CISCO Connect

Hybrid Mesh Firewall

A Firewall for Every Situation

Neil Lovering, CCIE #1772 (30 years)
Senior Technical Solutions Architect
https://www.linkedin.com/in/neil-lovering-0408/

March 24, 2026

Abstract

The network has become far more complicated with Cloud, Hybrid Data Centers, Remote Workers and Virtual/Kubernetes operations. A single firewall can no longer protect everything, and multiple diverse firewalls are far too complex to manage.

The Cisco Hybrid Mesh Firewall introduces a common management environment for firewalls designed for the various and complex environments found throughout today's networks.

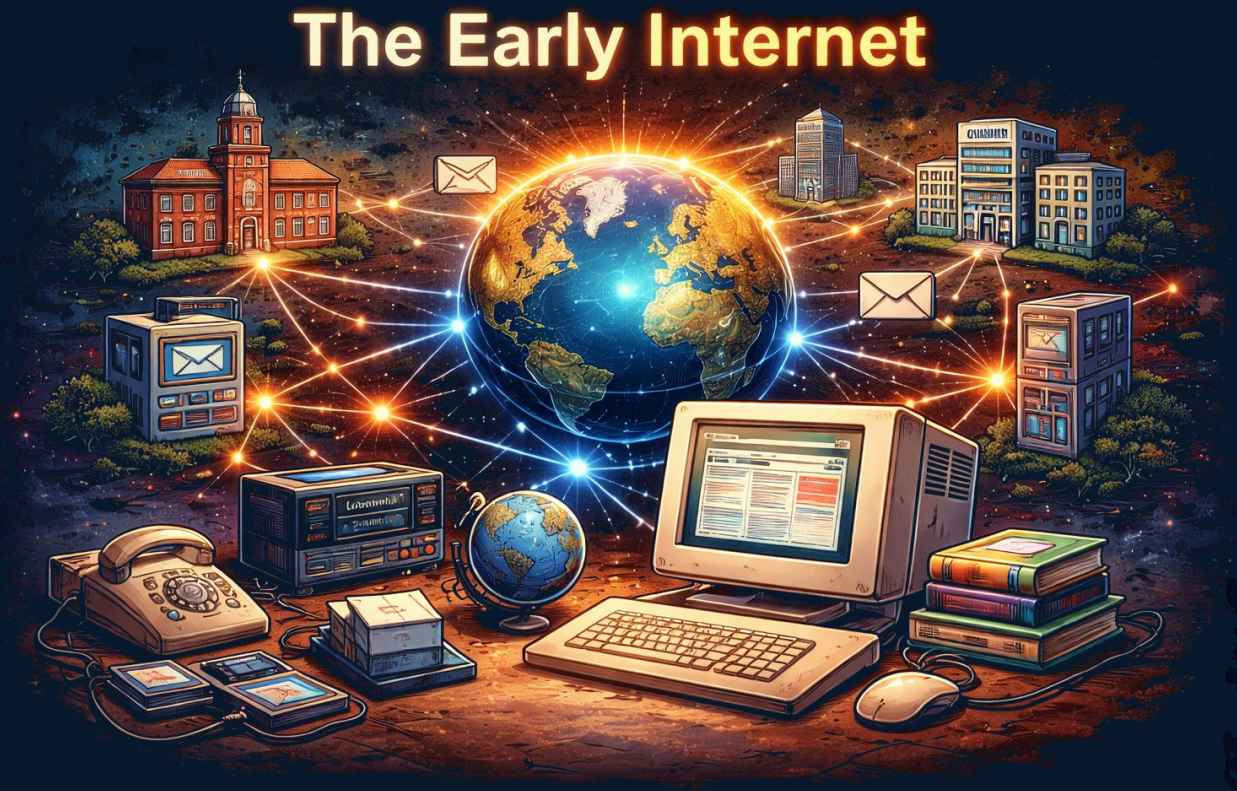
In this session, you will learn how Cisco can help you consolidate all of your diverse firewall requirements with the Hybrid Mesh Firewall and Security Cloud Control.

Agenda

1. The Evolution of the Firewall
2. Firewall vs. Hybrid Mesh Firewall
3. The Cisco Hybrid Mesh Firewall
4. Security Cloud Control

The Evolution of the Firewall

The History of Internet (1969 – 2000s)



1969: ARPANET
1983: TCP/IP

1991: WWW

The History of Firewalls (1980s – 2000s)

Late 1980s

Packet Filtering Firewall

Basic Network Filtering

Early 1990s

Stateful Inspection

Dynamic Traffic Monitoring

Mid 1990s

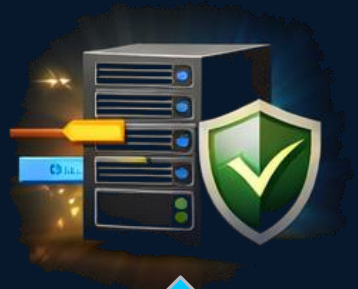
NAT and VPN

Address Translation and Secure Tunnels

Late 1990s

Application Proxy Firewall

Proxy-Based Protection



Early 2000s

UTM and IDS/IPS

United Threat Management

cisco

The History of Firewalls (2000s – 2020s)

Next-Generation Firewall

Advanced Threat Protection

Late 2000s

Early 2010s

SSL Decryption and Identity

Encrypted Traffic Inspection

Mid 2010s

Cloud Provider Firewalls

Cloud-Based Security

Late 2010s

SASE and Zero Trust

Secure Access Service Edge

Early 2020s

Hybrid Mesh Firewall

Distributed Enforcement and Unified Policy

cisco

Firewall vs. Hybrid Mesh Firewall

Firewall

fire·wall [fahyuhr-wawl]

