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

July 2025

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

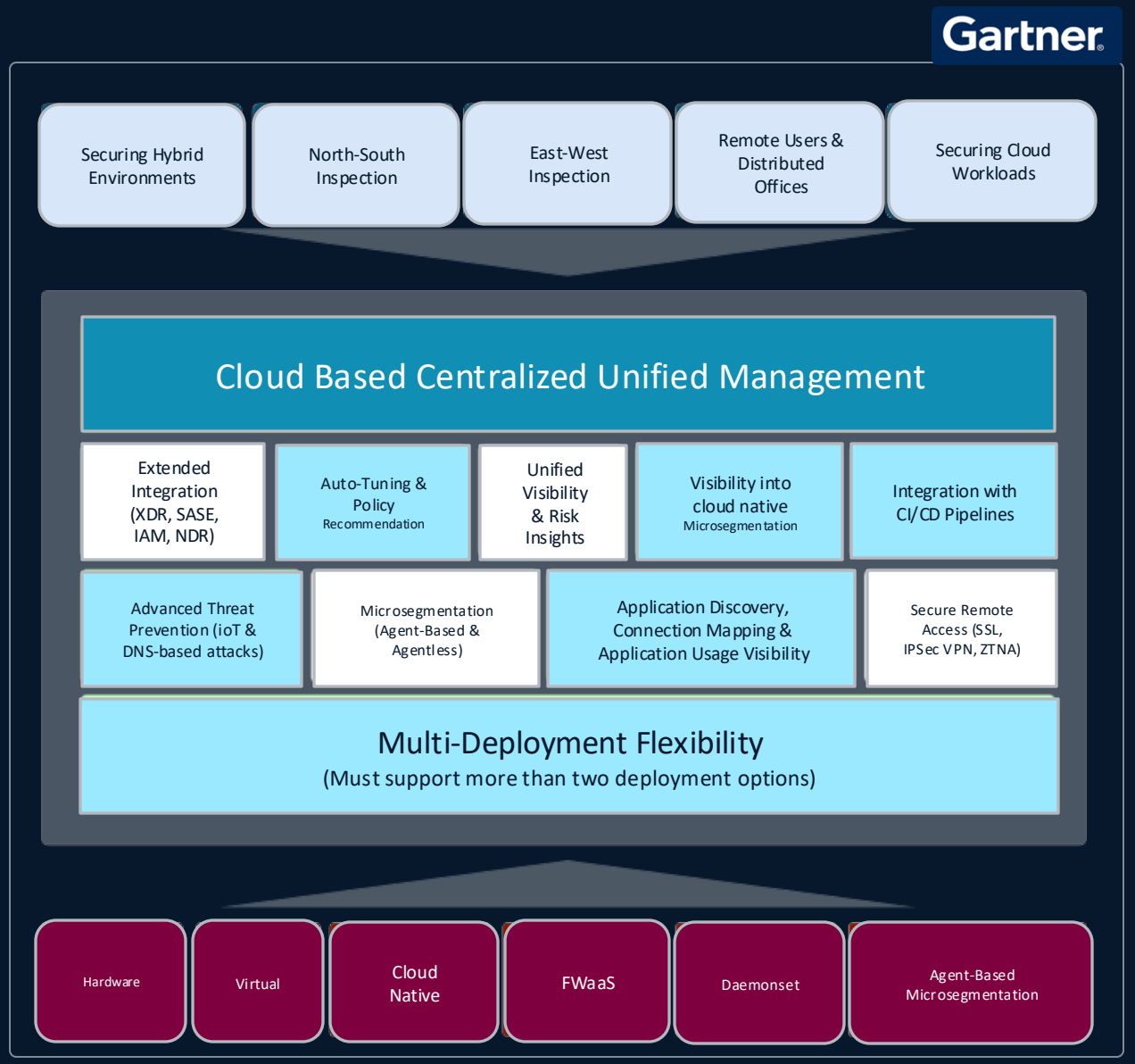
Gartner

Market Guide for Hybrid Mesh Firewall Platforms

Published 16 January 2024 - ID G00794201 - 15 min read

