

# A Defensible Datacenter Powered by an Agnostic Centralized Policy Plane

Jason Maynard, Solutions Designer



# Nothing but Truth!



We will never achieve 100% immunity



The adversary will never be 100% correct



The defender never needs to be 100% correct



Time is a power move for defenders



Initial access is inevitable

*Assuming breach drives better outcomes for defenders*



# Verticals & Common Themes: Impacts Vary

## Vertical: Healthcare Impact



Many times, the initial threat vector will propagate deeply and freely into patient care system impacting the ability to deliver timely critical care outcomes and loss of PHI. Access to Medical Record Numbers.

Impact to delivering timely patient care, potential death, and loss of PHI.

## Vertical: Financial Institution



Many times, the initial threat vector will propagate deeply and freely into financial environment causing payment processing delays, disrupt markets, and loss of PII.

Impact to payment processing, disrupts markets, and loss of PII.

## Vertical: Government



Many times, the initial threat vector will propagate deeply and freely into the environment causing disruption, impact to critical services, access to classified data, and loss of PII, & IP.

Impact impact to critical services, access to classified data, and loss of PII, & IP.

## Vertical: Industrial Environment



Many times, cyber attack will start in the business network and make its way to the critical operational environment causing downtime or worst human impact and loss of intellectual property.

Impact to critical processes causing damage and/or human risk and IP.

## Vertical: Higher Education













Many times, the initial threat vector will propagate deeply and freely into the environment causing disruption, impact to online learning, compromised research data, and loss of PII & IP.

Impact to learning, compromised research data, and loss of PII & IP.

*Complexity is the enemy of security!*

# Top 10 Attacks & Common Themes

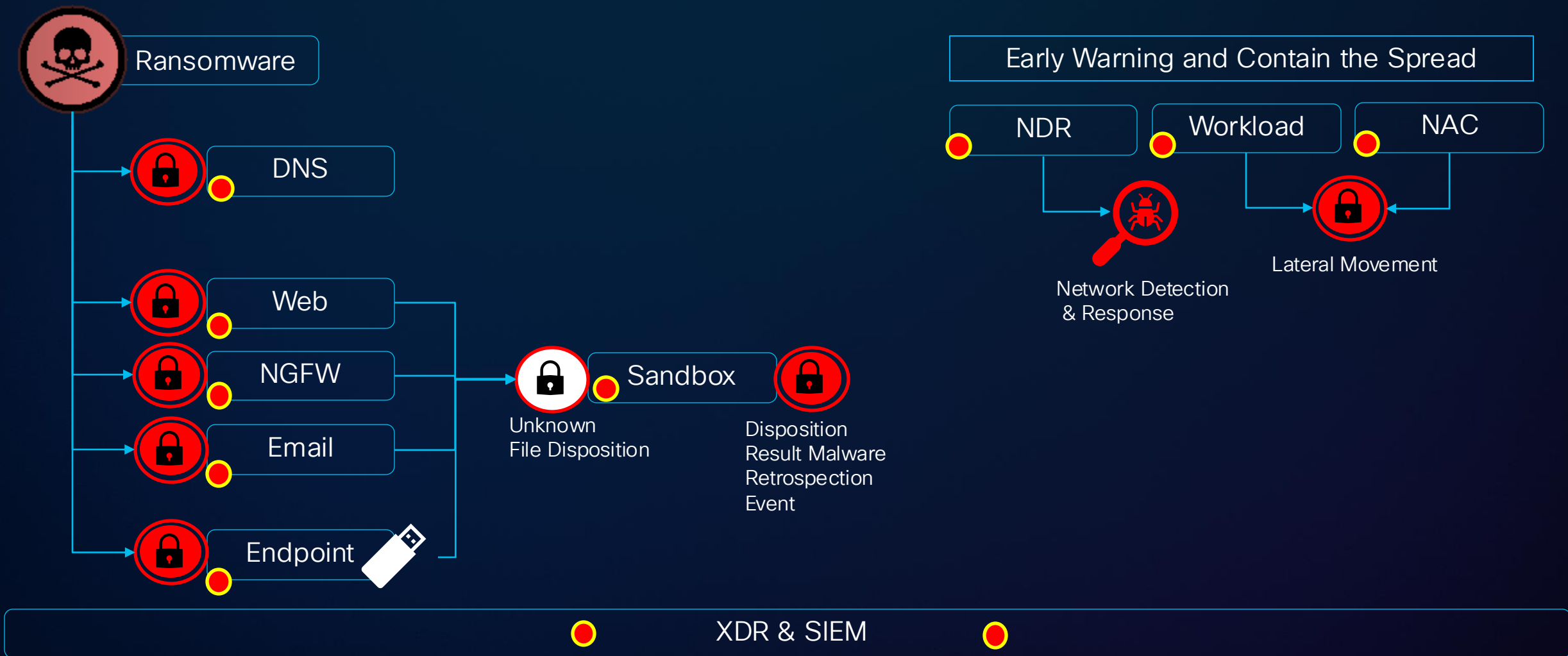
|   |                               |
|---|-------------------------------|
|    | Advanced Phishing             |
|    | Ransomware / Malware          |
|    | Social Engineering            |
|    | Distributed Denial of Service |
|    | Credential Theft              |
|    | Insider Threats               |
|    | Advanced Persistent Threats   |
|    | Vulnerability Exploit Attack  |
|   | Supply Chain Attacks          |
|  | AI Threats                    |



Preventative  
Controls

Prevention is key but 100% efficacy 100% of the time is unattainable.

# Prevention Opportunity: Ransomware

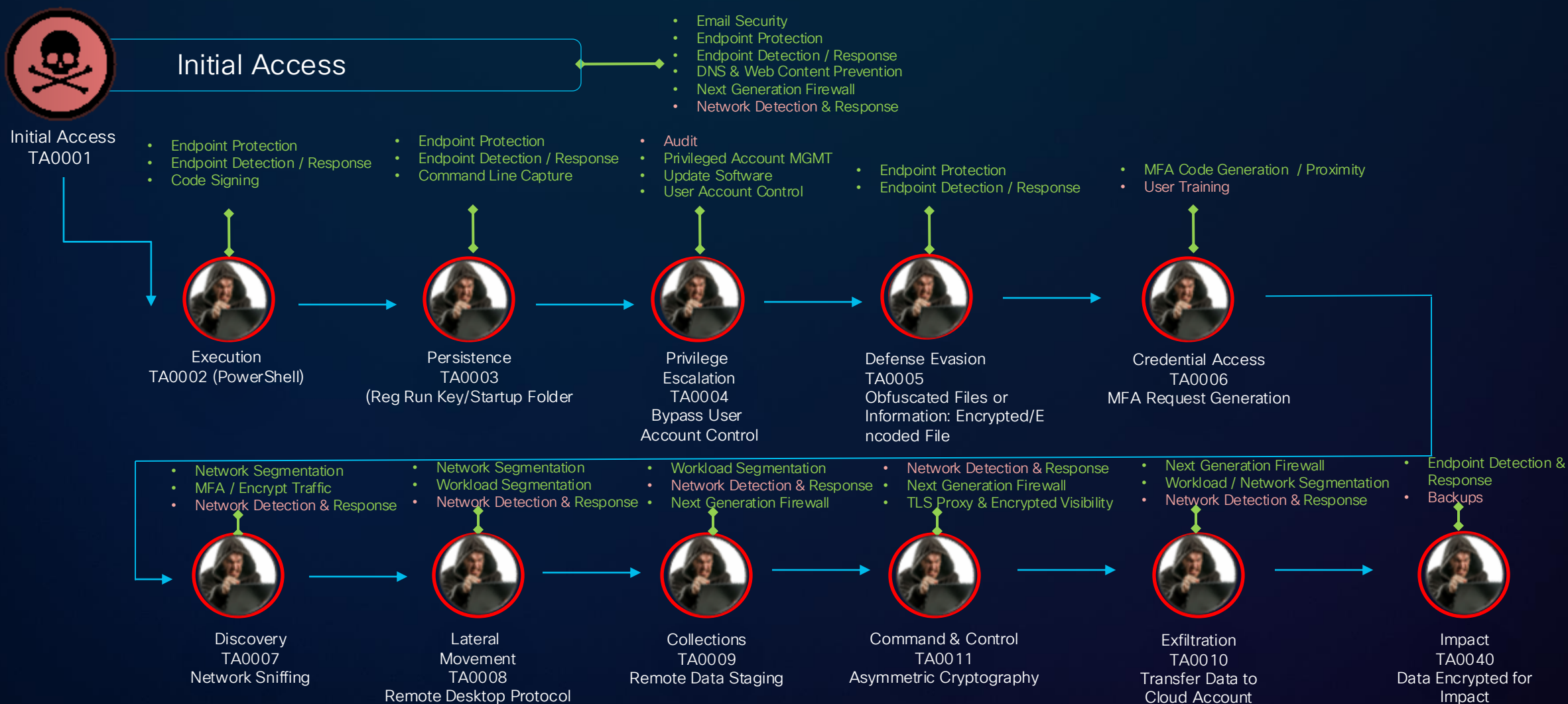


Platform based defense and nowhere to hide!



# The Anatomy of an Attack: After Initial Access

- Detection / User Awareness
- Prevention



*Understanding the Adversaries Abilities*

The attack does not take these steps in order as outlined. There is nuance to the attack and how one defends. This is an example and not comprehensive

