

Redefining Security with Cisco Hybrid Mesh Firewall

Anshul Kaushik, Cybersecurity Architect- ANZ Channels
ankaushi@cisco.com

Awais Khan, Cybersecurity Architect- ANZ Channels
awakhan@cisco.com



Securing the enterprise is increasingly challenging

Highly distributed applications

Nothing can be trusted

More vulnerabilities, exploited faster

← AI adoption makes it more challenging →

Hybrid Security



Customers

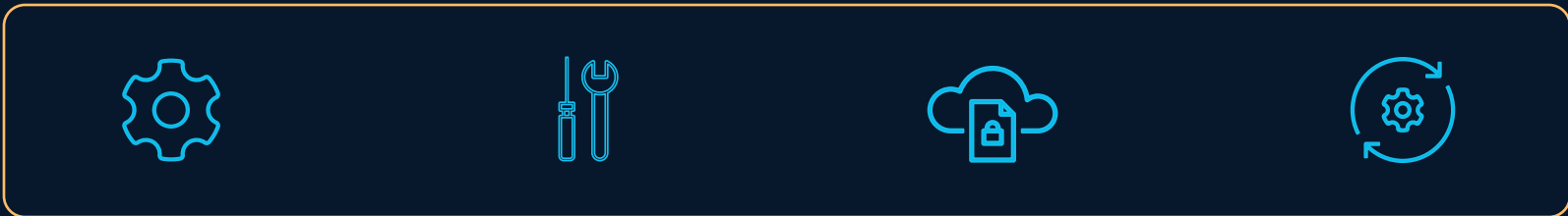
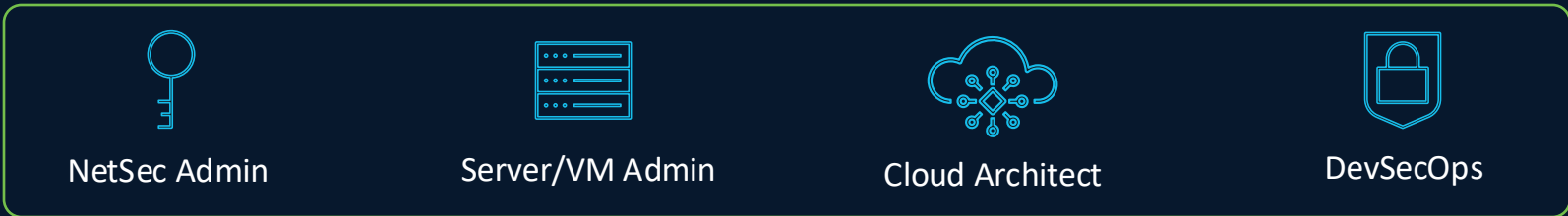
Industry/Analyst

Vendors

Hybrid Security = Hybrid Mesh Firewall

A **Hybrid Mesh Firewall** is a multideployment firewall platform with centralized cloud-based management, designed for hybrid environments. It integrates with CI/CD pipelines, supports cloud-native features, and provides advanced threat protection across diverse use cases, including IoT and DNS-based threats.

Hybrid Mesh Firewall – Why the need?



