The Essential SASE for Enterprises eBook

Practical Solutions for Today's Network Security Challenges

Achieving Flexibility, Security, and Performance in Enterprise Networks

It's no easy task to manage a modern enterprise network. Large companies face unique challenges requiring solutions that allow them to remain agile and efficient. Without the right balance, vulnerabilities quickly emerge, creating weak spots that adversaries can exploit.

Cloud deployments increase flexibility; however, without proper visibility, they pose significant security risks

On-premises servers provide stability for mission-critical legacy applications, but limit scalability and responsiveness to business demands

A hybrid workforce with both remote and in-office employees introduces unique challenges to secure access

Branch offices have special connectivity needs and access considerations

Essential software-as-a-service (SaaS) platforms such as Salesforce, Microsoft 365, and Google Workspace require special attention to security aspects

These diverse needs make it difficult to maintain a consistent security posture that considers the full network attack surface.

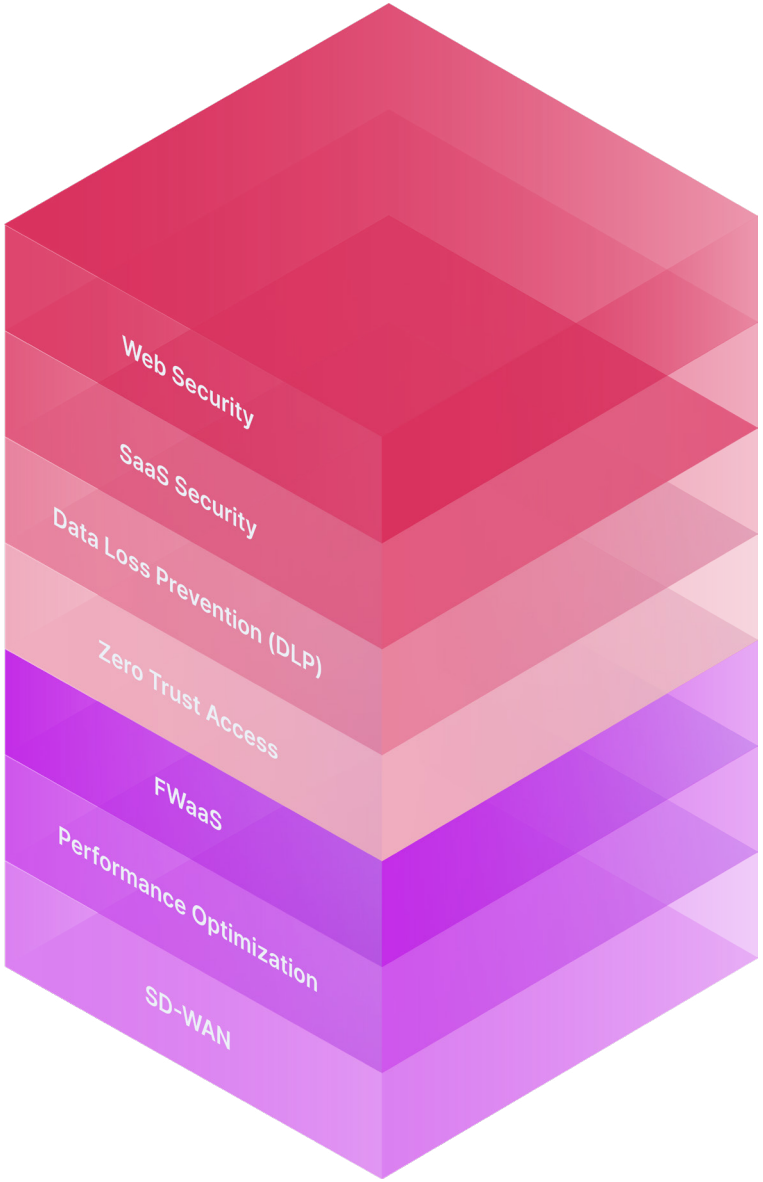
Juggling the demands of an enterprise network requires a perfect balance of security and performance. Let's take a tour through practical network security use cases enterprises face daily and explore how Secure Access Service Edge (SASE) solves these challenges for a secure, unified, and productive network environment.