# Initial Access Will Be Accomplished

TA0001 Initial Access: The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

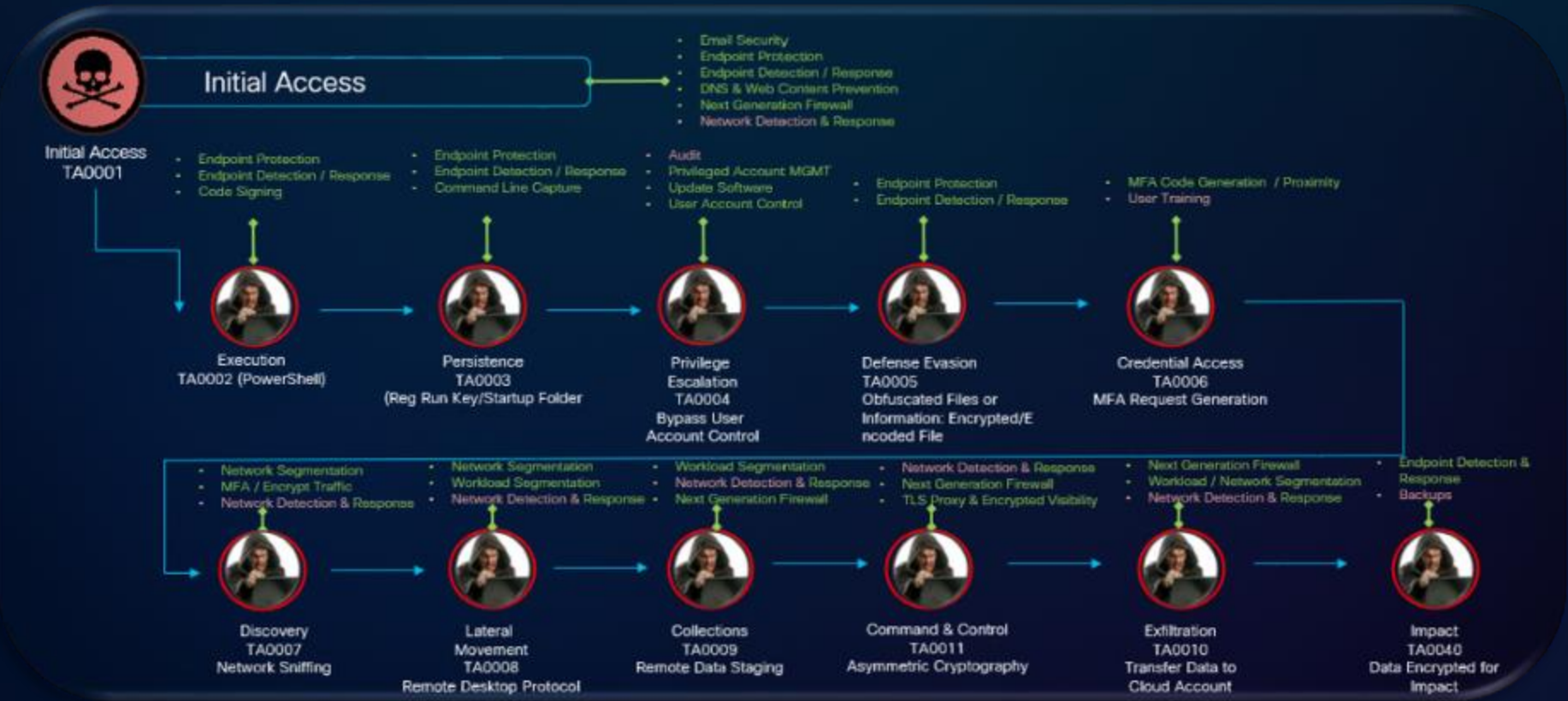
Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

-  T1659: Content Injection
-  T1189: Drive-by Compromise
-  T1190: Exploit Public-Facing Application
-  T1133: External Remote Services
-  T1200: Hardware Additions
-  T1566: Phishing
-  T1091: Replication Through Removable Media
-  T1195: Supply Chain Compromise
-  T1199: Trusted Relationship
-  T1078: Valid Accounts
-  T1669: Wi-Fi Networks

*Assuming breach drives better outcomes for defenders*

# Common Threat Theme!

- Detection / User Awareness
- Prevention



Lateral  
Movement  
TA0008

60 – 70 % of all breaches involve lateral movement

*Adversaries continue to advance unchecked!*

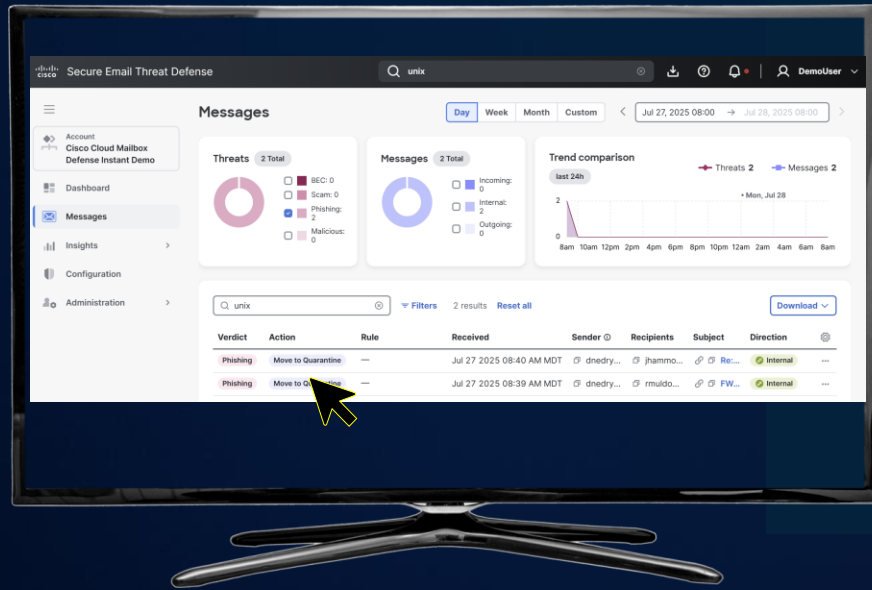
The attack does not take these steps in order as outlined. There is nuance to the attack and how one defends. This is an example and not comprehensive





# SOC Center of Excellence

## Prevention Opportunity



# The Anatomy of an Attack



# Incident Response Investigations and Threat Hunting



# Talos

# Security Operations Center



Advanced Phishing



Ransomware / Malware



Social Engineering



Distributed Denial of Service



Credential Theft



Insider Threats



Advanced Persistent Threats



Vulnerability Exploit Attack



Supply Chain Attacks



AI Threats

## Cisco XDR

- Incident Response Workflow & Attack Chains
- Playbooks and Workflows
- Talos Incident Response Services

## Cisco Splunk

- Custom Vertical Risk Dashboard
- Attack Analyzer
- Governance & Compliance
- SOAR

Evolving threats but this has been the story all along. The difference is the velocity



# The Defenders Opportunity Campus Network



Visibility

Policy

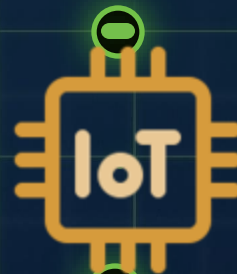
Simulation

Enforcement

Zero Trust

Defcon Policy

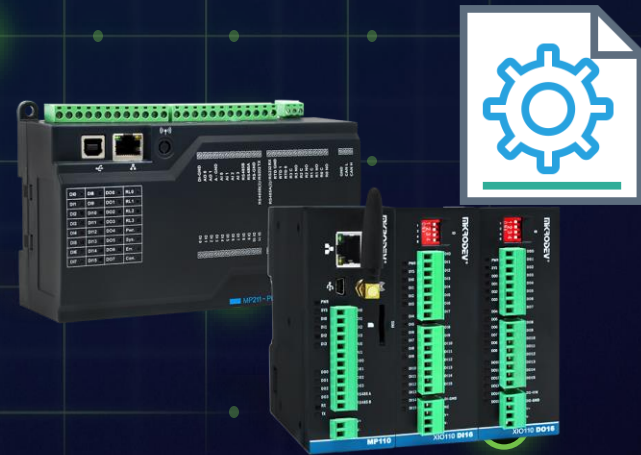
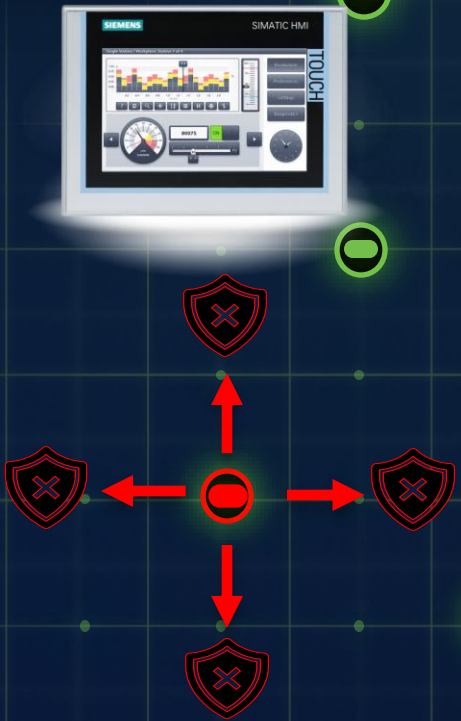
Risk Profiles



# The Defenders Opportunity

## Operational Network

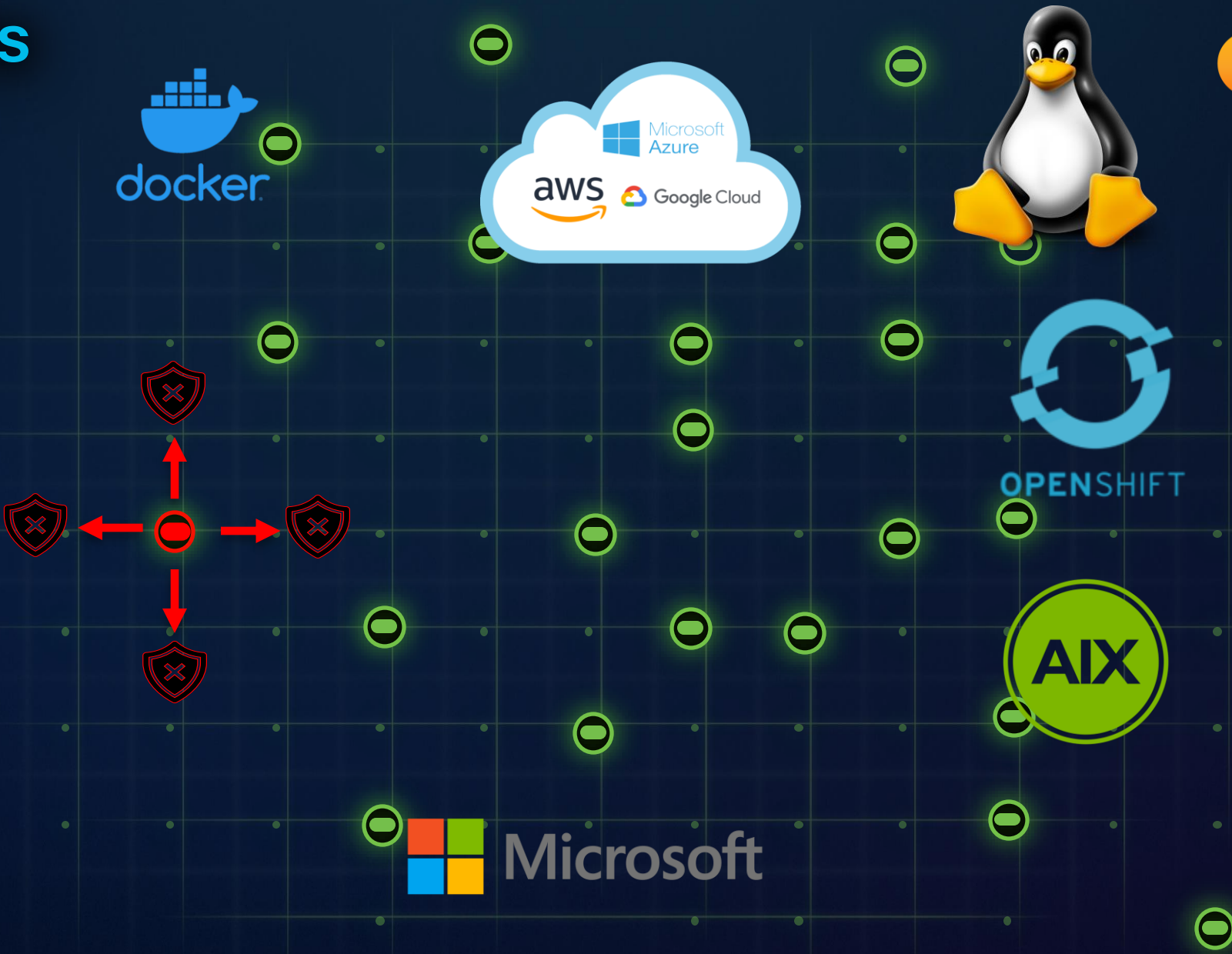
- Visibility
- Policy
- Simulation
- Enforcement
- Zero Trust
- Defcon Policy
- Config Files
- Risk Profiles