By Analyst(s): Rajpreet Kaur, Adam Hils

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs



Cisco’s Hybrid Mesh Firewall: Vision & Foundation

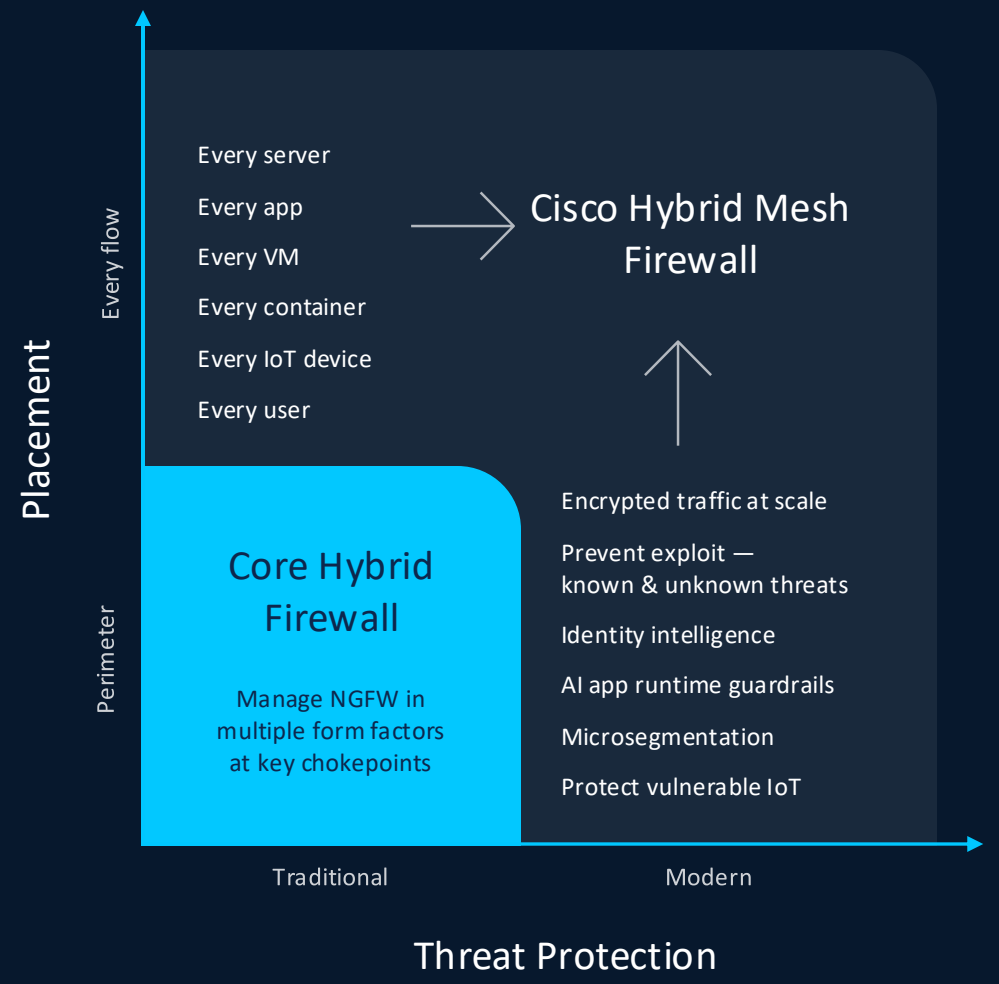
Firewalling needs to evolve to meet today’s challenges