Management and Visibility

Before anything else, an enterprise IT team needs management control and visibility into the network. It doesn't matter how good your tools are, if the IT team cannot see what's going on within the network it leaves your organization vulnerable.

Most companies use a patchwork of point solutions meant to solve a specific need. A typical enterprise might use separate solutions for SD-WAN, VPN, and endpoint security, leading to management silos and increased vulnerability.

A unified SASE service brings the essential elements of network security into one console. If problems do arise, the increased visibility means the team is better prepared to deal with them within a single, cohesive view.



Secure Access to Cloud and On-Prem

IT administrators for the modern enterprise must support secure connections from anywhere to anywhere, worldwide. For example, a remote sales team needs to access on-prem with the same reliability as office employees.

SASE transforms the corporate VPN from a few clustered locations into a globally distributed network, offering robust, secure access for enterprise teams of any size.

This global reach ensures that employees experience consistent performance and security. By eliminating legacy VPN bottlenecks, SASE also improves productivity and simplifies IT management.

Application-by-Application Access Permissions

Enabling a secure connection regardless of location is only part of modern secure access. Organizations also need to ensure only authorized personnel can access company data and resources. A key part of SASE is to dole out user permissions on a per-application basis. Not per server, or data center, or region – but per application.

The idea of per-application permissions is based on the Zero Trust model where no one is assumed to be trustworthy by default. Each access request is evaluated based on identity and context such as device posture, location, and time of day.

This ensures both security and productivity: employees access the data they need, while attackers are kept from moving across your network.

SaaS Security

Software-as-a-service platforms like Salesforce, Microsoft 365, Monday.com, and Asana are an essential part of modern work but are easily identifiable targets. A SASE solution can ensure that only your workforce accesses data stored in enterprise SaaS solutions by using IP address allowlisting. This means that, even if an attacker gains credentials, they will be blocked unless they are accessing from an approved IP address managed by the SASE service—adding an extra layer of security beyond simple permissions.

In addition to access, SaaS security requires visibility into SaaS platforms. One of the primary ways to do this is inline shadow IT discovery where the SASE solution monitors traffic to see exactly which SaaS platforms employees are using—both sanctioned and unsanctioned. This is critical since employees may be uploading company data to unsanctioned SaaS platforms without necessary safeguards.

Just as important, however, is visibility into how users are connecting sanctioned SaaS to other SaaS applications. Consider an employee integrating a sanctioned file-sharing SaaS with a lesser-known task management app. Without IT visibility, sensitive documents could be accessed and shared without proper controls, creating a major blind spot.

Consider an employee integrating their Microsoft 365 account with multiple unsanctioned mail app as shown in Fig. 1. Without IT visibility, sensitive documents could be accessed and shared without proper controls, creating a major blind spot.

