Common-Services on : finance-app-agent ICMP
100 ALLOW tion : finance-app-agent ion-Services : AD-DNS ICMP ...1 more
100 ALLOW backend ent : Wiki-Development TCP : 3306 (MySQL)
100 ALLOW AcmeCorp : Users : Sales app TCP : 22 (SSH)
100 ALLOW frontend app TCP : 8081
100 ALLOW nter : Common-Services db TCP : 22 (SSH)
100 ALLOW db db TCP : 4567
100 ALLOW backend db TCP : 3306 (MySQL)
100 ALLOW nter : Common-Services frontend TCP : 80 (HTTP)
100 ALLOW -TME : AcmeCorp : Users frontend TCP : 80 (HTTP)
100 ALLOW Corp : Users : Contractors frontend TCP : 80 (HTTP)
100 ALLOW AcmeCorp : Users : Sales frontend TCP : 80 (HTTP)
100 ALLOW Corp : Users : Developers frontend TCP : 80 (HTTP)
100 ALLOW app backend TCP : 3306 (MySQL)

We also understand things

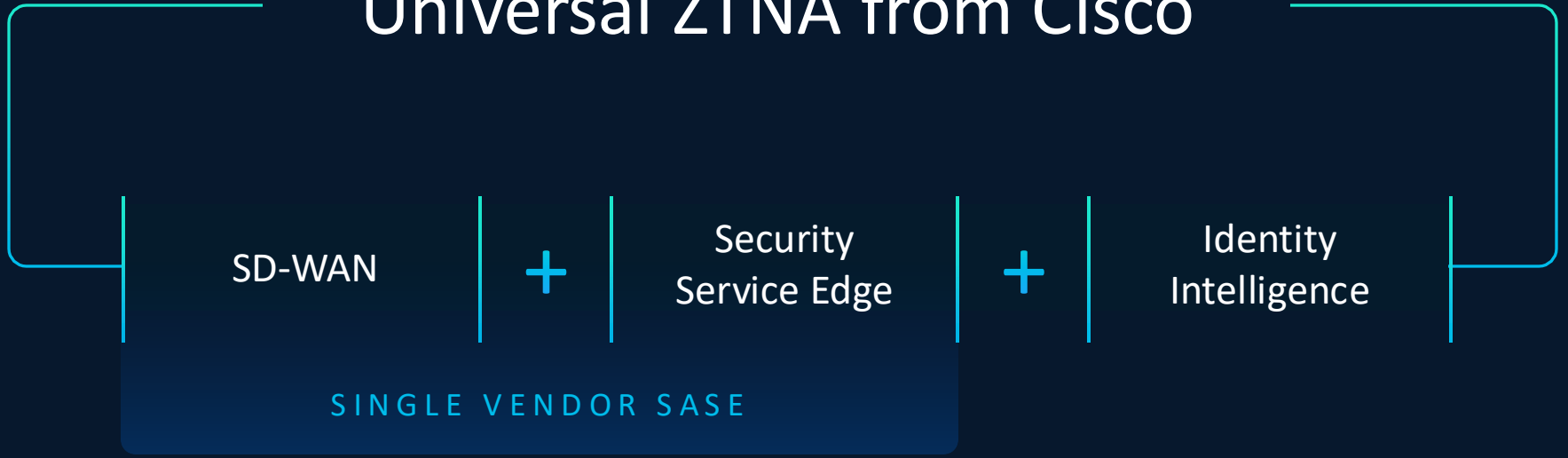
OS version | Mac ID | OPSWAT checks | DHCP | Traffic flows | DNS and certificate


IOT Device
10.40.100.51 tme-csw\lee winlaptop1 Location... Windows11-Workstati... Luxshare Precision ... Windows 11 Pro
10.40.100.61 68-3A-1E-53-7... slc-lab-m... Location... Cisco-Meraki-Device Cisco Meraki
10.40.100.62 68-3A-1E-53-7... slc-lab-m... Location... Cisco-Meraki-Device Cisco Meraki
lee@tme-csw.lab Datacenter Windows11-Workstati... Intel Corporate
10.40.100.61 tme-csw\lee winlaptop2 Location... Windows11-Workstati... CE LINK LIMITED Windows 11 Pro
jorgquin@tme-c... Datacenter OS_X_Catalina-Works... Apple, Inc. OS X
Windows Device