Our North Star

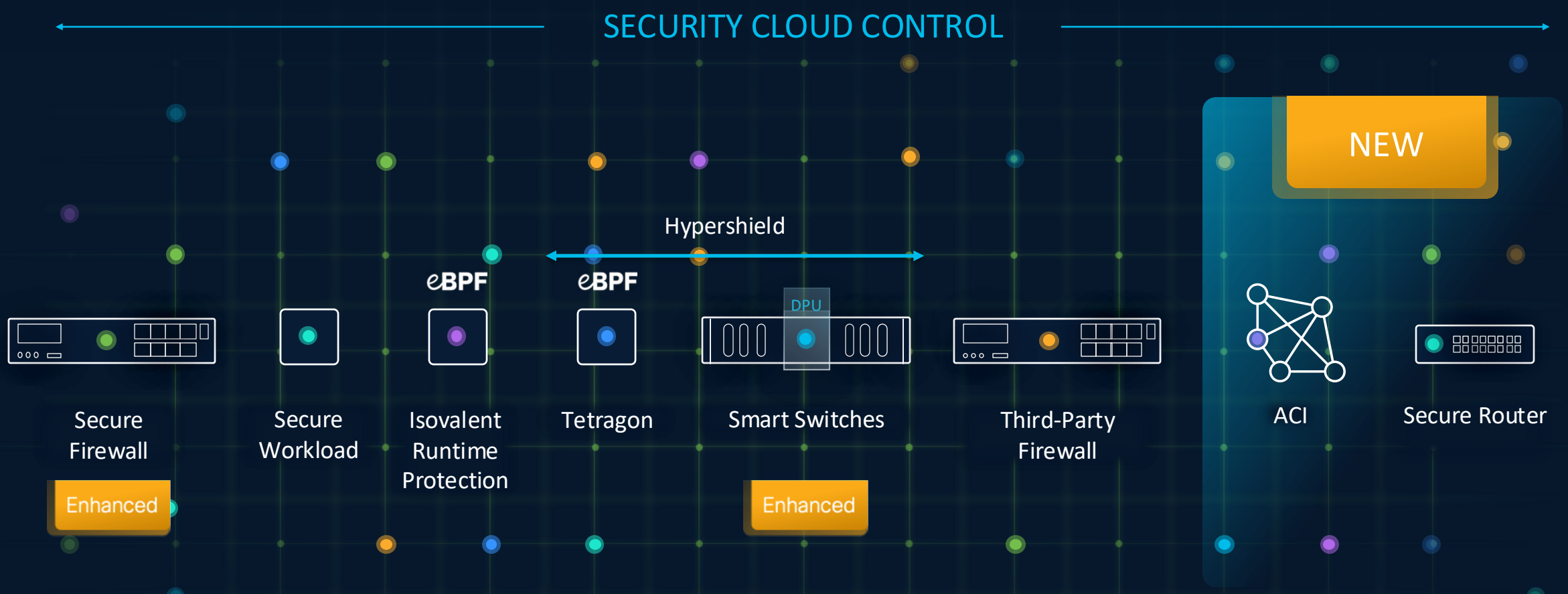
Make it easy for organizations to

- Reduce attack surface
- Prevent compromise
- Stop lateral movement

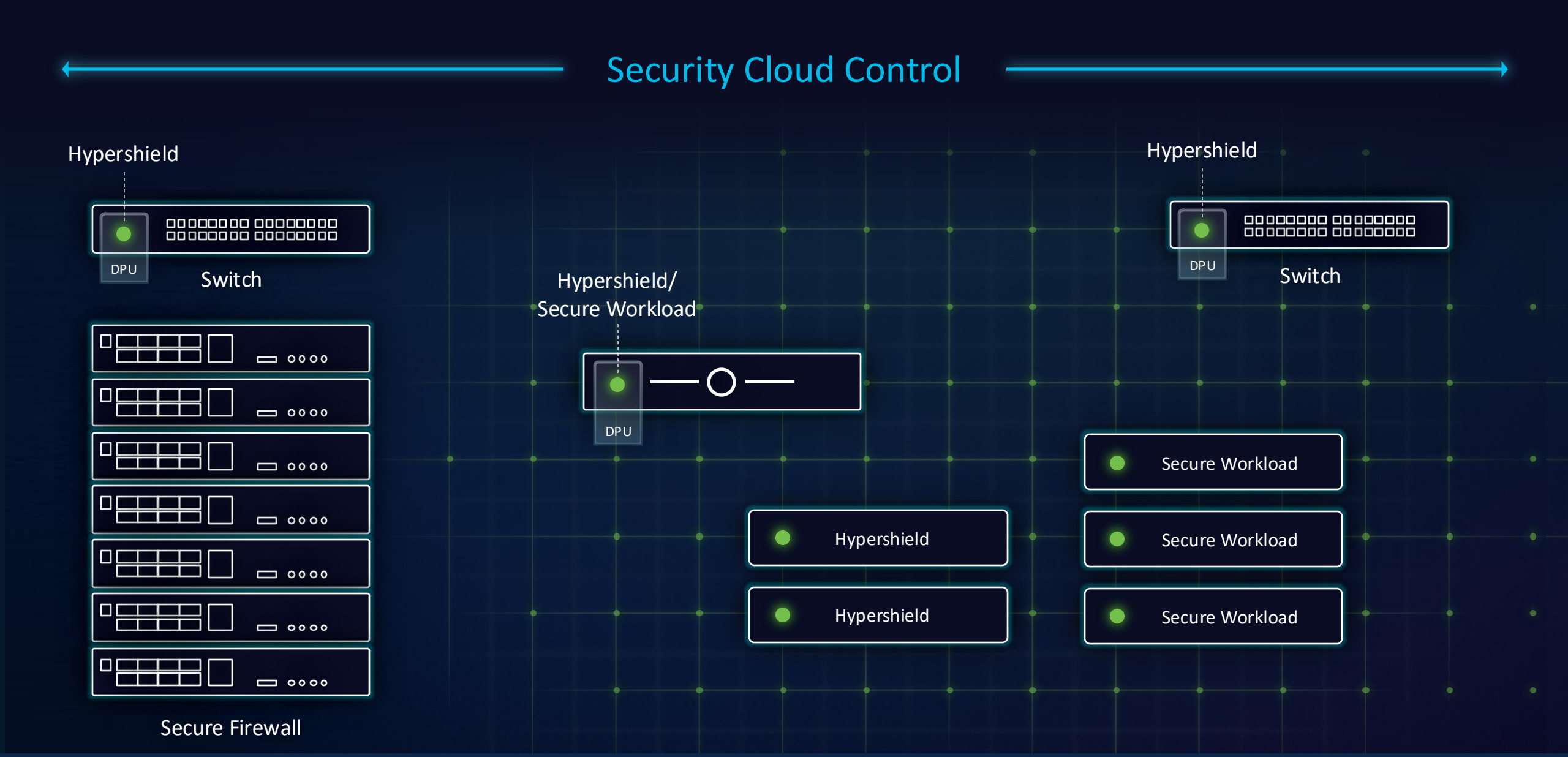
in the modern data center, cloud, campus, and factory