# The Defenders Opportunity Datacenter

- Visibility
- Policy
- Simulation
- Enforcement
- Zero Trust
- Exploit Protection
- Risk Profiles



# The Defenders Opportunity Private Applications

Visibility

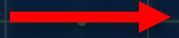
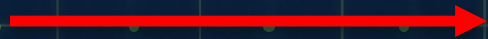
Policy

Enforcement

Zero Trust

Risk Profiles

Step up Auth



# 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

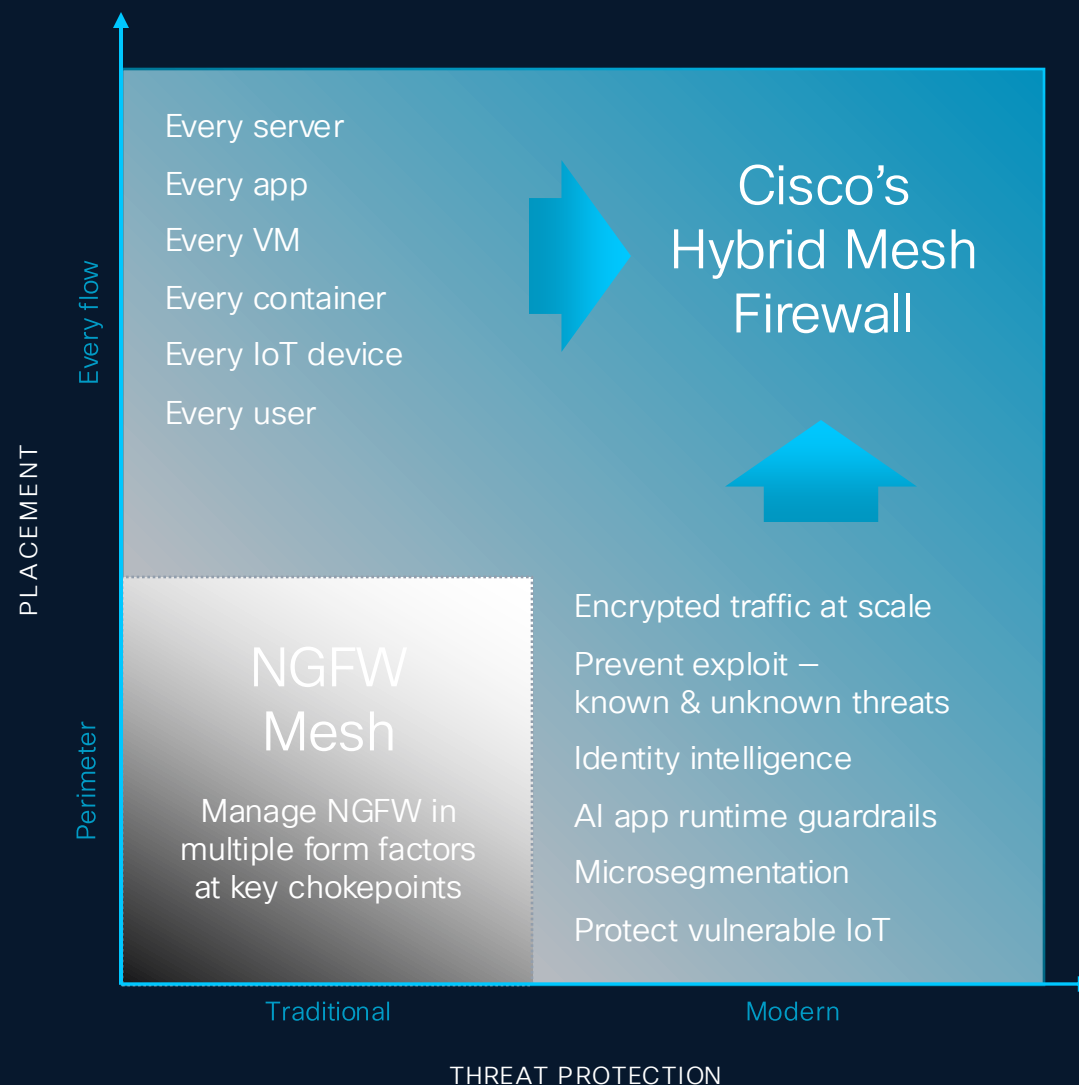
AI increasing attack surface and attack sophistication



# Firewalling Needs to Evolve to Meet Today's Challenges

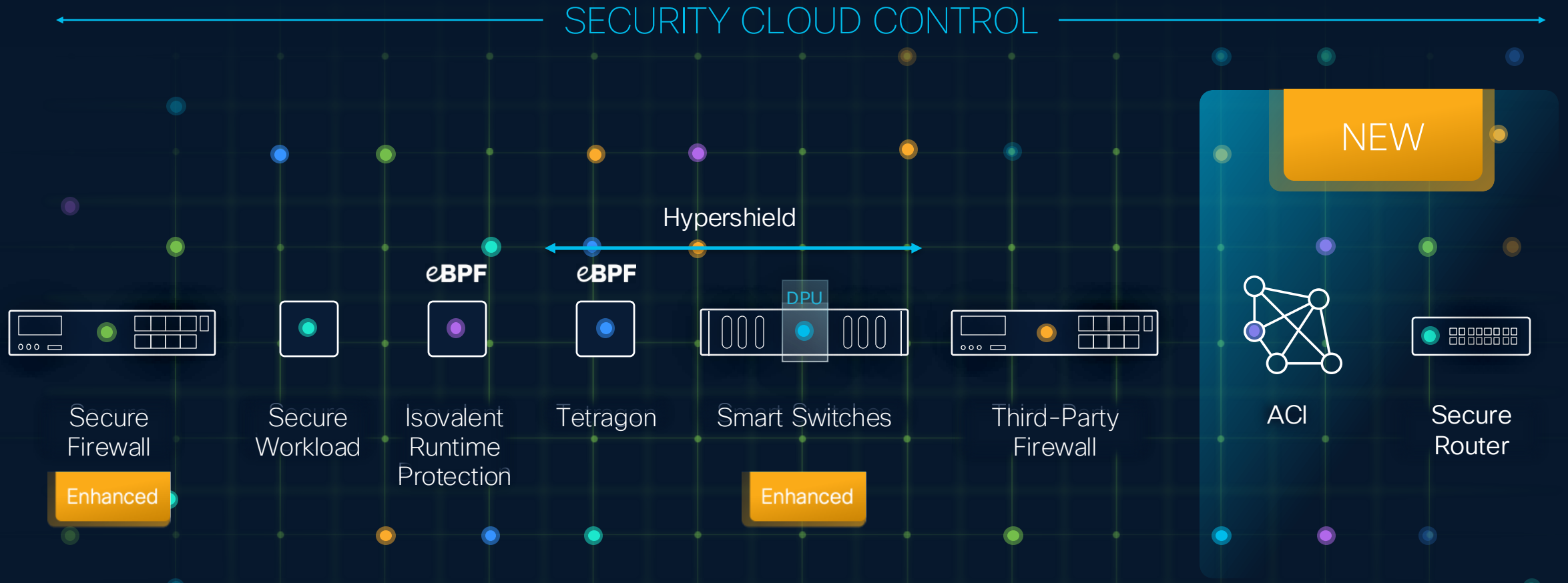
## OUR NORTH STAR

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





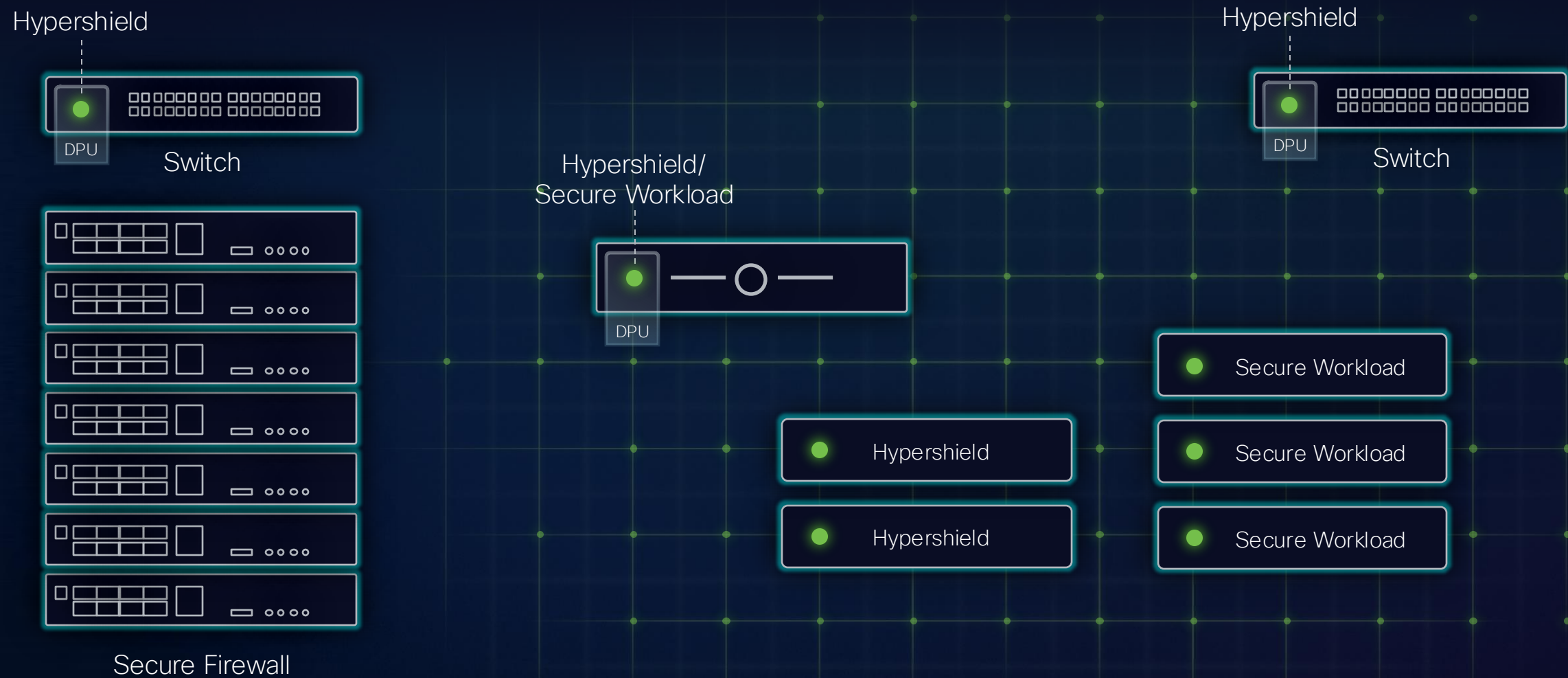
# Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

