Infinity
Platform

CHECK POINT™

A CISO'S GUIDE TO HYBRID MESH FIREWALL PLATFORMS

Essentials for meeting tomorrow's security needs with confidence

A CISO'S GUIDE TO HYBRID MESH FIREWALL PLATFORMS

HYBRID IS THE NEW NORM

If you need to secure your hybrid environment – or if you require more than two forms of firewall deployments to cover your hybrid workforce and environment – then this is the guide for you.

Every new cloud, remote site, private datacenter or hybrid employee adds complexity to your distributed digital environment. As a result, there is high demand for unified solutions that protect the most critical areas of an organization's IT infrastructure.

Hybrid mesh firewall platforms have emerged to address this gap, providing unified security management to protect diverse digital environments through multiple firewall form factors.

According to Gartner[1], "A hybrid mesh firewall (HMF) is a multi-deployment mode firewall, including hardware, virtual appliance and cloud-based options, with a unified cloud-based management plane."

[1] Gartner® Magic Quadrant™ for Hybrid Mesh Firewall by Rajpreet Kaur, Adam Hils, Charanpal Bhogal, 25th August 2025. GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

WHY TRADITIONAL NETWORK SECURITY IS NOT DELIVERING

As a CISO, you need to contend with balancing security risk and business needs such as agility to define a policy that meets your company's objectives.

Increasing cyber resiliency across all aspects of your infrastructure–data center, cloud, work-from-home, roaming users, branch offices, and enterprise networks—involves managing not just one, but multiple firewall types, adding management complexity to other security obstacles in the mix.

As detailed below, risk management, regulatory compliance, administration overhead, and budget issues are all challenges that arise in securing your distributed enterprise.

Increased Risk of Cyber Attacks

In the hybrid working model, each environment requires different firewall enforcement points, increasing the risk of cyber vulnerabilities and breaches.

For instance:

- The perimeter of an enterprise network often requires on-premises firewalls.
- Data centers, with their specific segmentation needs, may rely on a combination of hardware and virtual firewalls.
- The Firewall-as-a-Service (FWaaS) approach streamlines security for global and hybrid workforces.
- Cloud-native firewalls, tailored for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) environments, provide scalable and flexible protection.

However, the complexity does not stop there. These firewalls often need to integrate with diverse systems and controls, including IoT (Internet of Things) devices, Cloud Security Posture Management (CSPM), and SD-WAN. Security teams often don't have enough personnel nor the time to spend learning the various ins and outs of multiple security tools from different vendors. This results in security gaps and a weakened risk posture, a situation which can be addressed by a consolidated architecture.

Compliance Complexity

When organizations secure their attack surface using multiple best-of-breed solutions, the result is a Swiss cheese-type infrastructure riddled with blind spots. It becomes extremely challenging to maintain compliance consistently while managing multiple tools and their unique policies.

Administration and Operations Overhead

One of the largest problems stemming from a best-of-breed architecture is that security administrators have to move between numerous different consoles to create and update policies and keep security controls up to date. Having a patchwork of disparate tools results in your cyber security IT staff needing to spend time and resources learning new features and dashboards.

For security operations (SecOps) analysts, a centralized view of events is critical to avoid the hassle of dealing with an overabundance of uncorrelated alerts, as such complexity costs time and effort, increasing your risk of falling victim to cyber threats.

A consolidated solution is needed to eliminate silos, centralize management, increase visibility, improve efficiency, and shift to a unified approach that strengthens your security posture.

Procurement and Budget Limitations

Budgets are always a top concern for security executives. With more point products come more licenses and more security personnel to operate them, which means a higher budget is required for your security department. Moreover, each new tool requires integration into your existing security stack, costing time, effort and money.

With multiple enforcement types leading to different pricing models, traditional models with complex pricing and licensing are no longer sufficient. As cyber security needs change, organizations should have the flexibility to deploy different firewall form factors without being confined to a single type.

The fastest way to reduce your total cost of operations is by reducing the total number of security tools that your organization uses, and automating cross-product and cross-tool workflows for effective mitigation and operations across your digital infrastructure.

A NEW ERA OF NETWORK SECURITY: THE HYBRID MESH FIREWALL

WHAT IS A HYBRID MESH FIREWALL (HMF)?

According to Gartner[1], "A hybrid mesh firewall (HMF) is a multideployment mode firewall, including hardware, virtual appliance and cloud-based options, with a unified cloud-based management plane. HMF's are designed to support hybrid environments and evolving use cases by offering mature continuous integration/continuous delivery (CI/CD) pipeline integration, native cloud integration, and advanced threat prevention capabilities extending to Internet of Things (IoT) devices and DNS-based attacks."