ISE_tag = Contractors_Users
Contractors
Common Services
core-services
AD-DNS
loadbalancer
vdesktop-infra
CIMC
IoT/OT
ISE_tag = Sales_Users
ISE_tag = Developers_Users
Campus
Sales
Developers
Contractors
AWS
csw-time-account
us-west-2
acme-saas-prod-vpc-aws
Production
dpu-demo-app
dpu-app1
dpu-app1
finance-app-lb
finance-app
openshift-demo
oc-sock-shop
ecomm-app-agent
finance-app-fw
ztna-acme-app
loadbalancer
Development
Fw-l3-dc-apps
Dev-jumphost
Finance-app-fw-l3
Fw-l2-dc-apps
legacy-webserver
Wiki-Dev
vmagent-estore-app
ecomm-app-fw
finance-app
db
backend
app
frontend


Action
Source
Destination
Protocols / Ports
Allow
contractors-users
vdesktop-infra
TCP: 443
Common Services
Agentless
Ingress to Common-Services
vdesktop-infra
Agentless
Ingress to Prod Zone
ISE_tag = Contractors_Users
ISE_tag = Contractors_Users
contractors
Action
Source
Destination
Protocols / Ports
Allow
contractors-vdi
Finance-app-lb
TCP: 443

Universal ZTNA from Cisco



Seamless Access

We handle the plumbing

Go to work

Modern Private Apps

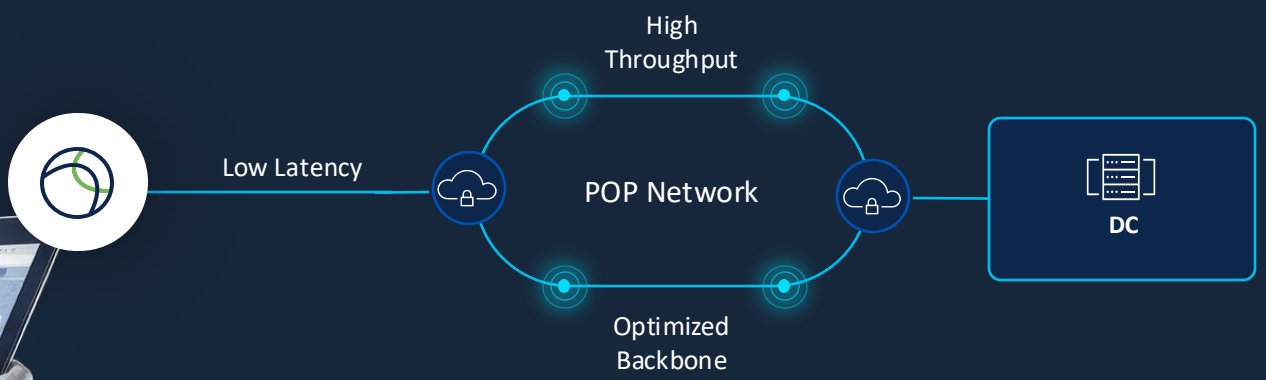