**No Rip and Replace**

# Security Cloud Control



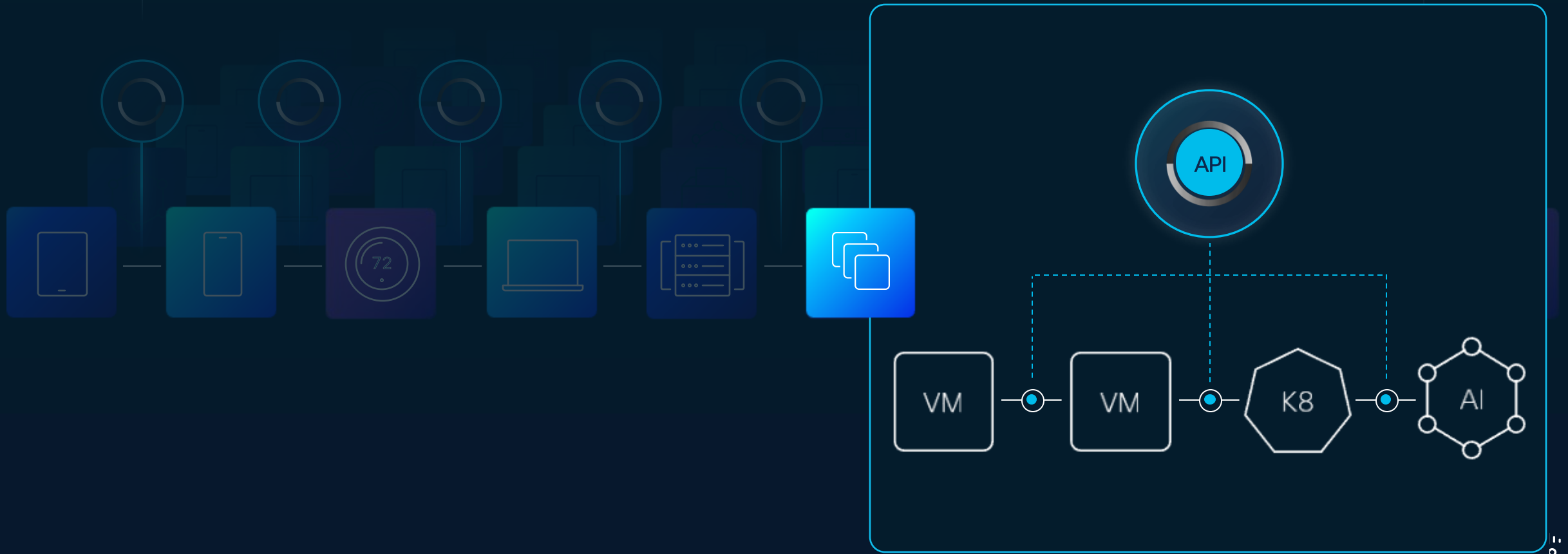
Enforcement points change, rules don't

# Autonomous Segmentation

FUTURE

CONTINUOUS VALIDATION  
ACROSS ENTIRE CHAIN

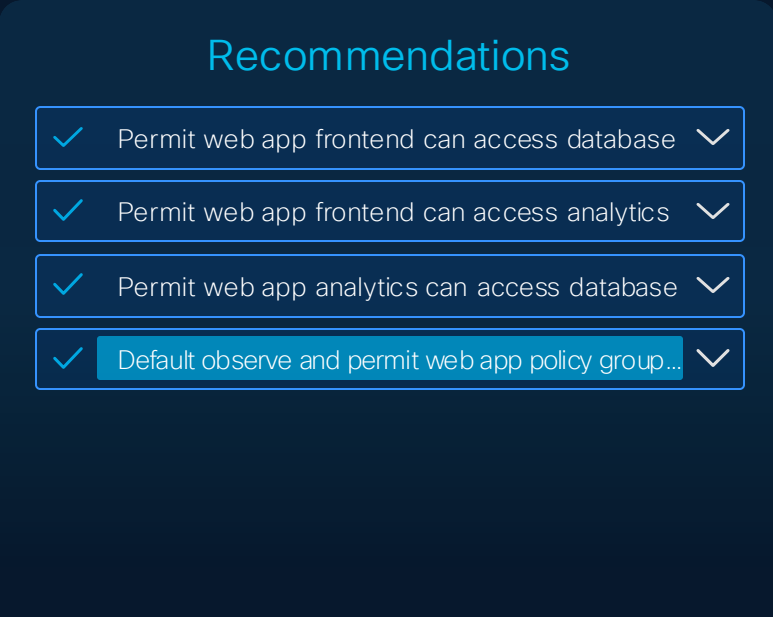
See the inner  
workings of apps



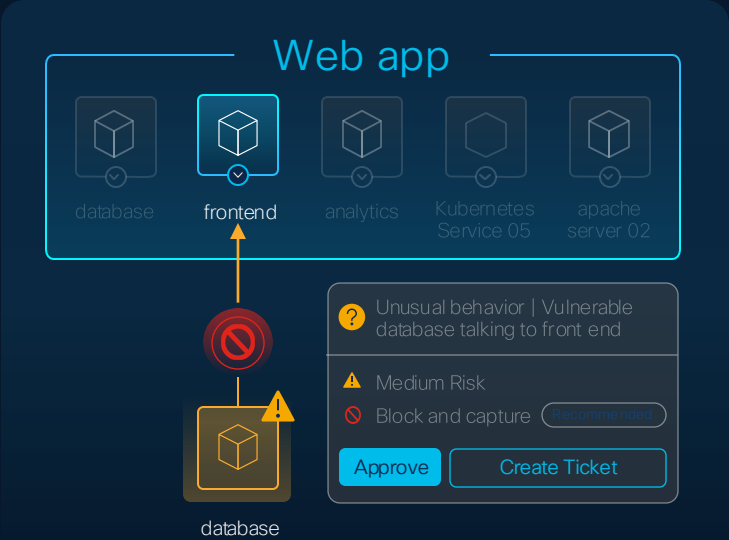
# Autonomous Segmentation



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



Flexible segmentation rules that help avoid app fragility

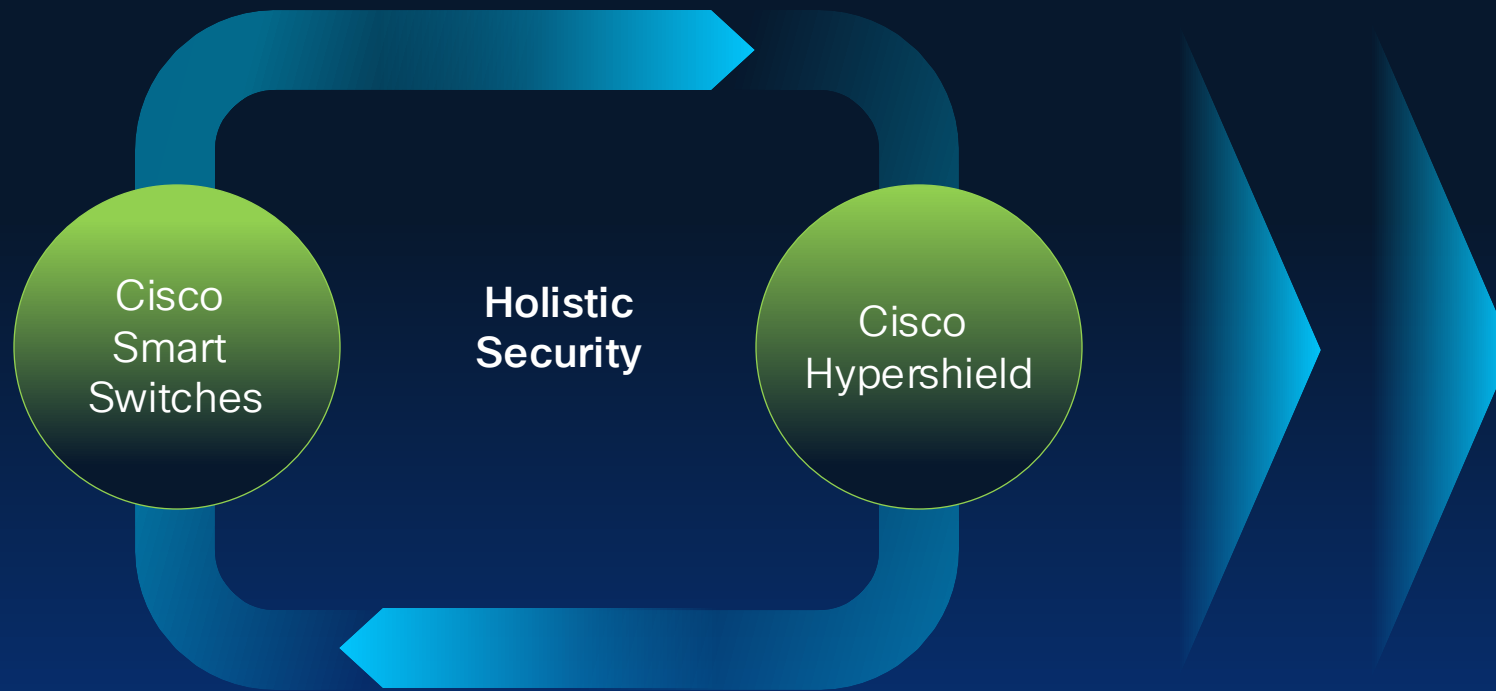


Policies updated to stricter rules in response to suspicious events



# Enable Segmentation Using the Same Switch Fabric

Infusing security into the network fabric



## Segmentation use cases

Cloud Edge

Zone-based  
segmentation

Data Center  
Interconnect (DCI)

