Cisco **Security**

Defenders Struggle with Prescriptive Base Controls in a Hybrid World

Jason Maynard
Field CTO Cybersecurity Canada
CCIE, CC[N|I|D]P, SFCE, C|EH, RCSS, GICSP, GRID, GPEN, GDAT, GCPN, AWS Cloud Practitioner, AWS Solutions Architect, AWS Security, Azure Fundamentals, Azure Security Engineer
MITRE ATT&CK: CTI, SOC Assessments, Threat Hunting Detection Engineering, Adversary Emulation Methodology, Purple Teaming Methodology
ATTACKIQ: Purple Team, Mitre Att&ck, Breach Attack Simulation
Splunk Power User, Splunk Administrator

Adversarial Success

Salt Typhoon

Salt Typhoon, a Chinese state-sponsored advanced persistent threat (APT) group, has been implicated in a series of sophisticated cyberattacks targeting global telecommunications providers.

These attacks are characterized by their stealth, persistence, and strategic focus on espionage and data exfiltration.

Elevating defensive capabilities through understanding

Salt Typhoon: The Capabilities

MITRE | ATT&CK®

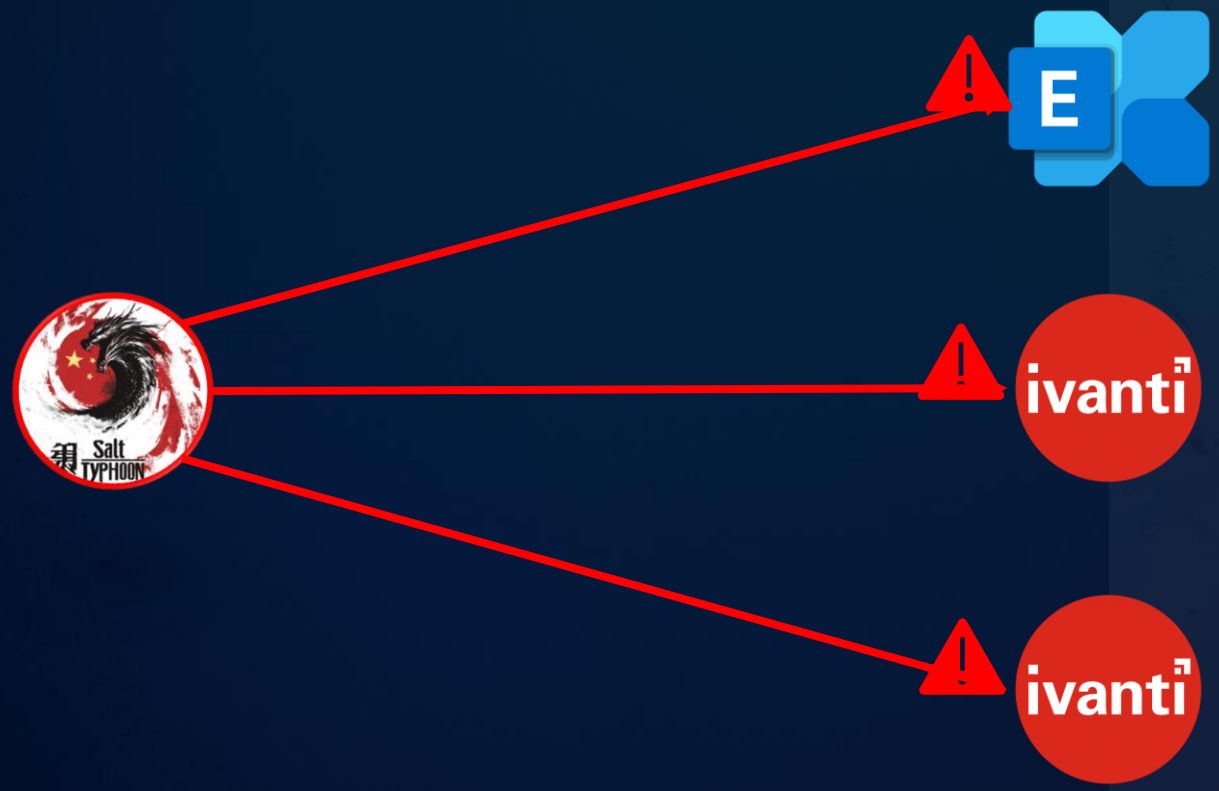
Tactics	Techniques
Reconnaissance	
Resource Development	
Initial Access	Exploit Public Facing Application (T1190)
Execution	Command and Scripting Interpreter (T1059)
Persistence	Create or Modify System Process (T1543.003)
Privilege Escalation	Exploitation for Privilege Escalation (T1068)
Defense Evasion	
Credential Access	Credential Dumping (T1003)
Discovery	Network Service Discovery (T1046)
Lateral Movement	Remote Services (T1021), RDP Hijacking (T1021.002), SMB/Windows Admin Shares (T1021.002), Pass the Hash (T1550.002), Lateral Tool Transfer (T1570), Exploitation of Remote Services (T1210)
Collection	
Command and Control	
Exfiltration	
Impact	Data Manipulation (T1565)

Elevating defensive capabilities through understanding

Attack Path and Common Themes

Initial Access: Exploit Public Facing Application (T1190)

MITRE | ATT&CK



CVE-2021-26855 (ProxyLogon): Exploited to compromise Microsoft Exchange servers.

CVE-2023-46805: Used to bypass authentication in Ivanti Connect Secure VPN.

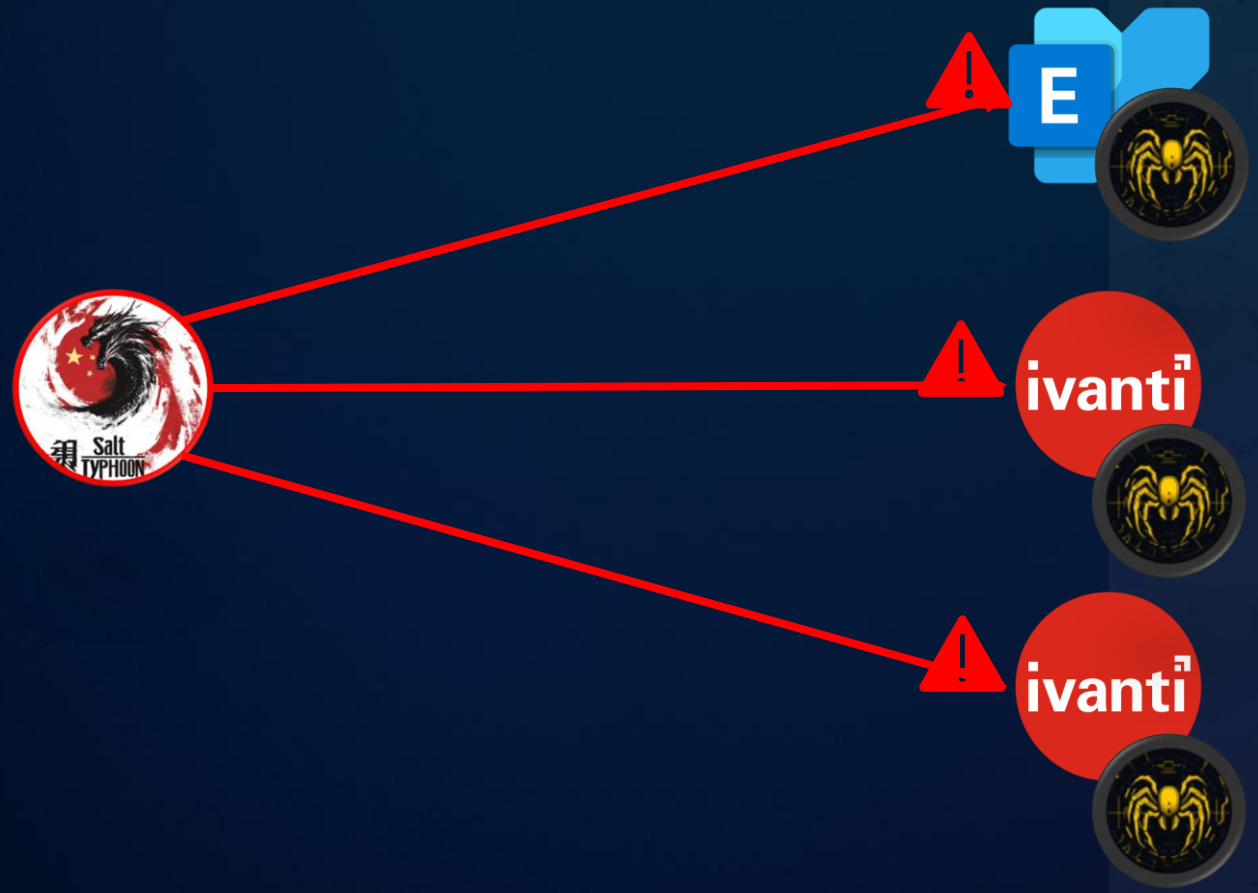
CVE-2024-21887: Command injection vulnerability in Ivanti Policy Secure.

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

These exploits allow the group to deploy malware and establish a foothold in the target network.

Attack Path and Common Themes

Execution: Technique: Command and Scripting Interpreter (T1059)



PowerShell: Used to download additional payloads, such as the GhostSpider backdoor.

Windows Command Shell: Executes commands to enumerate system information and deploy tools for lateral movement.

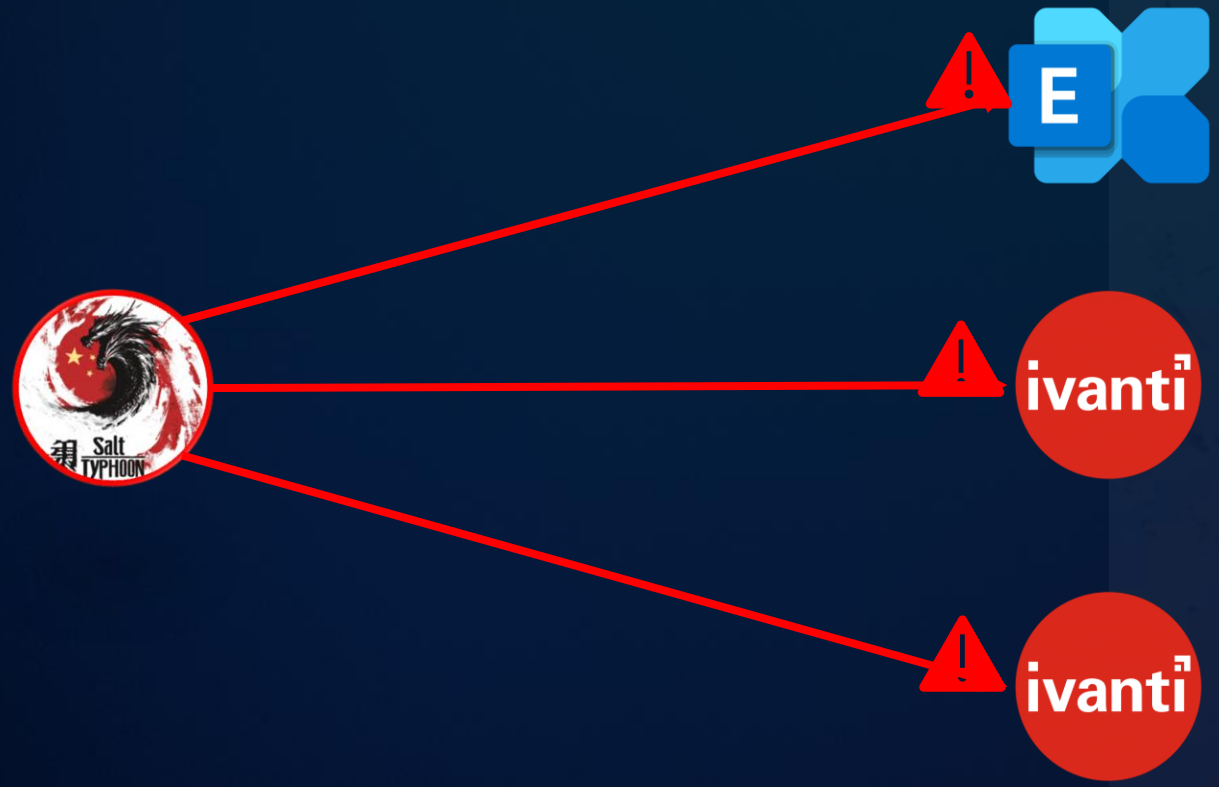
Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

Once inside, Salt Typhoon uses PowerShell and other scripting tools to execute malicious commands.

Attack Path and Common Themes

Persistence: Create or Modify System Process (T1543.003)

MITRE | ATT&CK



Crowdoor Backdoor: Adds registry entries to execute malicious code automatically.