Legacy Private Apps

SaaS Apps

Internet

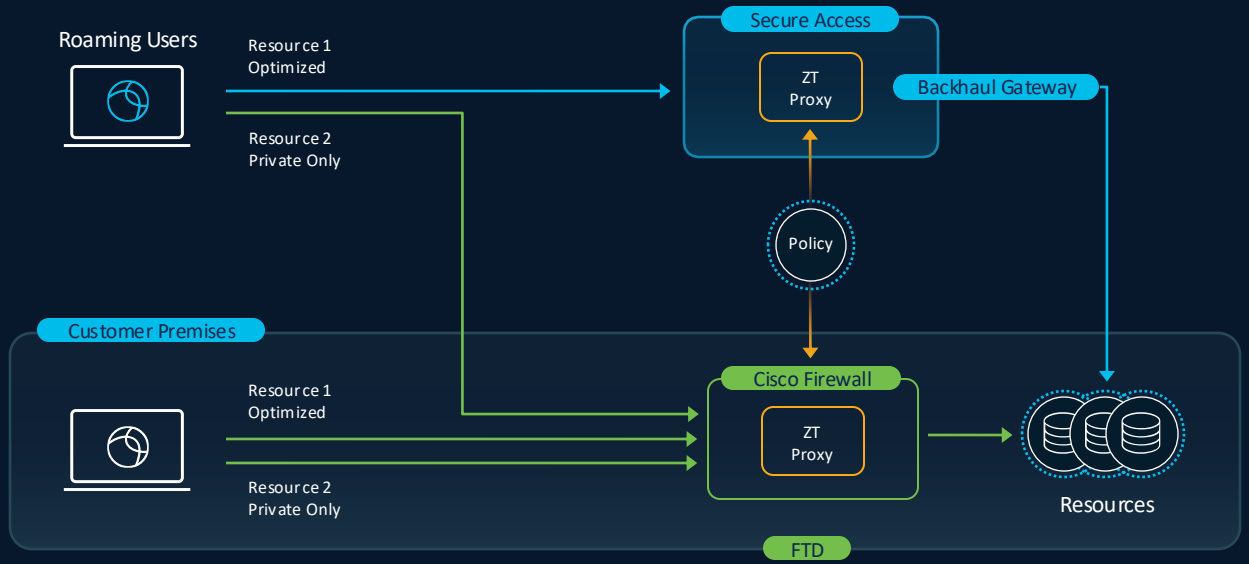
Cisco’s modern PoP architecture

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



Hybrid Private Access for flexible enforcement*

Single set of ZTNA policies used in cloud and on-premise

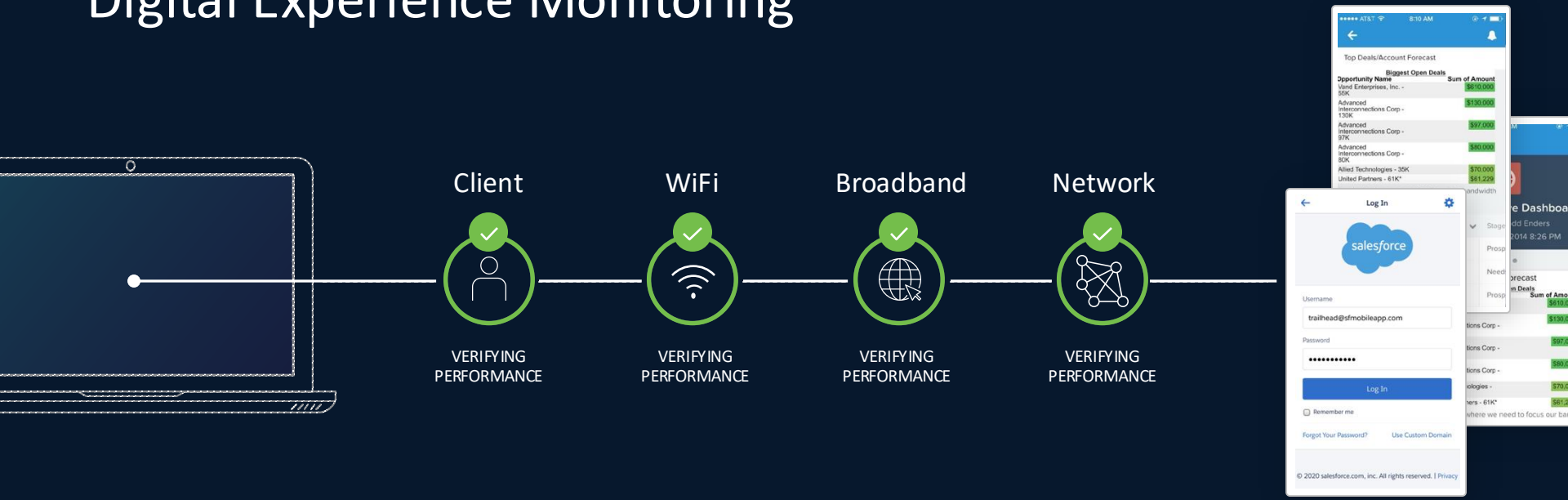


* Capabilities are planned but not yet available or guaranteed.

Enforce zero trust using identity context

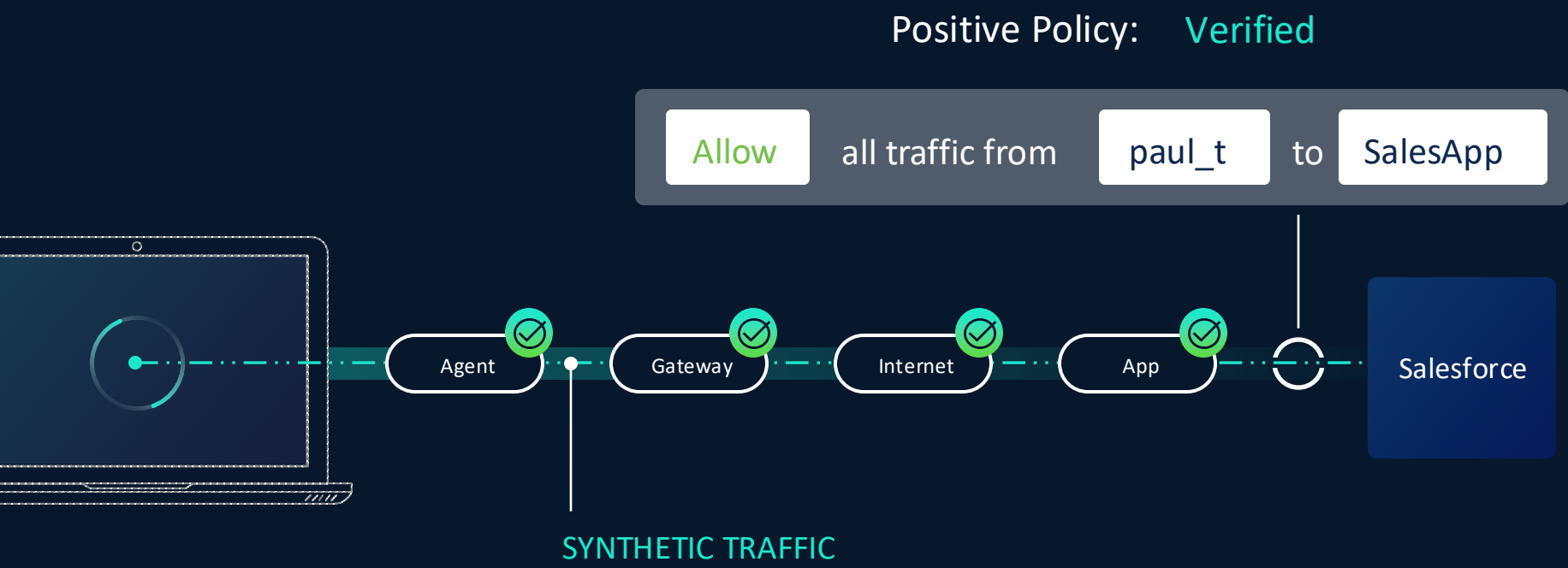
Leverage security group tags for granular access policy