Cisco Hybrid Mesh Firewall



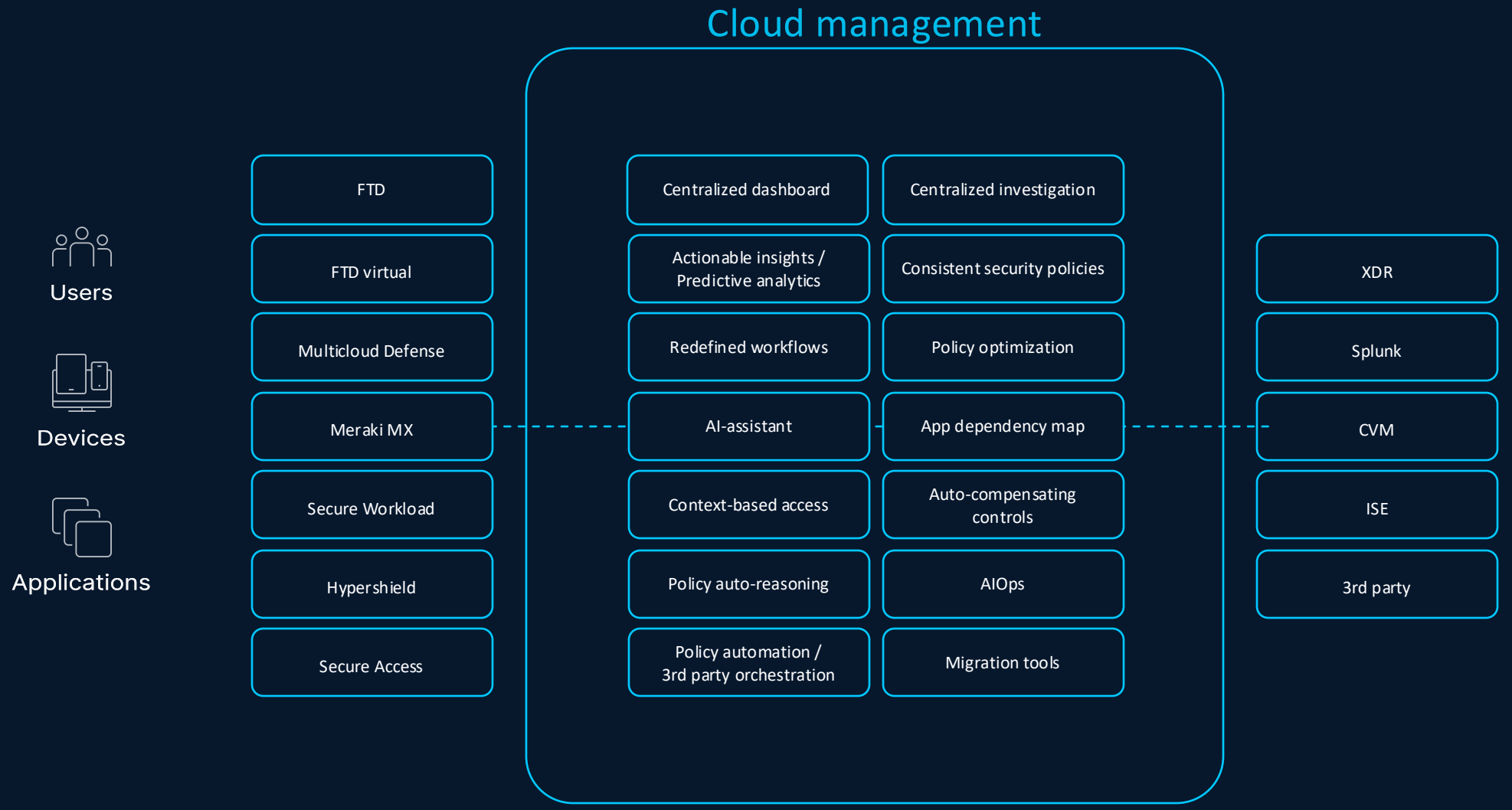
Write policy once, enforce across the mesh



