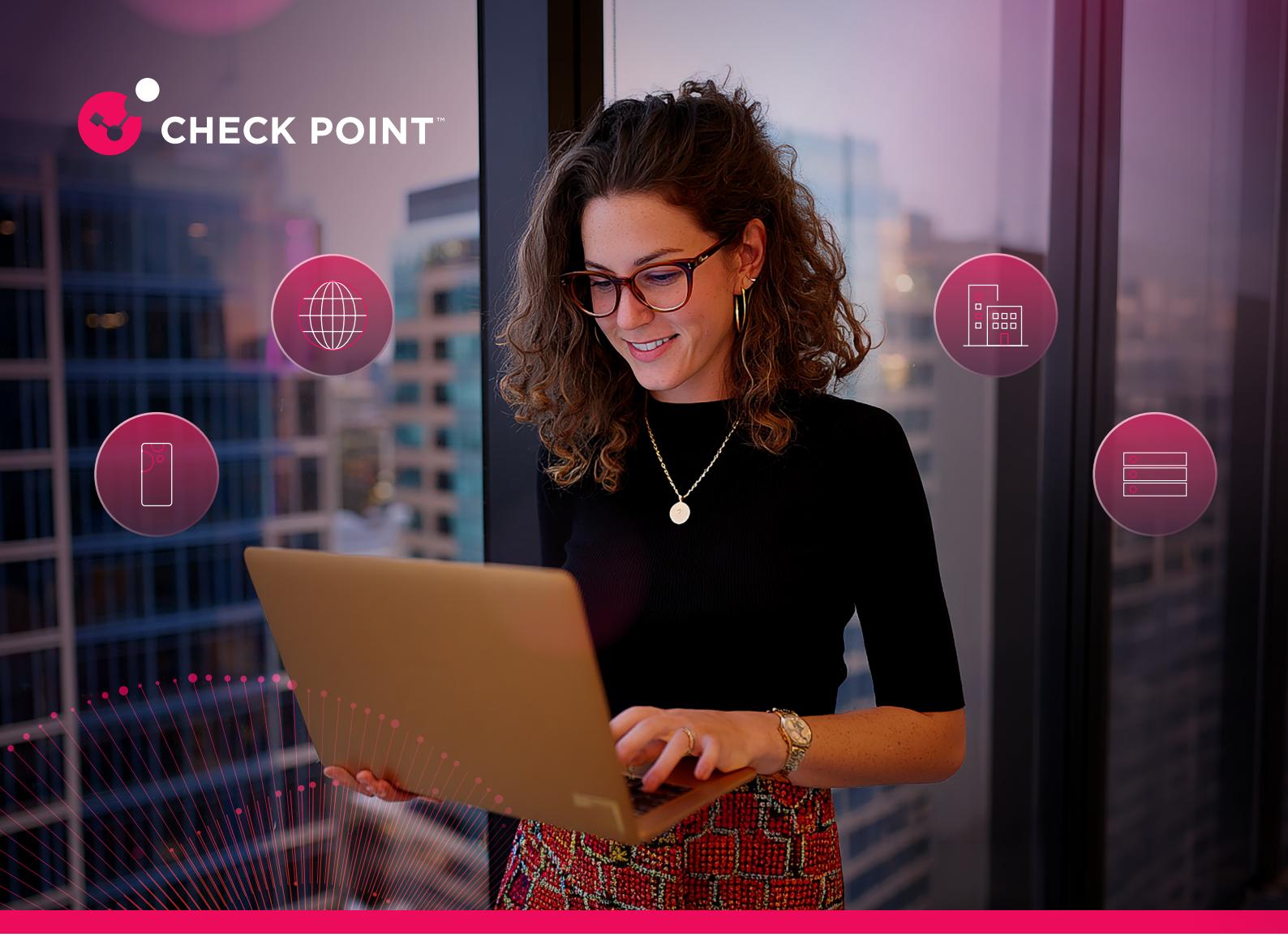


HYBRID MESH NETWORK SECURITY

Consistent Protection
Across the Distributed Enterprise

From Centralized Networks to Distributed Trust

Enterprise networks are undergoing a fundamental transformation: applications, users, and data are now distributed across on-premises data centers, public and private clouds, SaaS platforms, branch locations, and remote endpoints. This transformation is rendering traditional, perimeter-centric security architectures insufficient.