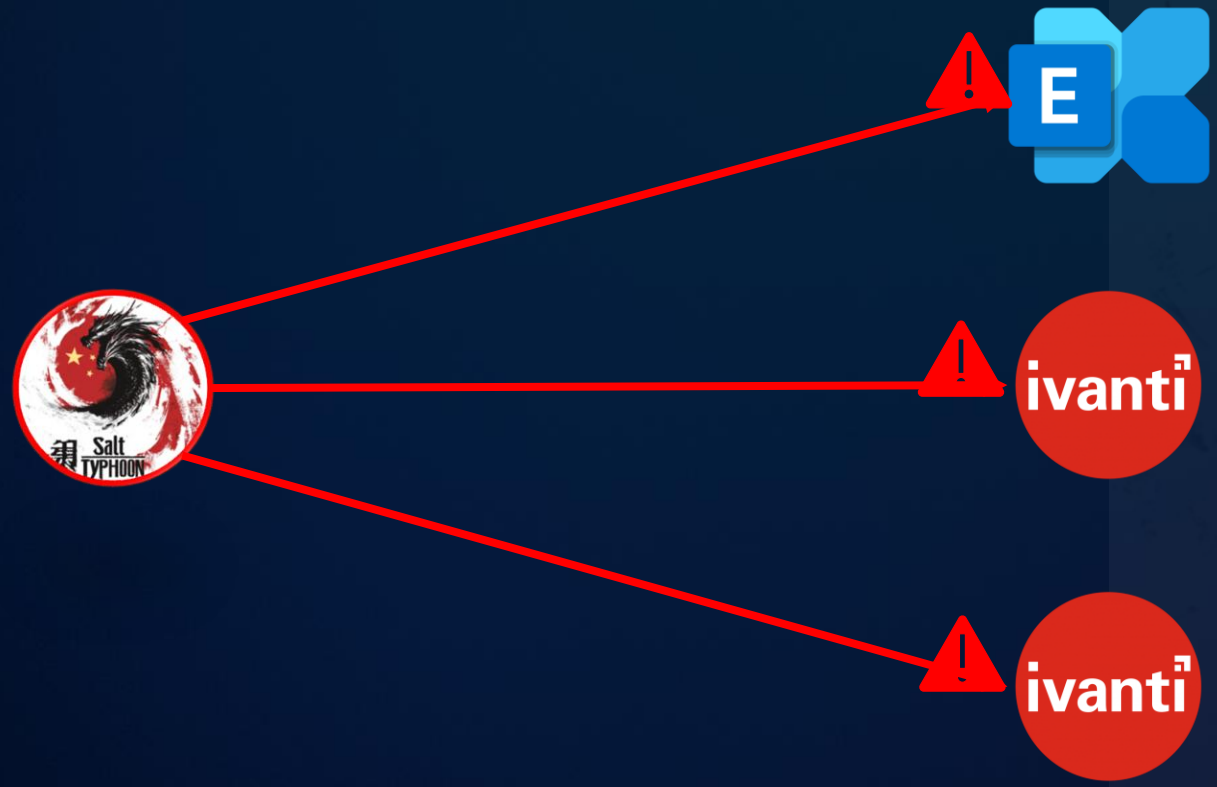
SparrowDoor: A custom backdoor that establishes persistence via DLL search-order hijacking..

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

The group creates Windows services or modifies registry keys to ensure malware persists across reboots.

Attack Path and Common Themes

Privilege Escalation: Exploitation for Privilege Escalation (T1068)



LSASS Memory Dumping: Uses tools like Mimikatz to extract credentials from memory.

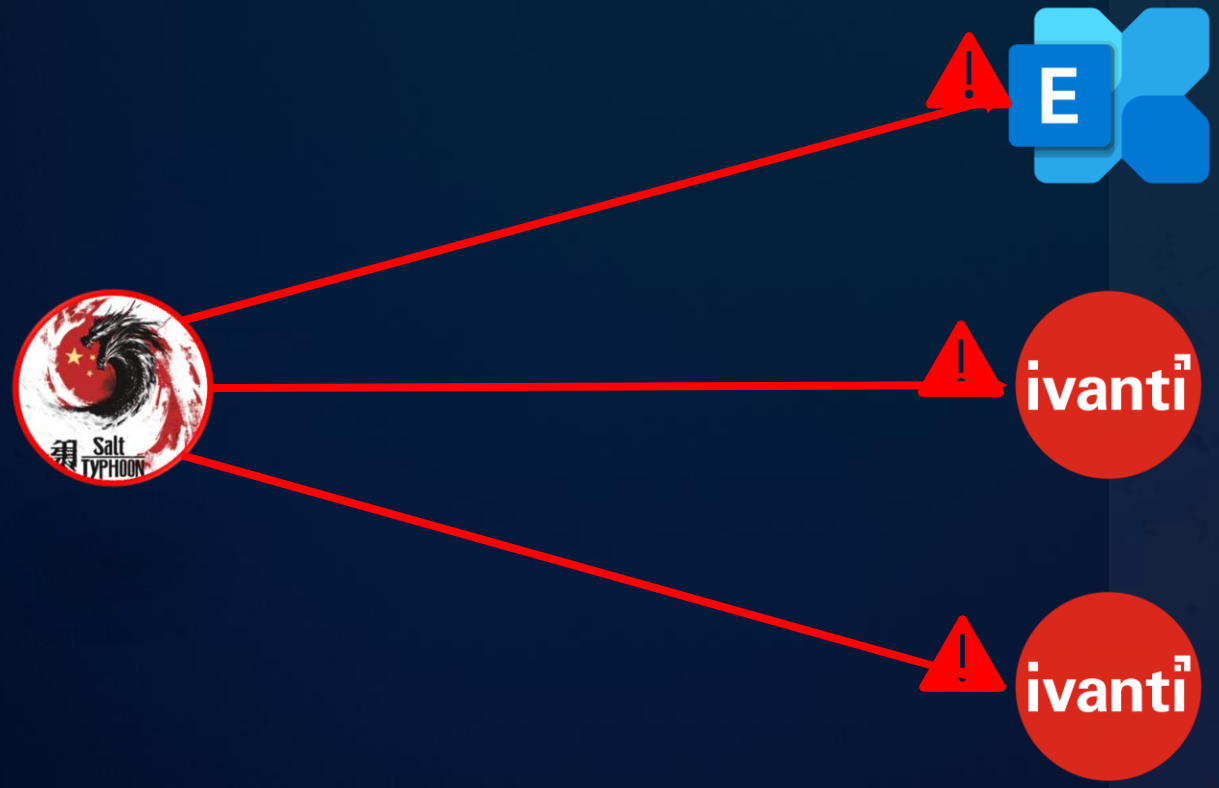
Token Manipulation: Elevates privileges by impersonating system tokens.

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

Salt Typhoon exploits vulnerabilities or misconfigurations to gain higher privileges

Attack Path and Common Themes

Lateral Movement: Technique: Remote Services (T1021), Pass the Hash (T1550.002), Lateral Tool Transfer (T1570), Technique: Exploitation of Remote Services (T1210)



The group uses legitimate remote access tools like RDP, SSH, and SMB to move laterally.

- RDP Hijacking (T1021.002): Takes control of existing RDP sessions to access other systems.
- SMB/Windows Admin Shares (T1021.002): Accesses shared folders to deploy tools or exfiltrate data.

Technique: Pass the Hash (T1550.002)

- Salt Typhoon uses stolen password hashes to authenticate to other systems without needing plaintext passwords.

Technique: Lateral Tool Transfer (T1570)

- The group transfers tools like PsExec, WinRAR, and custom malware (e.g., GhostSpider) between systems to facilitate movement and data exfiltration.

Technique: Exploitation of Remote Services (T1210)

- Exploits vulnerabilities in remote services (e.g., unpatched SMB or RDP) to gain access to additional systems.

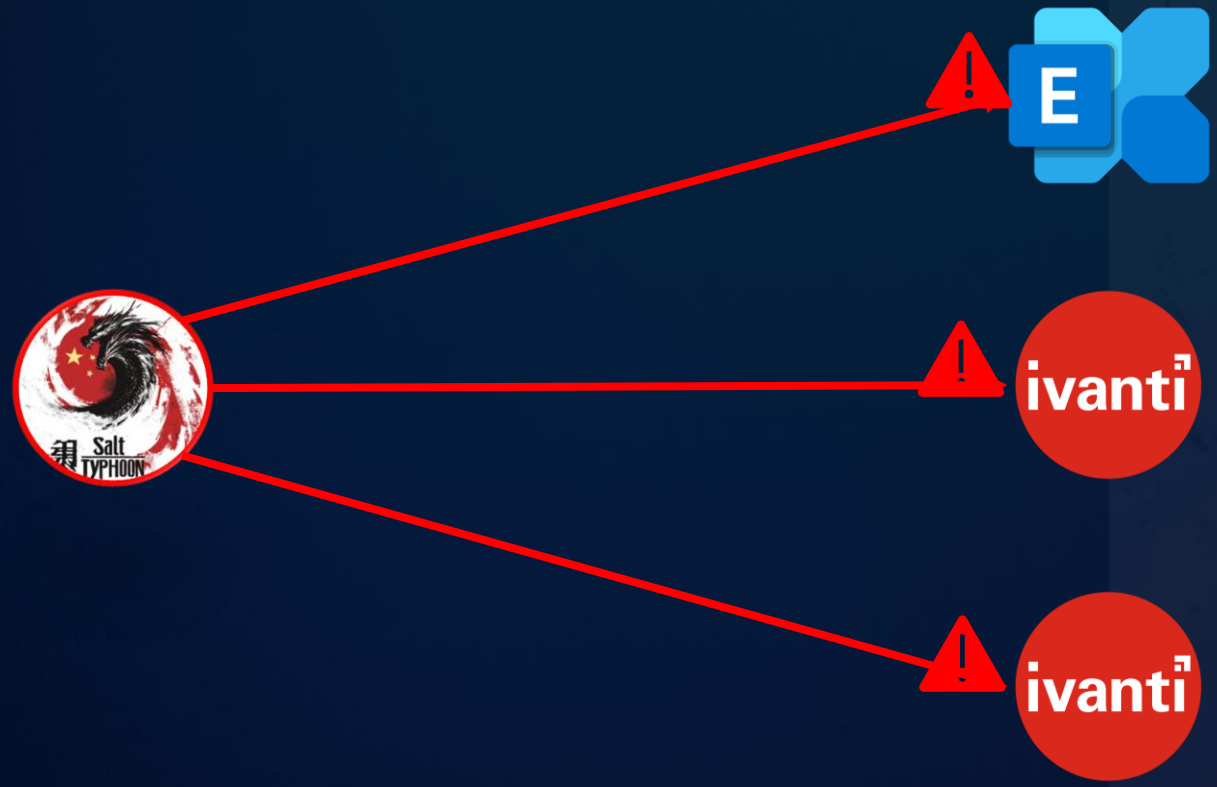
Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

Lateral movement is a critical phase of Salt Typhoon's operations, enabling the group to expand control within the network.

Attack Path and Common Themes

Credential Access: Credential Dumping (T1003)

MITRE | ATT&CK



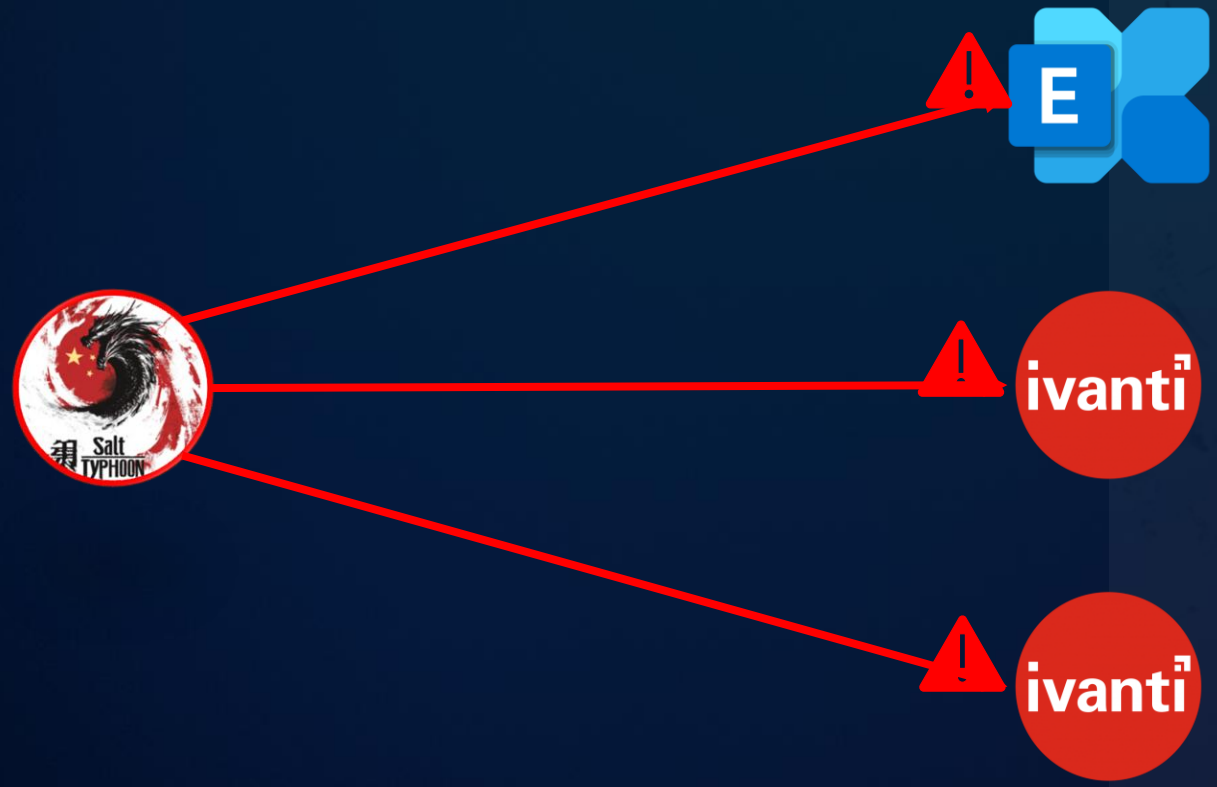
LSASS Dumping: Captures credentials stored in the Local Security Authority Subsystem Service (LSASS).

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

Salt Typhoon uses tools like Mimikatz and ProcDump to extract credentials from memory or disk.