- (n) A partition made of fireproof material to prevent the spread of a fire from one part of a building or ship to another or to isolate an engine compartment, as on a plane, automobile, etc.
- (n) A person, thing, or event that acts as a barrier or protection against something undesirable
- (n) Digital Technology, an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system
- (v) To isolate, block, or protect something by applying strict boundaries

Traditional “Next-Gen” Firewall Struggles Today

Pervasive Traffic Encryption against Deep Packet Inspection

- TLS 1.3
- DNS-over-HTTPS
- QUIC (HTTP/3)
- Certificate Pinning

New Protocols with single-flow throughput constraints

- Stream multiplexing in HTTP/2
- QUIC

Evasive Network attachment point in hybrid cloud

- Application connection abstraction with Multipath TCP and QUIC

Data Sovereignty and Cloud Management Considerations

- On Prem
- Cloud
- Sovereign Cloud
- Customer Hosted

Securing Modern Applications Is Increasingly Challenging

Highly distributed

- Spanning data center, cloud
- Containers
- Automated deployments

Nothing can be trusted

- Need deep threat inspection and major trust boundaries

  AND

- Analyze every flow to limit lateral movement

Patching is hard

- High vulnerability rate
- Mitigation is too slow
- New exploits of AI models

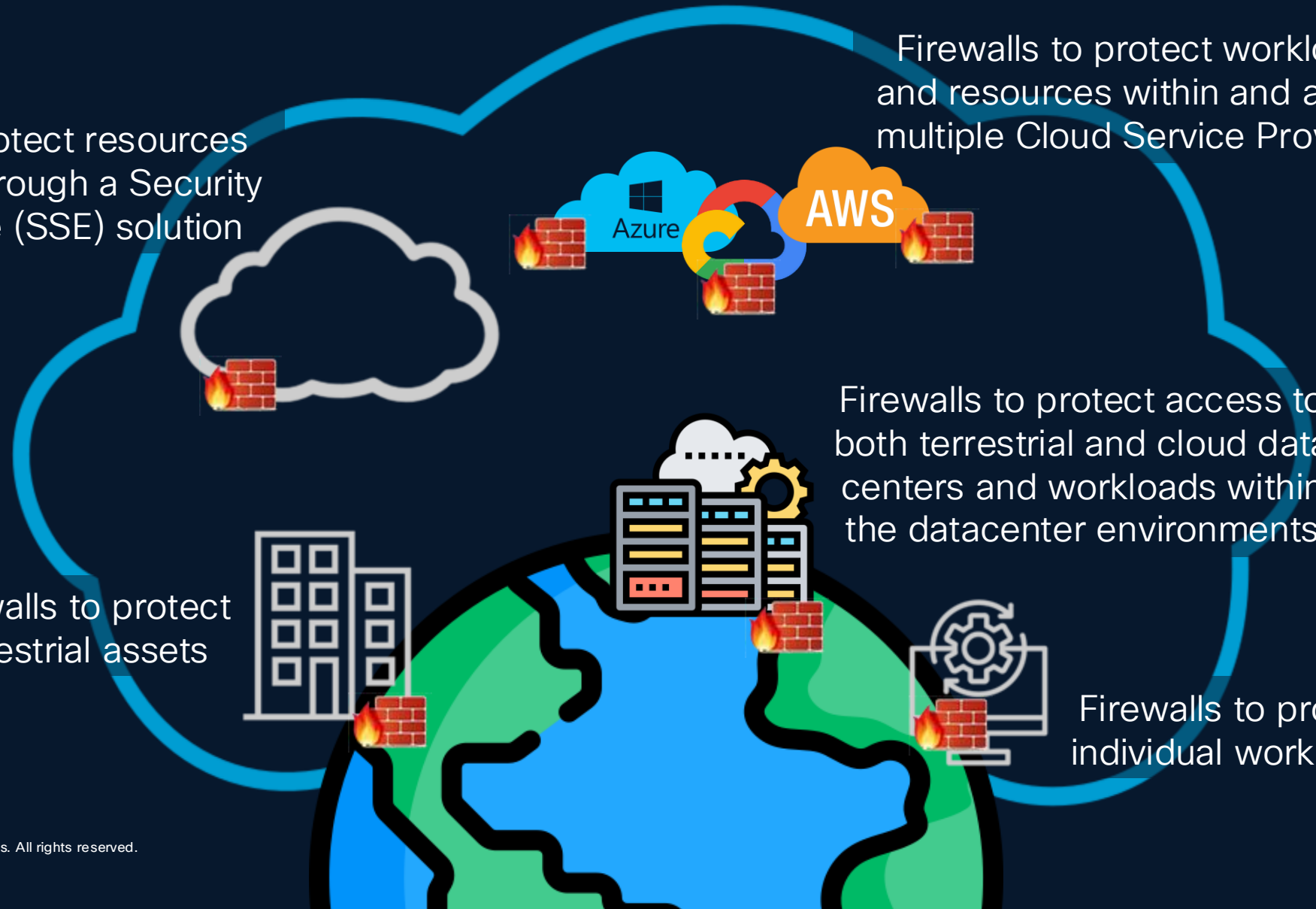
AI increasing attack surface and attacker sophistication

The Challenge Today

Independent Challenges

Firewalls to protect resources that connect through a Security Services Edge (SSE) solution

Firewalls to protect workloads and resources within and across multiple Cloud Service Providers



Firewalls to protect access to both terrestrial and cloud data centers and workloads within the datacenter environments