Traditional enterprise networks were designed around predictable traffic flows and clearly defined boundaries. Security controls were centralized, and trust was implicitly granted once traffic passed through the perimeter.

Today, enterprise environments are:

- **Hybrid,** spanning on-premises, cloud, and SaaS environments.
- **Highly dynamic,** with workloads and users constantly changing.
- **Decentralized,** with access occurring virtually anywhere.

As a result, legacy hub-and-spoke network architectures struggle with access and security rules across multiple systems and locations, fragmented visibility, as well as performance bottlenecks.

Modern enterprises require a security model that aligns with how networks operate today.

What is Hybrid Mesh Network Security?

Hybrid Mesh Network Security is a modern architectural approach that applies consistent security controls across all connectivity points—data center, cloud, branch, remote users, and applications—managed from a unified platform.

It is designed to empower enterprises by applying security controls wherever network connectivity exists. Rather than forcing all traffic through a single inspection point, enforcement controls include:

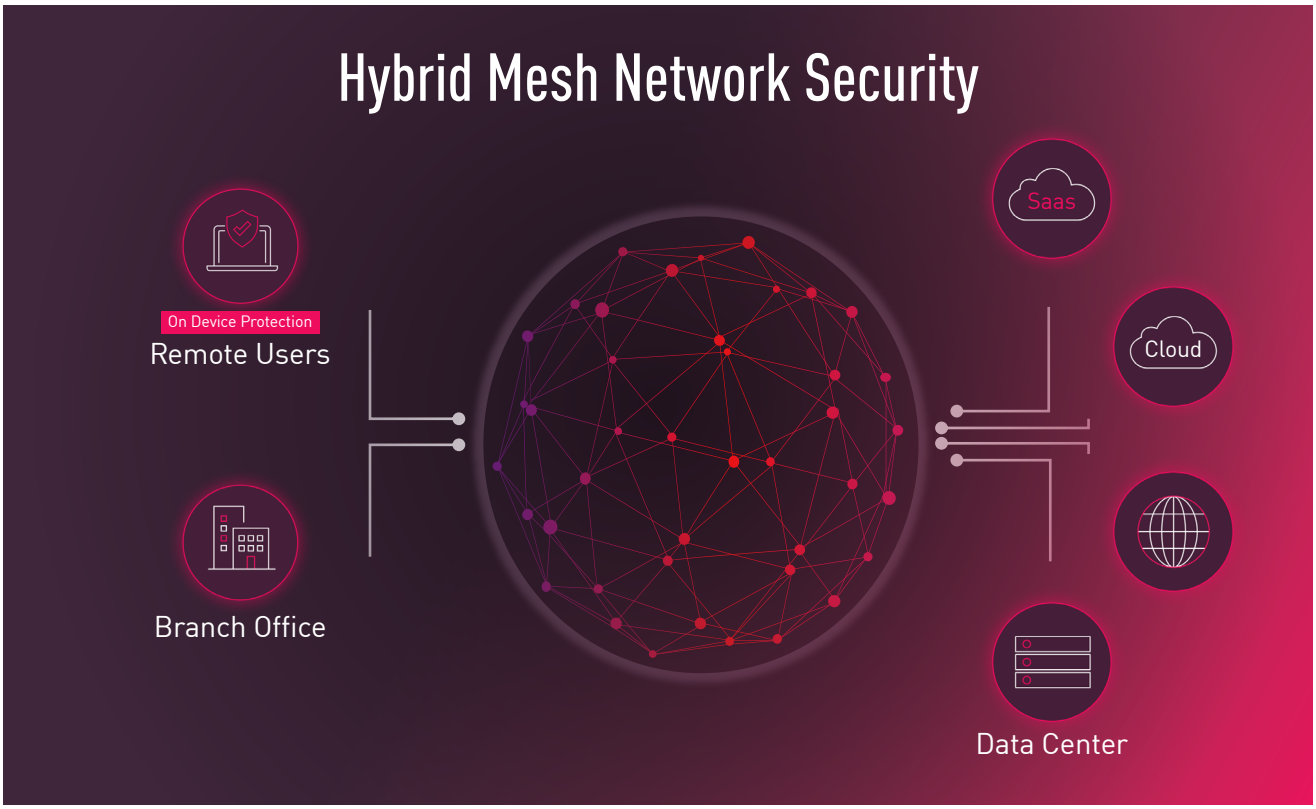
- Hardware and virtual appliances.
- Cloud-based points of presence (PoPs)
- User device agents
- Browser extensions for all leading commercial browsers
- Mobile device agents