Attack Path and Common Themes

Discovery: Technique: Network Service Discovery (T1046)



Tools like NBTscan and PowerShell scripts are used to gather information about the network environment

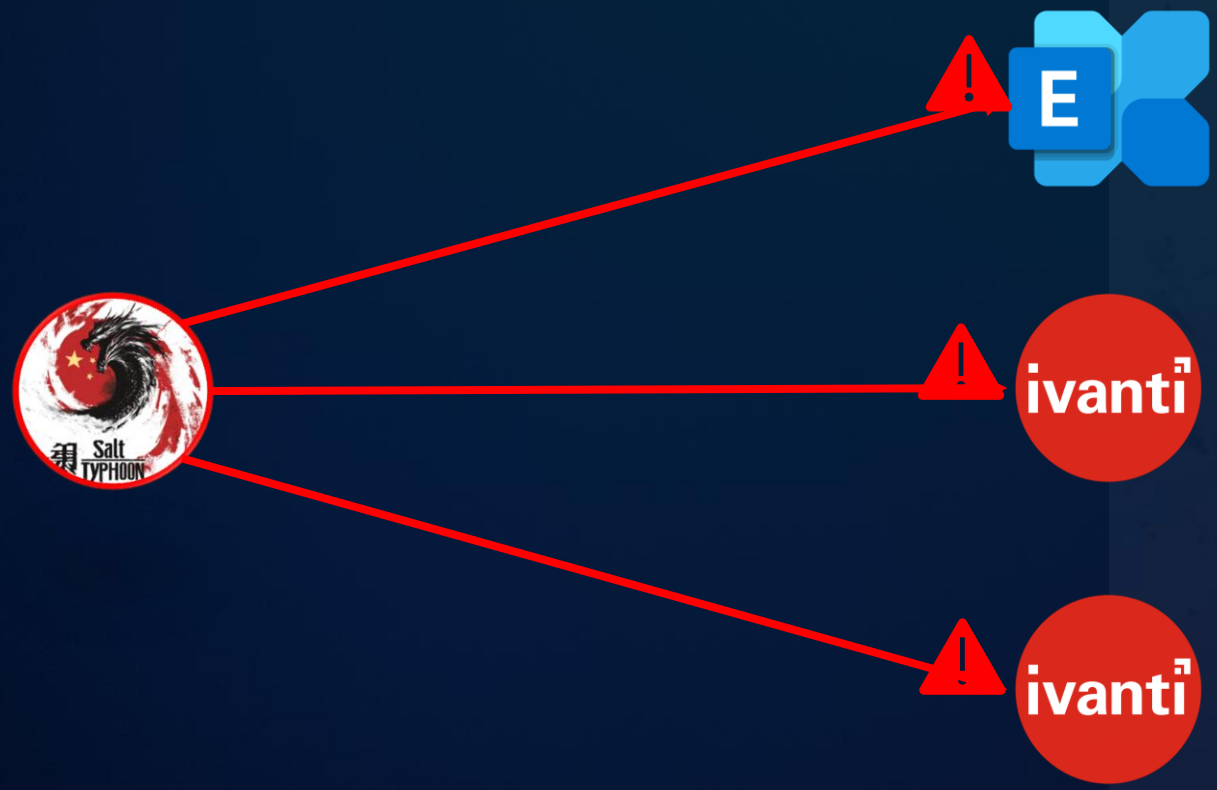
Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

The group maps the network to identify additional targets, such as domain controllers and file servers.

Attack Path and Common Themes

Exfiltration: Exfiltration Over C2 Channel (T1041)

MITRE | ATT&CK



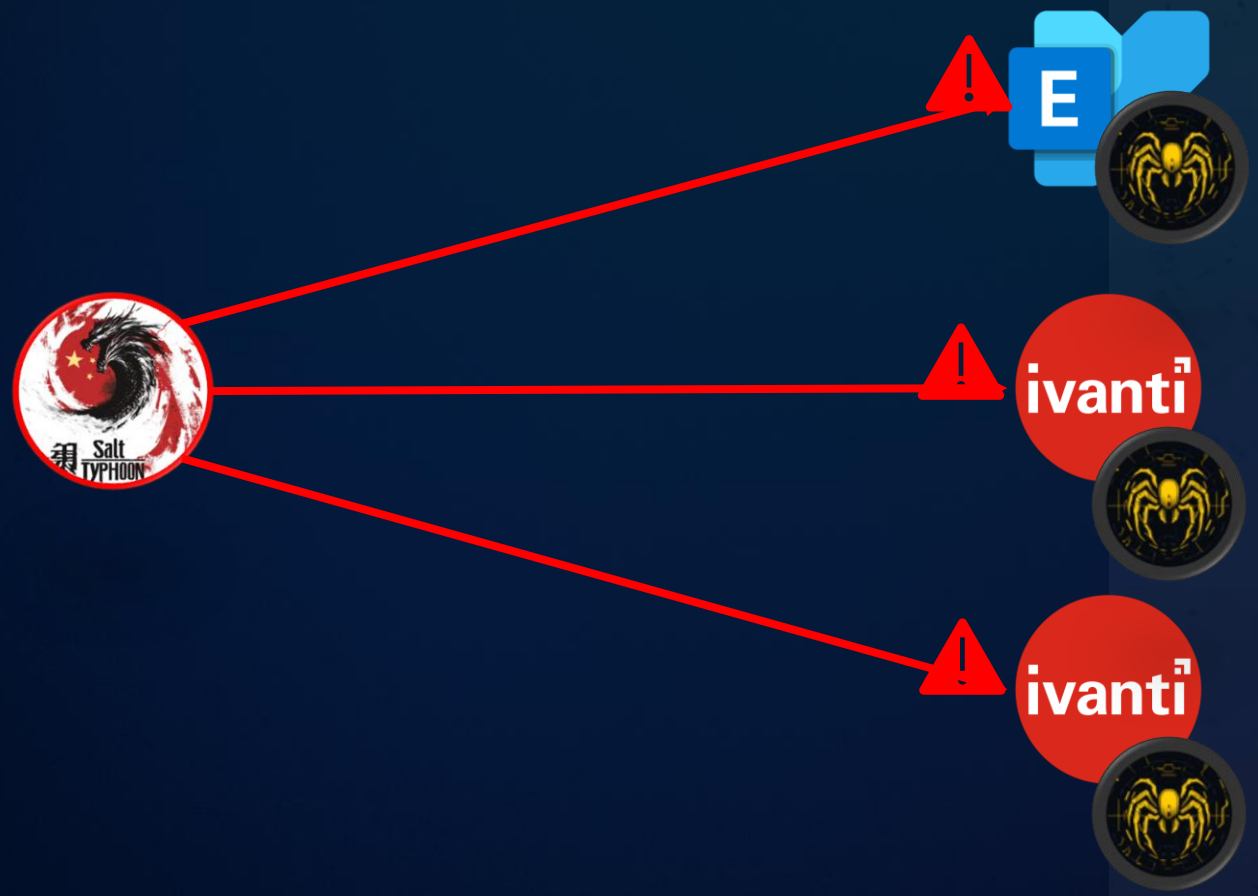
Tools like WinRAR are used to compress and encrypt data before exfiltration.

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

Salt Typhoon exfiltrates stolen data (e.g., call records, text messages) over encrypted command-and-control (C2) channels.

Attack Path and Common Themes

Impact: Data Manipulation (T1565)



GhostSpider Backdoor: Provides persistent access for long-term espionage and potential future disruption.

Note: this is not an exhaustive list, and the adversary always looks at ways to elevate their capabilities.

The group may manipulate or delete data to disrupt operations or cover their tracks.

60% – 70% of all breaches involved lateral movement

Vulnerabilities play a significant role in breaches

Segmentation opportunity for defenders but difficult to operationalize

Cisco **Security**

Hybrid Mesh Firewall

Cisco Innovation

Securing the enterprise is increasingly challenging

Highly distributed, fine-grained apps

- Spanning data center, cloud
- Containers
- 1000s of microservices

Nothing can be trusted

- Distributed perimeter necessary but no longer sufficient
- Need security in every flow to stop lateral movement

More vulnerabilities, exploited faster

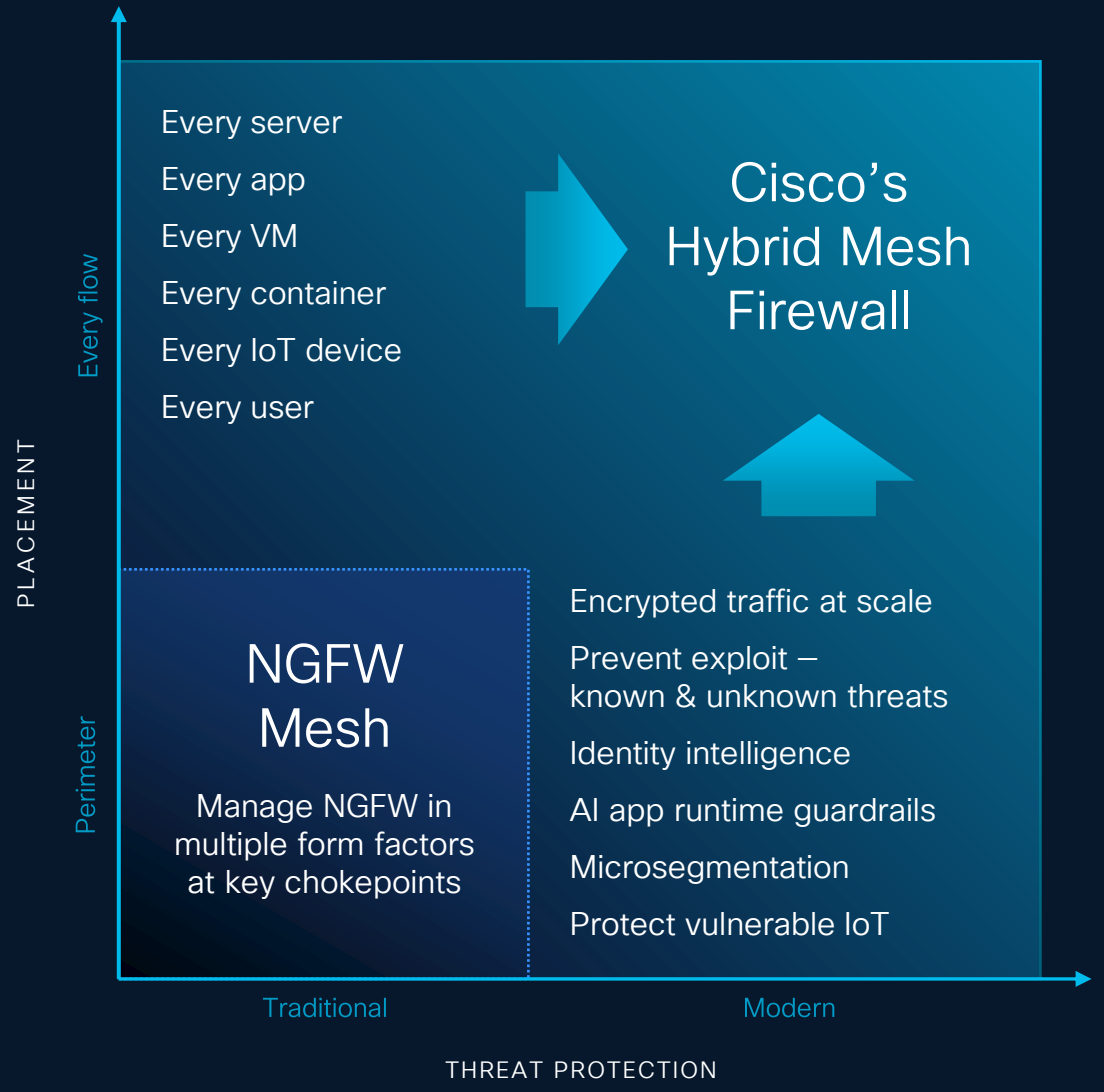
- Weeks to hours to minutes
- Patching can't keep up
- New AI model risks

AI increasing attack surface and attack sophistication

Firewalling needs to evolve to meet today's challenges

OUR NORTH STAR

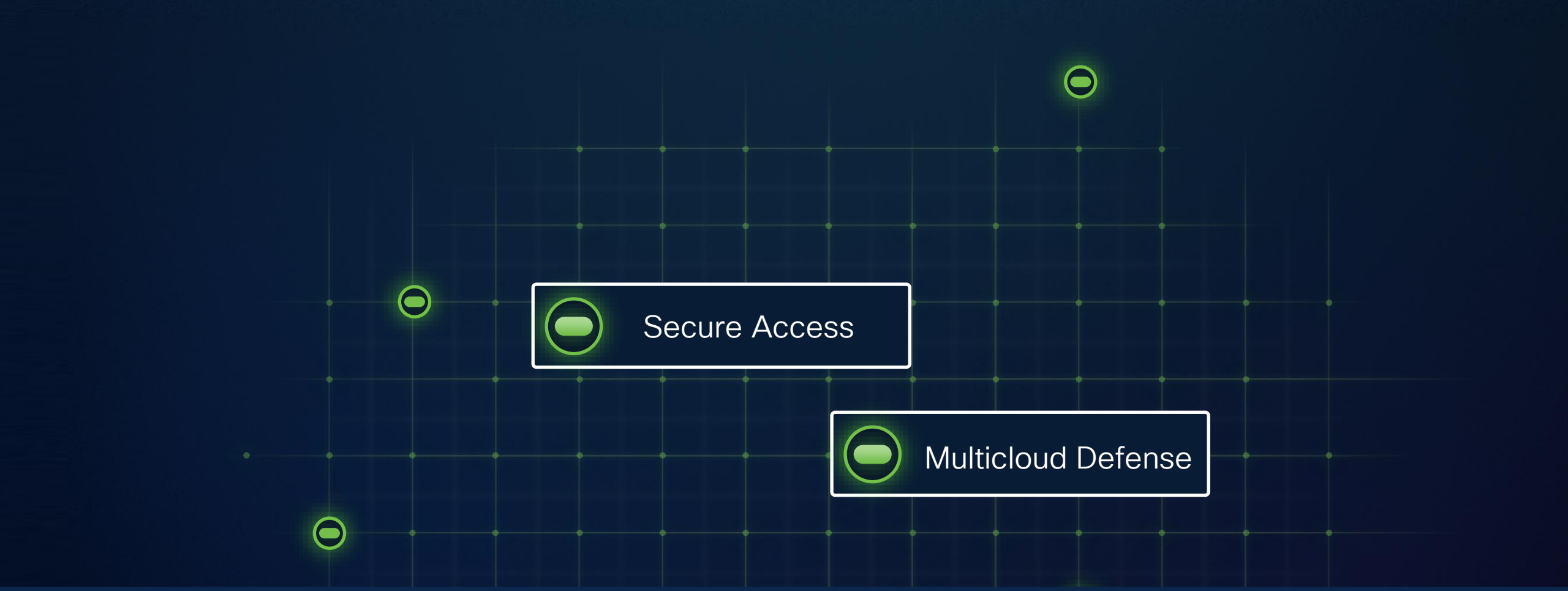
Make it easy for organizations to reduce attack surface, prevent compromise, and stop lateral movement in the modern data center, cloud, campus, and factory