End-to-end visibility with Digital Experience Monitoring



Historical performance and recommendations

Policy Assurance*

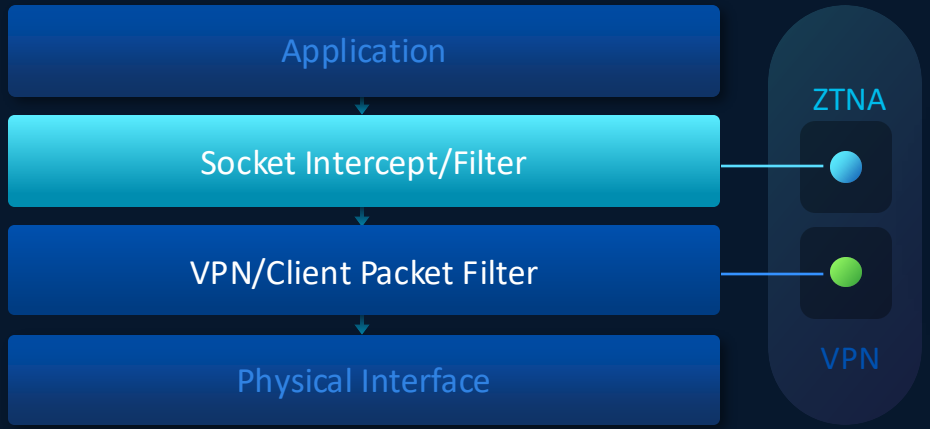


* Capabilities are planned but not yet available or guaranteed.

Depictions are examples only.