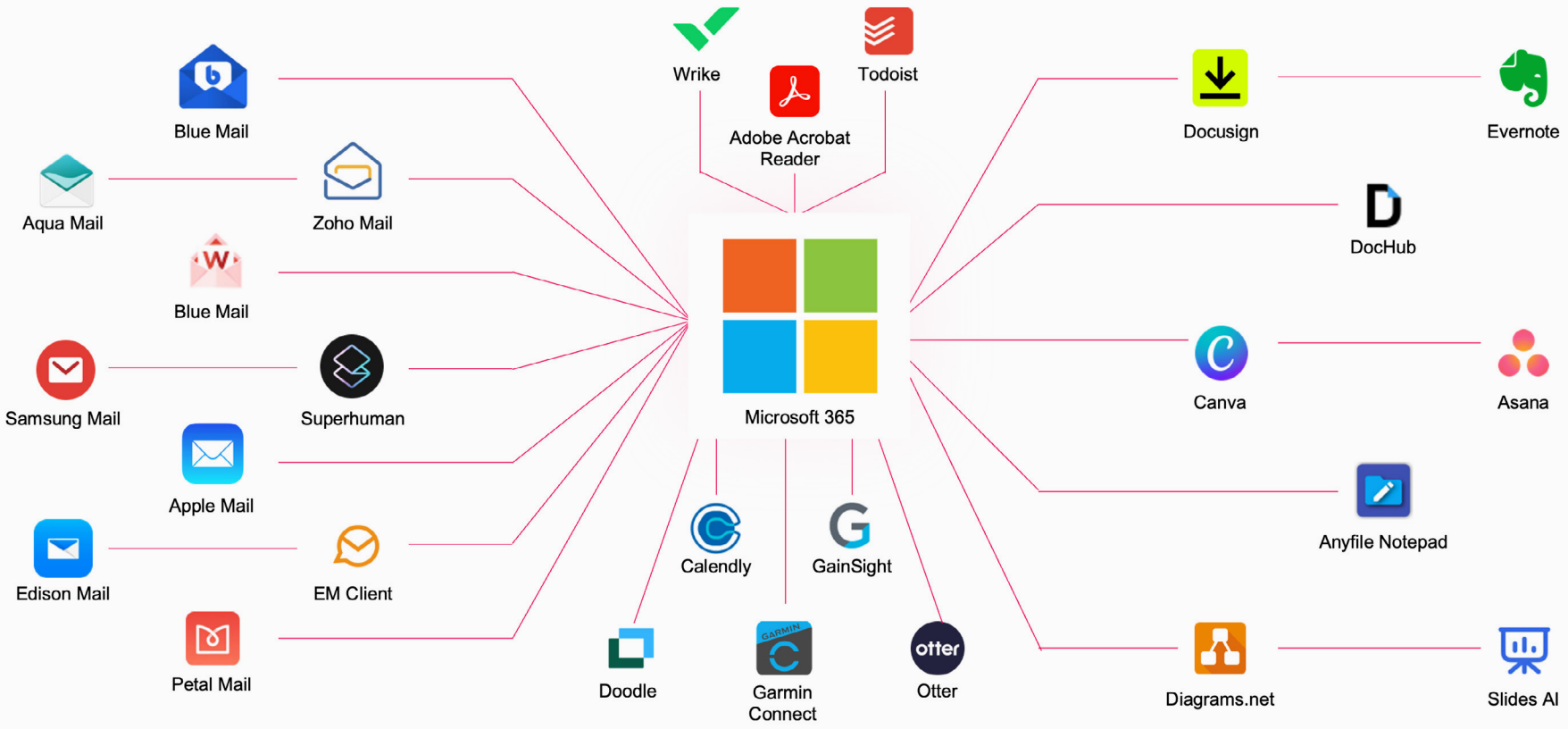

Blue Mail
Aqua Mail
Zoho Mail
Blue Mail
Samsung Mail
Superhuman
Apple Mail
Edison Mail
EM Client
Petal Mail
Wrike
Adobe Acrobat Reader
Todoist
Microsoft 365
Calendly
GainSight
Doodle
Garmin Connect
Otter
Docusign
Evernote
DocHub
Canva
Asana
Anyfile Notepad
Diagrams.net
Slides AI

Fig.1

Networking

Fast connections are key for ensuring a consistent and secure experience for employees, whether they are working from home, a branch office, or on the road. Legacy MPLS-based networks are cost-prohibitive, complex to maintain, and can be limited in terms of direct cloud access. These outdated models are difficult to scale in a modern enterprise setting, where remote work and global teams require efficient connectivity.

SASE integrates advanced networking capabilities, offering a robust solution to these challenges.

By leveraging a global backbone, SASE provides flexible connections to cloud services and applications wherever employees are located.

This approach is scalable and flexible, providing full mesh networking capabilities that ensure each location can connect directly to one another as needed without a performance penalty.

Employees enjoy faster connections without compromising security, and IT teams benefit from centralized network control and simplified policy management.

