AN INTRODUCTION TO HYBRID MESH NETWORK SECURITY

An Architecture for the AI-driven Hyper Connected World

Industry Trends

The modern enterprise is going through major transformations fueled by the shift to cloud, hybrid work models, and explosive adoption of AI. Essentially, applications have migrated to cloud and SaaS, delivered across multiple public and private cloud platforms and data centers, users have dispersed to work from home or on the go, and when compounded with the AI explosion, the new corporate network has become exponentially more complex, impacting business agility, security, overall experience, and costs.

Addressing this warrants a fresh look at the Enterprise architecture and the connectivity fabric.

Current Approaches and Their Limitation

Organizations are addressing these challenges in several ways, each with its pros and cons.

On-premises

This approach is based on deploying Next Generation Firewalls at network entry points to on-prem sites, such as offices, manufacturing plants, data centers, and more. Appliances do a great job of inspecting all inbound and outbound traffic to and from the site and detecting and preventing risky transactions. Their limitations lie in protecting remote users to cloud applications and the internet. For these use-cases, user connections need to be backhauled through physical locations in which the appliances are deployed, increasing operational complexity, adding latency and creating traffic bottlenecks and scalability challenges. Appliances are also not a good fit for smaller branch offices or coworking offices in which deploying appliances may not be possible. Overall, this results in degraded user experience and lower productivity, as well as creating greater workload and operational costs for the IT team.

Cloud only (SASE)

Cloud-delivered solutions help alleviate the scalability and backhauling concerns of appliances. They also help reduce management complexity. They do, however have their own limitations which result from having to route all user traffic through cloud-based data centers from which the SASE service is delivered. This also creates latency in many cases, as well as increased cost and security concerns as traffic may be decrypted and processed in unknown, and potentially untrusted, cloud locations.

Hybrid approach

A hybrid approach combines both on-premises appliances and cloud-delivered security services. It leverages the advantages of both approaches, delivering a solution which benefits from the best of both worlds.

Comparing the three approaches:

	On-Premises	Cloud (SASE)	Hybrid
Connectivity	Limited	Mesh only	Agile mesh
Enforcement point	Site	Cloud	Site and/or cloud
Performance	Limited	Limited	Optimal
Cost	Medium	High	Optimal

Making the case for a Hybrid Approach

While the pandemic drove enterprise architectures to cloud-only SASE for remote workers, the post-pandemic era has brought significant changes with return to office (R20) mandates and a more hybrid demographic. Further, with greater emphasis on data governance and regulatory requirements, many organizations are adopting a workload-based stance that's also hybrid. This has been amplified with AI being brought under the purview of private clouds and data centers under the moniker of Private AI, with large enterprises wanting to have tight oversight over AI models for regulatory requirements and data sensitivity.

New performance requirements at the edge have brought in increased demands for low latency, and local decision making without compromising quality of experience, including with the onset of Agentic AI.

Bottomline, enterprises want choice and flexibility. Locking themselves into an on-premises only or cloud-only model, limits their choice and may cause performance degradation, security inconsistencies or compliance issues.

Based on these, a hybrid architectural approach is the right one.

For this to work it needs to have the right elements of networking and network security (SASE) also delivered as a central hybrid component to truly make the hybrid mesh network security architecture effective.

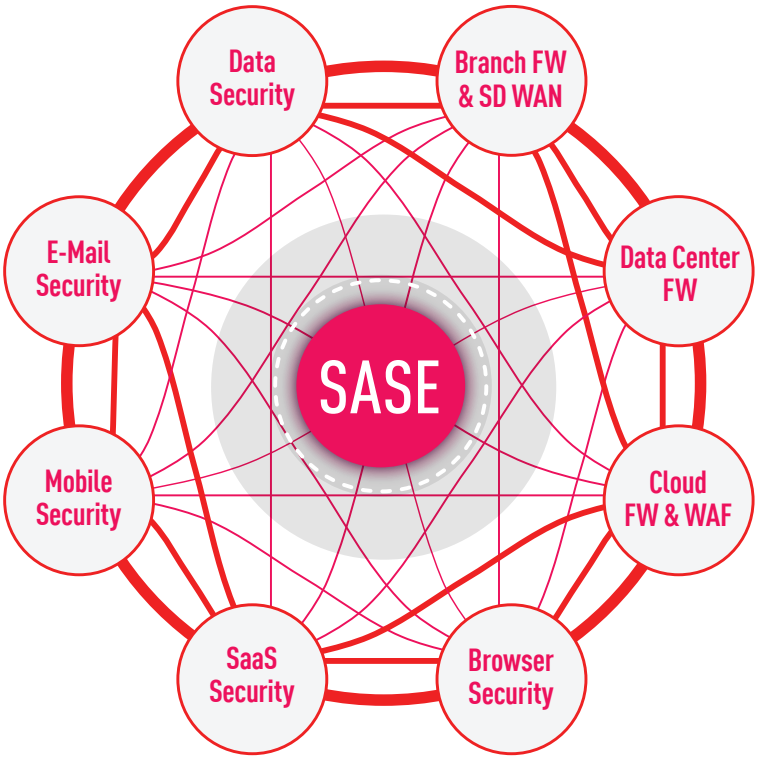
The Hybrid Mesh Network Security Architecture

At Check Point, we recognize the need for a hybrid approach to deliver network security and have developed an architecture over the years that delivers on this promise.

All organizations are unique, and so are their networks. The right security solution is the one that best matches an organization's specific needs, can deliver optimal security and performance across all users and sites, and can adapt, evolve and scale to keep up with the speed of business while reducing costs. The reality is that no single approach can deliver this. The only way it can be achieved is by combining all the above approaches into a unified and flexible architecture that can adapt to each organization's specific and unique deployment model. This is the goal and vision of the Hybrid Mesh Network Security architecture.