This reduces risk, simplifies operations, and improves performance for day-to-day work.

Hybrid Mesh Network Security is characterized by:

- **Consistent enforcement** across data centers, clouds, branches, and remote access points.
- **Centralized policy definition and management** ensuring consistency.

This enables secure and optimized connectivity between users, servers and applications, whether local or cloud-based, regardless of location, while maintaining a uniform security approach.



Security enforcement is as close to remote users and branches as possible, while policy, logging, and threat intelligence are centrally managed.

Core Principles of Hybrid Mesh Network Security

Unified Policy Management

Security enforcement is as close to remote users and branches as possible, while policy, logging, and threat intelligence are centrally managed.

Seamless Hybrid Integration

Security controls adapt to diverse environments without requiring separate architecture or management tools.

Distributed Threat Prevention

Advanced threat prevention capabilities, such as intrusion prevention, antimalware, and zero-day protection, are applied close to users and workloads to minimize latency and maximize protection.

Identity Aware and Contextual Access

Access decisions are based on user identity, device posture, and contextual signals, not solely on network location.

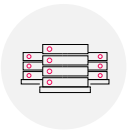
Business Outcomes

Organizations adopting Hybrid Mesh Network Security achieve measurable benefits:

- **Reduced risk** through consistent, comprehensive security enforcement.
- **Optimized user experience** by eliminating unnecessary traffic backhauling.
- **Improved operational efficiency** via centralized management and automation.
- **Greater business agility** to support cloud adoption and digital initiatives.

With Hybrid Mesh security evolves from constraint into a strategic enabler.

Main Hybrid Mesh Network Security Use Cases



Securing Data Centers

- East–West traffic visibility & enforcement
- Zero-Trust workload-to-workload access
- High throughput with ultra low latency



Securing Applications

- Unified App Security Across Environments
- Inline runtime prevention
- API-First Security



Securing Remote Users

- Private & Public access
- Identity-first, continuous access control
- Device posture verification
- Simplicity & visibility



Unified Management

- Identity-Centric Management
- End-to-End Visibility across the mesh
- Cross-Domain Correlation & Risk Prioritization



Securing The Cloud

- One consistent policy
- Cloud-Native Visibility & Control

Check Point enables Hybrid Mesh Network Security through a comprehensive, integrated portfolio:

Check Point Firewall, Maestro Hyperscale Firewall	High performance and scalable on-prem, virtual & hyperscale firewalls, providing advanced network security enforcement.
Check Point Cloud Firewall	Cloud native protection for public cloud environments, supporting dynamic scaling and cloud specific architectures.
Check Point SASE Private & Internet Access	Secure remote access and identity aware connectivity for users and devices.
Check Point Portal	Centralized AI-powered management & security control plane.
ThreatCloud AI	Realtime threat intelligence and AI-driven prevention shared across the entire mesh.
Hybrid Mesh Network	A distributed, encrypted, self-healing, any-to-any global private network fabric connecting branches, clouds, data centers, and PoPs.

Together, every enforcement point can become an active sensor that feeds the AI-mesh intelligence, improving protection, cutting detection and prevention time from minutes to sub-milliseconds.

Summary

As enterprise networks continue to evolve, security architectures must evolve alongside them. Hybrid Mesh Network Security provides a scalable, resilient approach to protecting distributed environments without compromising visibility, performance, or control.

By adopting a hybrid mesh model powered by Check Point, organizations can confidently secure their networks today while preparing for the challenges of tomorrow.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com