Organizational Challenges

Multiple teams, organizations and environments

Inconsistent islands of policy controls across environments

Gartner – Hybrid Mesh Firewall

Core & Optional Capabilities



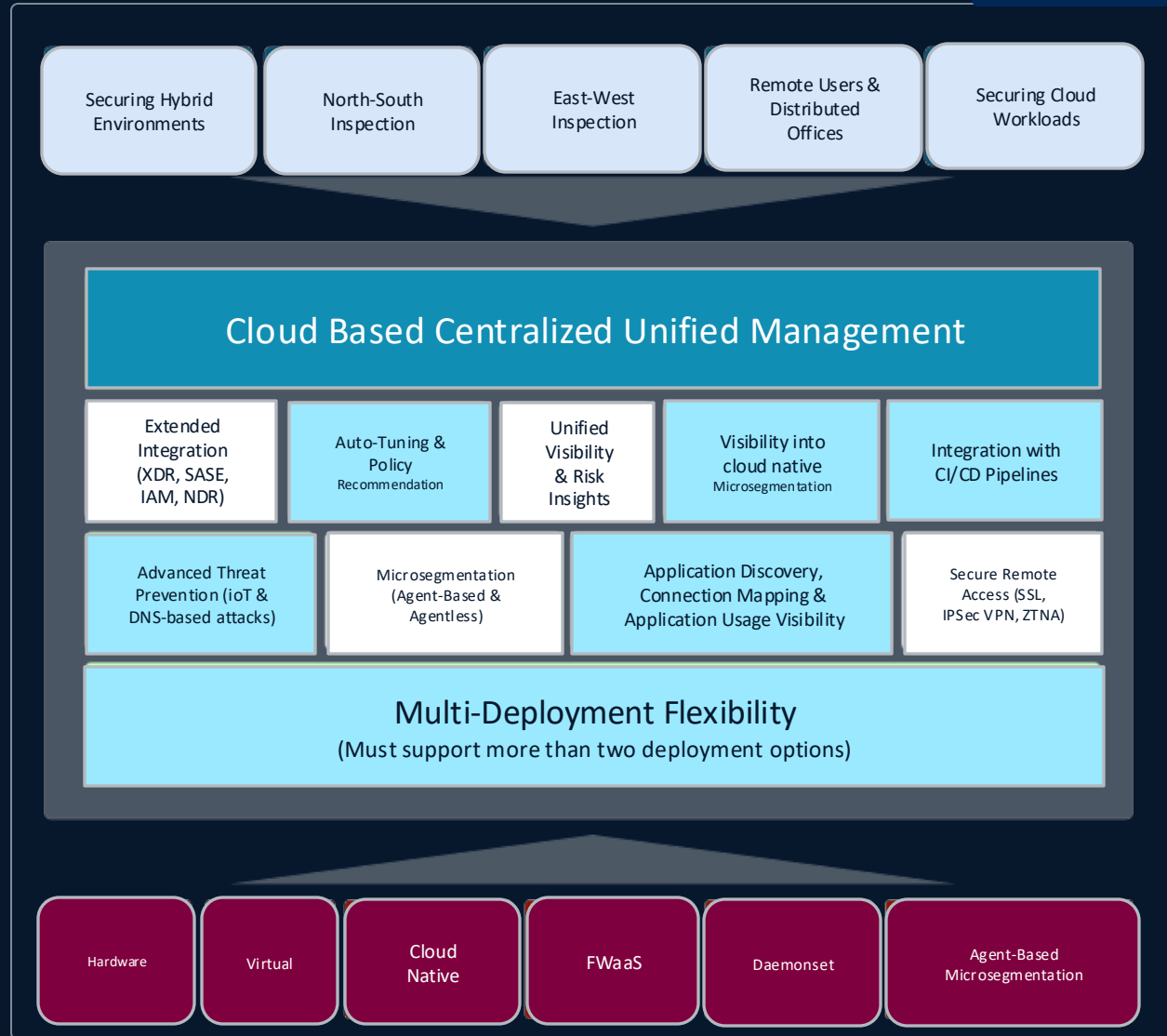

Gartner

Market Guide for Hybrid Mesh Firewall Platforms

Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hills

Initiatives: [Infrastructure Security](#); [Build and Optimize Cybersecurity Programs](#)