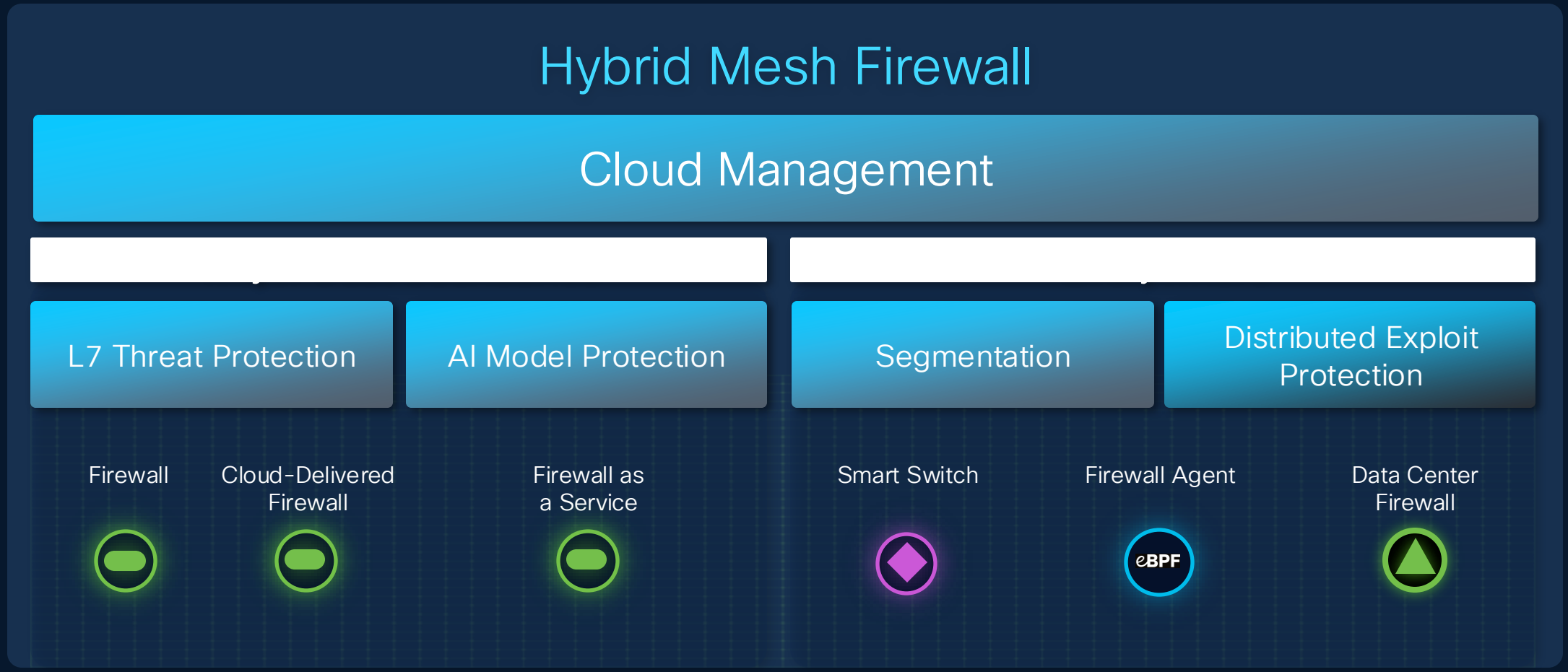
Firewalls to protect terrestrial assets

Firewalls to protect individual workloads

Hybrid Mesh Firewall

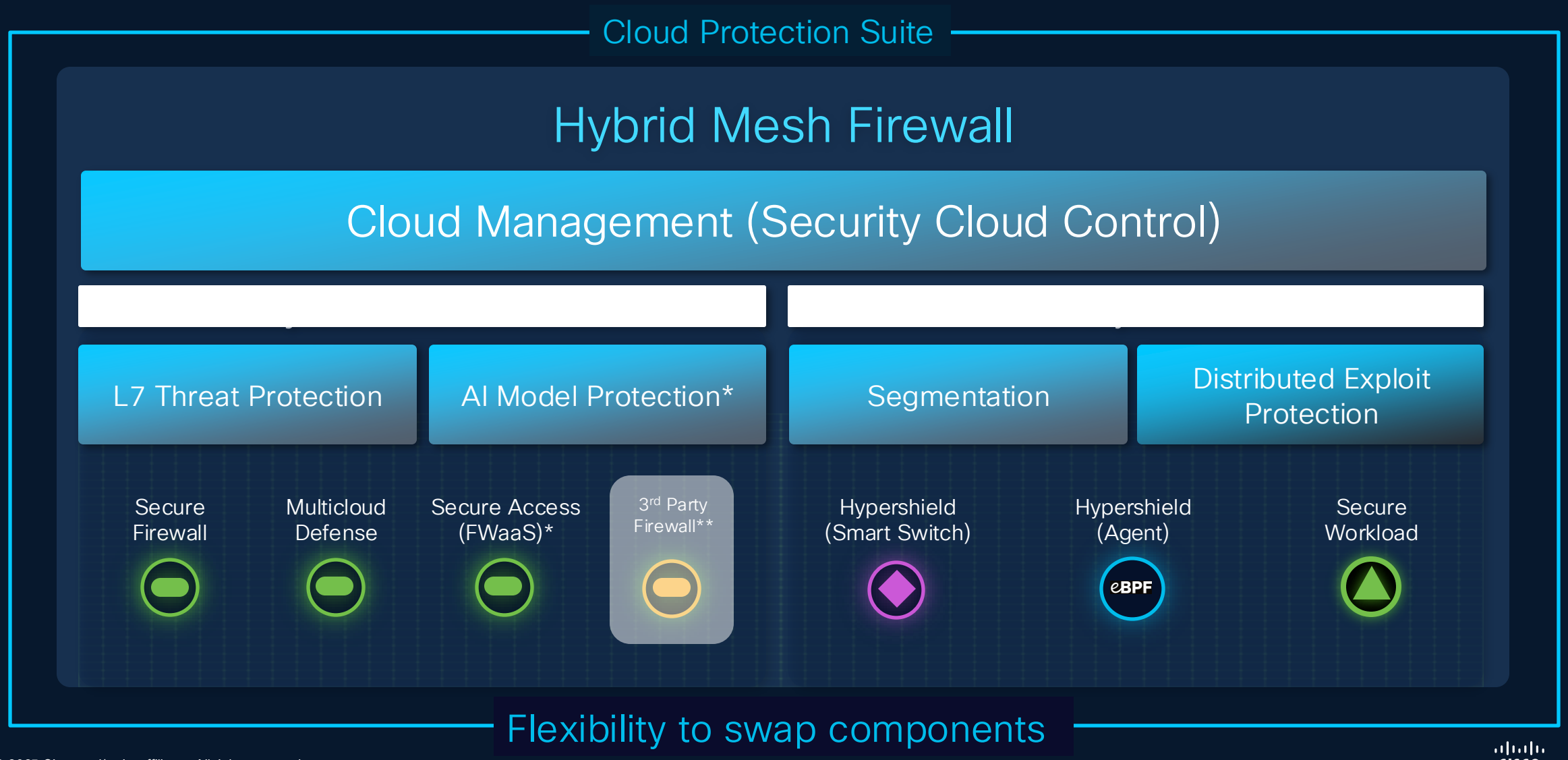
- Distributes firewall enforcement across on-prem, cloud, and endpoints instead of relying on a single perimeter firewall
- Uses centralized policy with distributed enforcement points (physical, virtual, cloud-native, and host-based)
- Enables identity- and context-based security with improved scalability and reduced latency, while limiting lateral movement