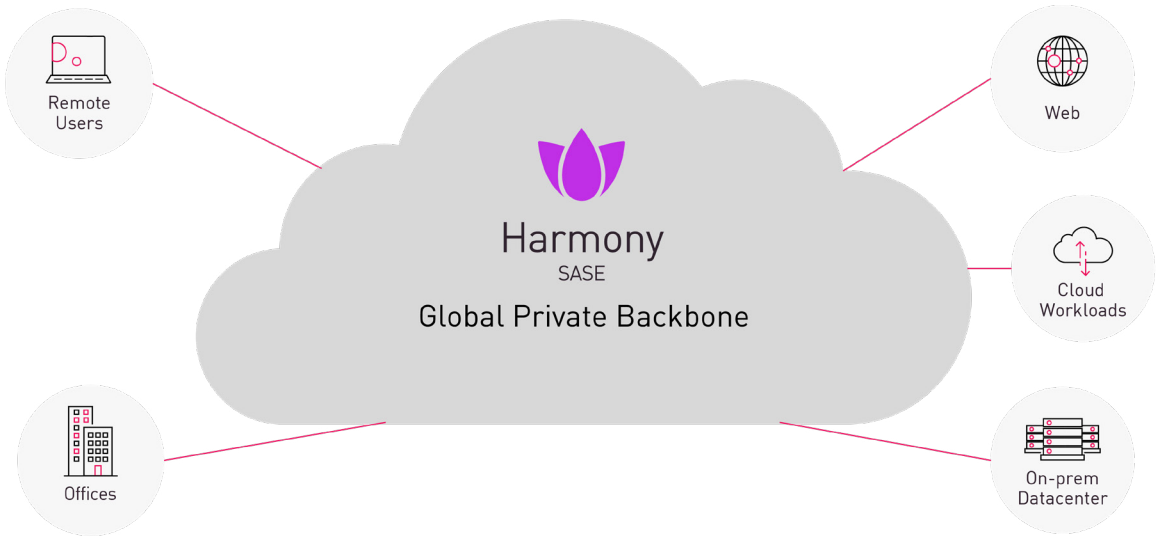


Fig.2

Agentless Access

Enterprises increasingly work with contractors and partners, as well as support BYOD scenarios where traditional agent-based security isn't always practical. Granting secure access to these users is challenging—too few permissions create productivity bottlenecks, while too many can open significant vulnerabilities.

A SASE secure agentless access model lets temporary users access the resources they need without installing security agents. Access is instead granted to individual applications through a secure web portal.

By eliminating the need for complex DMZs, Harmony SASE also reduces attack surface areas and limits potential entry points for cyberattacks. This allows IT to manage access securely while simplifying the overall process.