What is the Hybrid Mesh Network Security Architecture Made of?

This unique approach combines security enforcement points in multiple form factors, enabling enterprises to mix and match them to best meet their unique network architecture and needs. Hybrid Mesh Network Security form factors include hardware and virtual appliances, cloud-delivered points of presence (PoPs), user device agents, browser extensions for all leading commercial browsers, and mobile device agents. This enables organizations to effectively secure branch offices, data centers, cloud deployments, SaaS applications, and mobile users.



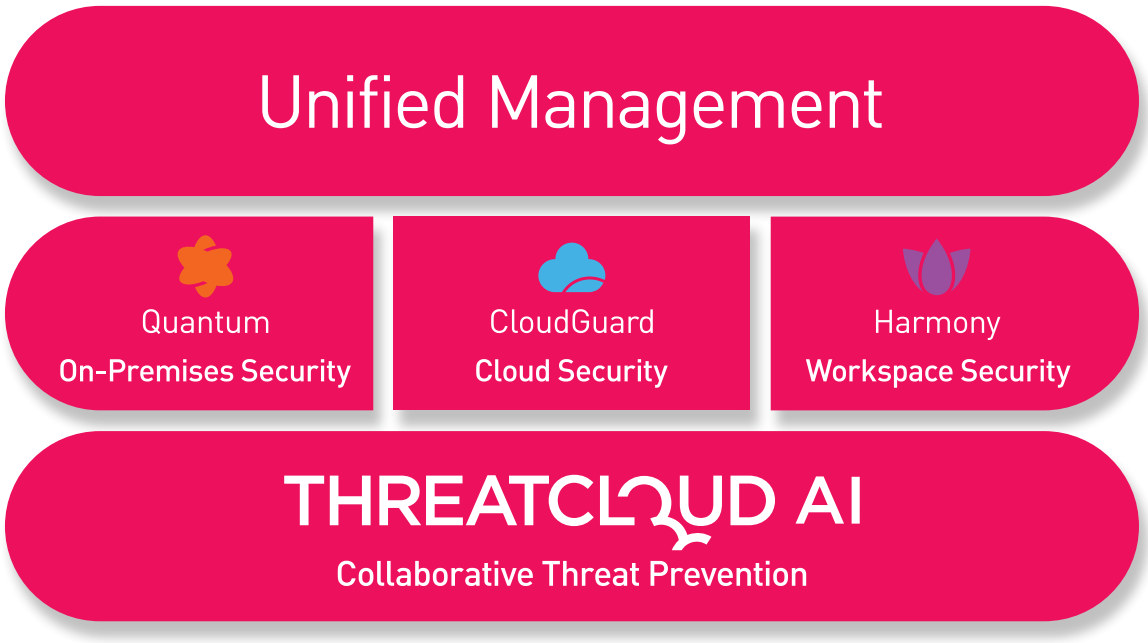
At the heart of the Hybrid Mesh Network architecture lies SASE. With its globally distributed presence of more than 80 PoPs, private backbone interconnectivity and seamless scalability, it is the connecting tissue of all network components. Connectivity between the different edge types, however, doesn't rely solely on the SASE network, as the other security form factors are able to communicate directly between themselves or externally to SaaS and web resources.

For example, remote users browsing via the on-device agent, which provides complete secure internet access, can connect directly to the destination website without needing to pass through the cloud SASE service. This greatly improves the user experience and helps reduce cloud-processing costs.

Another example, one in which the SASE network is leveraged, is a remote user wishing to securely connect to public cloud applications. By connecting to the nearest SASE PoP, the user's traffic doesn't have to be backhauled through an on-prem appliance, delivering better user experience and improved productivity.

Hybrid Mesh Network Security – The Architecture driving Check Point's Infinity Platform

The hyperconnected world creates a myriad of unique enterprise security use-cases, each demanding the right and most accurate approach. The Hybrid Mesh Network Security architecture has the right DNA to deliver this, and fulfils the promise of consistent, effective, high-performance security across the organization, while optimizing costs and boosting ROI. It is the underlying driving force behind Check Point's Infinity Platform, which offers all the security enforcement form factors mentioned above. With Harmony SASE at its core, the Infinity Platform harnesses Harmony Browse, Harmony Mobile, Harmony SaaS, Harmony Enterprise Browser, Quantum appliances and CloudGuard cloud security. All working in concert with a unified management system, and powered by ThreatCloud AI, our AI-driven threat intelligence service. ThreatCloud AI consists of more than 50 AI-powered threat analysis engines, delivering a 99.9% block rate, the highest in the industry, as tested and validated by Miercom.



Check Point's Infinity Platform, powered by architecture, delivers the security and performance organizations need to succeed in today's AI-driven hyperconnected world.

Check Point's SASE solution, the core component of Hybrid Mesh Network Security, is already used by thousands of customers to deliver a more secure, and up to 10x faster user experience, while reducing cloud associated costs. We are continuously investing more resources, including a new dedicated development center in India, to further enhance our SASE solution. We are also continuously investing in unifying policies across all Check Point's Hybrid Mesh Network Security components, including SASE, and on-prem and cloud firewalls, for a more streamlined experience and stronger and more consistent security.

Benefits

Check Point's Hybrid Mesh Network Security architecture delivers numerous benefits:

- Flexible deployment model to best match any network architecture
- Tightly integrated approach for simplicity and ease-of-use.
- Unified Policy and Management
- Delivers optimal performance, security and cost
- Open garden approach, enabling integration with 3rd party solutions

To learn more

- CPX keynote – Securing the Hyperconnected world in the era of AI
- CPX keynote – Strategy in Action
- Infinity Platform – web page
- Infinity Platform – solution brief
- Miercom report

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

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