Enforcement points change, rules don’t

Introducing Cisco Security Cloud

Unified security platform

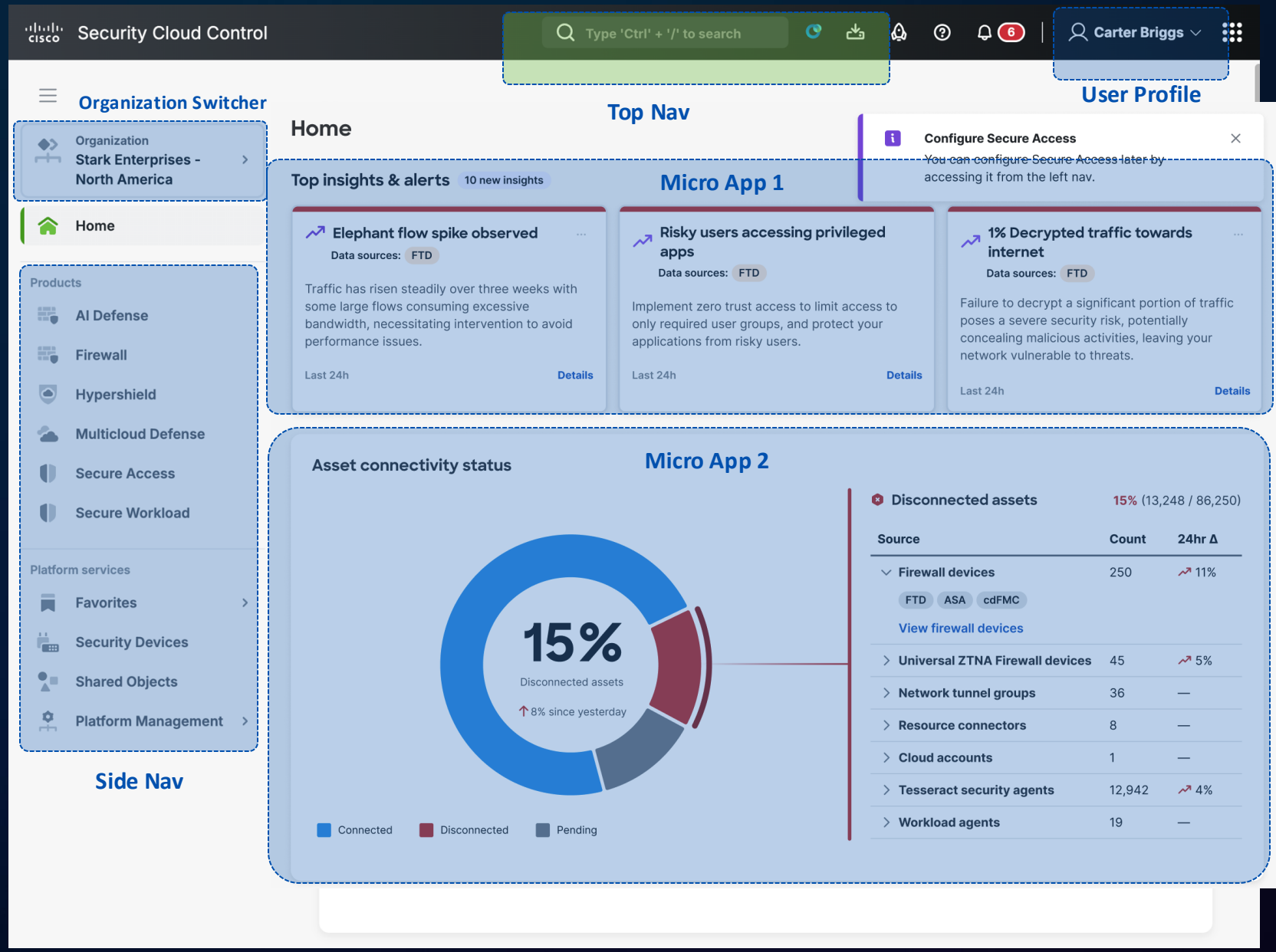


Cisco Security Cloud Control

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



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