# Introducing Cisco Smart Switch

NEW



Network + Security  
in one switch



Separate workflows and  
separate data flows for  
networking and security



Up to 84% TCO savings





# Cloud-Native Firewall with Firewall Threat Defense

Automated  
Deployment

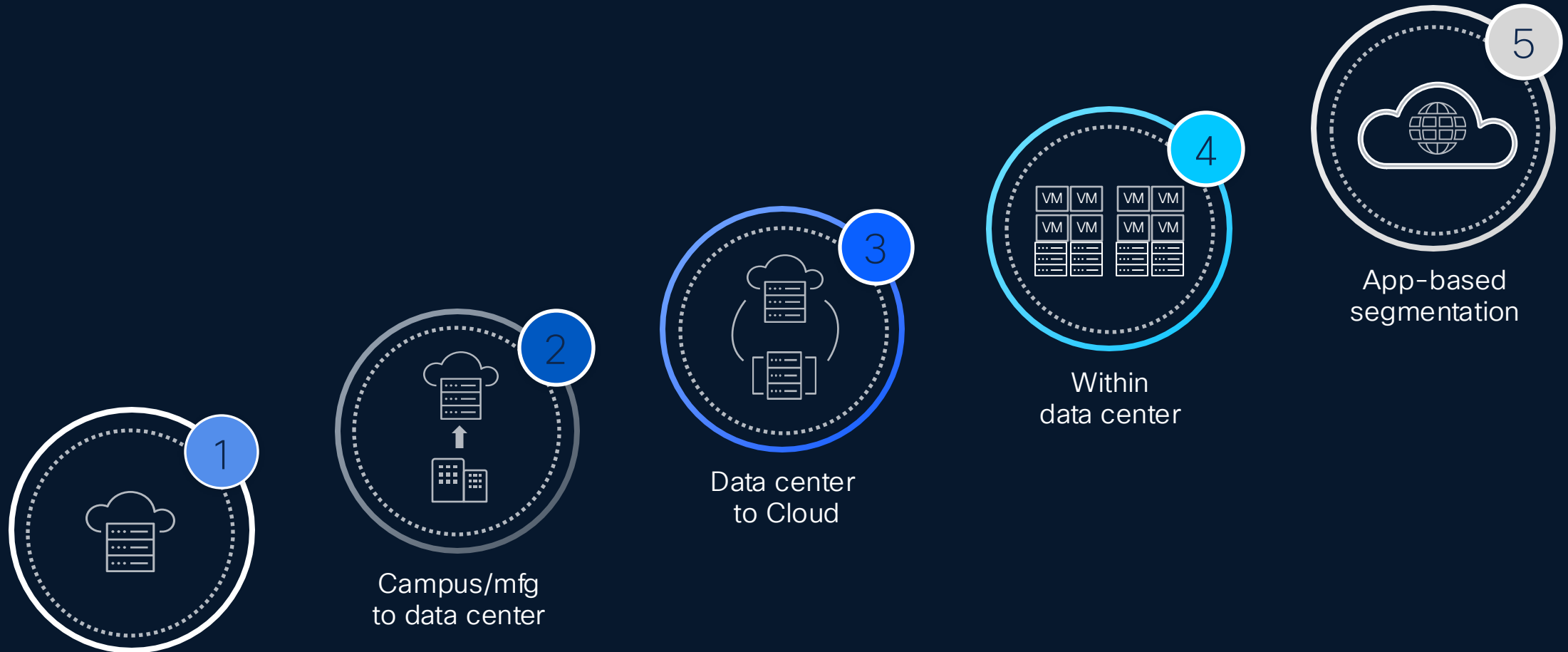
Auto-Scaling

Self-Healing

Enables firewalling at scale across multi-cloud environments

# Stopping Lateral Movement Segmentation that Works

# Segmentation that Meets You Where You Are





# Optimal Segmentation For:

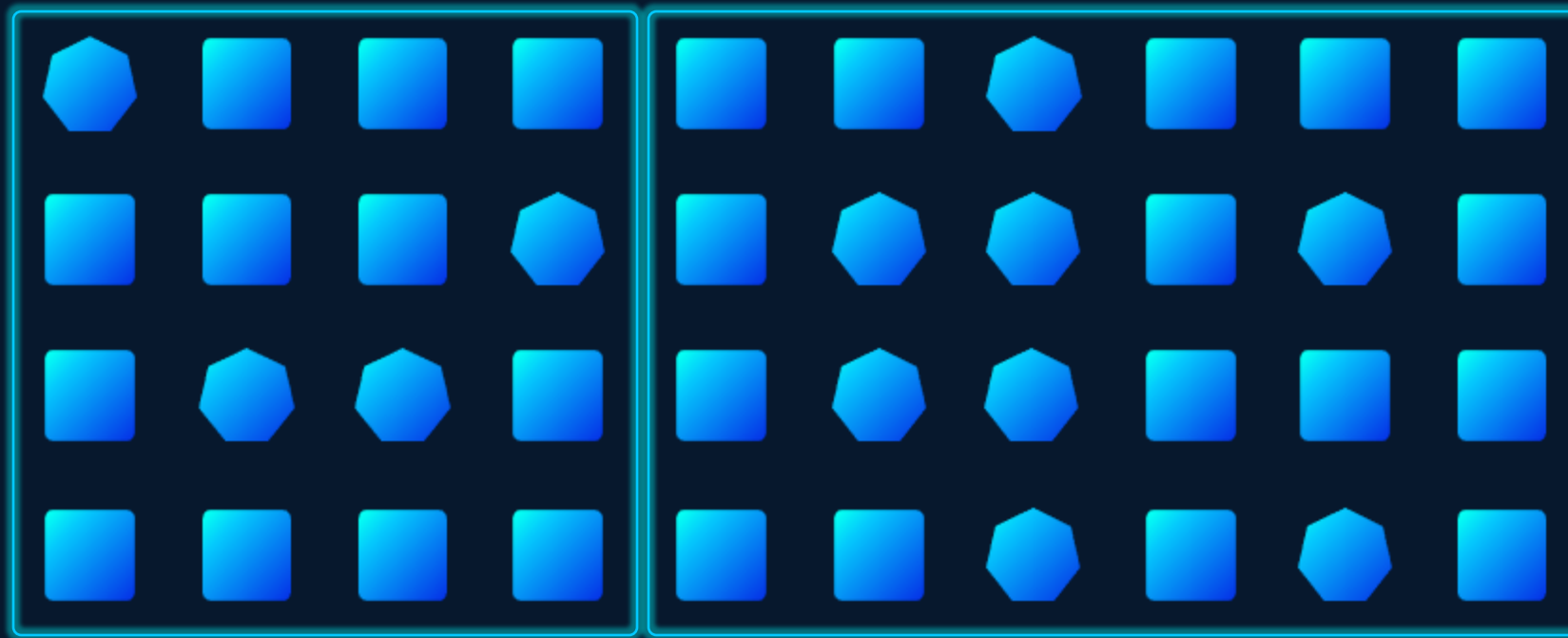
Traditional Workloads

IoT Devices

Kubernetes Workloads

## MACROSEGMENTATION

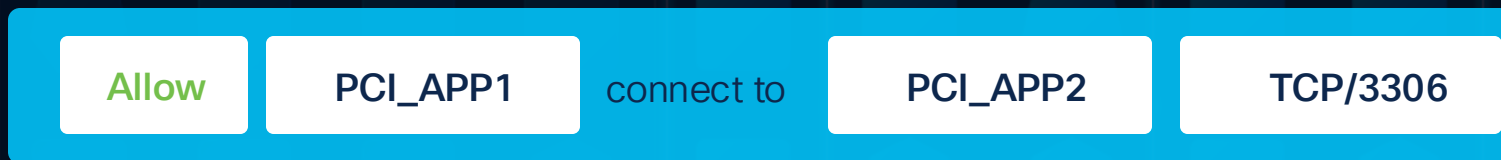
## MICROSEGMENTATION



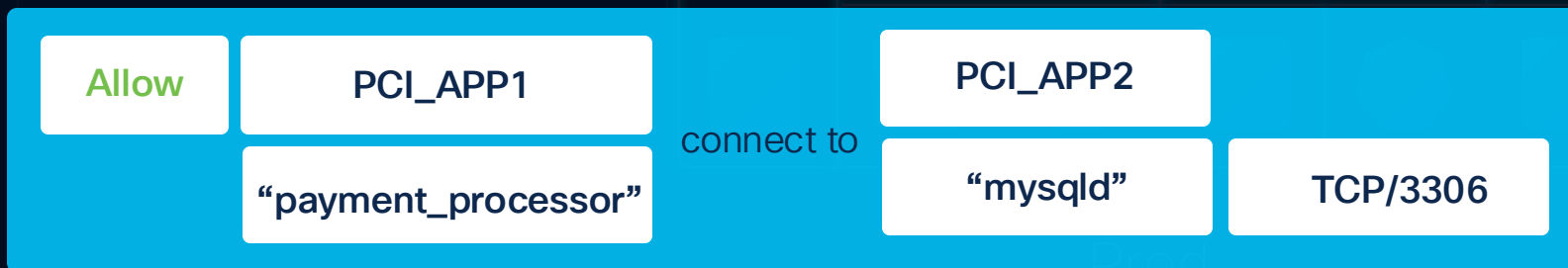
Dev

Prod

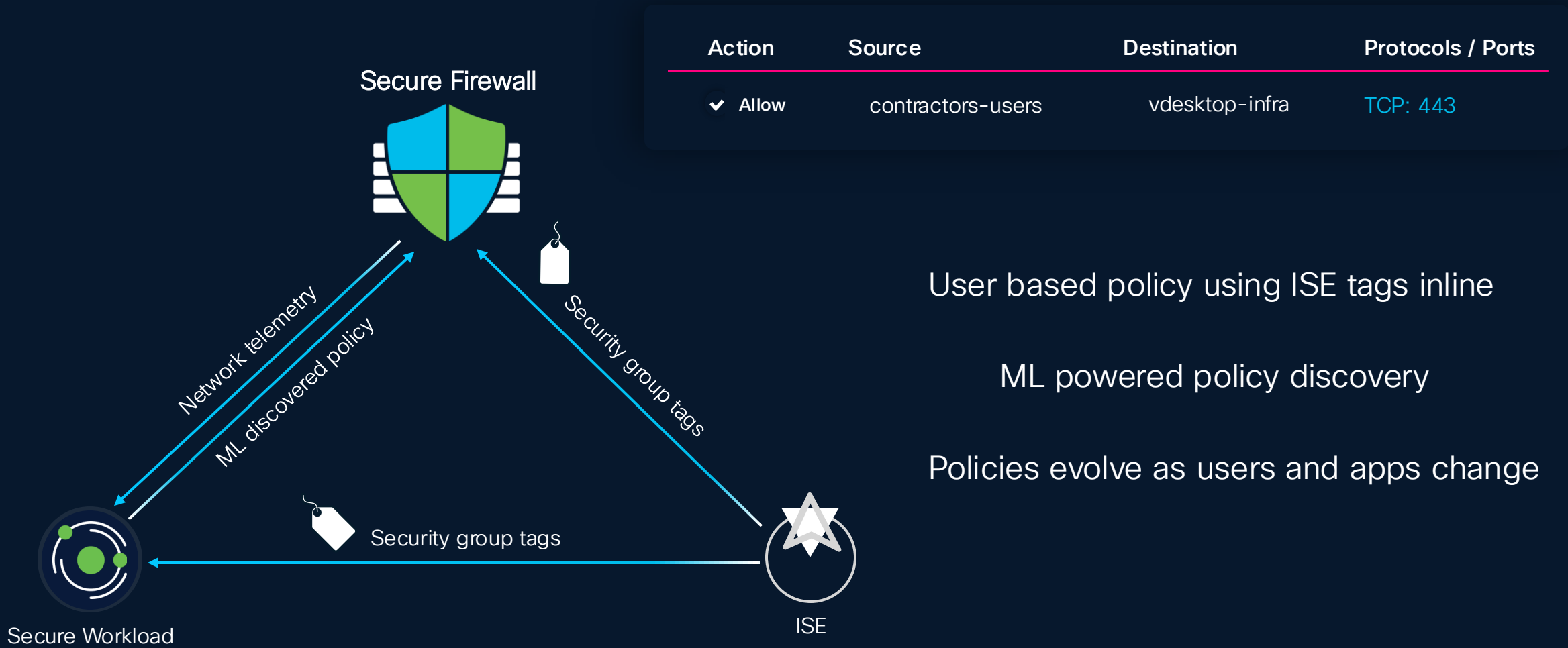