Core Components

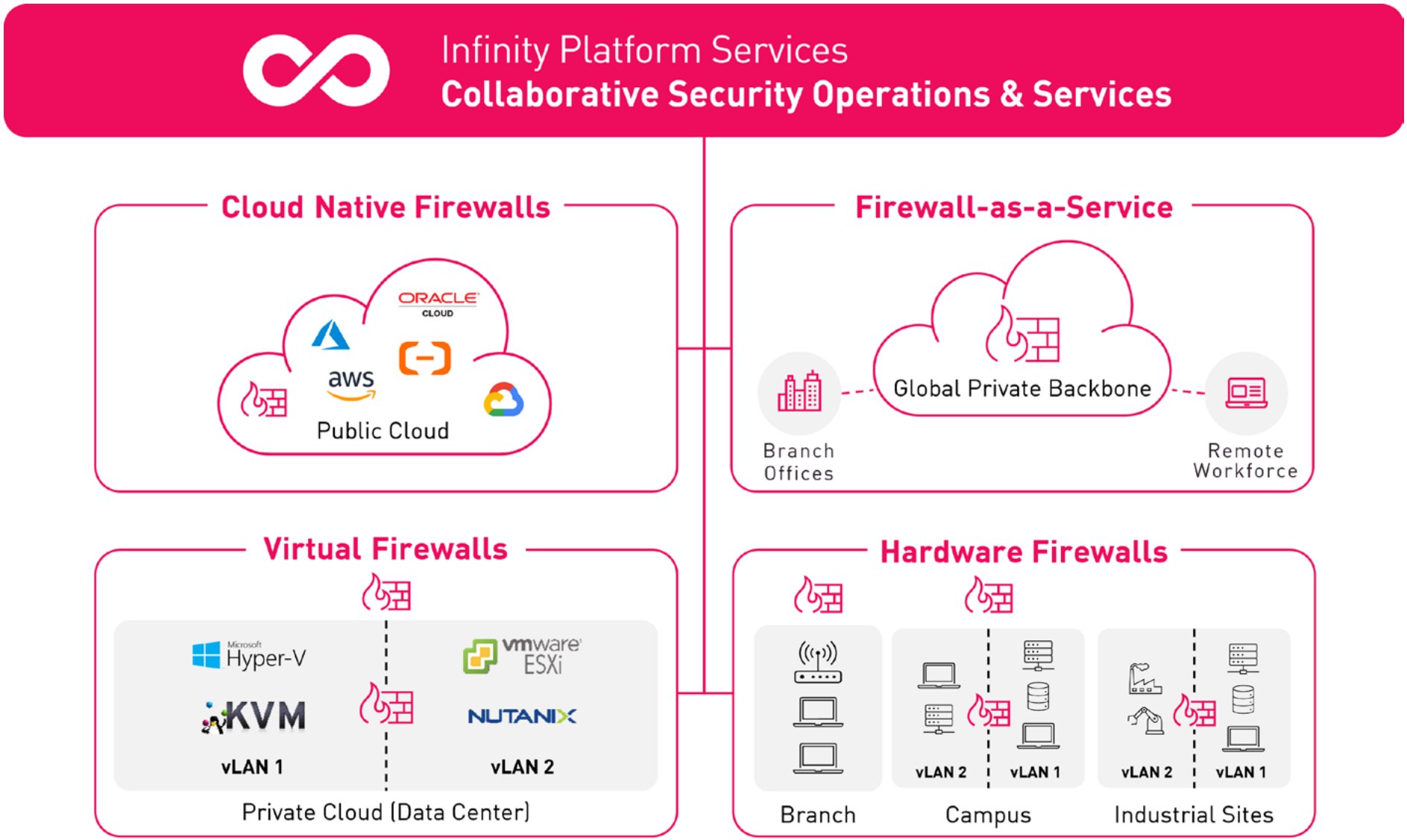
An HMF comprises the following core components:

- **Hardware firewalls** (on-premises) that are used for managing east-west traffic within data centers, protecting highly regulated industries with strict compliance requirements, and securing the perimeter of branch offices.
- **Cloud native firewalls** that safeguard all cloud-based workloads across private, public and hybrid clouds, including infrastructure as code, containers, and serverless functions.
- **Virtual firewalls** that protect virtualized machines and servers in multi-cloud environments and software-defined data centers.
- **Firewall-as-a-Service (FWaaS)** that secures remote workers and branch offices, allowing companies to scale depending on their needs, without the need for on-premises hardware.
- **Unified management** that is both cloud-based and mature – offering automation and orchestration capabilities in a single pane of glass.