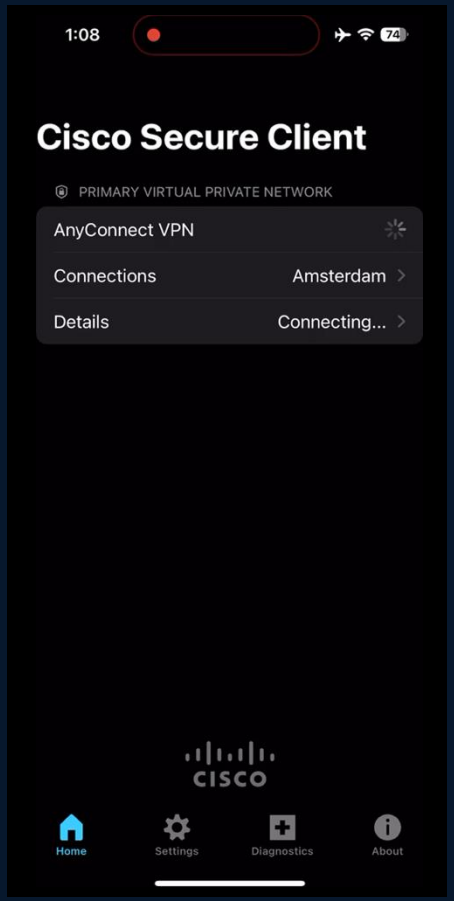
ZTNA and VPN coexistence and fallback

DNS interception and socket intercept



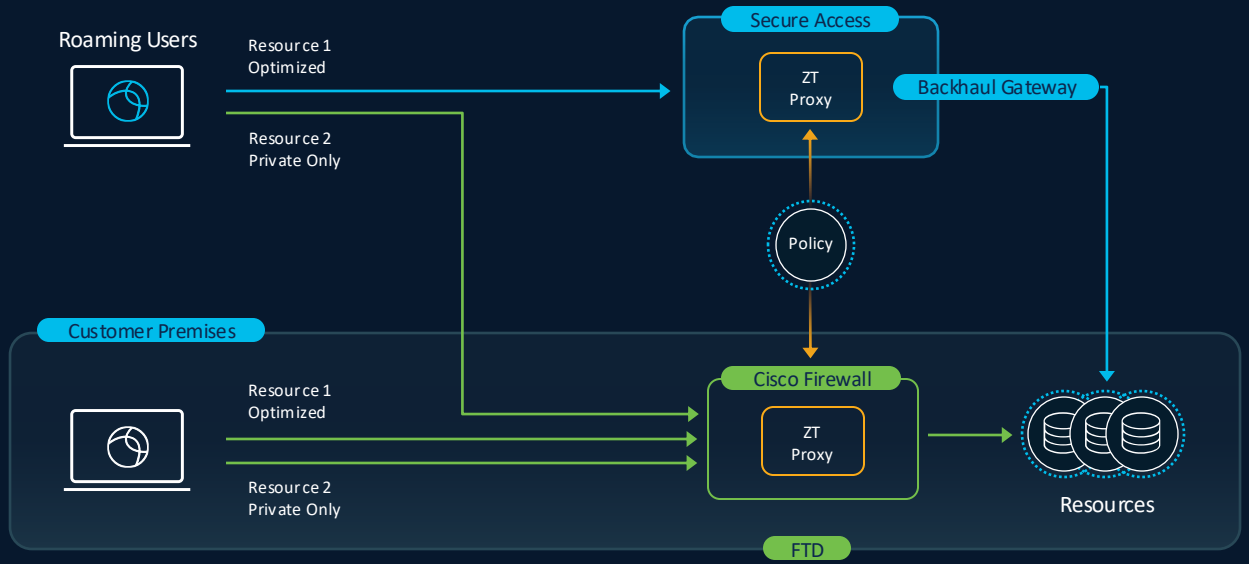
Secure Client
Intelligent Control

Only possible with unified VPN + ZTNA client


1:08
74
Cisco Secure Client
PRIMARY VIRTUAL PRIVATE NETWORK
AnyConnect VPN
Connections
Amsterdam
Details
Connecting...
cisco
Home
Settings
Diagnostics
About

Hybrid Private Access for flexible enforcement*

Single set of ZTNA policies used in cloud and on-premise

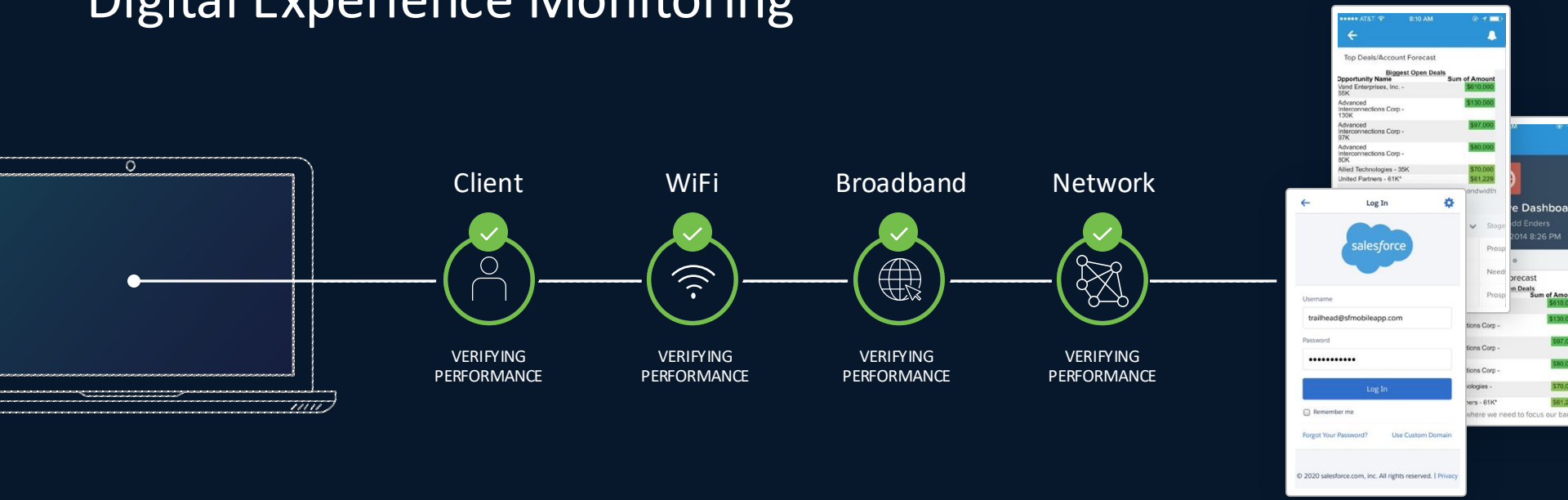


* Capabilities are planned but not yet available or guaranteed.