Cisco's Hybrid Mesh Firewall: Vision & Foundation

Firewalling needs to evolve to meet today's challenges

Our North Star

Make it easy for organizations to

Reduce attack surface

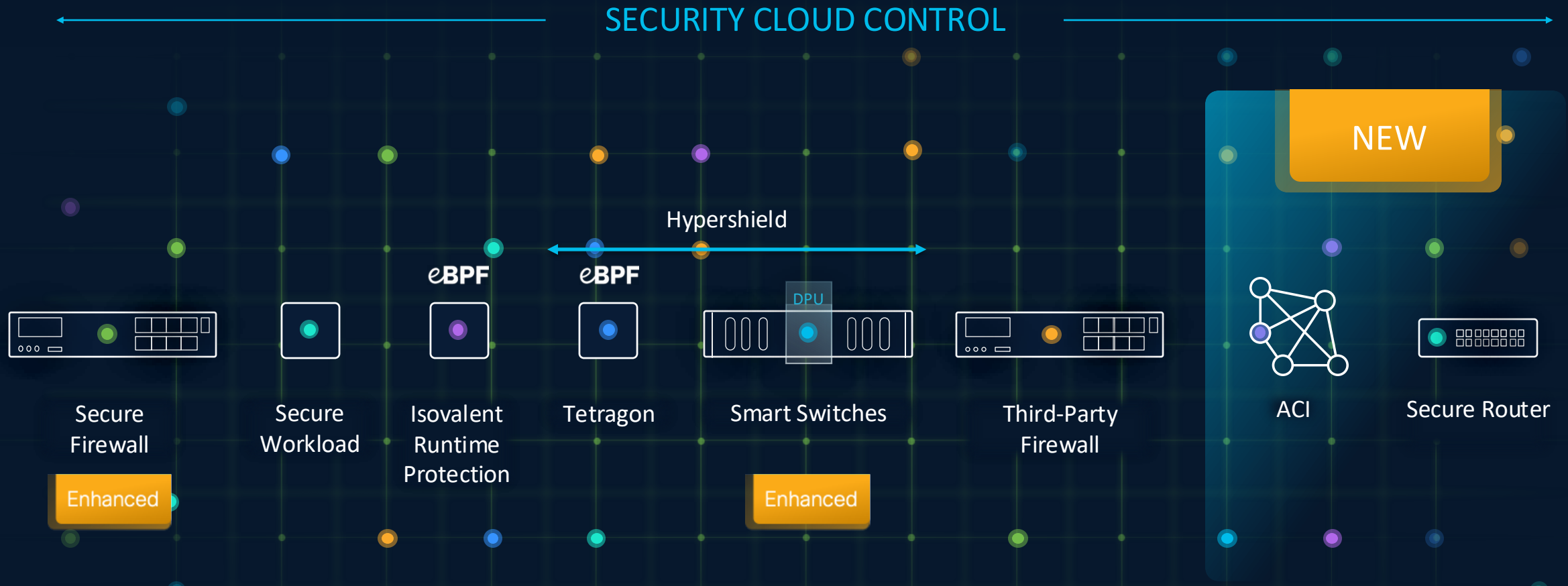
Prevent compromise

Stop lateral movement

in the modern data center, cloud, campus,
and factory

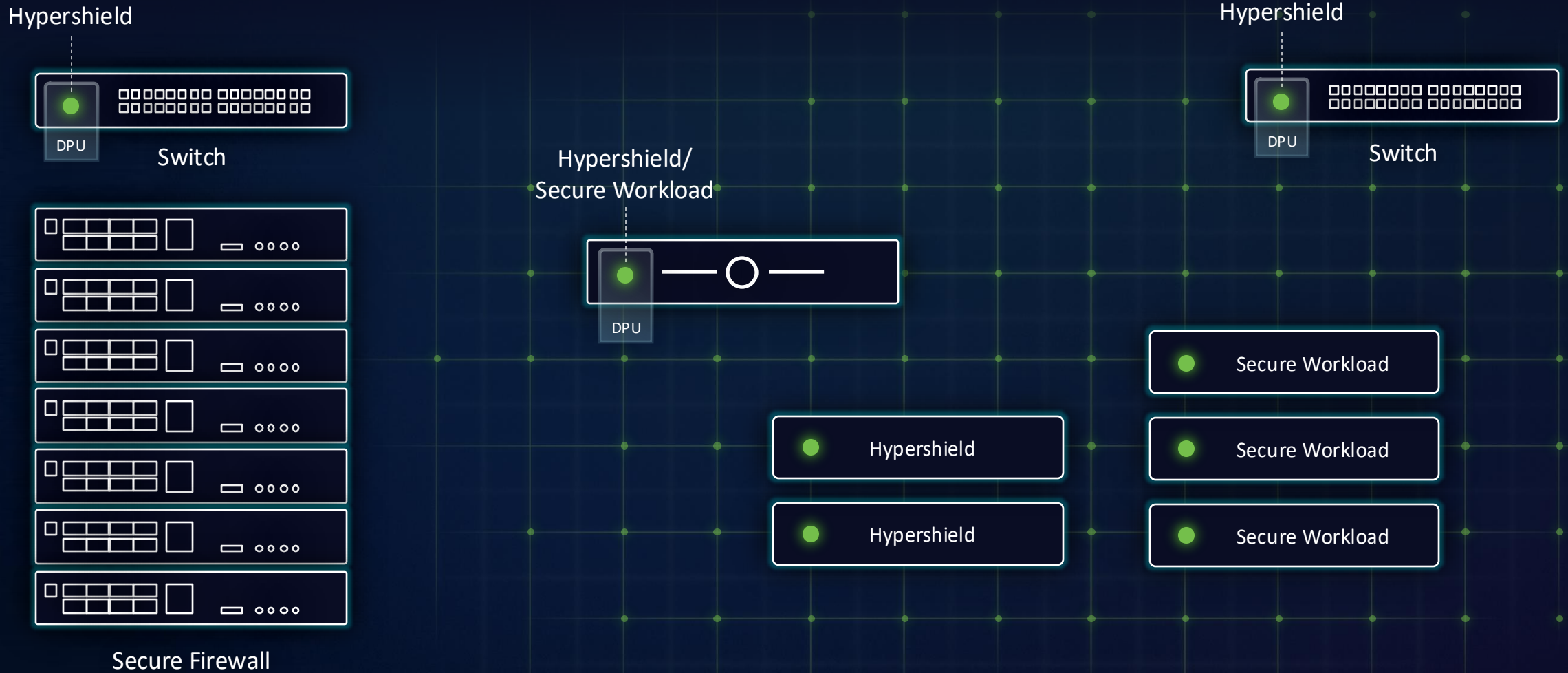


Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

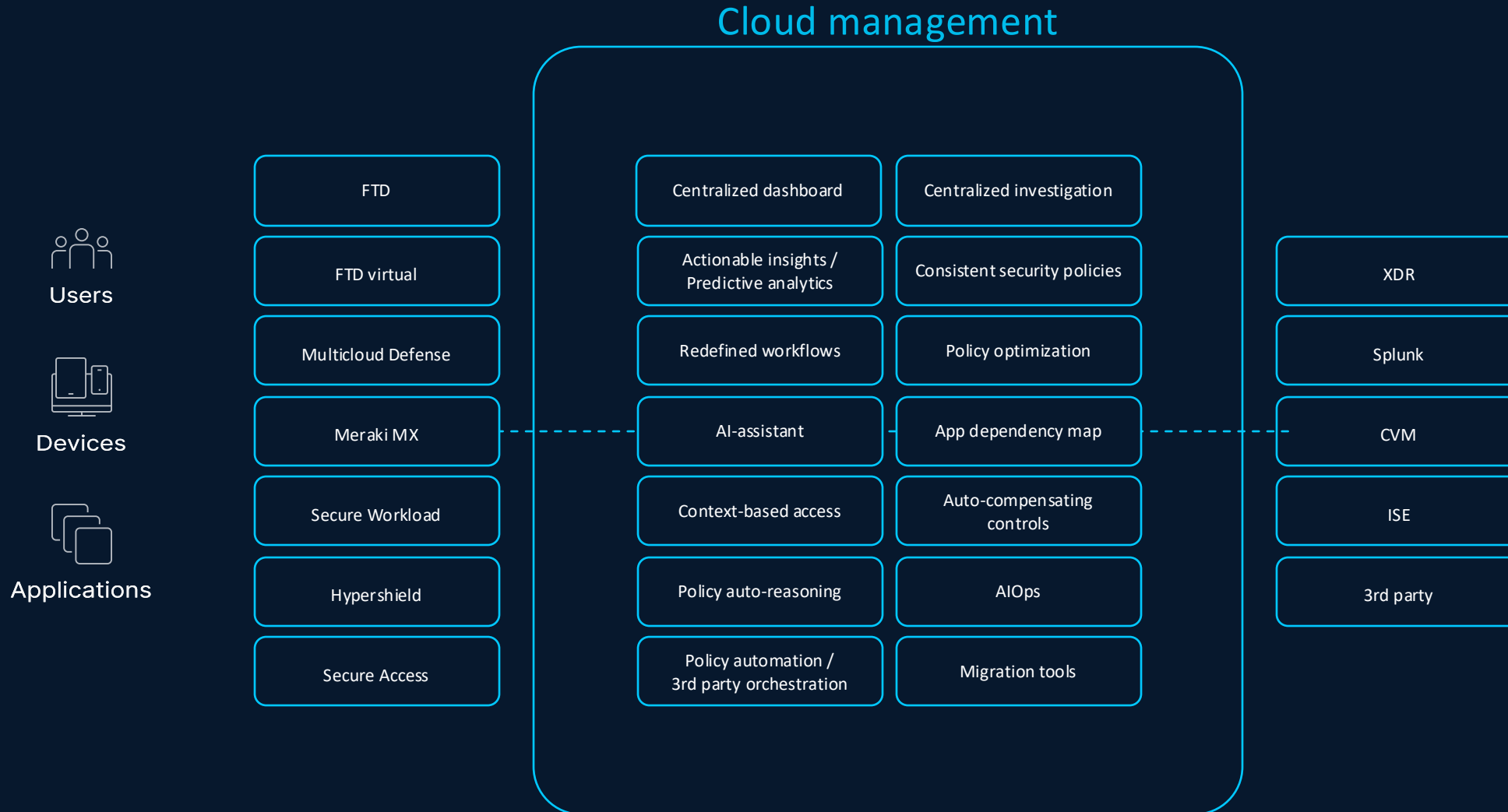
Security Cloud Control



Enforcement points change, rules don't

Introducing Cisco Security Cloud

Unified security platform



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. At the top, the Cisco logo and 'Security Cloud Control' are visible. A search bar contains the text 'Type 'Ctrl' + '/' to search'. The user profile 'Carter Briggs' is shown in the top right. The left navigation pane (Side Nav) includes an 'Organization Switcher' for 'Stark Enterprises - North America', a 'Home' button, and a 'Products' menu with items like AI Defense, Firewall, Hypershield, Multicloud Defense, Secure Access, and Secure Workload. Below this is a 'Platform services' menu with Favorites, Security Devices, Shared Objects, and Platform Management. The main content area (Top Nav) features a 'Home' section with 'Top insights & alerts' (10 new insights) and two 'Micro App' widgets. The first Micro App shows 'Elephant flow spike observed' and 'Risky users accessing privileged apps'. The second Micro App shows '1% Decrypted traffic towards internet'. A 'Configure Secure Access' notification is present. The bottom section, 'Asset connectivity status', features a donut chart showing 15% disconnected assets (up 8% since yesterday) and a table of disconnected assets.