For organizations with hybrid environments, the HMF simplifies IT security architecture through a single centralized management pane, facilitating unified administration and security operations to secure every environment – including on-the-go employees, branch offices, on-premises data centers, cloud environments, remote endpoints, and IoT devices.

HMF Architecture

As shown on the next slide, the HMF architecture unifies all the above types of firewalls with a common cloud-based management plane:



Hybrid Mesh Firewall Architecture as delivered by the Check Point Infinity Platform

Benefits of Hybrid Mesh Firewall Platform

The most salient benefits of adopting an HMF approach to cyber security are:

Improved security posture resulting from consistent, comprehensive policy enforcement across all systems and control

Lower management overheads- thanks to a single console for administration and security operations across enforcement points

Lower total cost of ownership thanks to vendor consolidation, fewer solutions to procure and flexible pricing models

FUTURE-PROOFING YOUR SECURITY WITH EIGHT HYBRID MESH ESSENTIALS

Selecting a hybrid mesh firewall platform requires careful research. To help you confidently select the right HMF platform for your organization, here are eight HMF capabilities you should consider.

EASE OF MANAGEMENT AND ADMINISTRATION

HMFs should enable IT and security teams to accomplish more in less time with these key capabilities and features:

Unified Console that Reduces Overhead

Network IT and Security teams may need shared and distinct responsibilities, for example, SD-WAN configuration, perimeter and IoT security, cloud and XDR. With a unified console for managing policy configuration and settings across firewalls, unified event management and security operations, administrators and analysts can collaborate more easily sharing a common user interface and language while shortening the learning curve for their specific roles.

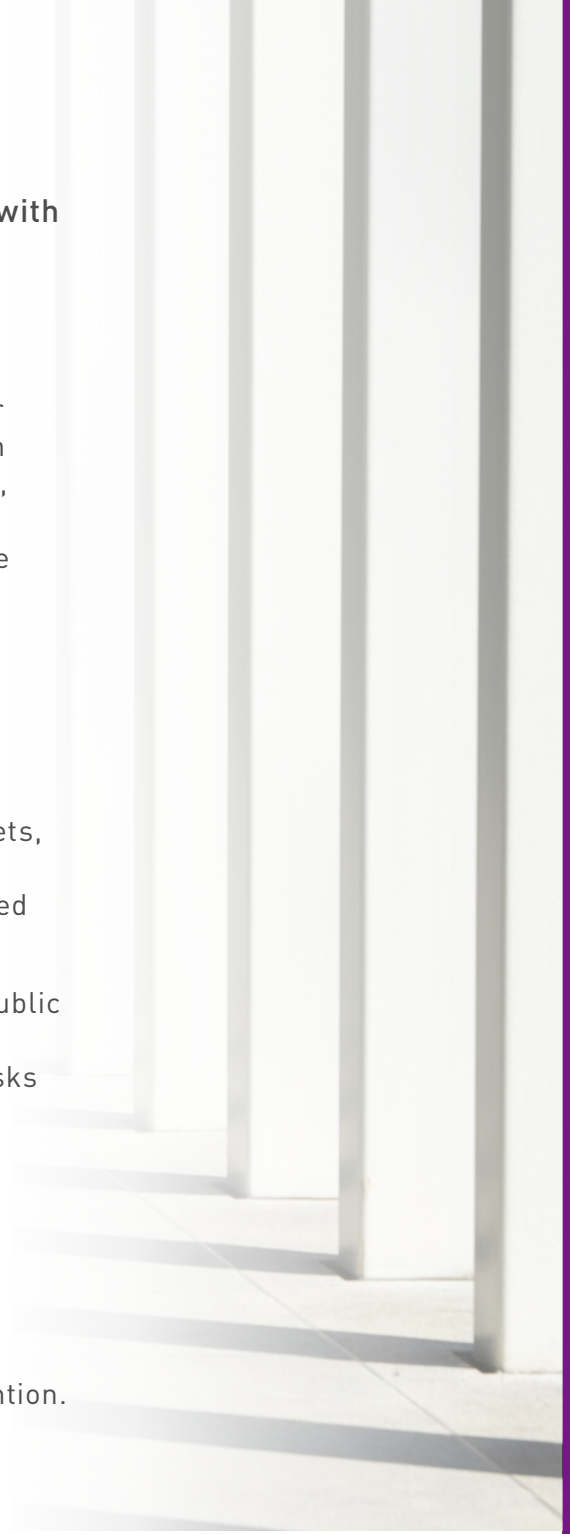
Generative AI Assistants and Model Context Protocol Servers