Hybrid Mesh Firewall

Next-Generation Firewall

Price-performance leader | Encrypted traffic at scale | Cloud-native

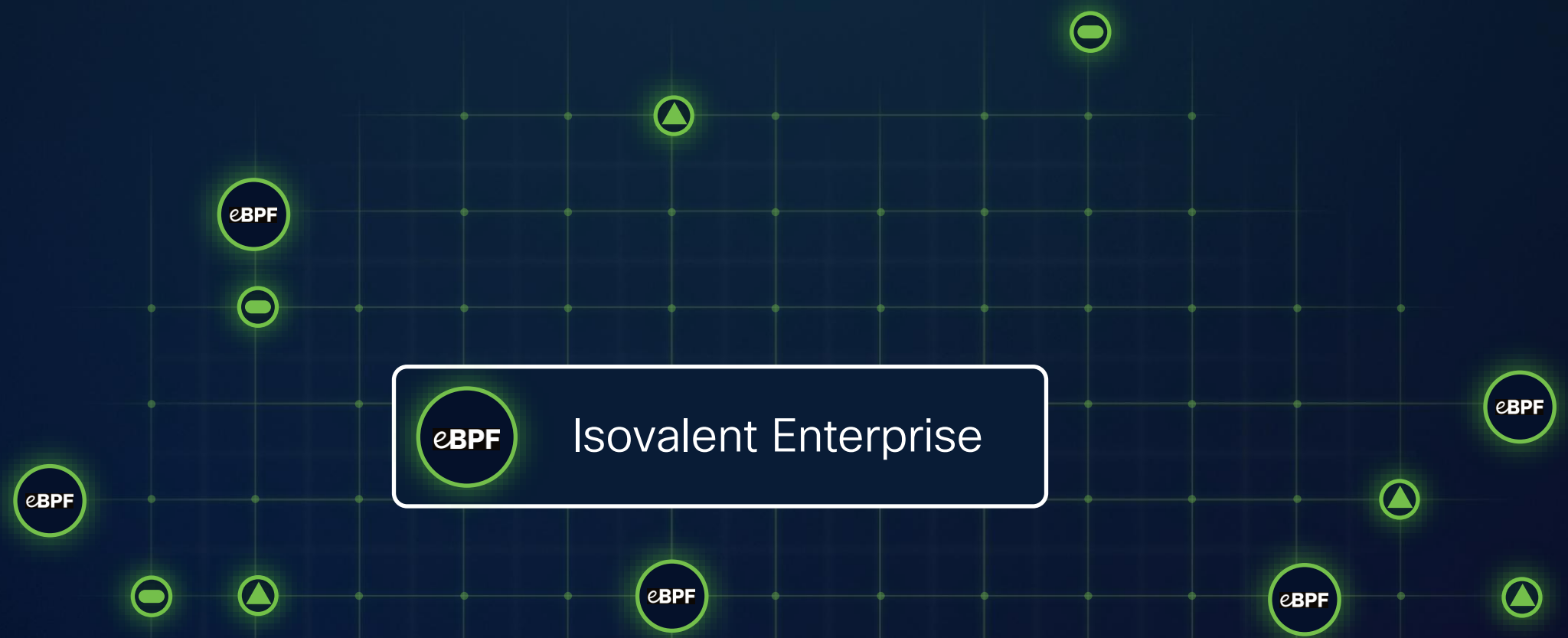


Security Service Edge with FWaaS

Cloud Firewall

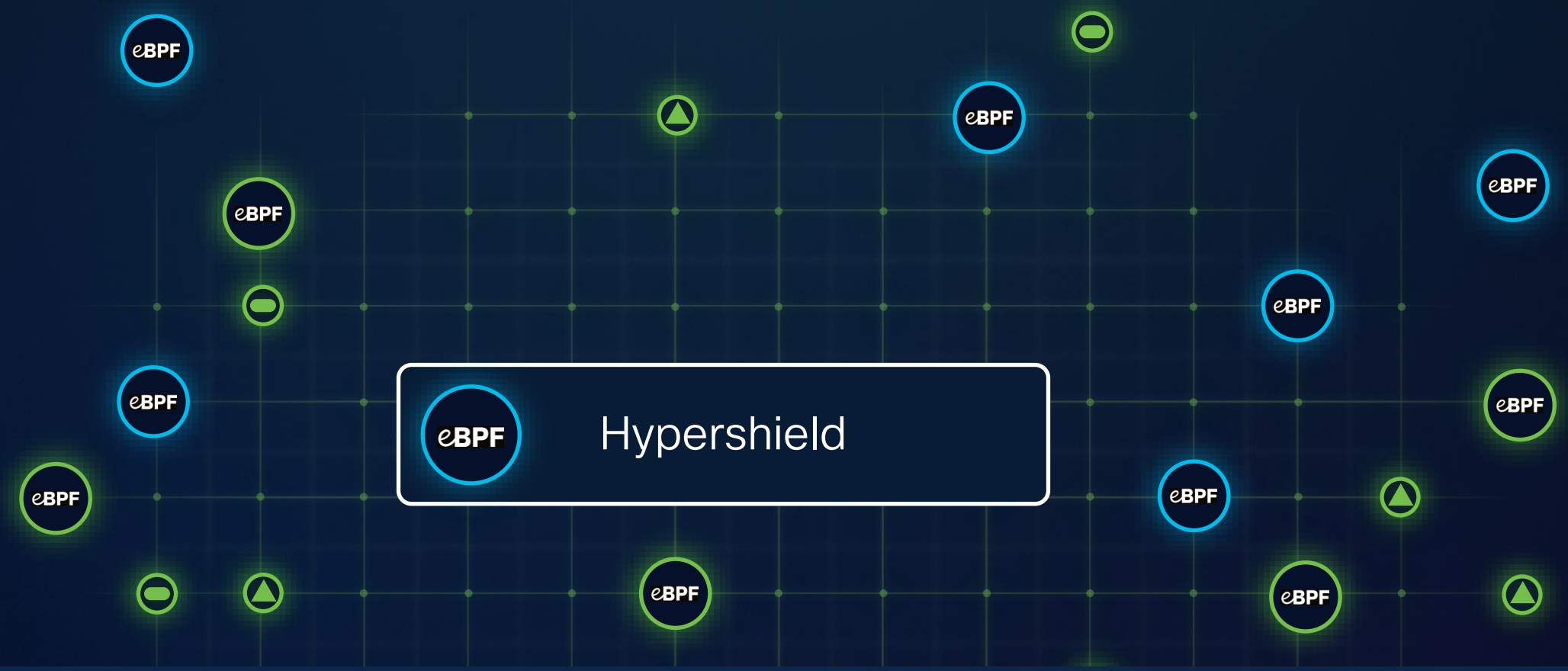
Leader in traditional microsegmentation

Highly scalable | Broad platform support | SaaS option

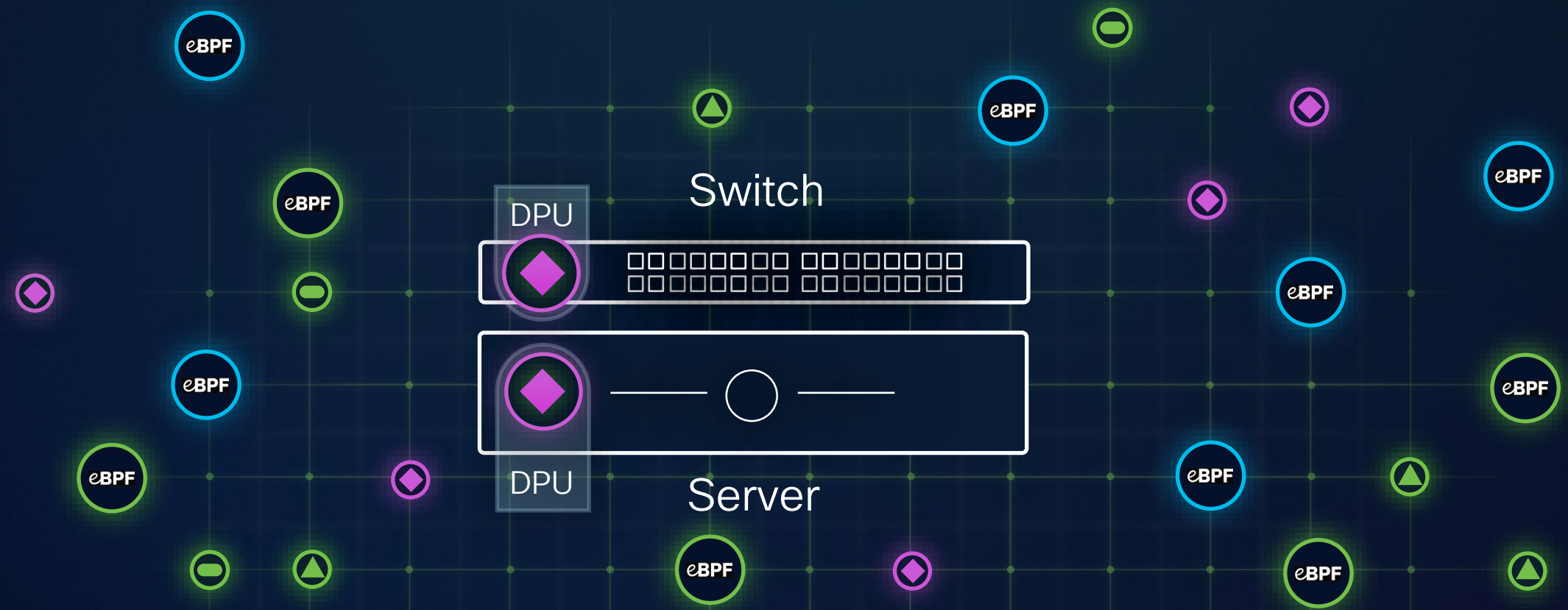


The network fabric for modern apps

Network| Security | Observability



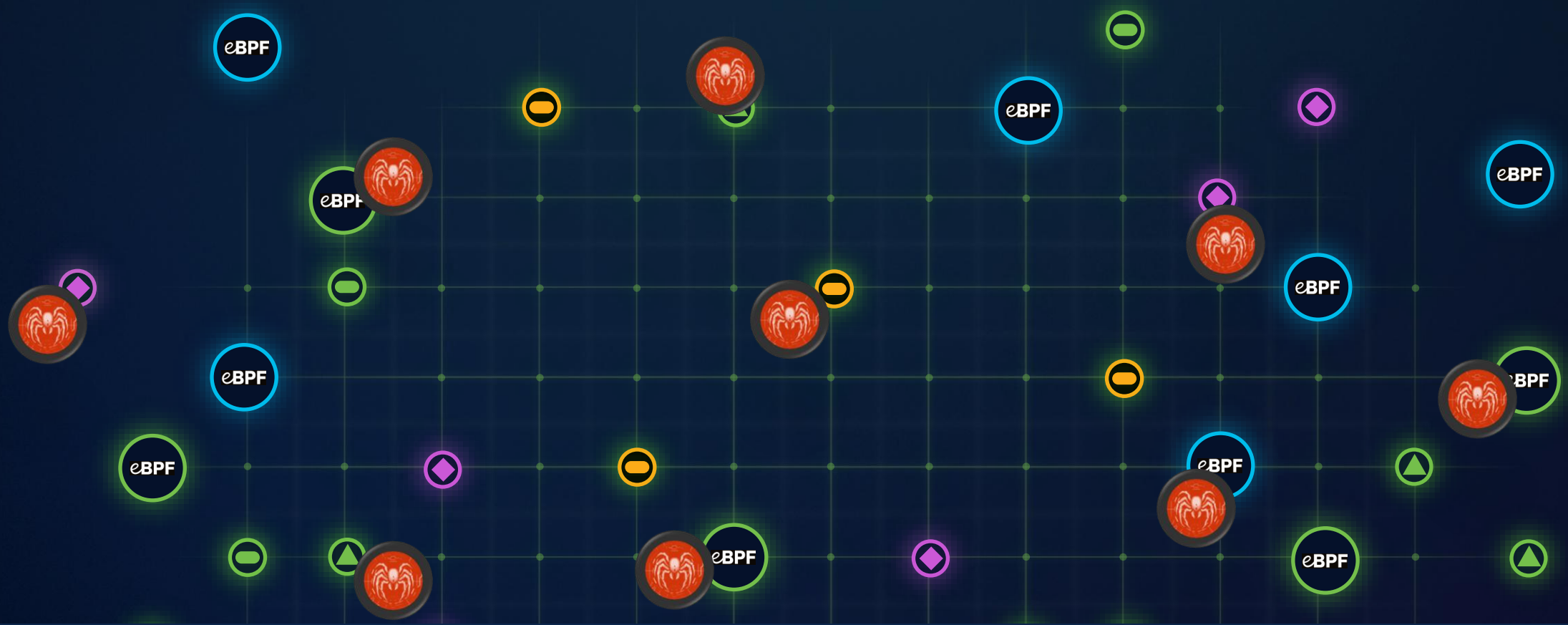
Autonomous segmentation
Distributed exploit protection