Enforce zero trust using identity context

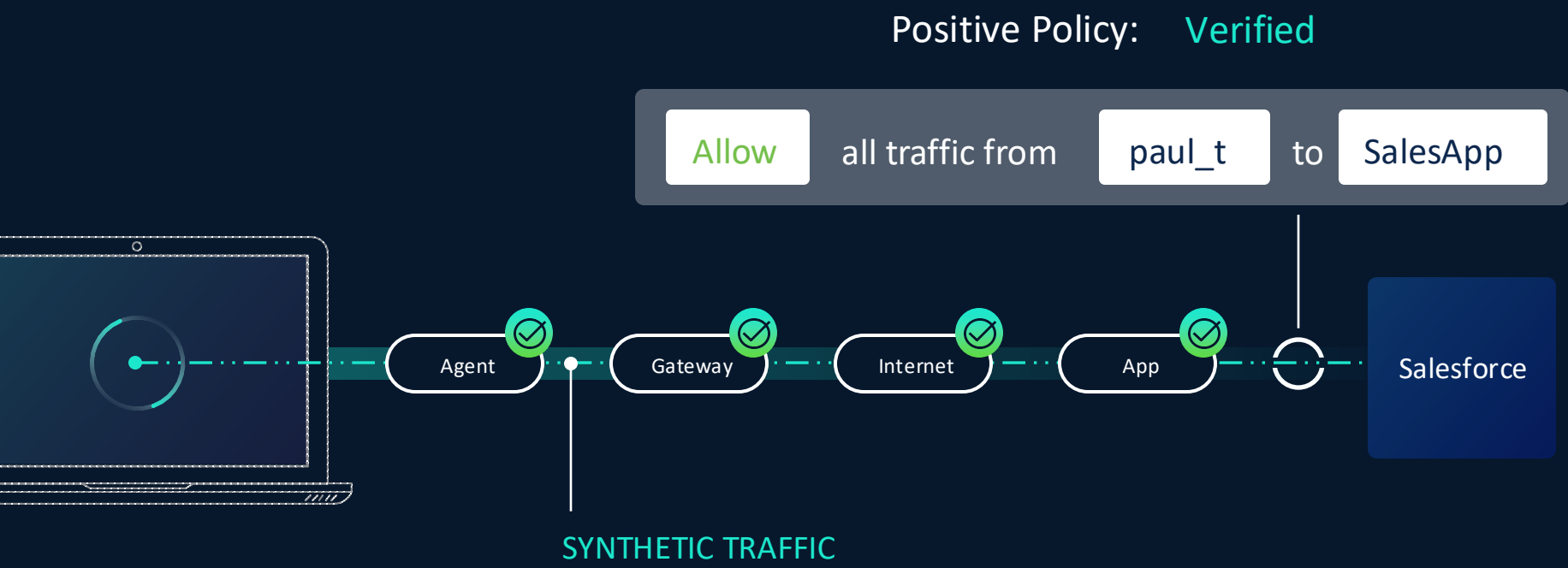
Leverage security group tags for granular access policy

End-to-end visibility with Digital Experience Monitoring



Historical performance and recommendations

Policy Assurance*



* Capabilities are planned but not yet available or guaranteed.

Depictions are examples only.

Summary


Universal Zero Trust Network Access
Cloud Management (Security Cloud Control)
Extend
Identity Context
Unify
Application Access
Build
Operational Resilience
Identity
Intelligence/MFA
ISE & SD-WAN
integration
Secure Internet
Access
Secure Private
Access
Digital Experience
Monitoring
Policy
Assurance
SD-WAN
Firewall/Network Infrastructure
Splunk
Cisco XDR
Telemetry