Hybrid Mesh Firewall



The Cisco Hybrid Mesh Firewall

The Cisco Hybrid Mesh Firewall



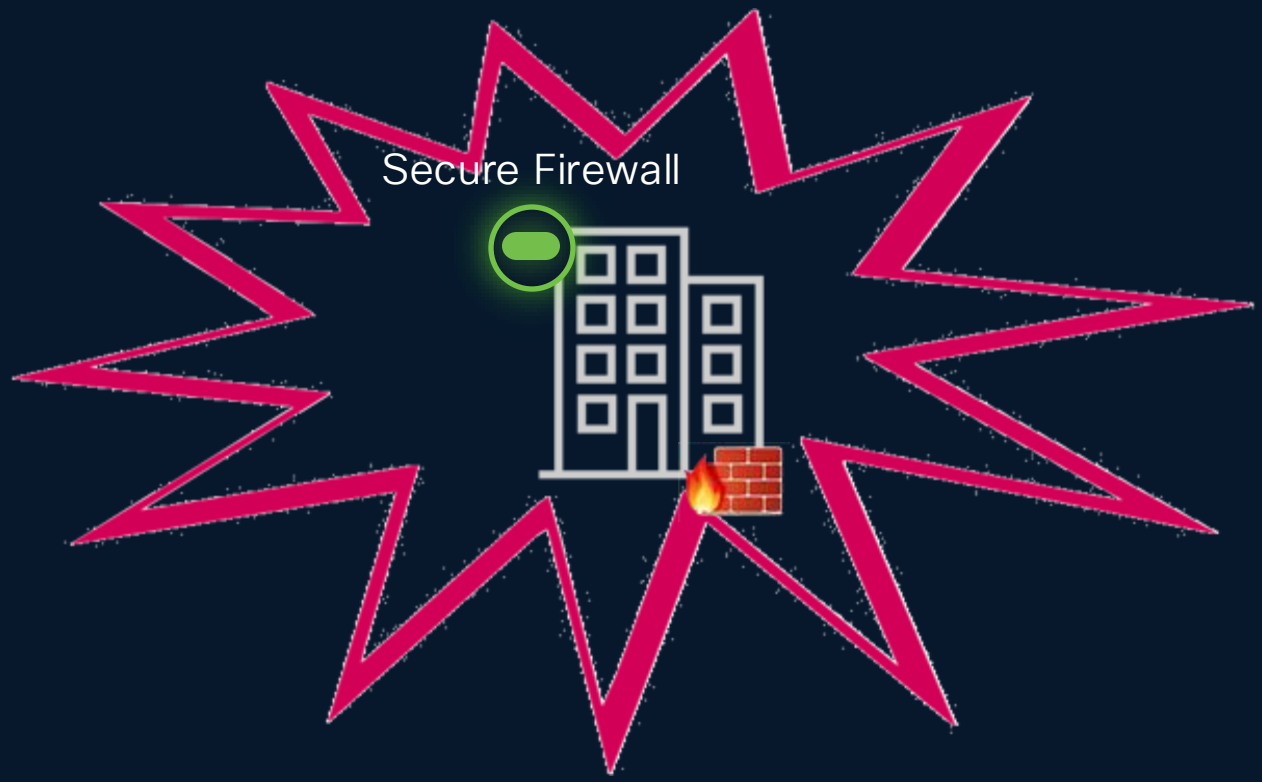
*AI Defense and Secure Access are add-ons to the Cloud Protection Suite
**Future

cisco

The Cisco Hybrid Mesh Firewall in Action

Cisco Secure Firewall

- Provides next-generation firewall protection combining stateful inspection, application visibility, intrusion prevention (IPS), malware protection, and encrypted traffic inspection
- Uses Cisco Talos threat intelligence to detect and block emerging threats in real time
- Enables centralized policy management and visibility through platforms such as Cisco Secure Firewall Management Center and Cisco Security Cloud Control