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	—

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

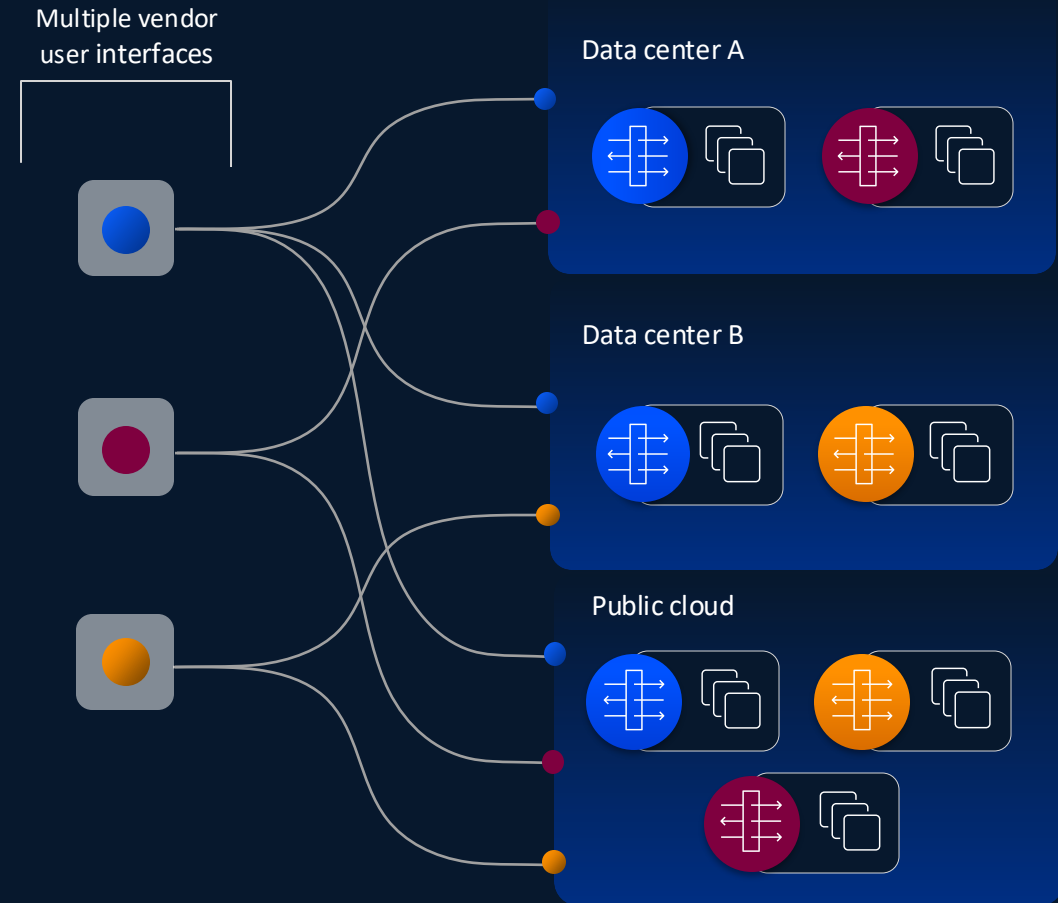
Cisco Mesh Policy Engine

Today, firewall policy management is fragmented

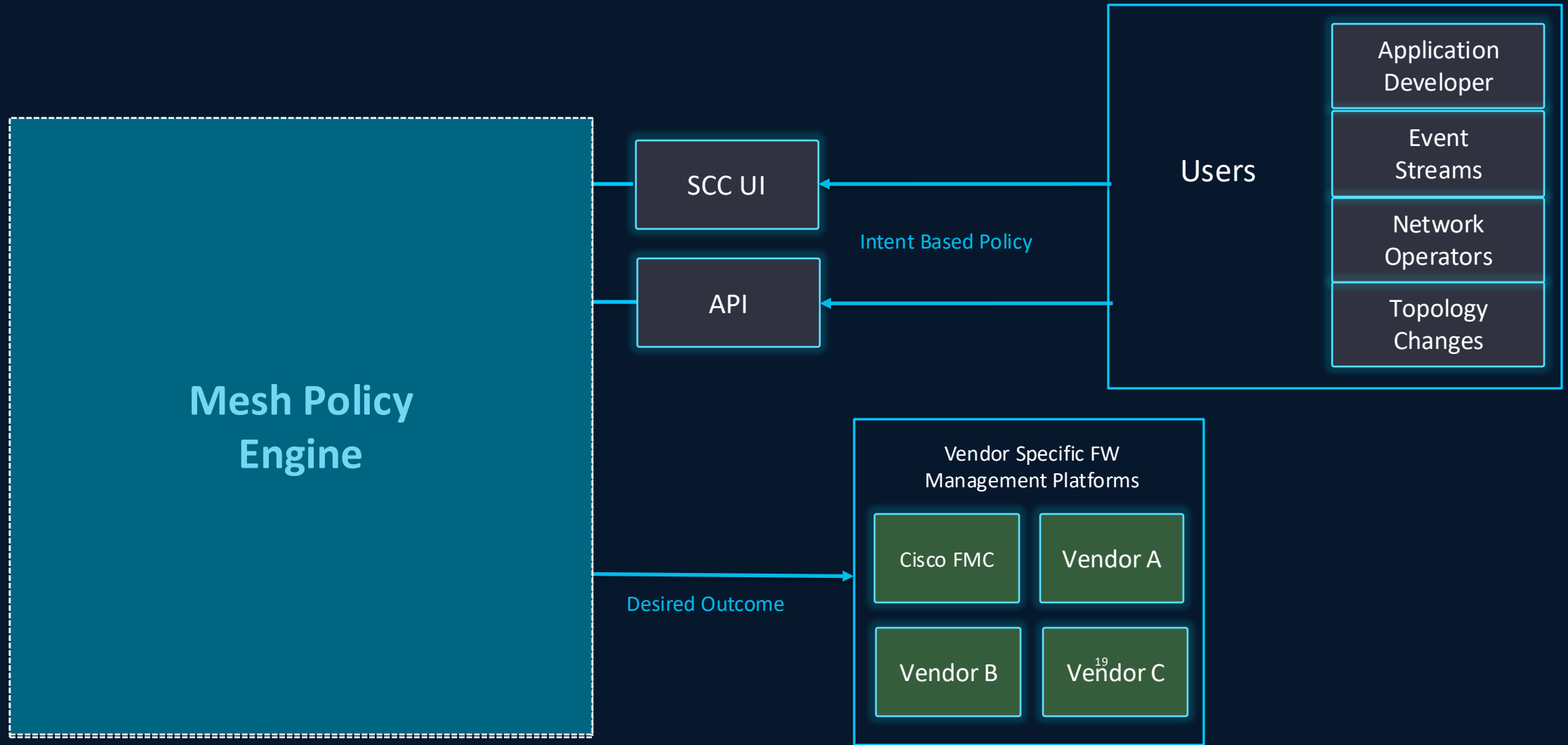
Traditional policy management

- Policy configuration is device-by-device
- Translating one intent to multiple policies across vendors takes time and is error-prone
- Adding firewall devices over time makes the problem exponentially worse

Solving these challenges requires a different approach



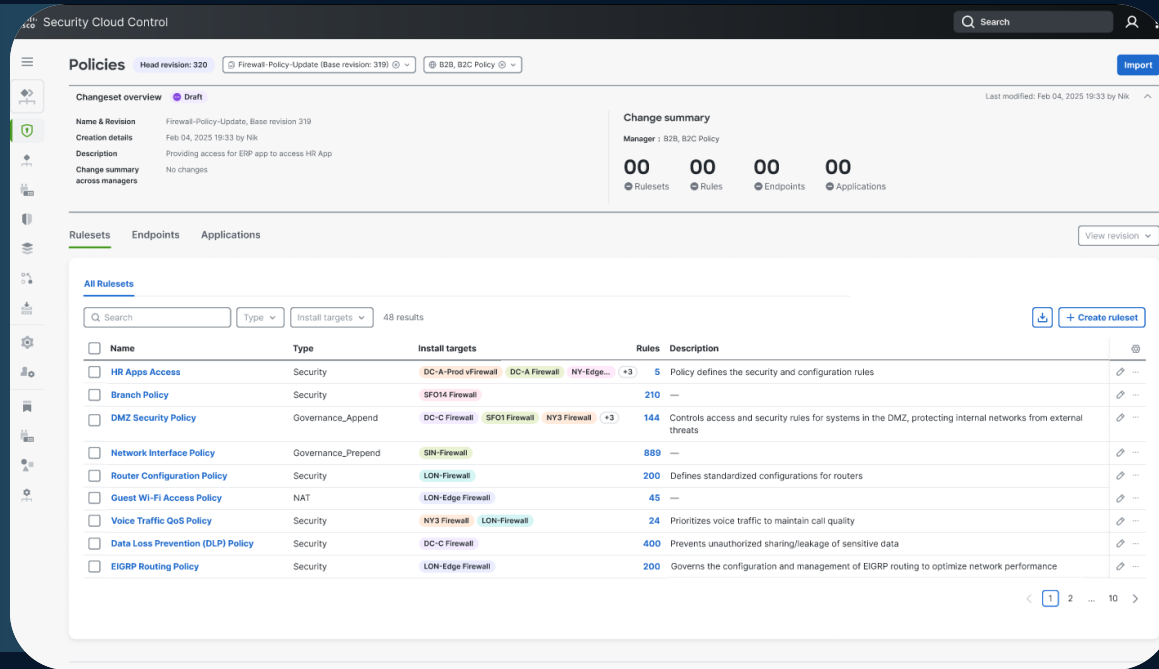
Policy Workflow & Architecture



Cisco 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

Data center A



Data center B



Public cloud



Program once, enforce everywhere

The screenshot displays the Cisco Security Cloud Control interface for creating a new rule. The rule is titled "ERP-to-HR app" and is currently in a "Draft" state. It is associated with the "Firewall-Policy-Update (Base revision: 319)" policy. The rule is enabled, with logging turned on and a time range set. The rule's order is 01, and its description is "Controls traffic flowing from ERP to HR Application".