## Flow-Based Rule



## Process-Based Rule



# Smarter Firewalling with Secure Workload & ISE



# Traditional Segmentation for Workloads



All types  
of workloads

Windows | Linux | Cloud



Virtual Machine



BareMetal

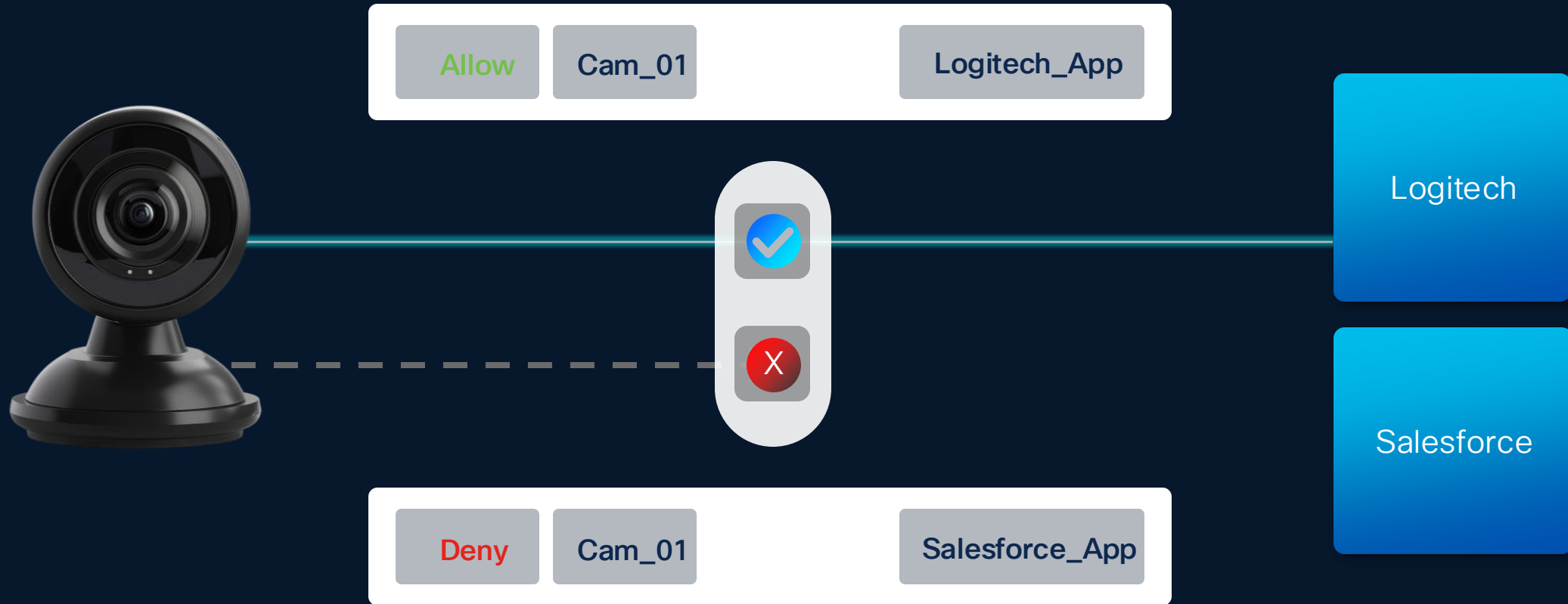
SaaS  
delivered

Get started quickly without  
hardware investment

Confident  
outcomes

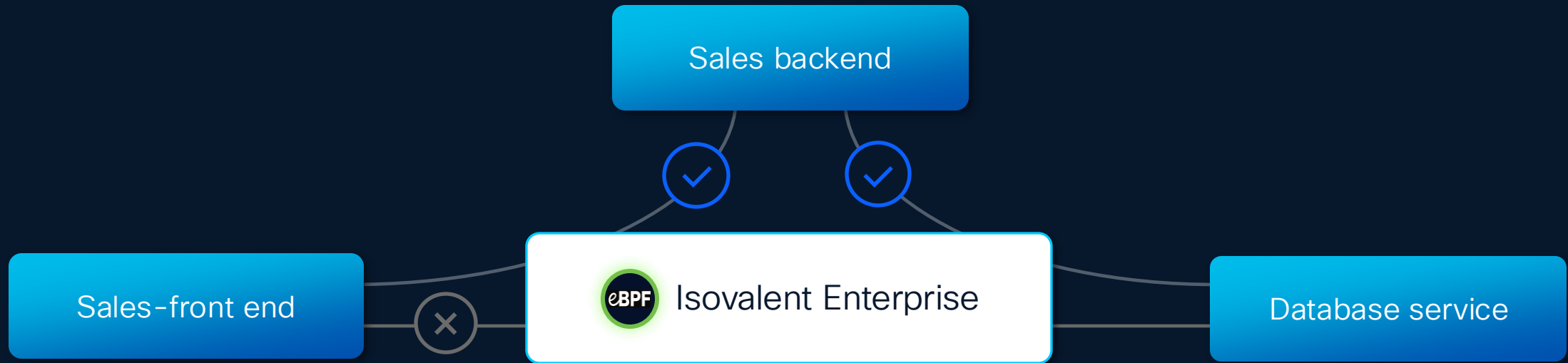
Speed up time to value  
with implementation services

# Segment IoT Devices Using ISE and Firewall





# Cloud-Native Segmentation for Kubernetes



Discover microservice  
interactions

Enforce policies in the  
Kubernetes fabric

# Advanced Threat Protection Preventing Modern Attacks

# Over 95% of data center traffic is encrypted

# Traditional Approaches to Decryption Do Not Scale





A blue circular logo with a white border and the letters 'AI' in white, positioned in the top right corner of the slide.