Serving as a personal assistant for their specific jobs, Generative AI (GenAI) assistants drastically reduce the time needed to perform common tasks. GenAI assistants help administrators update policies and controls, resolve trouble tickets, and verify protection against the latest vulnerabilities (e.g. checking if an IPS signature exists for a certain CVE). They also help security analysts with AI-guided incident response, writing and running playbooks and threat hunting at scale.

Also leverageing GenAI, Model Context Protocol (MCP) servers let you connect public AI tools, such as Claude and ChatGPT, to your security management APIs, so you can interact with your management system more easily and perform complex tasks faster, e.g. troubleshooting, preparing for audits and more.

Cloud-delivered Platform that is Always Up to Date

A cloud-delivered platform lets you continually operate with the latest security technology, controls, and innovative features through continuous, non-disruptive updates to your infrastructure. Unlike platforms that rely on software updates, a cloud platform pushes new features without requiring any administrator intervention.



AGILITY TO TRANSITION AND MANAGE WORKLOADS IN ANY HYBRID ENVIRONMENT

HMFs should give you the freedom and agility to transition and manage workloads in any hybrid environment, with security serving as an enabler rather than inhibitor.

Hybrid Networks

HMFs should support ever-growing bandwidth needs as applications expand from on-prem data centers to the cloud. They should also drive efficient use of on-premises and cloud infrastructure assets so you can repurpose resources where they are needed most. For example, gateway or firewall orchestrators can provide cloud elasticity to on-prem datacenters, redirecting firewall resources to protect workloads in other parts of your IT estate.

Hybrid Workforce

Hybrid workforces require zero trust access to enterprise resources to securely connect from anywhere. FWaaS that delivers full mesh any-to-any connectivity with zero trust policies can address this need. When combined with a global private backbone, connectivity becomes even more reliable for employees working remotely or on the go, as well as branch offices.

Hybrid Clouds

The HMF platform should seamlessly integrate with leading cloud platforms and orchestration tools and support features such as dynamic security policies and scalability. These capabilities allow you to grow your cloud security elastically while keeping pace with dynamic business requirements.

ROBUST CLOUD SUPPORT THROUGH INTEGRATION WITH ORCHESTRATORS

Dynamic Policy Enforcement

By integrating with orchestrators, the HMF tracks changes in the cloud environment and adjusts policy enforcement dynamically and enables set-and-forget cloud security administration, allowing admins to set policies once and enforce the right policies in the right places throughout their cloud infrastructure. That means each new workload that is spun up is immediately secured with the appropriate security control policies.

Check the number of on prem and public cloud orchestrators integrated with an HMF to allow you the agility to move between different providers based on your needs.

Support for Cloud Production Environments

HMFs cater to emerging use cases by supporting CI/CD production environments through API-based integration with standard tools such as Jenkins, Ansible and Terraform.

ENABLES CONSISTENT THREAT PREVENTION OF THE LATEST THREATS

Preventing the latest threats consistently requires several critical components:

AI-powered Threat Intelligence

Given the ever-evolving threat landscape, it is imperative that all your firewalls – cloud, FWaaS, virtual, and on-prem – are enabled by AI-powered threat intelligence. An HMF infused with AI/ML capabilities will excel in identifying never-before-seen threats by relying on big data and threat analysis rather than only existing Indicators of Compromise (IoCs).

Continuous Threat Exposure Management

Despite investing heavily in top security products and tools that uncover threats and vulnerabilities, a core gap remains: Security teams see the exposures, but they can't prove they're covered. To address this gap, Continuous Threat Exposure Management (CTEM) unifies what has traditionally been disconnected, covering the full CTEM cycle - scoping, discovery, prioritization, validation, and mobilization.

CTEM starts with Unified Threat Intelligence, giving organizations context about who's specifically targeting them, what campaigns are active, and more. It then combines that intelligence with continuous assessment and prioritization, based on exploitability, attacker relevance, and business impact. It then culminates in safe remediation, executing fixes and takedowns across controls, infrastructure, and workflows.