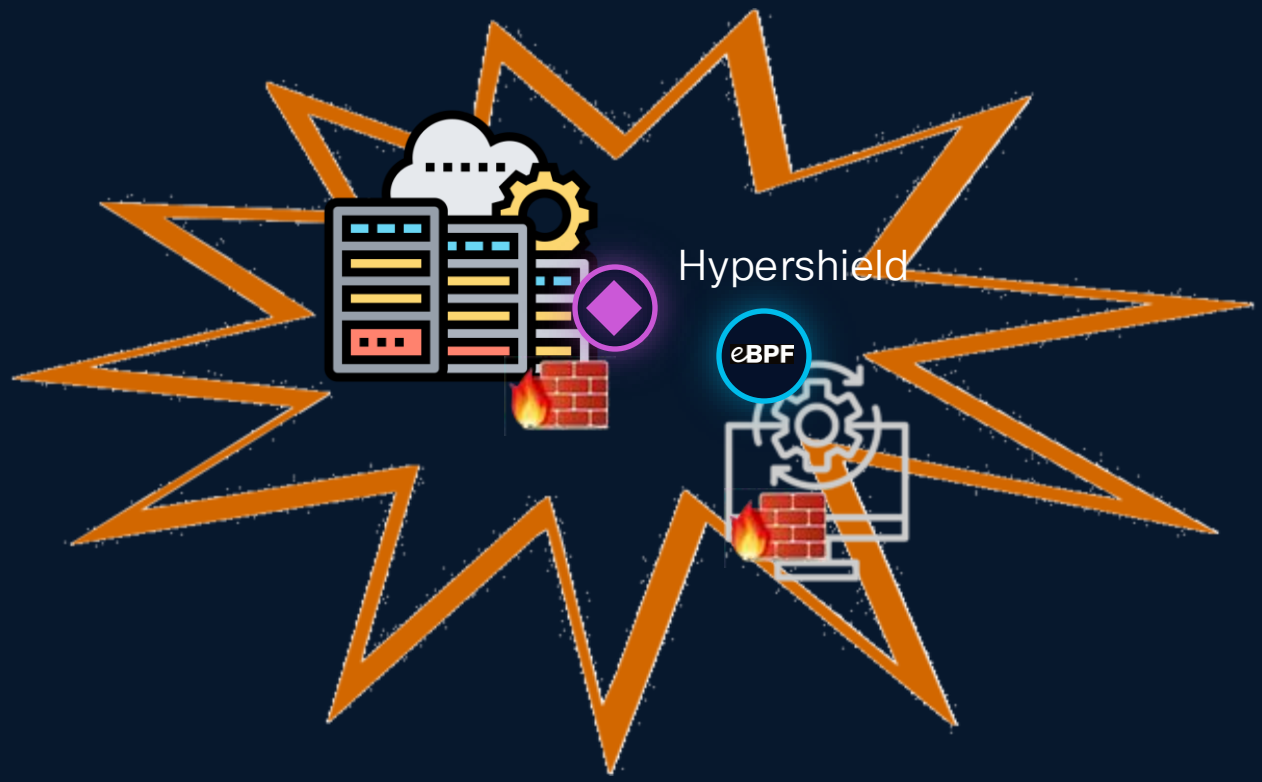


Cisco Secure Workload

- Provides deep visibility into application behavior and workload communications across data centers and cloud environments
- Enables microsegmentation based on application identity and dependencies to limit lateral movement
- Combines vulnerability awareness, runtime threat detection, and compliance monitoring to protect modern hybrid and multi-cloud workloads

Cisco HyperShield

- Embeds security enforcement directly into applications, operating systems, and infrastructure using technologies such as eBPF and hardware acceleration
- Delivers distributed microsegmentation and threat detection close to workloads instead of relying solely on centralized appliances
- Uses AI-driven automation to generate policies and rapidly deploy protections in response to vulnerabilities or threats



Cisco MultiCloud Defense

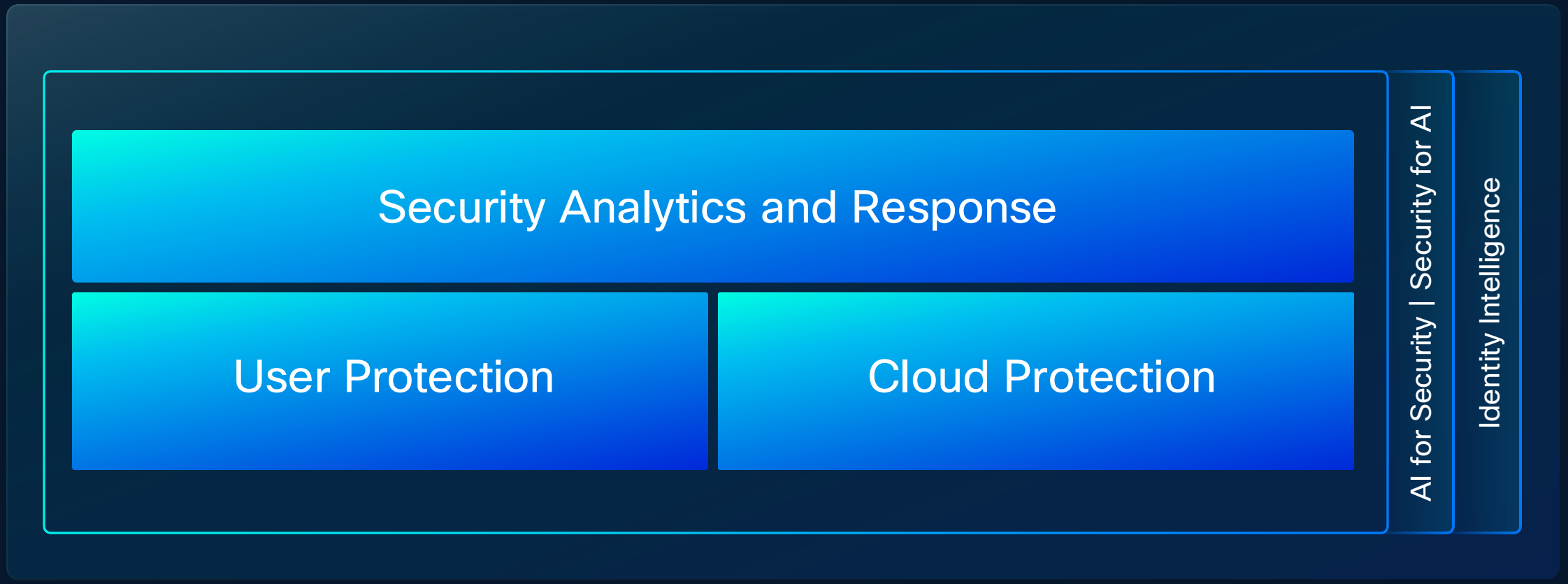
- Secures applications and workloads across multiple public clouds and Kubernetes environments through a unified platform
- Combines workload protection, API security, network security, and vulnerability management into a single CNAPP architecture
- Enables identity-based microsegmentation and runtime threat detection to prevent lateral movement across cloud environments