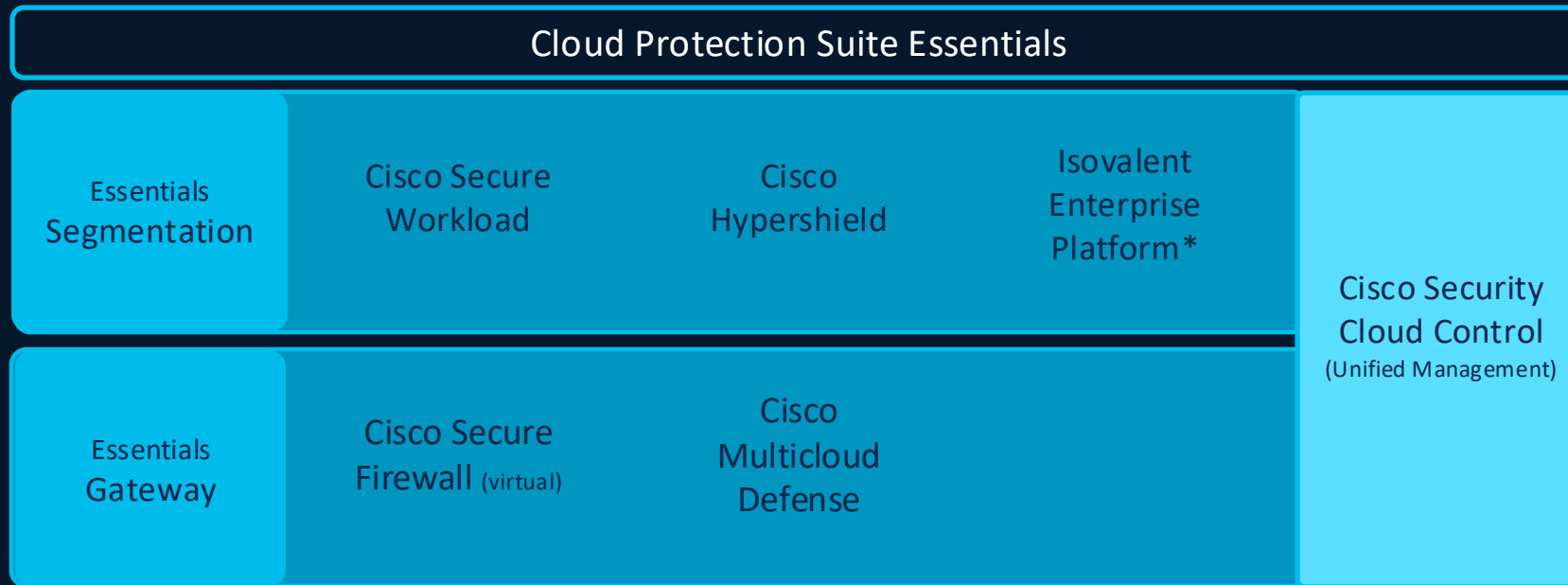
The "Review Deployment and impact" section shows a network topology diagram. The diagram is divided into three main segments: "Public Cloud", "Data Center_A", and "App Zone". In the "Public Cloud" segment, there is an "ERP" application and a "Cloud Edge Firewall". In the "Data Center_A" segment, there is a "DC-A Firewall". In the "App Zone" segment, there is a "DC-A-App vFirewall" and an "HR App". Arrows indicate the flow of traffic from the ERP application through the Cloud Edge Firewall, then through the DC-A Firewall, and finally through the DC-A-App vFirewall to the HR App.

Mesh Policy Engine intelligently understands your network topology to place the most effective policy on the relevant firewalls

1. Describe rule name and purpose
2. Define user and endpoint access
3. Deploy across network topology

Cisco Cloud Protection Suite

Simplicity, flexibility, and investment protection for easy adoption of Hybrid Mesh Firewall



*Not accessible via Security Cloud Control at this time

Cloud Protection Suite

Gateways

Workloads

Secure
Firewall

Multicloud
Defense

Secure
Workload

Isovalent
Enterprise

Hypershield

Key Takeaways

- ❖ **Micro-Perimeter Security:** Moves beyond traditional perimeters to secure hybrid cloud, containers, and SDNs
- ❖ **Unified, Distributed Firewall:** Centrally managed security across dynamic, distributed environments.
- ❖ **AI-Driven Protection:** Uses AI to detect and respond to evolving threats.
- ❖ **Consistent Policy & Integration:** Ensures unified governance and streamlined operations.

Thank you