Security fused into the network

Hypershield service on Cisco Smart Switches

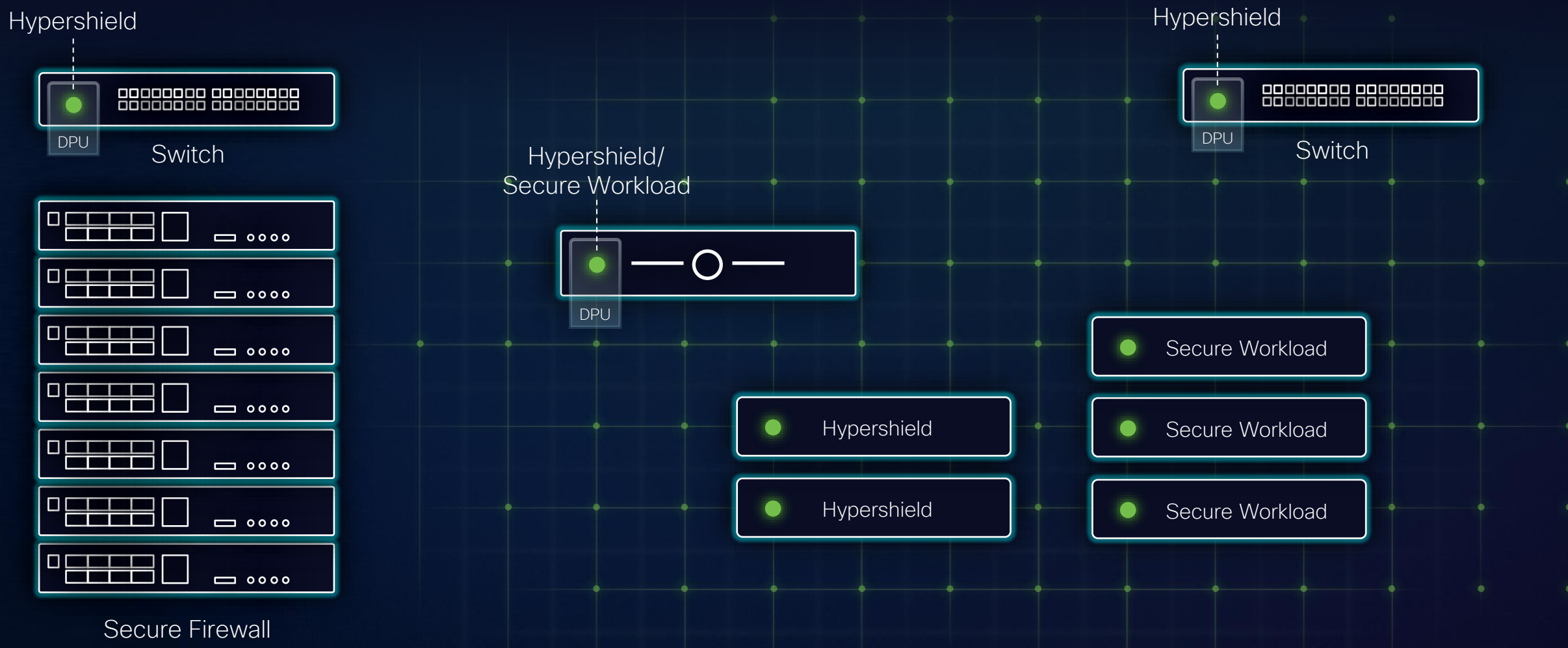
Third-party policy enforcement



Threats can be anywhere where best to build controls

No rip and replace

Security Cloud Control

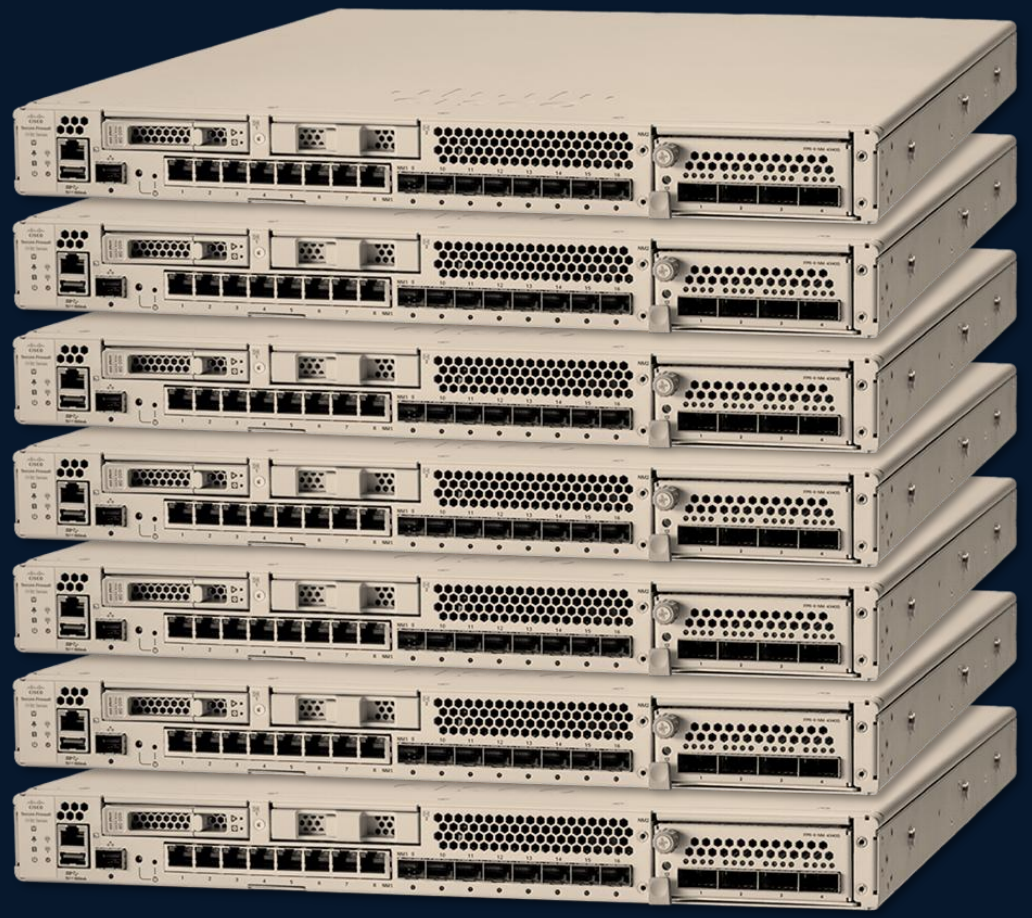


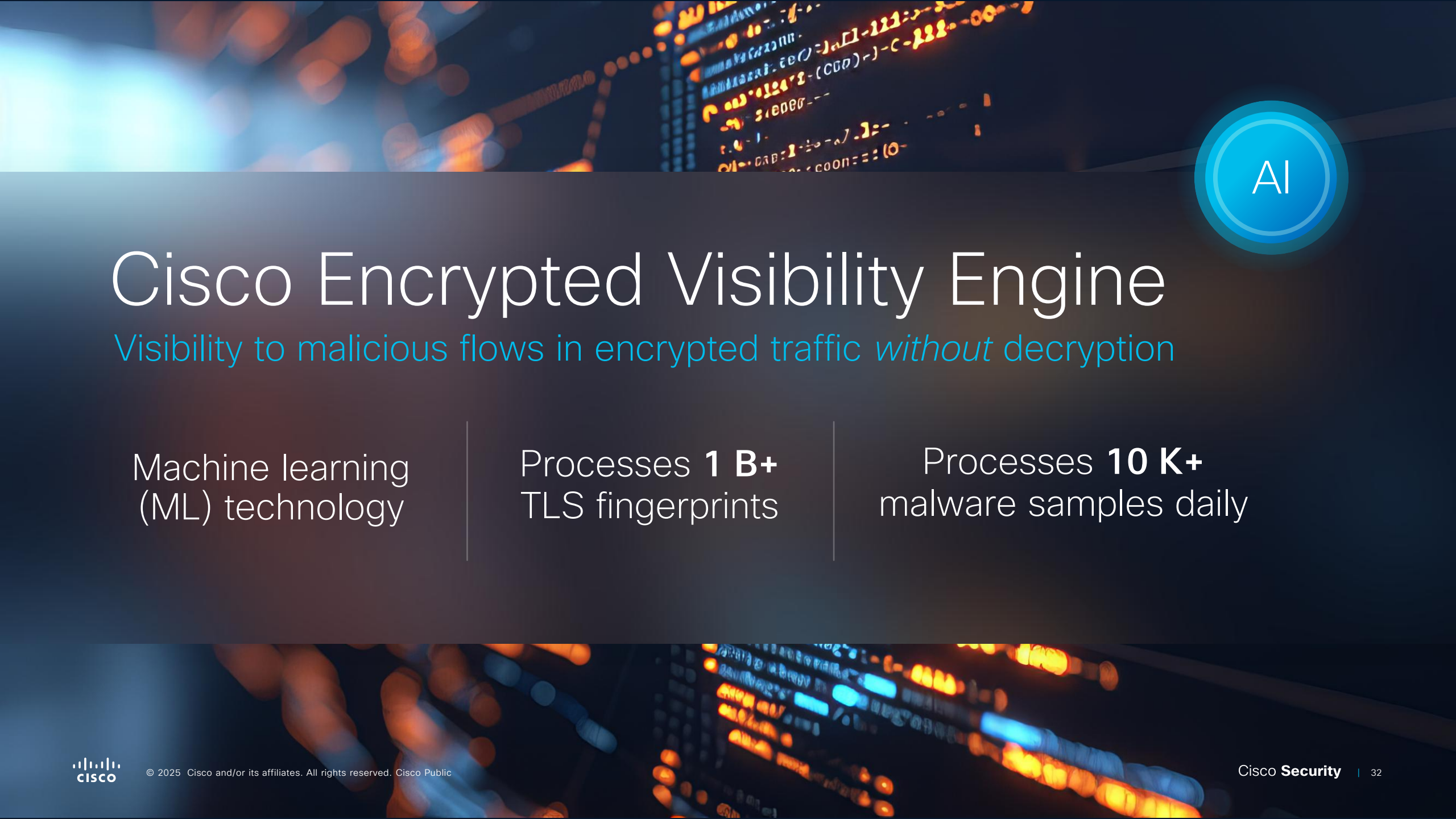
Enforcement points change, rules don’t

Advanced threat protection
Preventing modern attacks

Over 95% of data center traffic is encrypted

Traditional approaches to decryption do not scale





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)