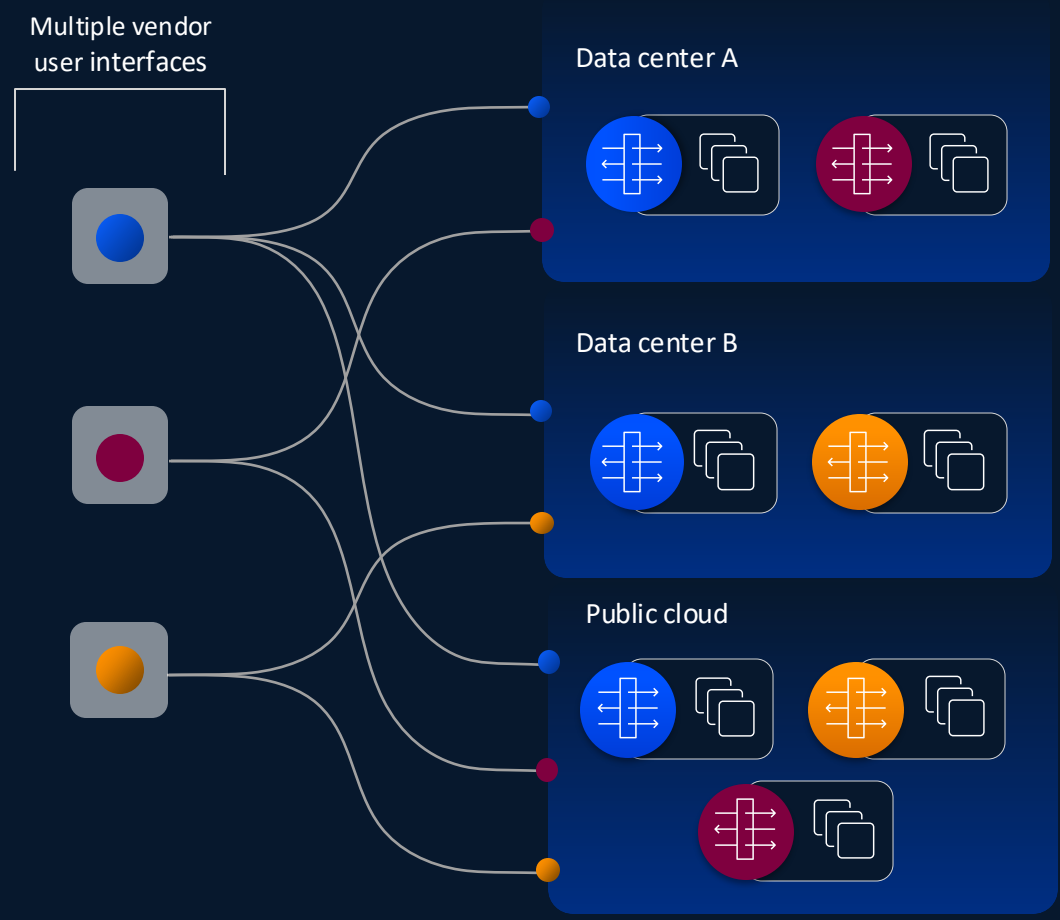
Cisco Mesh Policy Engine

Today, firewall policy management is fragmented

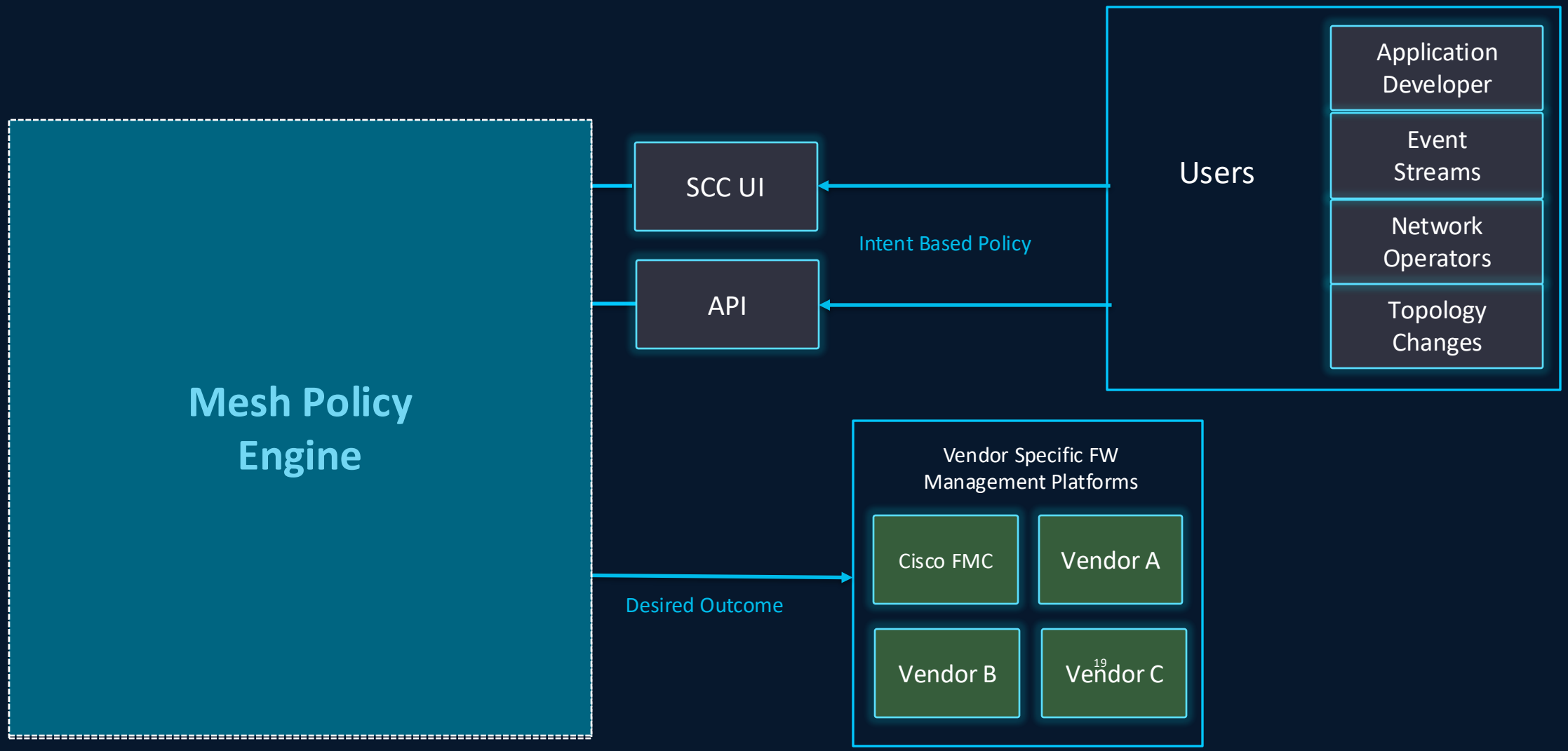
Traditional policy management

- 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



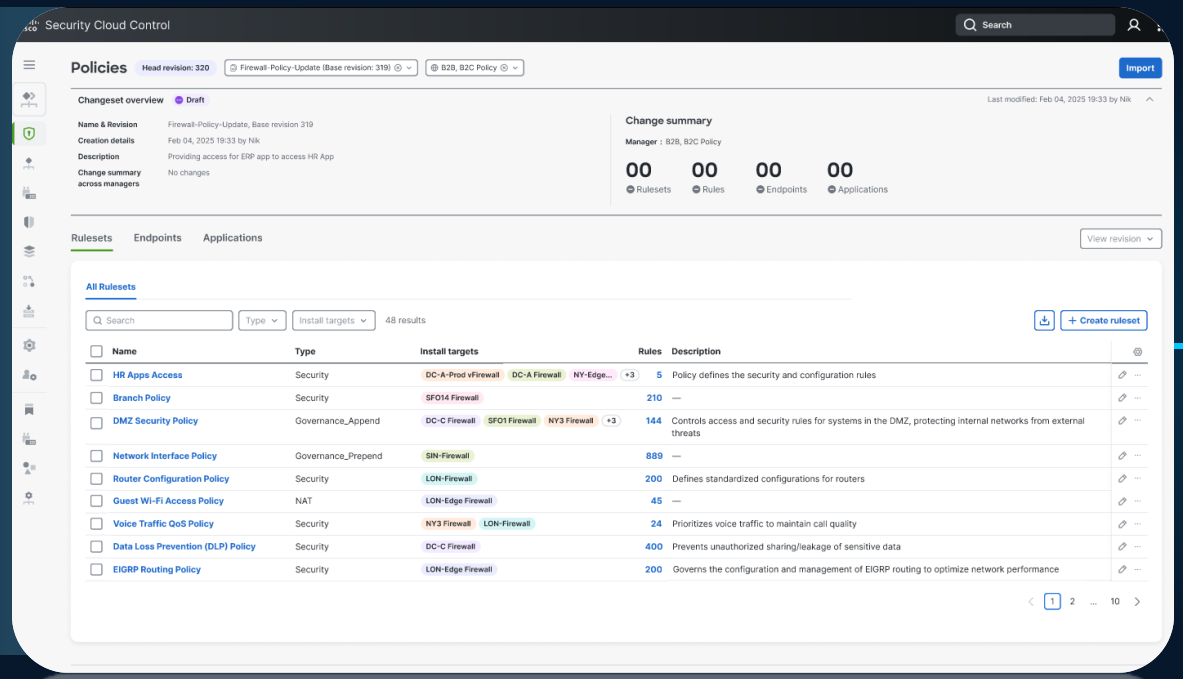
Policy Workflow & Architecture