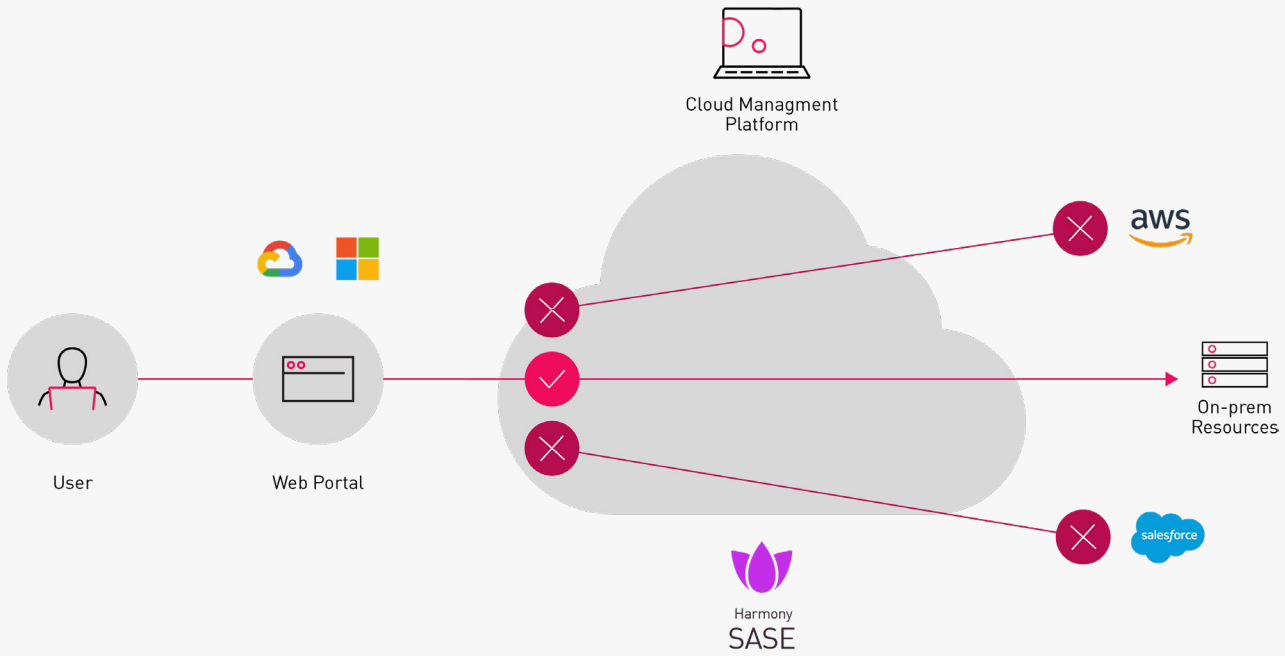


Fig.3

Harmony SASE:
The Unified Solution for Enterprise Network Security Challenges

Check Point delivers a comprehensive solution for enterprise network security, combining flexibility, security, and performance to meet modern organizational demands.

Unified Management and Visibility

Consolidates network security into a single management console, enabling IT teams to monitor and respond to threats efficiently. By reducing reliance on multiple point solutions, it minimizes security gaps and frees IT to focus on strategic tasks.

Secure, Scalable Access Anywhere

With over 75 global points of presence (PoPs), Check Point supports secure access to both on-premises and cloud resources from any location, with robust, optimized connectivity for office teams, remote workers, and contractors worldwide.

Zero Trust Application Access

Enforces Zero Trust Network Access (ZTNA) with per-application permissions, ensuring users access only what they need. This limits attack surfaces and prevents lateral movement, maintaining strong security.

Comprehensive SaaS Security

Secures SaaS applications with IP-based allowlisting and it prevents unauthorized integrations that could lead to data leaks or compliance issues.

Harmony
SASE

Safe Internet Browsing

Integrates advanced threat protection, allowing employees to browse freely while blocking web-based threats through real-time analysis and zero-day detection, ensuring productivity without compromising security.

Additionally supports zero-day phishing protection—critical given that approximately 90% of phishing sites are only active for one day—providing proactive protection that keeps threats at bay before they can become major problems.

Agentless Access for Flexibility

Supports agentless access for contractors, partners, and BYOD scenarios through a secure web portal, reducing complexity and minimizing attack surfaces for temporary or external users.

The solution is also a unified and scalable solution to address evolving enterprise network security needs—providing flexibility, security, and performance in a single platform.

Advanced RDP Support

Organizations using standard RDP clients can initiate agentless connections directly to remote desktops, removing the limitations of RDP over HTTPS being confined to a browser tab. Additionally, organizations can create policies to connect each user to a specific RDP host based on their identity. With a single access rule, enterprises can establish a dynamic access policy that determines the assigned RDP host for each user, whether on web-based or native-client RDP connections.

Learn more about how Check Point can transform your network security strategy.

Schedule a Demo

Harmony
SASE

Meet Check Point's SASE

2x Faster Internet Security | Full Mesh Private Access | Secure SD-WAN

The internet is the new corporate network, leading organizations to transition to SASE. However current solutions break the user experience with slow connections and complex management.

Check Point's SASE is a game-changing alternative that delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Check Point's SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Using Check Point's SASE, business can build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Check Point's SASE is part of our Workspace Suite, which helps organizations of all sizes secure their workspaces with a suite of products covering network security across browsers, devices, and cloud.

To learn more,
visit https://www.checkpoint.com/harmony/sase/
or schedule a demo.

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