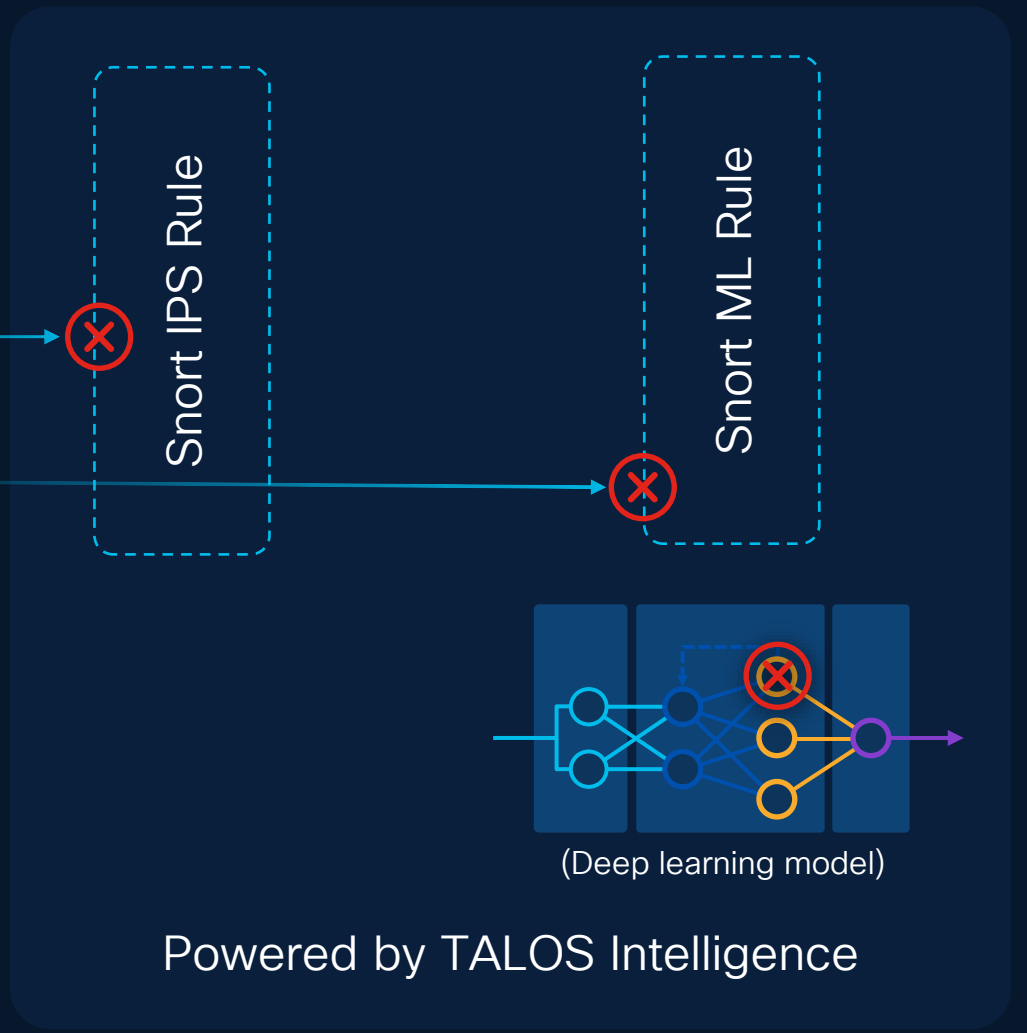
FUTURE

The leading IDPS, now with zero-day protection

SnortML extends IDPS protection to unknown variants of common attacks

Known SQL injection attack

Zero-day SQL Injection variant



NEW

Cloud-native Firewall
with Firewall Threat Defense

Automated Deployment

Auto-scaling

Self-healing

Enables firewalling at scale across multi-cloud environments

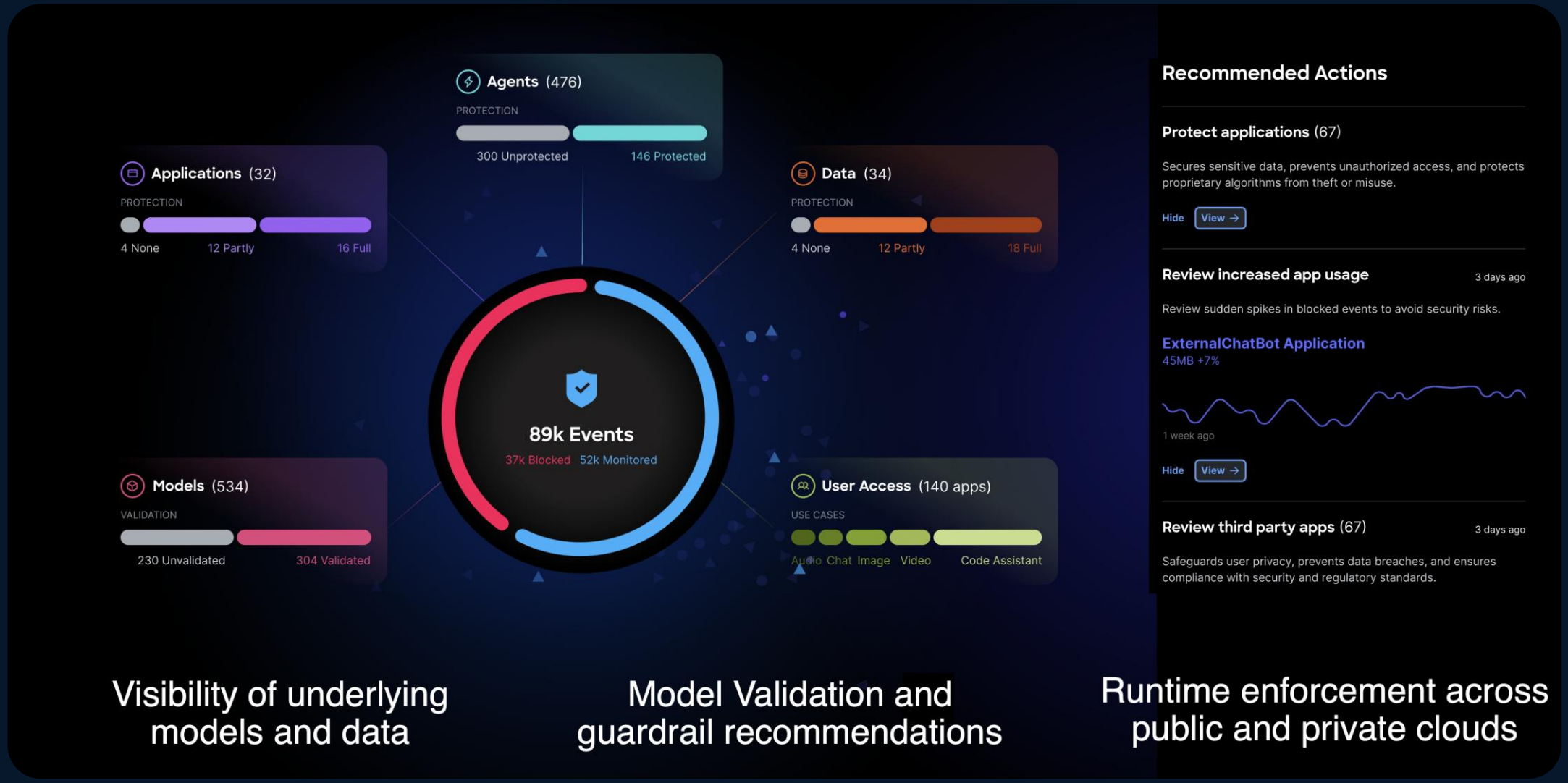
AI Defense

Securing the AI transformation


Safety
Profanity
Cost harvesting / repurposing
Harassment
Hallucinations
Hate speech
Off-topic
Toxicity
Social division & polarization
Self-harm
Financial harm
Security
Indirect prompt injection
Infrastructure compromise
IP theft
Meta prompt extraction
Prompt injection
Model theft
Training data poisoning
Sensitive information disclosure
Data exfiltration
Model denial of service

AI Defense

EARLY ACCESS



Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Delivered via the Hybrid Firewall

Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Cisco Security Cloud Enforcement Points

- Secure Firewall
- Secure Firewall Cloud
- Hypershield

AI Security Journey

Safely enable GenAI across your organization

Discovery

Uncover shadow AI, apps, models, and data

Detection

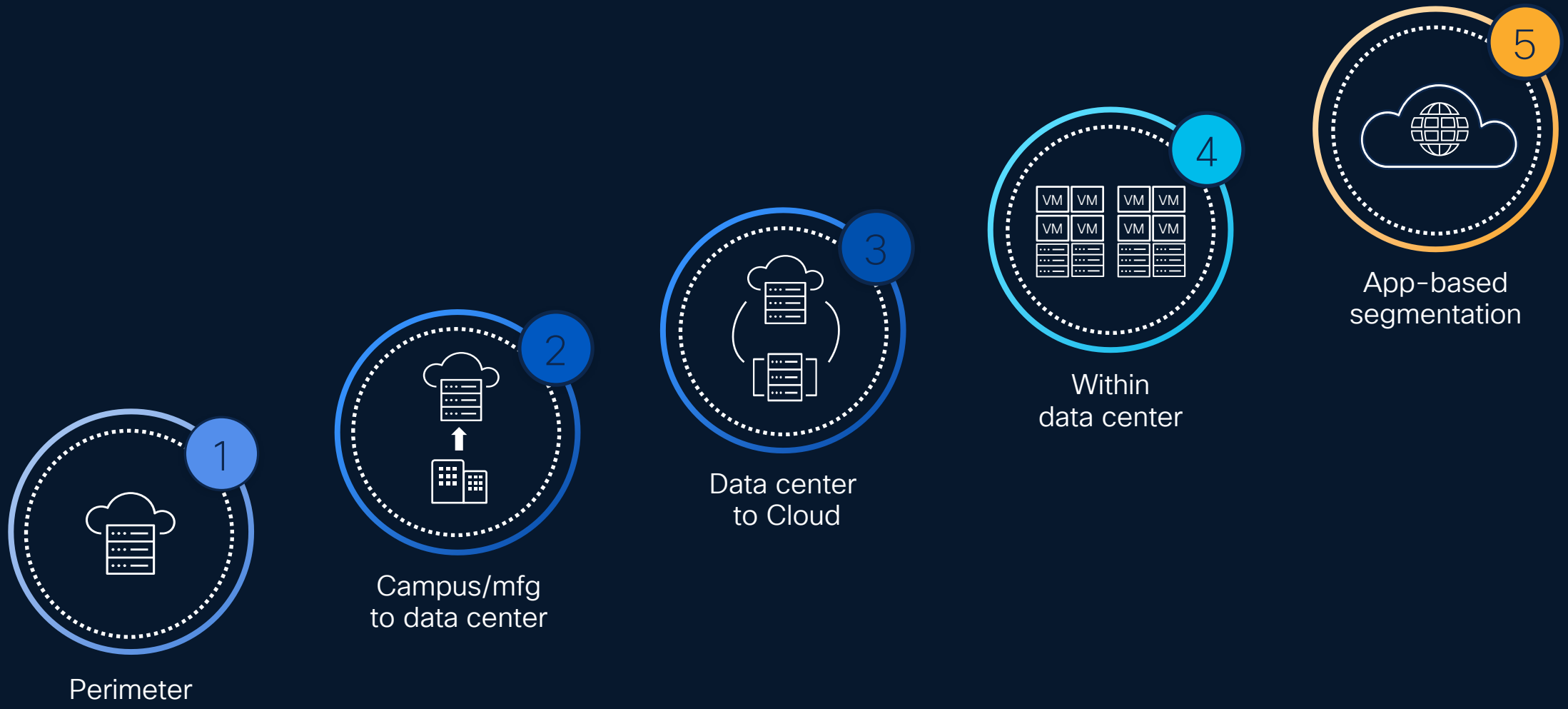
Test for AI risk, vulnerabilities, and adversarial attacks

Protection

Place guardrails and access policies to secure data and defend against runtime threats

Stopping lateral movement
Segmentation that works

Segmentation that meets you where you are



Optimal segmentation for:

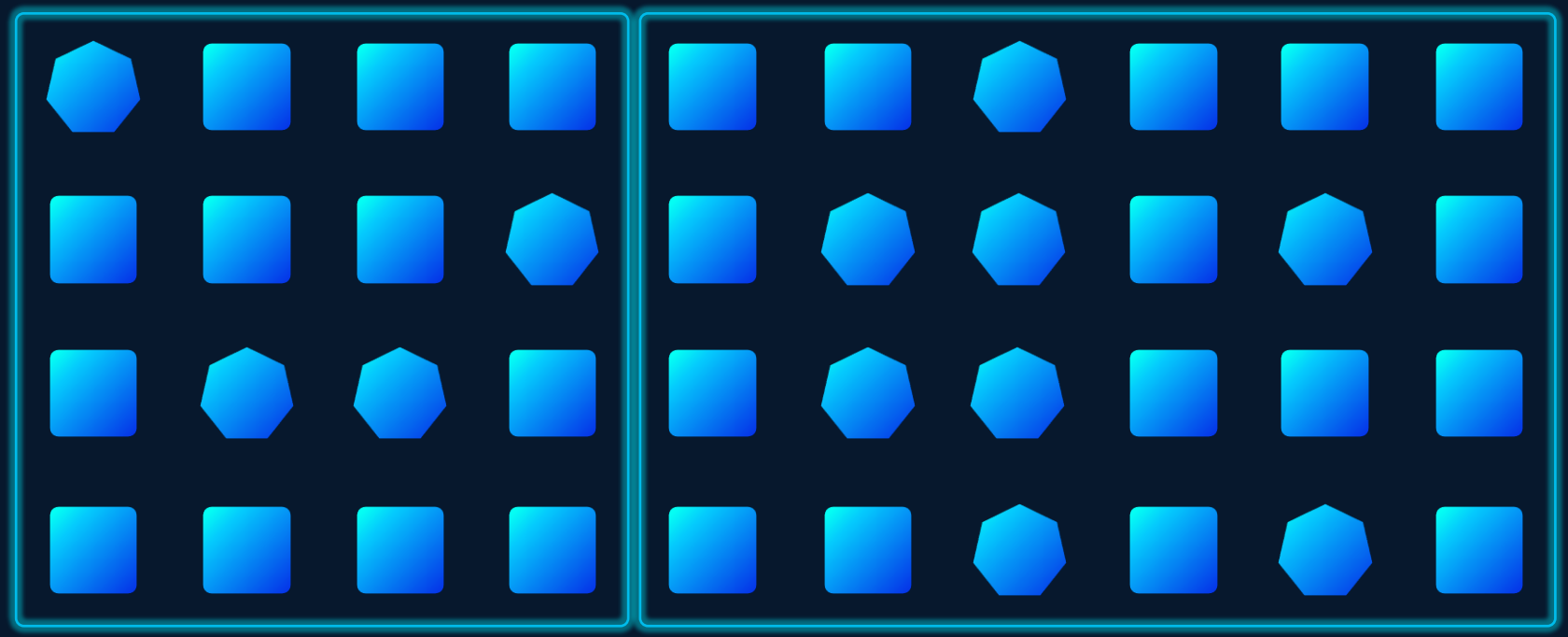
Traditional Workloads

IoT devices

Kubernetes Workloads

MACROSEGMENTATION

MICROSEGMENTATION



Dev

Prod

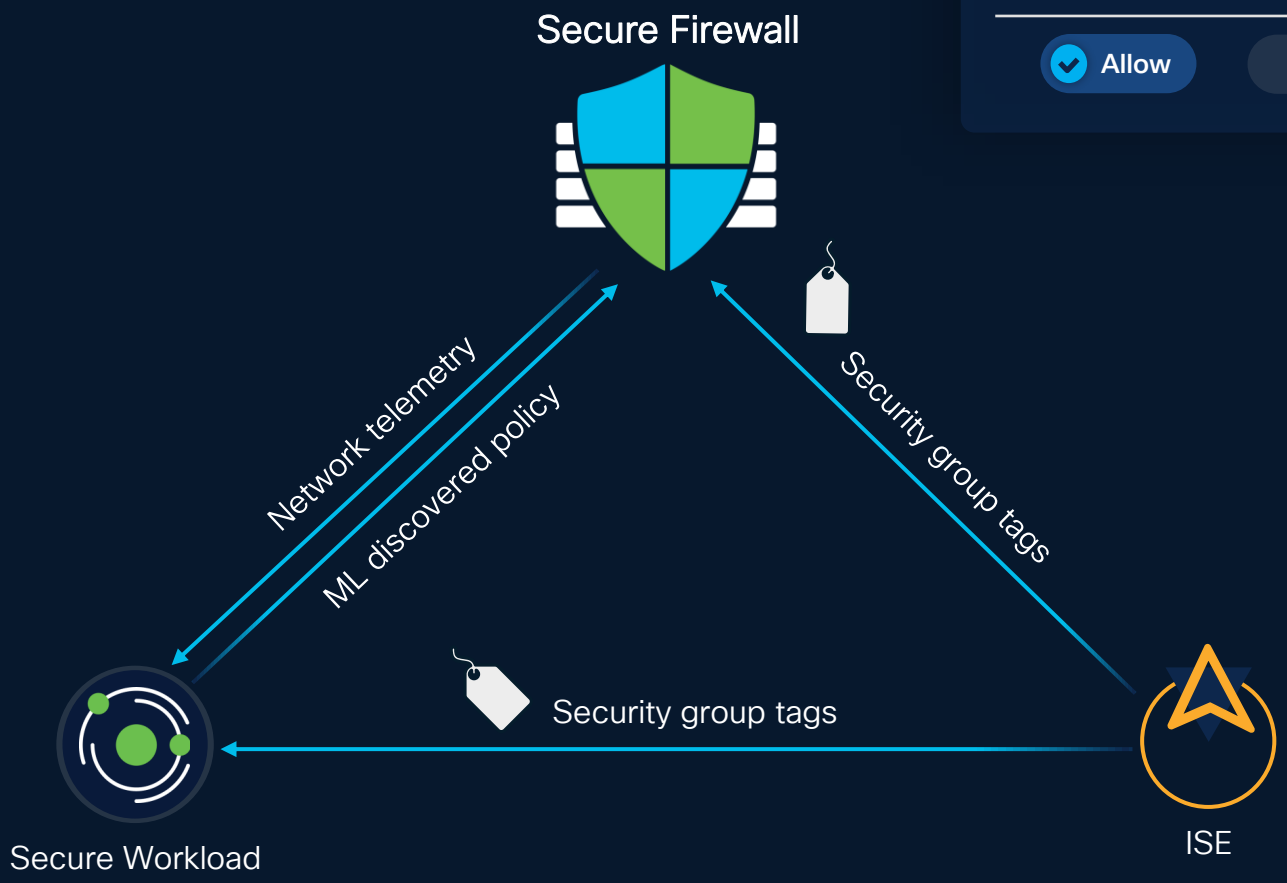
Flow-based rule

Allow	PCI_APP1	connect to	PCI_APP2	TCP/3306

Process-based rule

Allow	PCI_APP1	“payment_processor”	connect to	PCI_APP2	“mysqld”	TCP/3306

Smarter firewalling with Secure Workload & ISE



Action	Source	Destination	Protocols / Ports
Allow	contractors-users	vdesktop-infra	TCP: 443

User based policy using ISE tags inline

ML powered policy discovery

Policies evolve as users and apps change

Traditional segmentation for workloads

All types of workloads

Windows | Linux | Cloud

Virtual Machine

BareMetal

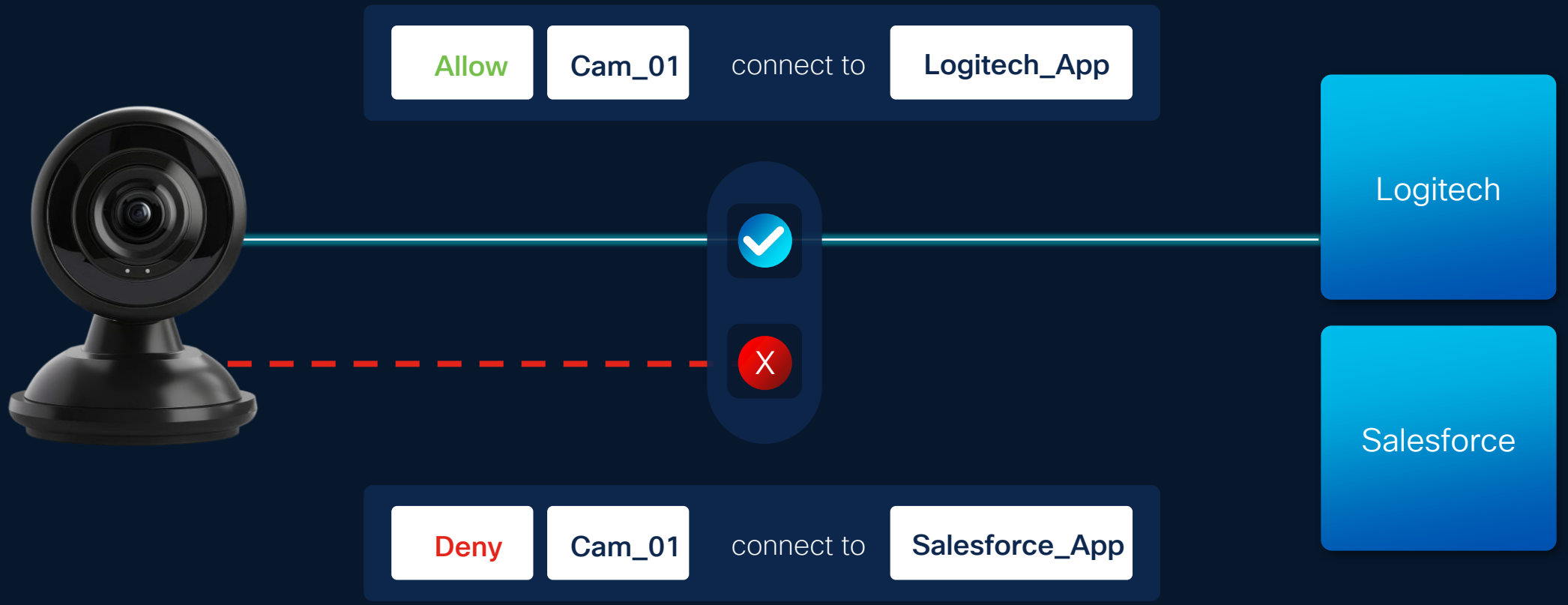
SaaS delivered

Get started quickly without hardware investment

Confident outcomes

Speed up time to value with implementation services

Segment IoT devices using ISE and Firewall



Cloud-native segmentation for Kubernetes

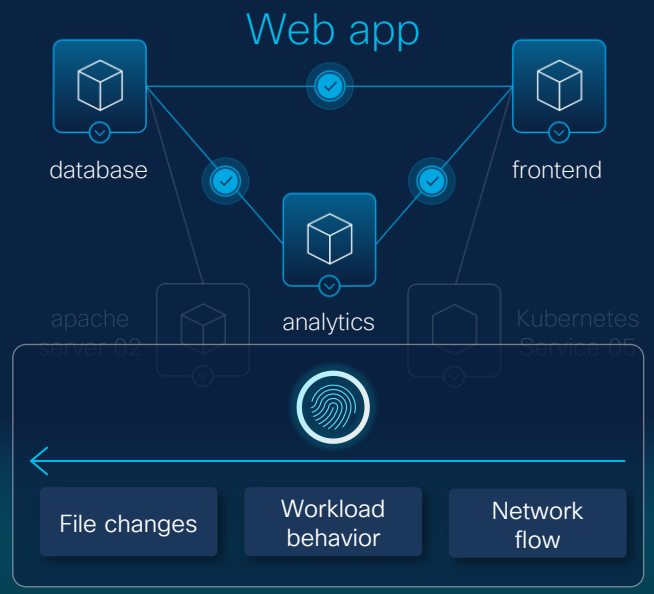
Discover microservice interactions

Enforce policies in the Kubernetes fabric

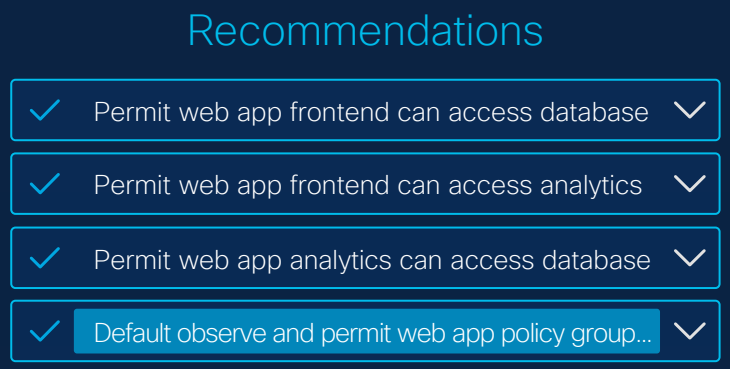
Hypershield: AI-native segmentation that works at scale

Autonomous segmentation

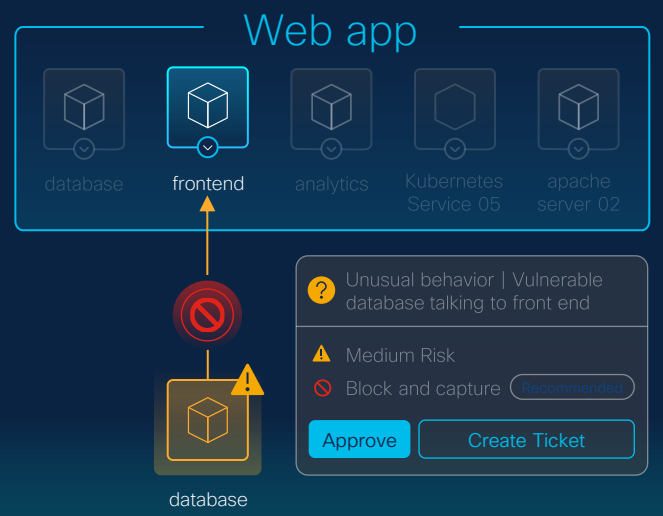
FUTURE



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



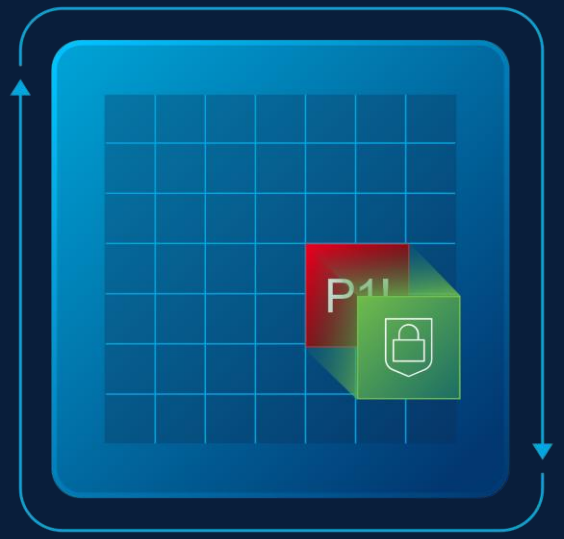
Flexible segmentation rules that help avoid app fragility



Policies updated to stricter rules in response to suspicious events

Compensating controls
Distributed Exploit Protection

Defender’s dilemma



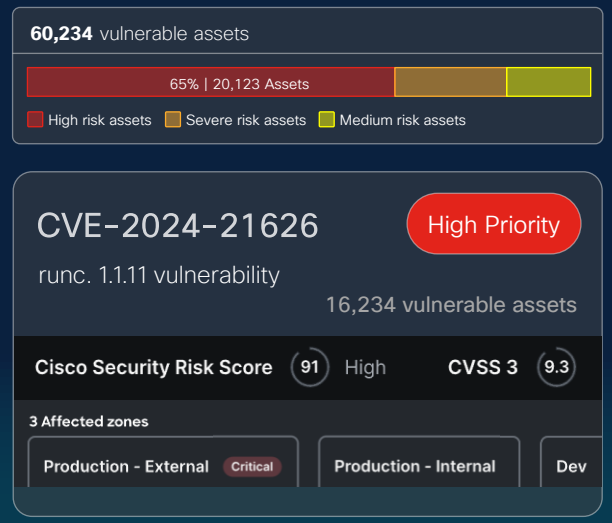
Mitigate known and unknown vulnerabilities