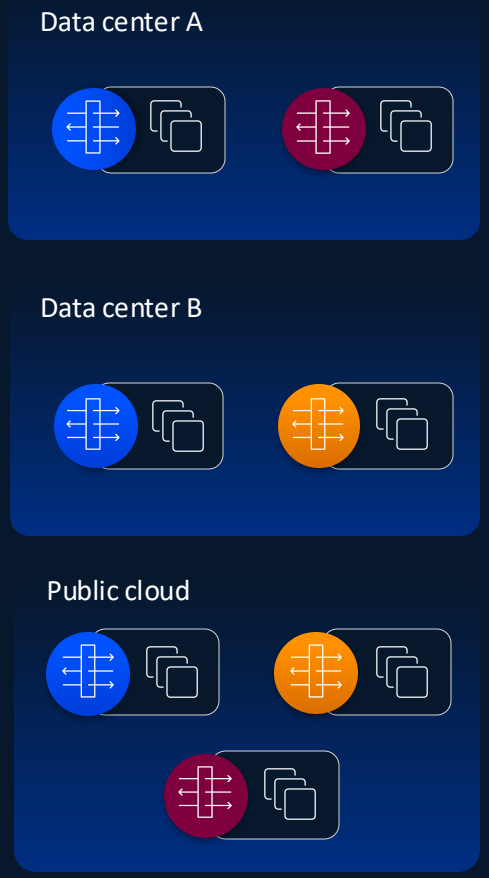
Cisco Mesh Policy Engine

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

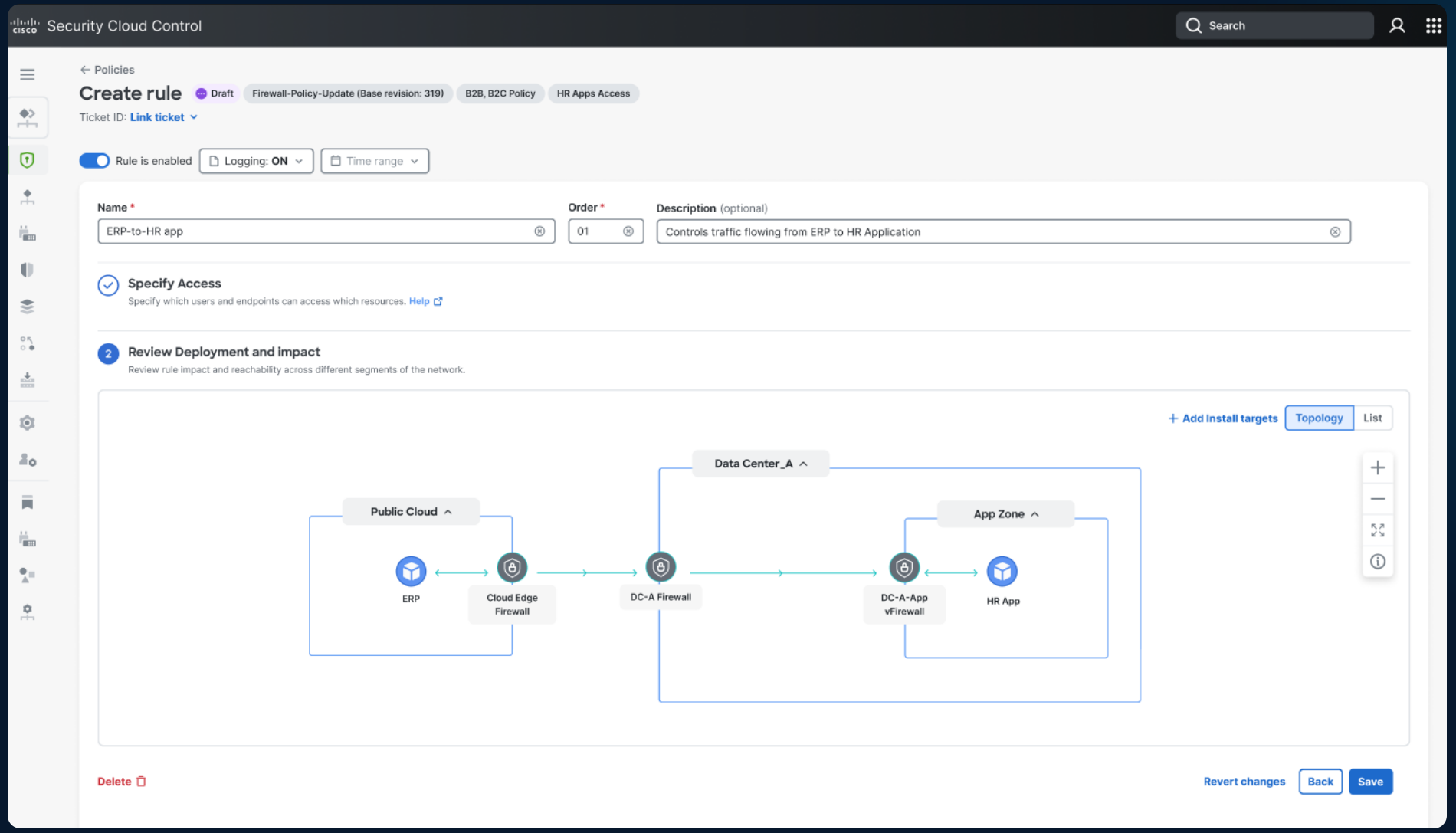
- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy **and** the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors



Cisco Security Cloud Control



Program once, enforce everywhere

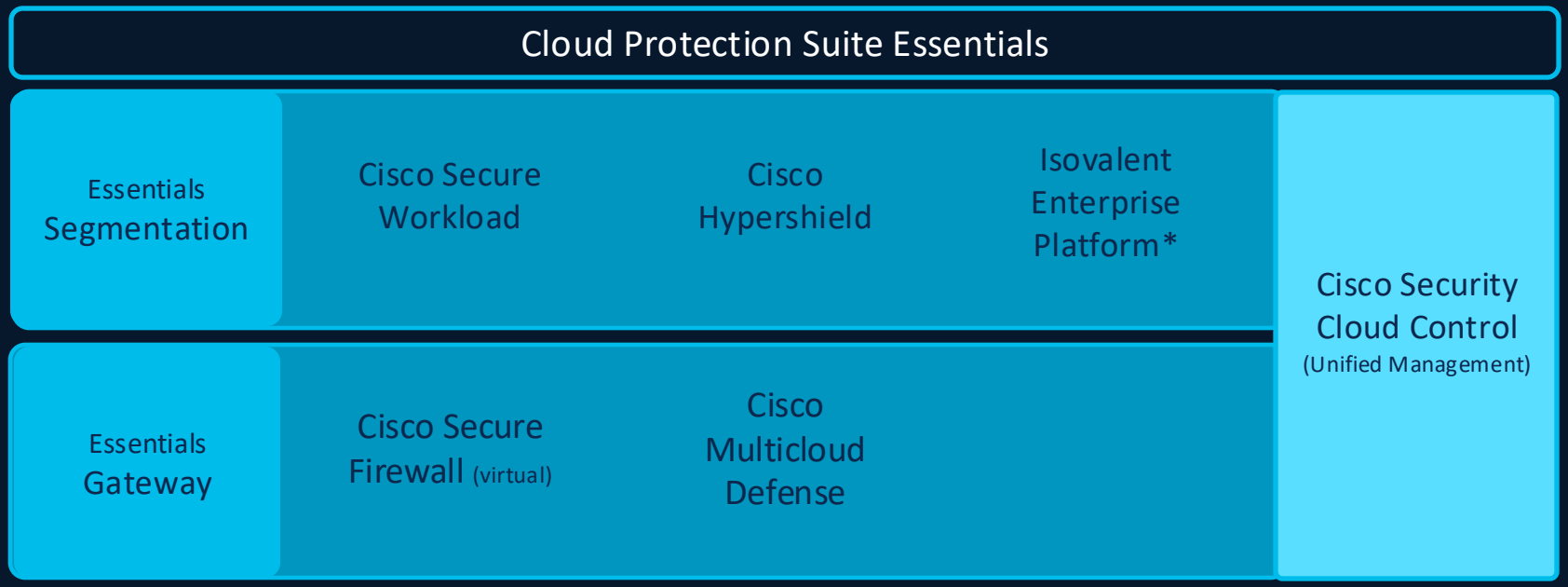


Mesh Policy Engine intelligently understands your network topology to place the most effective policy on the relevant firewalls

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