AI

# Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning  
(ML) technology

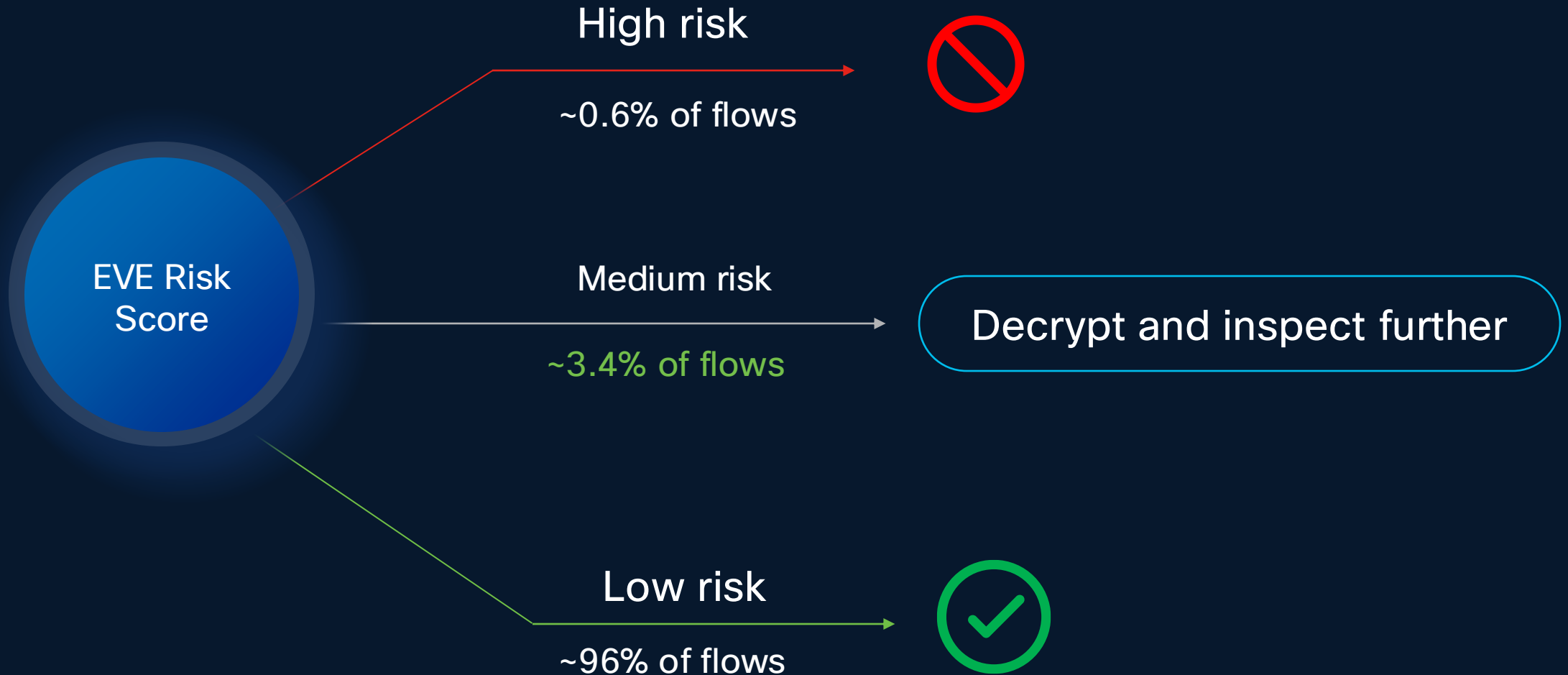
Processes **1 B+**  
TLS fingerprints

Processes **10 K+**  
malware samples daily



# Eve Changes the Game on Decryption

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



# The Leading IDPS, Now with Zero-Day Protection

Snort ML extends IDPS protection to unknown variants of common attacks



Known SQL injection attack

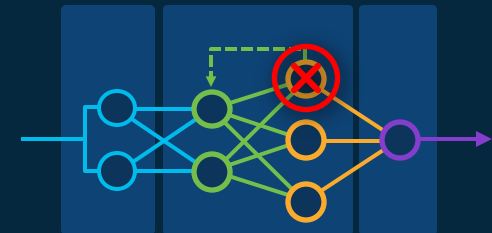
Zero-day SQL Injection variant



Snort IPS Rule



Snort ML Rule

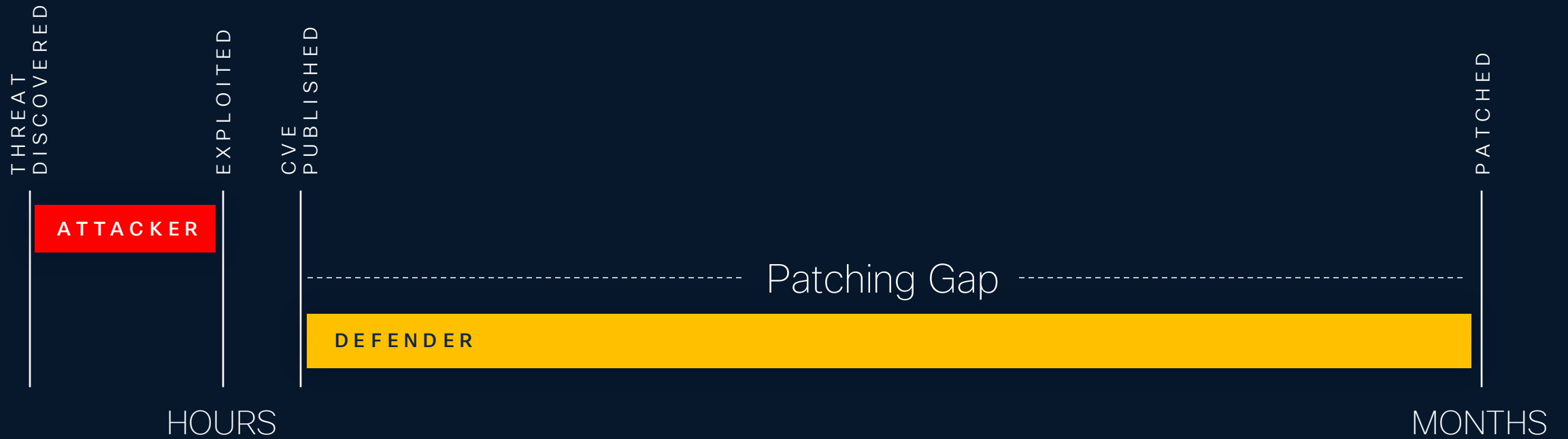


(Deep learning model)

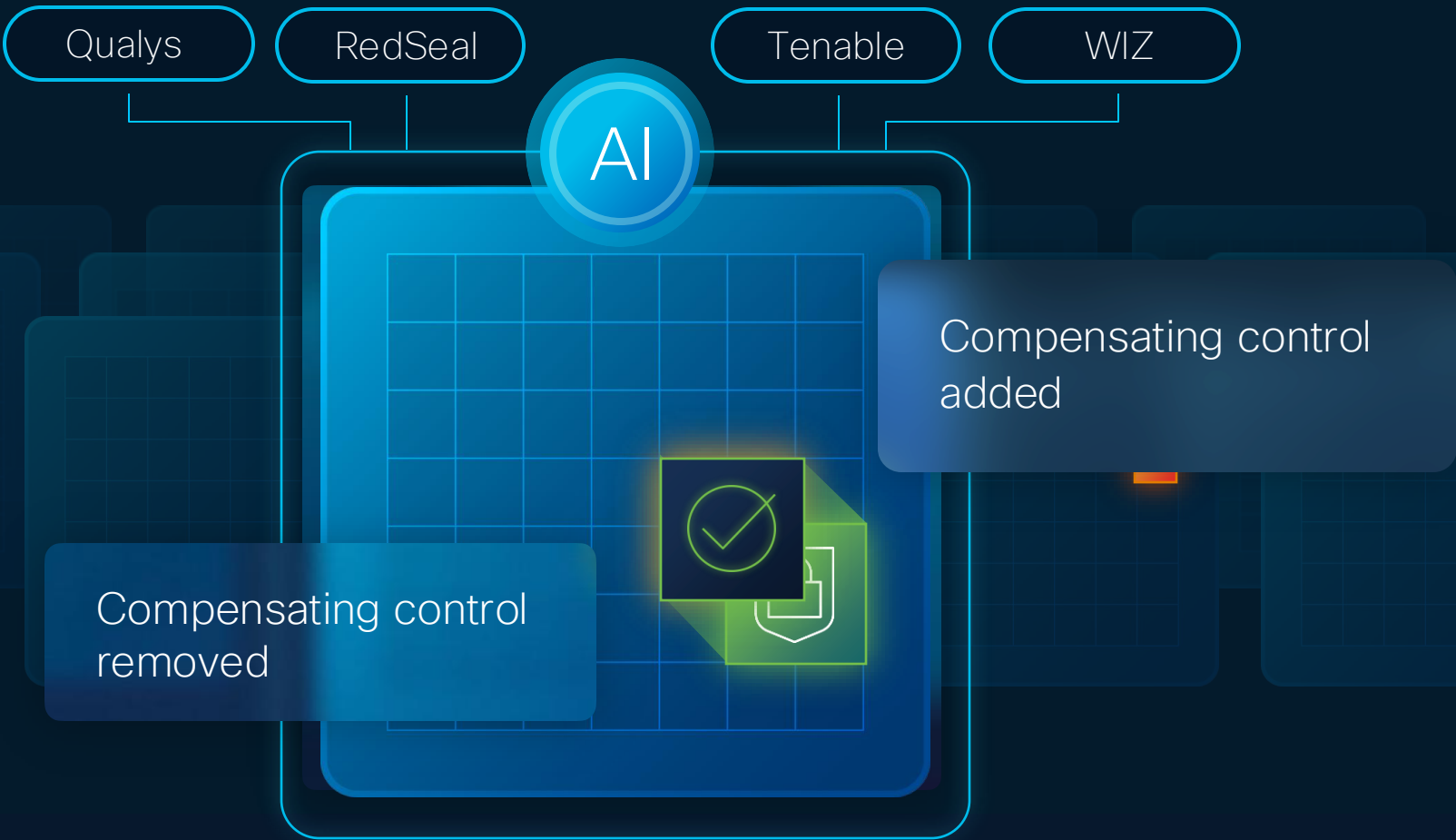
Powered by TALOS Intelligence

# Compensating Controls Distributed Exploit Protection

# Patching Is Hard



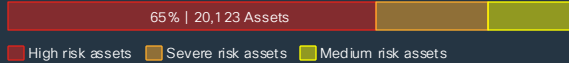
# Distributed Exploit Protection



# Closing the Exploit Gap with Automated Workflows

FUTURE

60,234 vulnerable assets



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

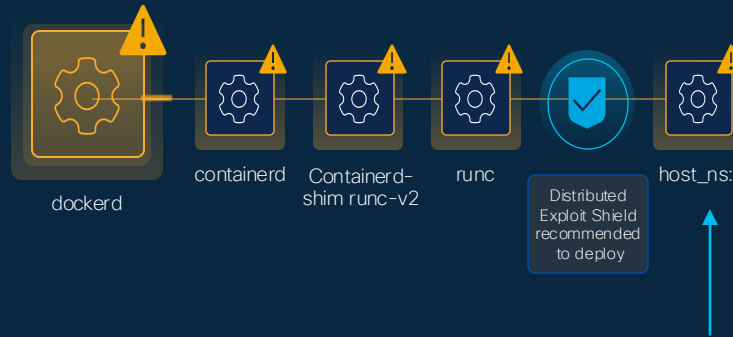
Production - External Critical Production - Internal Dev

Data-driven vulnerability prioritization

+19 threat and exploit intel feeds

+12.7B managed vulnerabilities

+1B security events processed monthly



✓ The Distributed Exploit Shield blocks new container processes with a current directory of "/" in the host name space.

✗ Block and alert

Surgical mitigating control  
that keeps application running



Confidence Score



Effectiveness Score

✓ The Distributed Exploit Shield was already tested in your environment

Tested against live production  
traffic to earn trust and  
increase confidence



# Security Cloud Control Unified Management

# Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling

AI Defense

3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield  
Secure Access (FW as a service) | Secure Router NGFW



Unified AI Assistant:  
Simplify policy administration **by up to 70%**

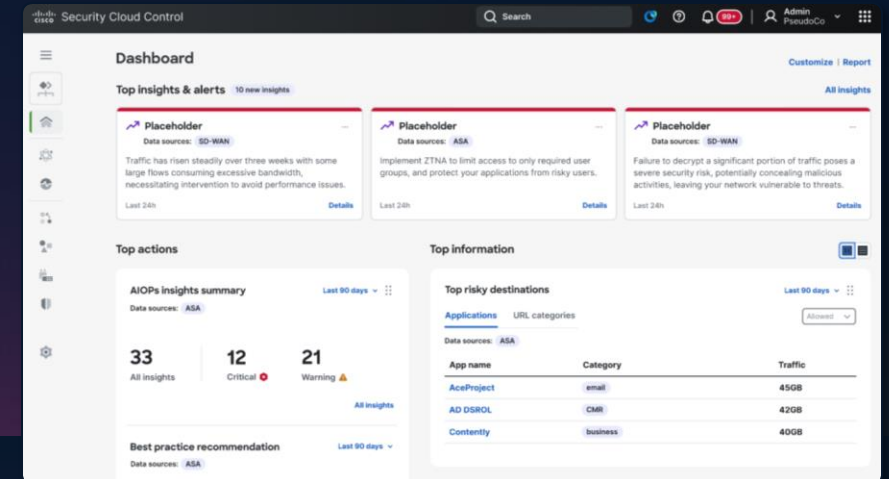
AVAILABLE AUG 2025

# Secure Router Policy Management Now in Security Cloud Control

## Cisco Secure Routers

In Security Cloud Control, you can now:

- Create objects and security policies
- Sync and manage existing secure router objects
- Create new security policies
- Visualize secure router events in SAL
- Sync RBAC model between SD-WAN Manager and Security Cloud Control



## Supported models

Cisco 1000 Series Integrated Services Routers  
Cisco 8000 Series Secure Routers



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

# Reduce Management Overhead with AI Assistant

Assist

+ Policy configuration

Augment

+ Troubleshooting

Automate

+ Policy lifecycle management

Cisco AI Assistant

You

Allow Lee access to Facebook but only from office source zone

AI Assistant

11:05 am PST

Here is your rule recommendation, This rule will be added in policy 'Test\_1' in the category, 'Geo\_Controls'.

| Rule Name   | Action | Source zone | Destination zone |
|-------------|--------|-------------|------------------|
| Rule_Test_1 | Allow  | Office      | guest_zone       |

>

AI Assistant

✓ 'Rule\_Test\_1' is successfully created in policy 'Test\_1'.