Generative AI Security

To enable safe usage of shadow or sanctioned GenAI tools, organizations need GenAI security solutions. Using AI-powered data analysis, GenAI solutions accurately classify conversational data within prompts as being sensitive or non-sensitive. They deliver GenAI application discovery, prevent data leakage in real time, and enable meeting regulations. GenAI security can be enforced by firewalls, whether hosted in the cloud, as-a-service or on premises.

DNS Security

Recursive DNS security verifies the safety of DNS requests as they are made, blocking risky access attempts at the lookup stage, further reducing the risk of reaching malware infection points and phishing sites.

Anti-Ransomware

As ransomware is on the rise, advanced endpoint solutions can monitor for specific ransomware behavior and identify unauthorized file encryption, detect and quarantine all elements of an attack and restore data from snapshots to ensure full business continuity, ideally leveraging process-level protection.

INTEGRATES WITH ENTERPRISE SECURITY CONTROLS AND ARCHITECTURE

Today's enterprises demand an integrated cyber security approach. When evaluating HMF platforms, prioritize a vendor that offers native built-in support or API-based integration with third parties to accommodate enterprise controls and architecture including XDR, Cloud-native application protection platforms (CNAPPs), ticketing systems, SIEMs, IoT security and software-defined wide area networking (SD-WAN). As pure play security vendors expand their offering and consolidate point products it is increasingly feasible to procure one HMF that covers most enterprise security needs while connecting to third party tools such as ticketing systems with prevalidated integrations.

SUPPORTS ZERO TRUST INITIATIVES

To support zero trust initiatives across your IT environments, HMFs should offer granular policy enforcement across enforcement points using attributes such as user, machine and device identities, data sensitivity, target application and risk.

This level of precision enables organizations to establish a robust defense mechanism, ensuring that only authenticated and authorized entities navigate the network. By implementing granular zero trust policies, organizations can fortify their defense mechanisms, mitigating the risk of unauthorized access and bolstering overall cybersecurity posture.

> "The ability to support the right integration with overlapping technologies in the network security architecture is an important characteristic of an HMF."
>
> - Gartner Market Guide for Hybrid Mesh Firewall Platforms

[2] Gartner® Market Guide for Hybrid Mesh Firewall Platforms, 16 January 2024, by Rajpreet Kaur, Adam Hils. Gartner is aregistered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

ACTIONABLE MONITORING AND AI-ACCELERATED FORENSICS

An HMF can potentially reduce the mean time to respond to an attack, or even prevent it altogether, through several key capabilities:

Unified Event Monitoring

Aim for complete event unification and visibility across all security products for efficient monitoring, search, and threat hunting.

Collaborative Prevention

Look for an HMF that not only detects but also prevents threats proactively through AI-based intelligence across multiple enforcement points–across clouds, networks and devices–including isolating hosts, initiating kill process, and notifying administrators.

Accelerated AI-powered Forensics

As mentioned above, generative AI assistants can accelerate security operations while increasing effectiveness through AI-guided incident investigation and response, as well as AI-accelerated threat hunting that slashes the time required to sift through artifacts at scale.

Built-in Playbooks

An HMF with embedded playbooks lets you extend the reach of siloed security solutions to stop attacks through collaboration of products, people, and processes, automating threat prevention and operations across your entire enterprise.

OFFERS AN AGILE PREDICTABLE PRICING MODEL

To enable the agility to accommodate shifting security needs, pricing models need to be predictable, yet enable switching from one enforcement point to another.

For example, an organization may start the year off with 60% of their firewalls located on-premises, 20% in the cloud and another 20% deployed as a service. A flexible pricing model will enable them to switch to 40% on-prem firewalls, 30% cloud firewalls and 30% FWaaS if they so choose, without requiring any new procurement.

One such model is an all-inclusive per user per annum pricing that includes all security hardware, software, subscriptions, 24x7 support and professional services. This model provides organizations with greater financial flexibility, enabling them deploy different firewall form factors without being confined to a single type–which is vital in the modern cyber security landscape.

> "With the introduction of multiple firewall deployment forms, features and services, vendors that offer transparent and easy-to-consume license forms will be differentiators in the market. Vendors offering price calculator tools for end users, and easy-to-transfer license forms between multiple deployment modes, will gain end-user traction. The dependency on large-bundled, complex contracts must go away."
>
> - Gartner® Market Guide for Hybrid Mesh Firewall Platforms