Cisco Secure Access

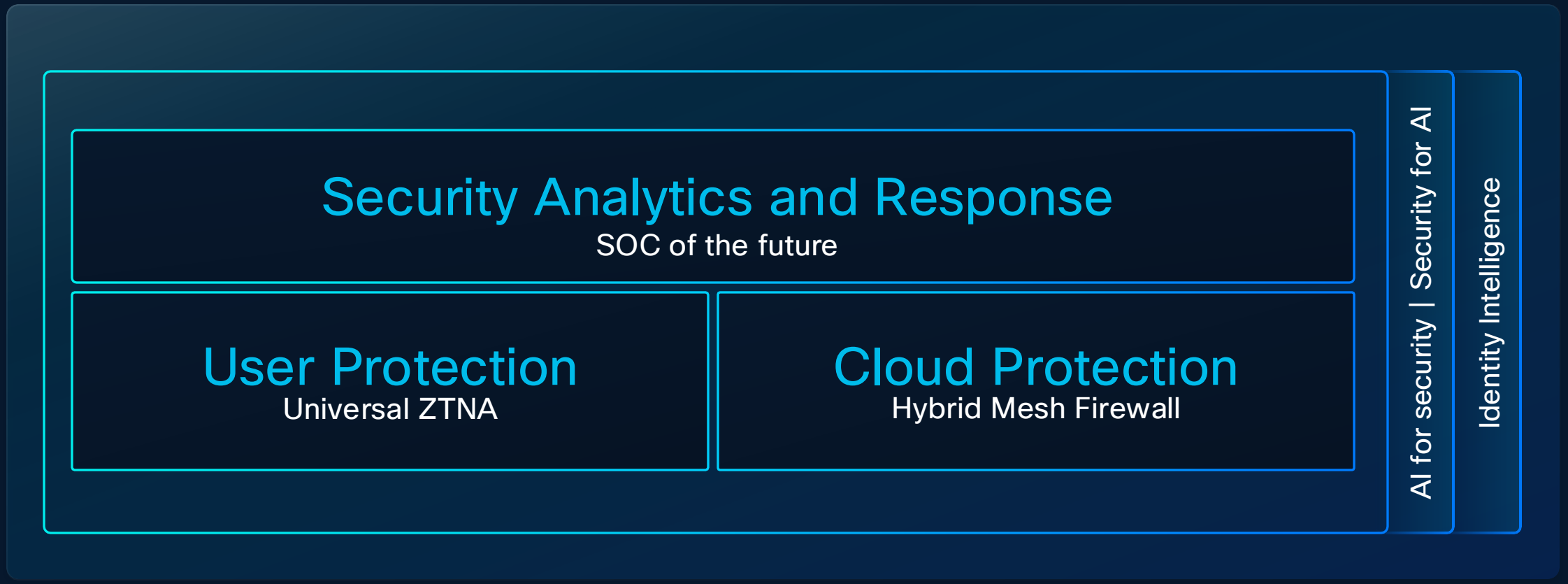
- Delivers cloud-based secure access to internet, SaaS, and private applications from any location
- Combines SWG, DNS security, CASB, and ZTNA capabilities within a unified Security Service Edge (SSE) platform
- Applies identity- and context-based policy enforcement with centralized visibility and management for hybrid work environments