11:05 am

Congratulations, your rule named, 'Rule\_Test\_1' is successfully created in policy 'Test\_1'. The rule is created in a **disabled state** as of now. You can enable it from your 'Test\_1' policy detail page.

[Go to policy detail page](#)

Ask the AI Assistant a question

>

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

# AI Assistance When You Need It





# Safety

Cost harvesting / repurposing

Hallucinations

Hate speech

Harassment

Profanity

Sexual content & exploitation

Social division & polarization

Self-harm

Disinformation

Environmental harm

Violence

Non-violent crime

Scams & deception

Financial harm

Off-topic

Cost harvesting / repurposing

Cost harvesting / repurposing

Profanity

Harassment

**Hallucinations**

Hate speech

Off-topic

**Toxicity**

Social division & polarization

**Self-harm**

Financial harm

# Security

Exfiltration from ML application

IP theft

Model theft

Meta prompt extraction

Infrastructure compromise

Model compromise

Training data poisoning

Targeted poisoning

Prompt injection

Indirect prompt injection

SQL injection

Command execution

Cross-site scripting

Model vulnerabilities

Model denial of service

Application denial of service

Indirect prompt injection

**Infrastructure compromise**

IP theft

Meta prompt extraction

**Prompt injection**

Model theft

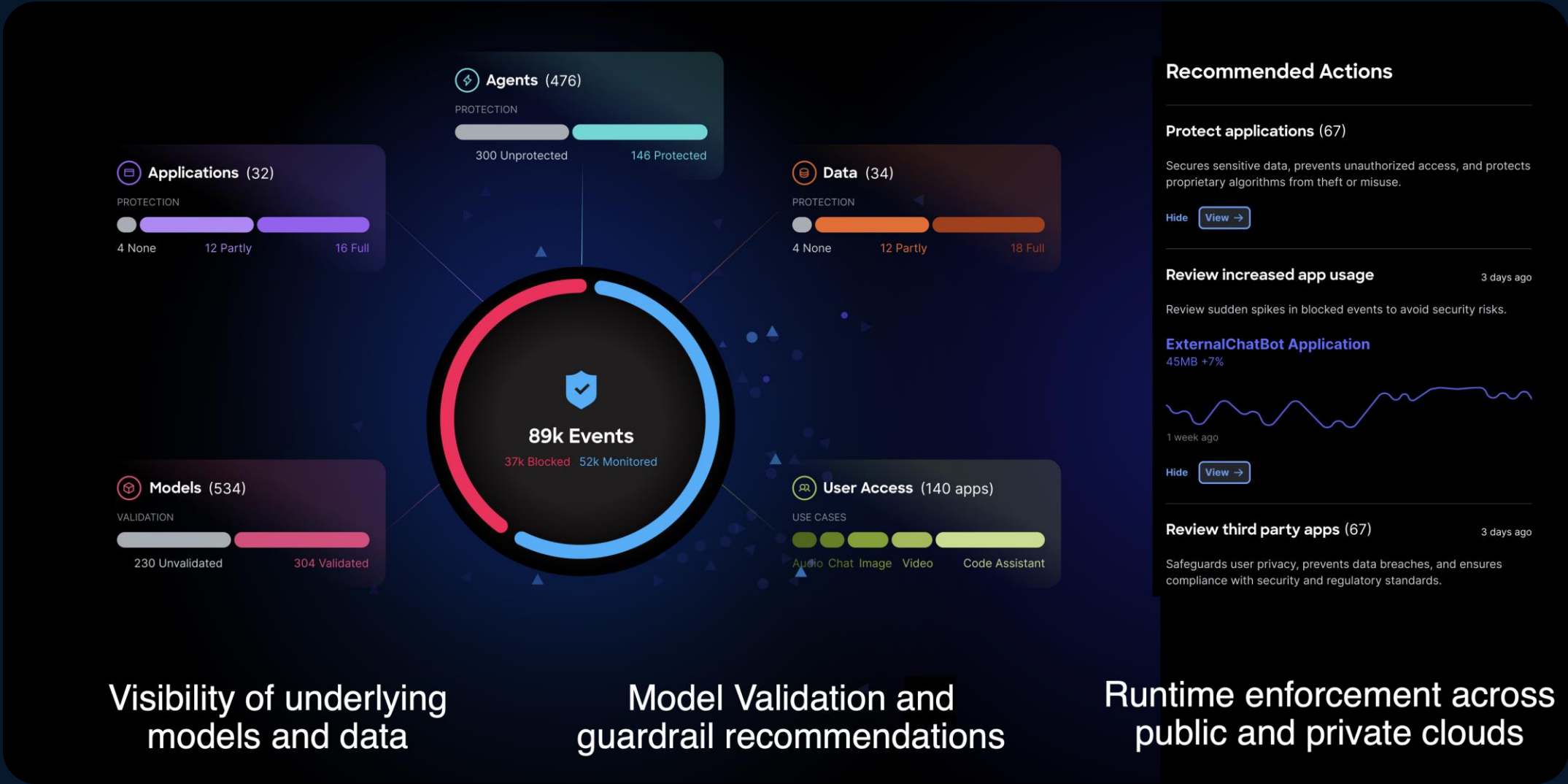
**Training data poisoning**

Sensitive information disclosure

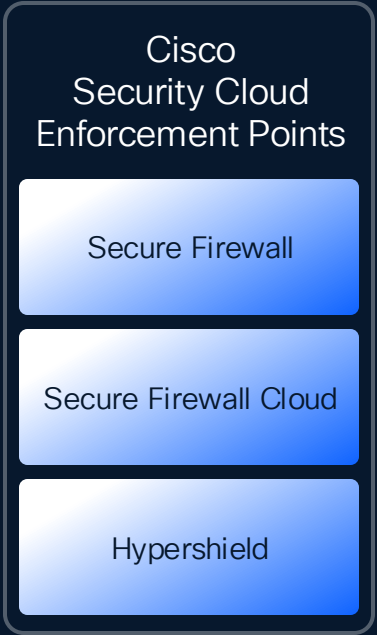
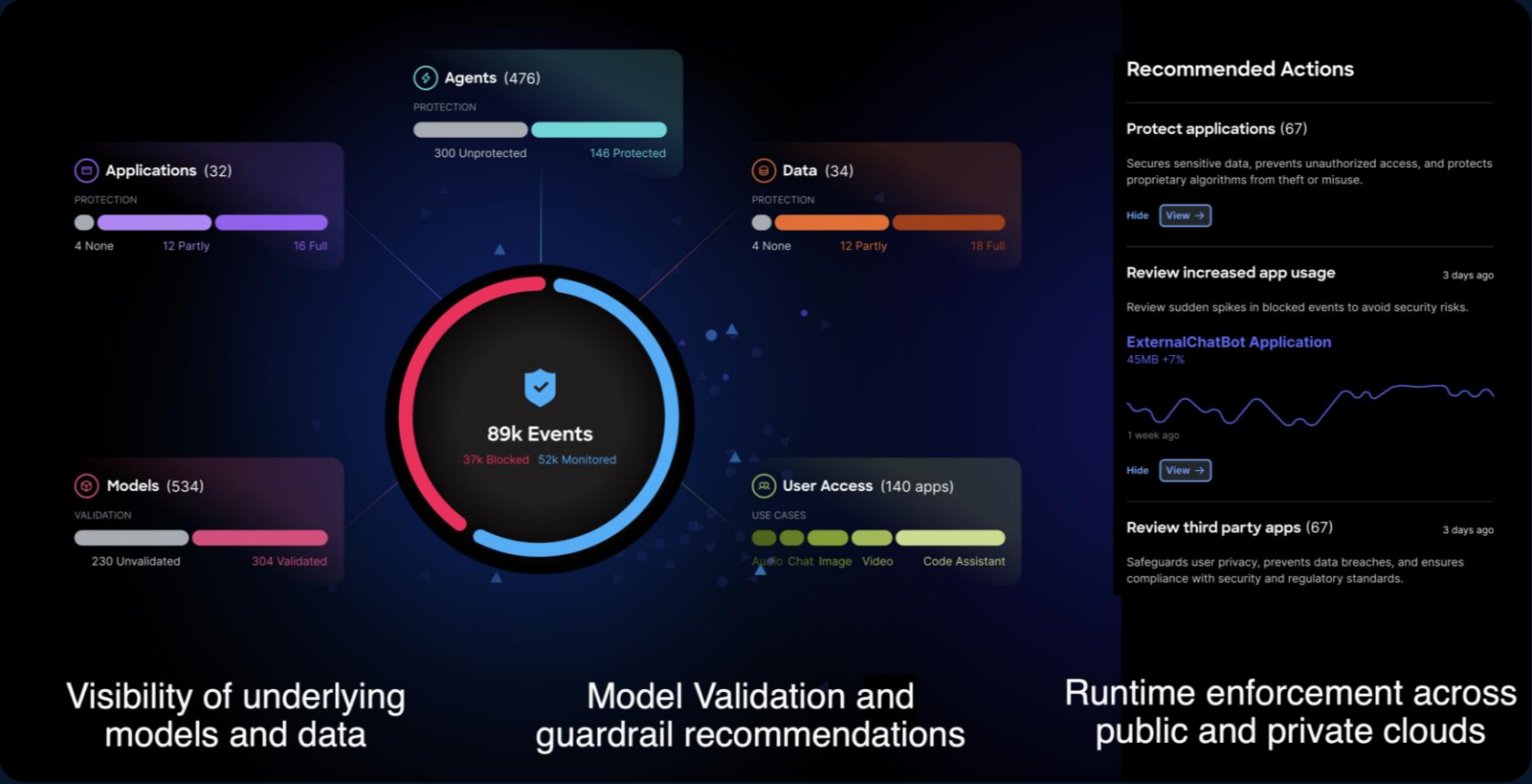
Data exfiltration

Model denial of service

# AI Defense



# Delivered Via the Hybrid Firewall



# 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

# Conclusion

- Lateral movement equals success for the adversary
- Hybrid Mesh Firewall is not all the same
- Zero trust is achievable with prescriptive based outcomes
- Secure Cloud Controller unifies and simplifies controls
- AI augmentation drives better outcomes
- Visibility, policy, simulation, enforcement, compliance



Possible when Powered with AI

**Thank you**