Do it in minutes, not months

All while keeping the app and business running

Closing the exploit gap with automated workflows

FUTURE

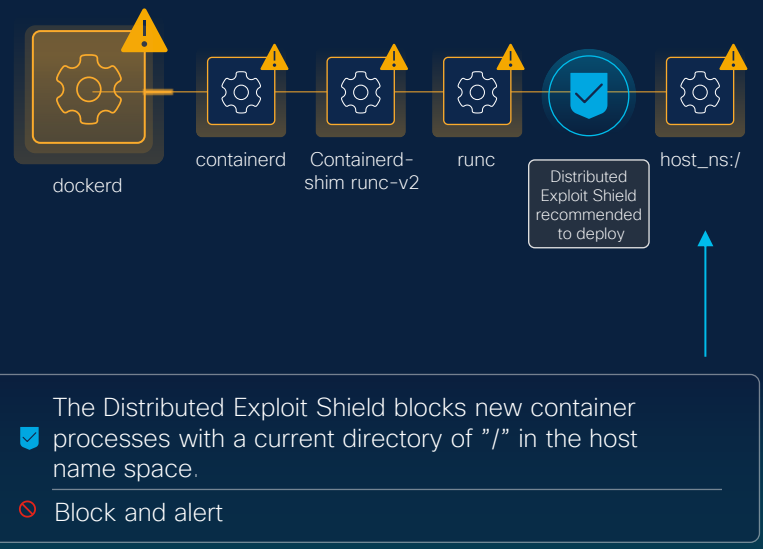


Data-driven vulnerability prioritization

+19 threat and exploit intel feeds

+12.7B managed vulnerabilities

+1B security events processed monthly



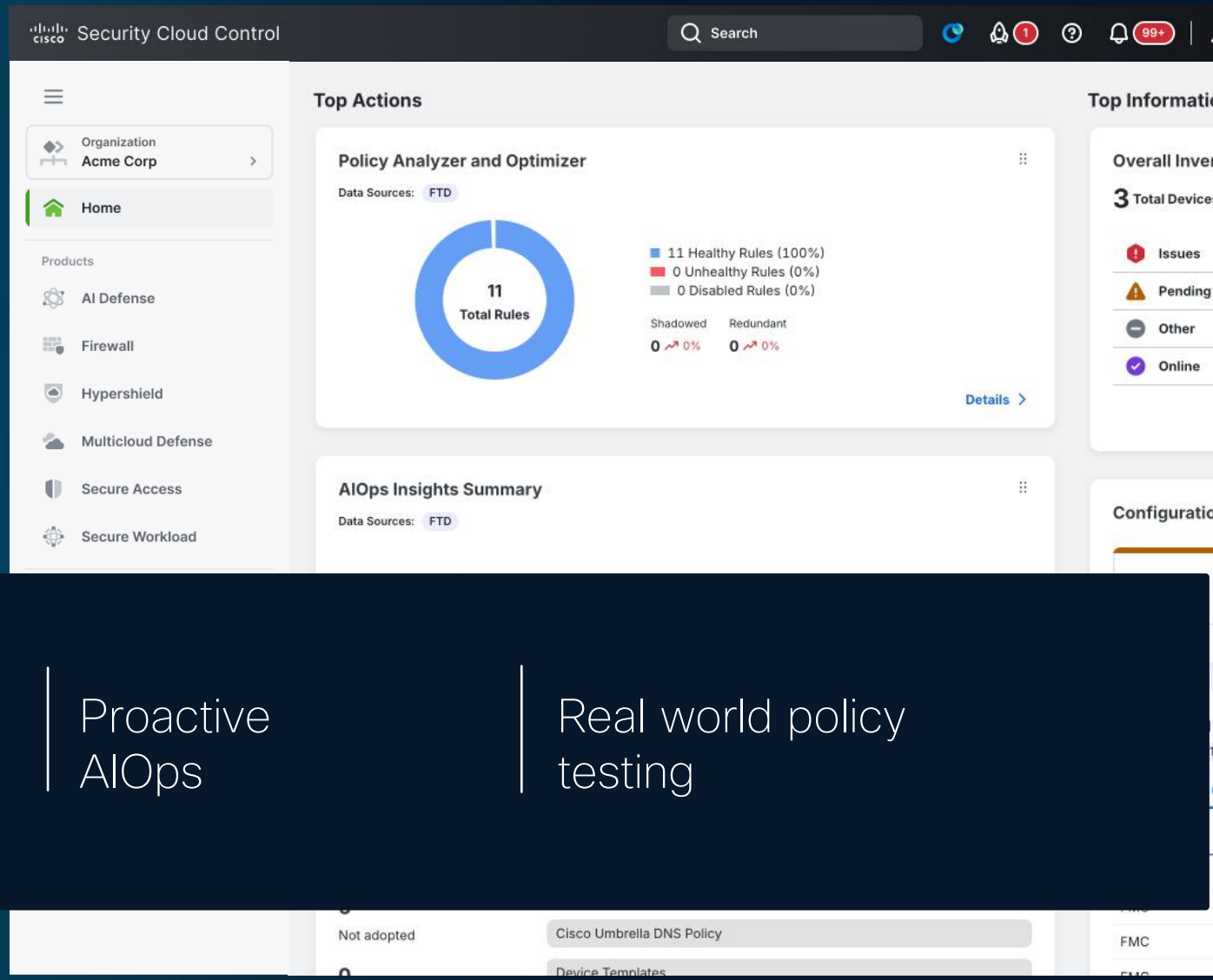
Surgical mitigating control that keeps application running

Tested against live production traffic to earn trust and increase confidence

Security Cloud Control
Unified Management

Security Cloud Control

Simplify policy administration by up to 70%



AI assistance for policy

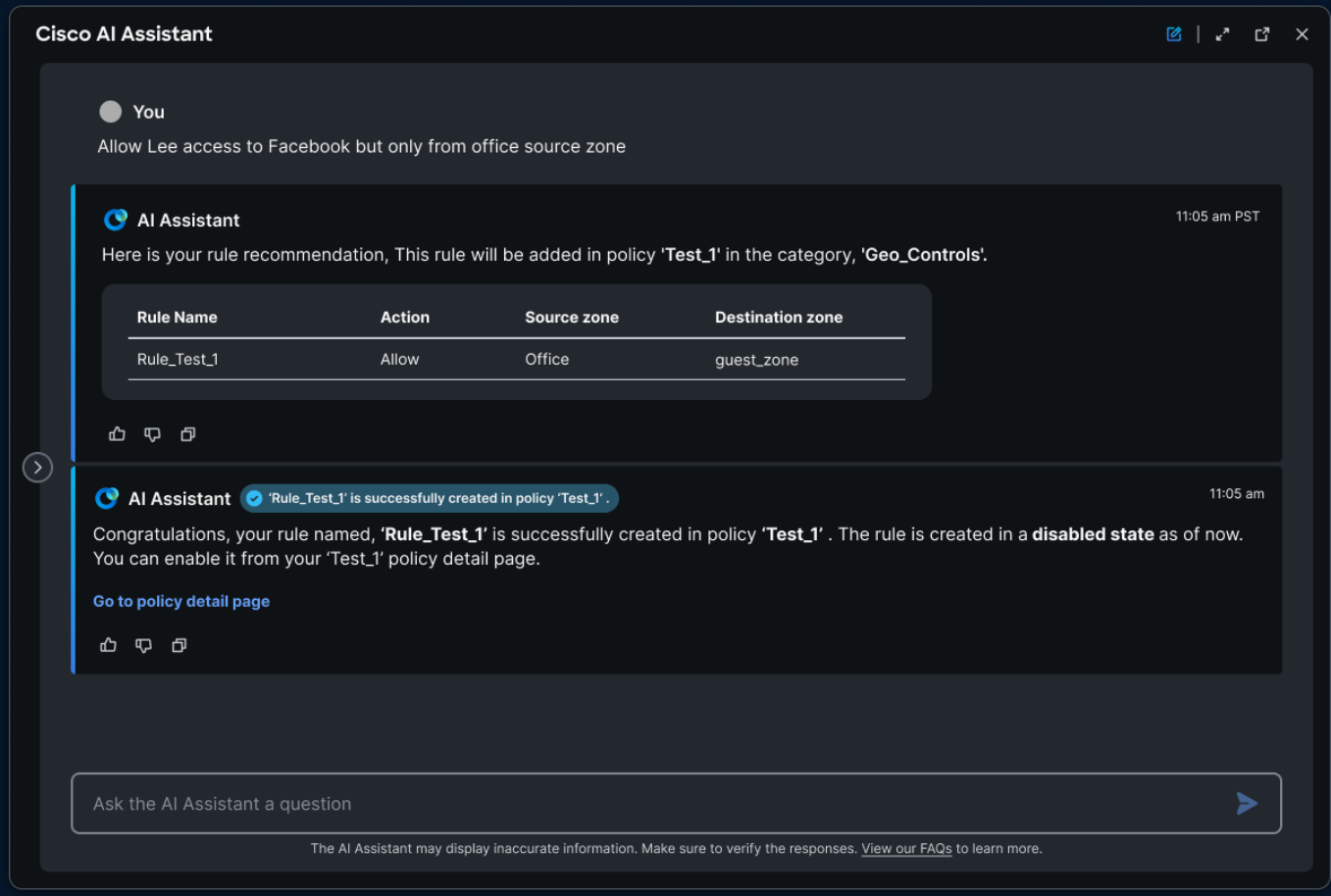
Proactive AIOps

Real world policy testing

Some capabilities are future.

Reduce management overhead with AI ops

- **Assist** + Policy configuration
- **Augment** + Troubleshooting
- **Automate** + Policy lifecycle management



Digital Twin: Upgrades

FUTURE

Primary Data Plane

VERSION 2.0

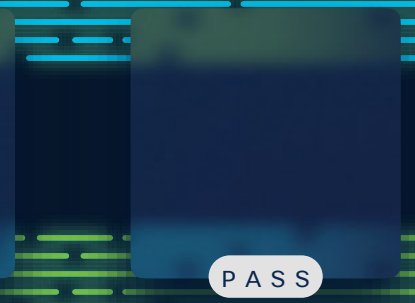
VERSION 2.1

Shadow Data Plane

Earns your trust

- [ ] EDIT/UPDATE
- [ ] TEST REPORTS
- [ ] SCHEDULE DEPLOYMENT
- [x] DEPLOY

Packets



Digital Twin: Policy Verification

FUTURE

Primary Data Plane

DEPLOYED POLICY

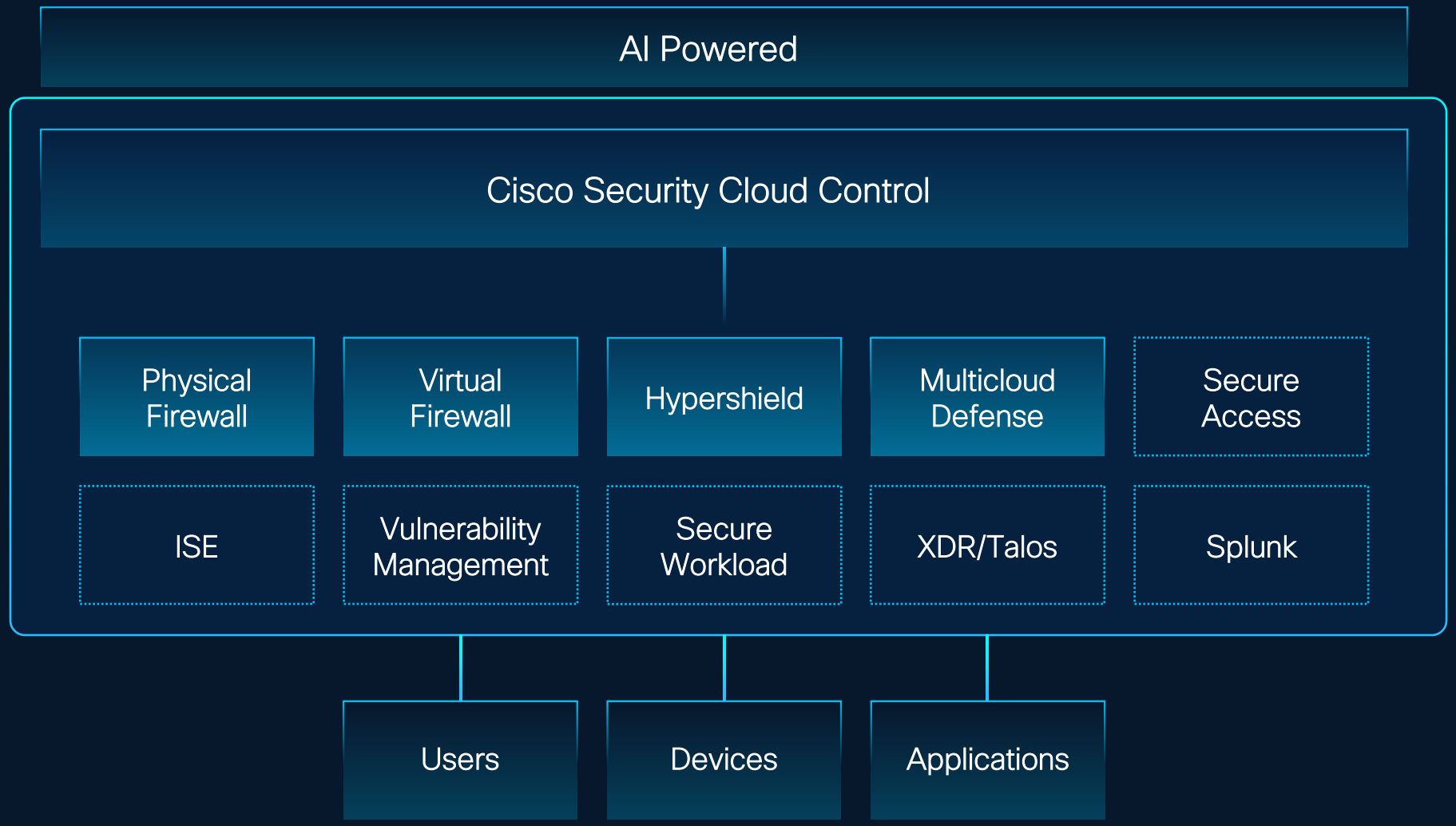
POLICY GROUP A

Shadow Data Plane

FLOWS

	Primary	Shadow
Flow count	10,234	10,234
Total allowed flows	10,234	10,231
Total denied flows	14,213	14,216

Security Cloud Control



- Unified coordination of security solutions
- Consistent policy enforcement and object sharing
- Support for hybrid environments including on-premises


CISCO