Security Cloud Control

The Cisco Security Cloud

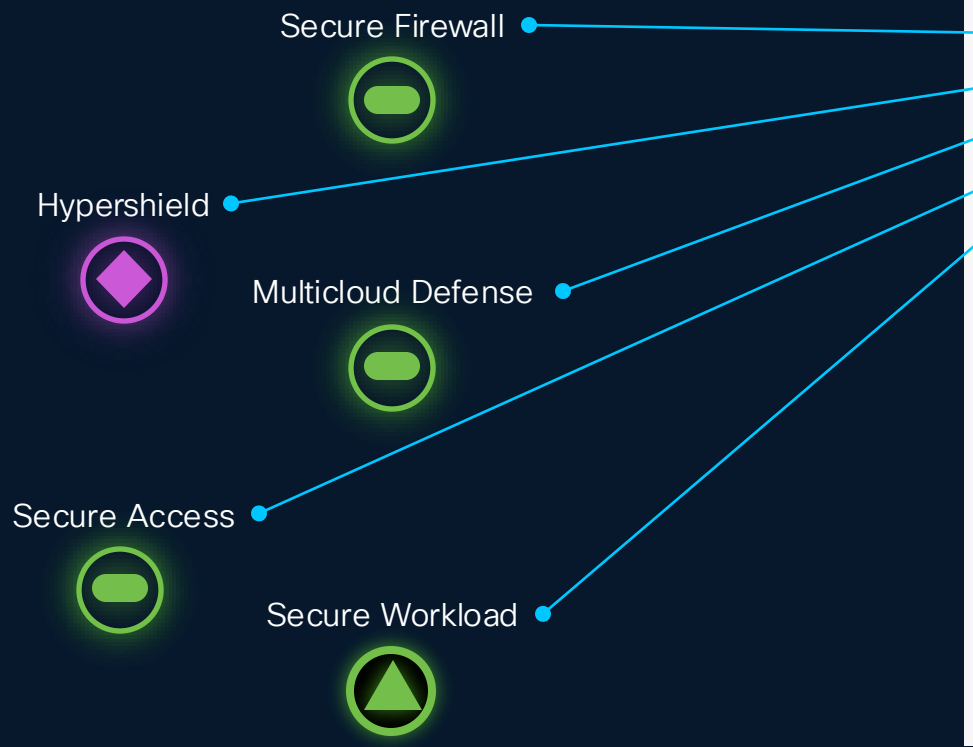


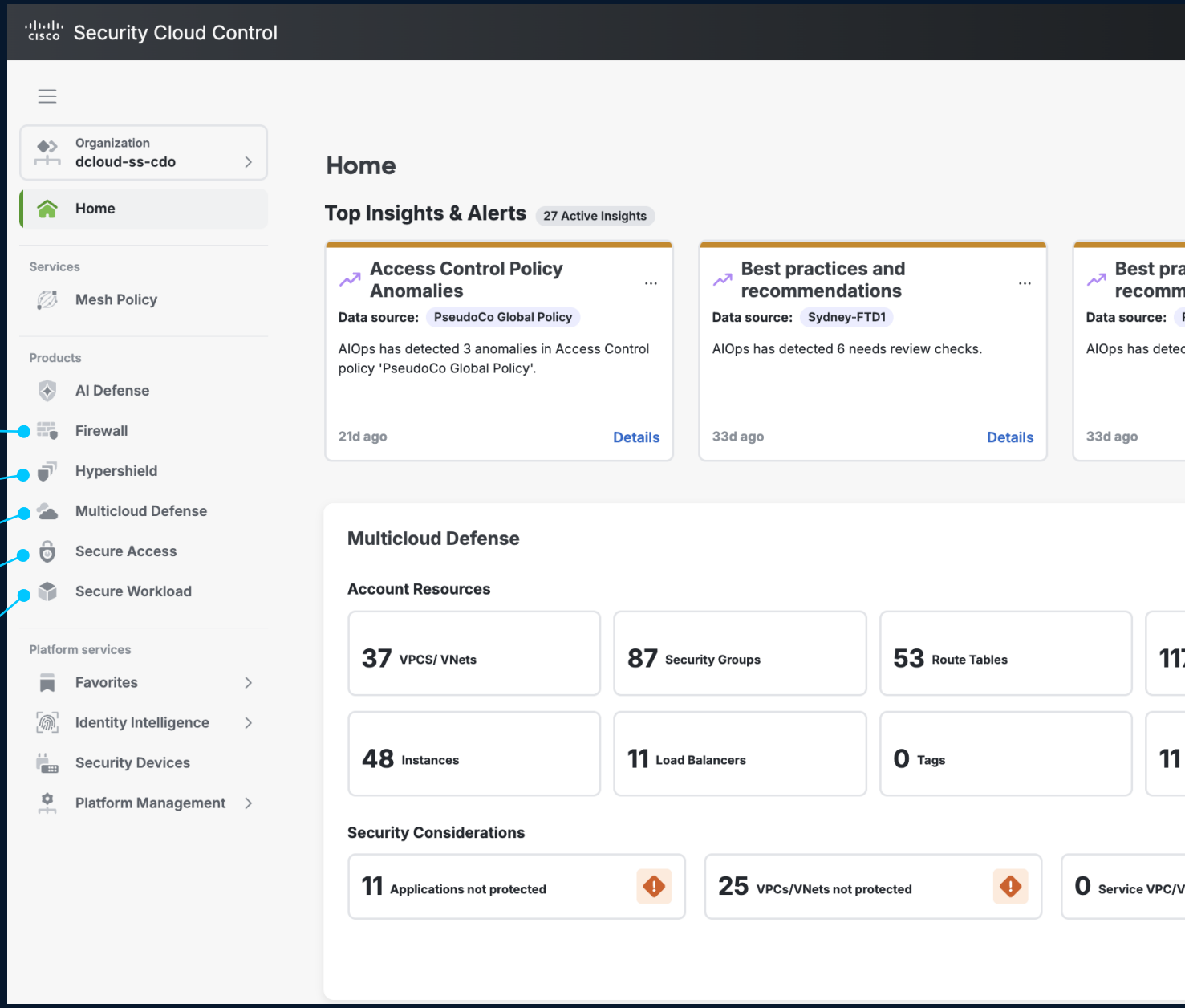
The Cisco Security Cloud



Security Cloud Control

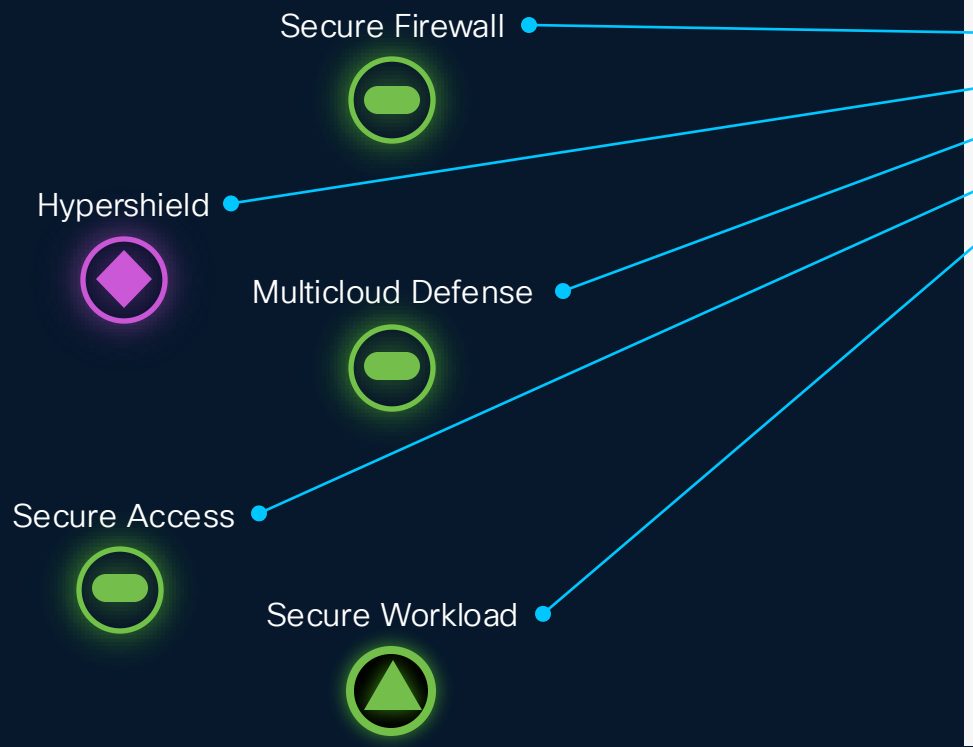
- One-stop shopping for all firewall functions in all environments
- Centralized firewall management

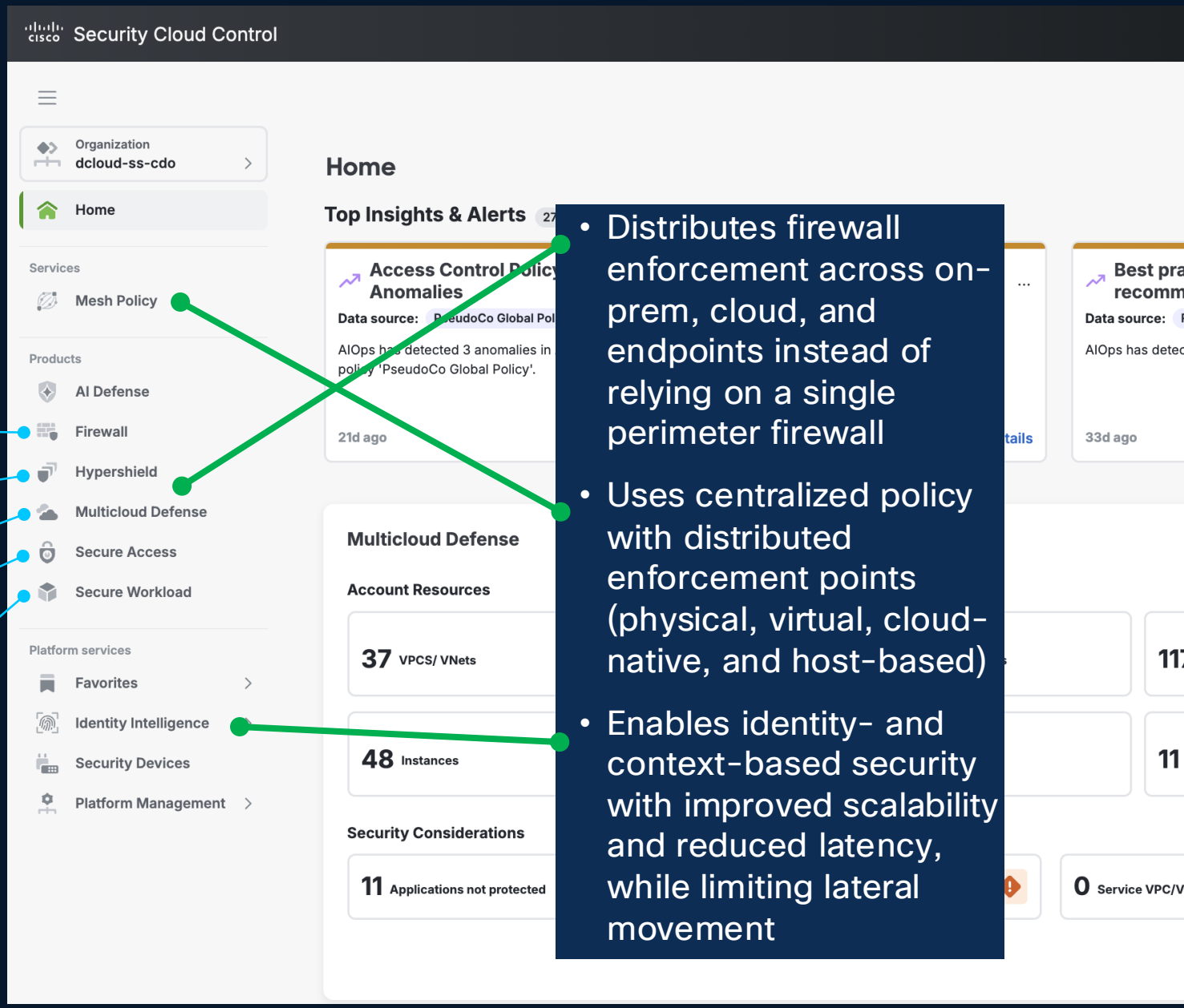




Security Cloud Control

- One-stop shopping for all firewall functions in all environments
- Centralized firewall management





- Distributes firewall enforcement across on-prem, cloud, and endpoints instead of relying on a single perimeter firewall
- Uses centralized policy with distributed enforcement points (physical, virtual, cloud-native, and host-based)
- Enables identity- and context-based security with improved scalability and reduced latency, while limiting lateral movement

CISCO Connect

Thank you


CISCO