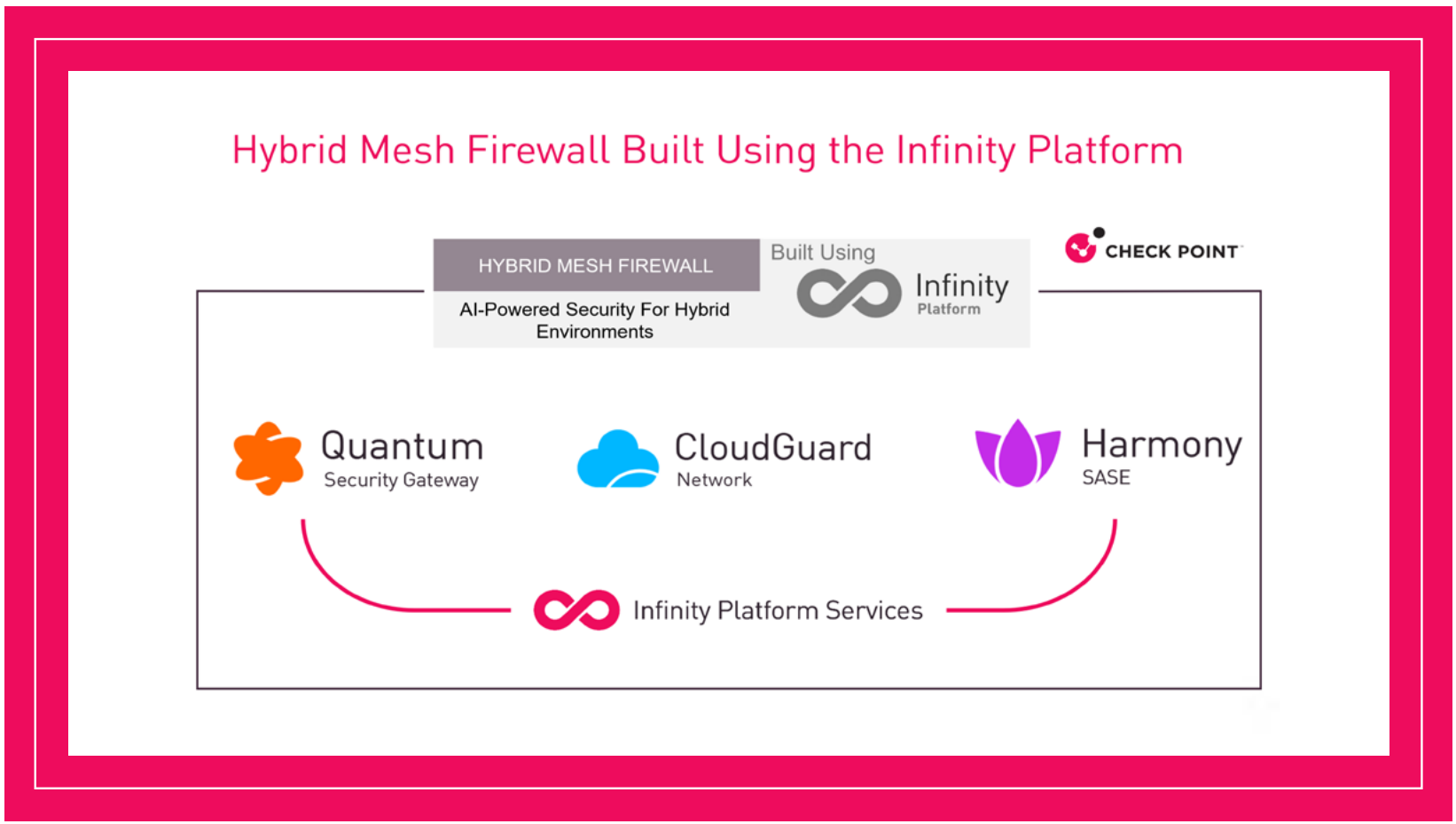
Infinity
Platform

HOW CHECK POINT HELPS

The Check Point Infinity Platform is uniquely AI-powered, and cloud-delivered, providing enterprise-grade security across the data center, network, cloud, branch office and remote users with unified management. Setting a new standard in enterprise cyber security strategy, the Infinity Platform delivers a Hybrid Mesh Firewall that lets you meet the needs of tomorrow with confidence.

Offering the agility to scale security anywhere and threat prevention that is second to none, the Infinity Platform protects diverse environments across hybrid networks, workforces and clouds - all from a unified management console with a flexible pricing model.

Test drive the Infinity Platform for yourself at https://portal.checkpoint.com/signin
or book a demo at https://www.checkpoint.com/demos



ABOUT

CHECK POINT SOFTWARE TECHNOLOGIES LTD

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the mostcomprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more about us, visit: www.checkpoint.com