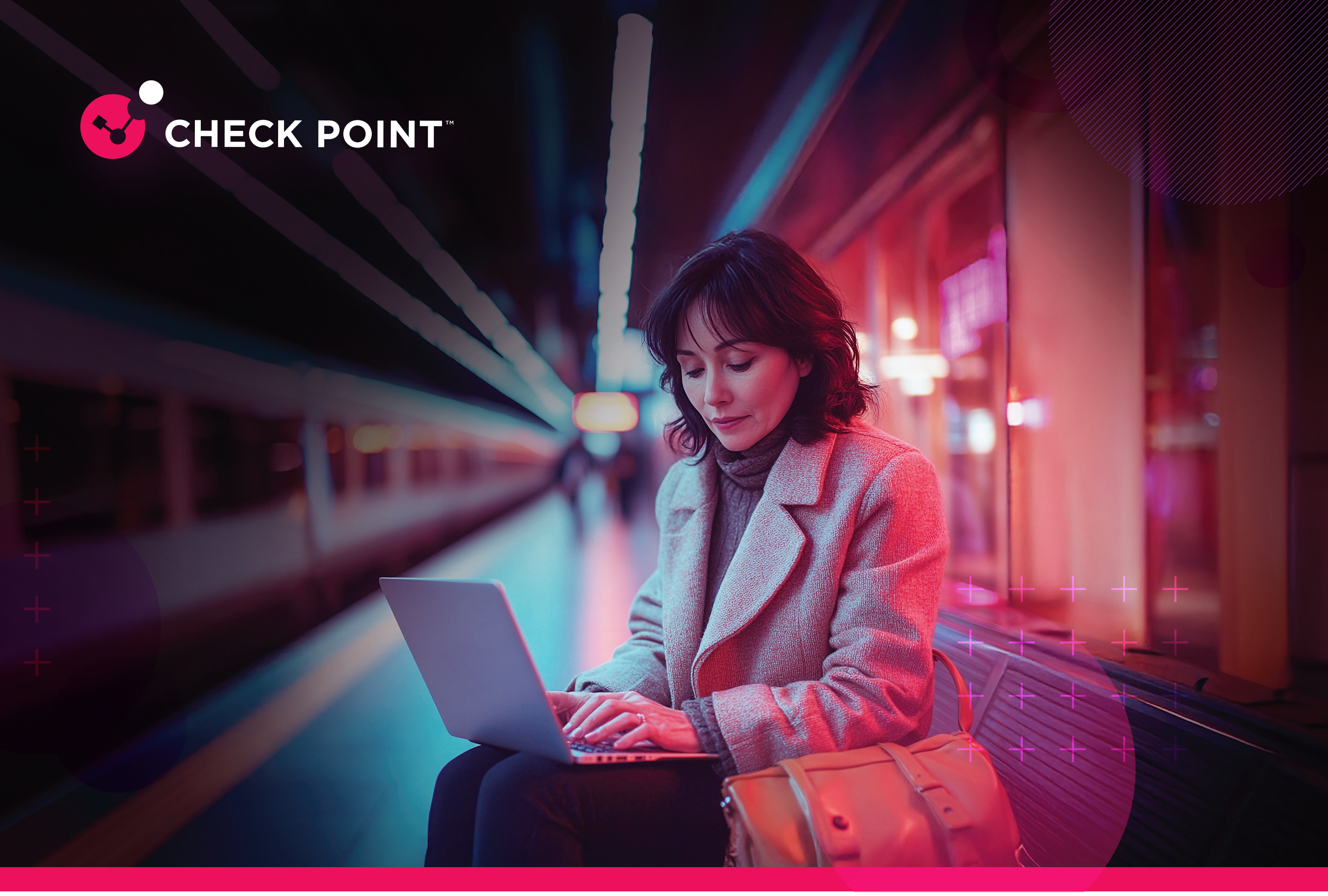
CHECK POINT™



CHECK POINT SASE

Unified Network Security for the AI Age

Security Beyond the Perimeter

Organizations are navigating fundamental shifts in how users access applications and data. Cloud services, SaaS, AI adoption, and hybrid work are creating a distributed, borderless environment that traditional security can't protect.

The result is a fragmented network architecture that creates security gaps and operational complexity:

- **Multi-Cloud Infrastructure:** 89% of organizations use two or more public cloud services[1]
- **Distributed workforce:** 88% of organizations support hybrid work models requiring least privileged access to sensitive corporate applications across cloud, SaaS, and data centers[2]
- **AI Adoption Explosion:** 75% of global knowledge workers are using AI in their jobs, adding potential productivity boosts and security risks[3]

At the same time that legacy network borders break down, the overall volume and sophistication of cyberattacks continue to rise. AI is further fueling this trend by helping attackers automate campaigns and rapidly evolve malware.

SASE has emerged as the architectural framework that addresses this fragmented landscape and expanding threat environment.

By converging network and security functions into a cloud-delivered platform, the SASE approach enables organizations to block threats that isolated point solutions miss, accelerate incident response, and improve the end user experience.

Meet Check Point SASE

Unified 10x Faster Internet Security, Zero Trust Access, SaaS Security, Mobile Security, and SD-WAN

BENEFITS

- **Single-vendor SASE** that consolidates diverse security capabilities into one streamlined platform
- **Blazing-fast secure internet access** for remote users and branch offices
- **Zero Trust Access** with full mesh connectivity between users, branches, and applications
- **Powerful visibility and control** over SaaS application use within your network
- **GenAI protection** for shadow AI discovery, DLP, risk scoring and categorization, and per-user, prompt-level visibility
- **Optimized SD-WAN connectivity** with full branch-level security and leading threat prevention
- **Fast deployment** and intuitive administration
- **Backed by Check Point ThreatCloud AI** our global threat intelligence platform that aggregates data from millions of sensors worldwide and 50+ AI engines to update protections in real-time

While organizations are shifting to SASE, their current solutions break the user experience with slow connections and complex management.

Offering a game-changing alternative, Check Point SASE delivers 10x faster internet security combined with full mesh Zero Trust Access, SaaS Security, Mobile Security, and optimized SD-WAN performance.

With a local browsing experience supporting tighter security and privacy, Check Point SASE boasts innovative on-device network protections and secures any enterprise application by integrating with your existing identity providers to enforce granular access policies for everyone: employees, contractors, and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized internet and network connectivity, ensuring uninterrupted web conferencing thanks to seamless link failover and a built-in steering policy for over 10,000 applications.

The Check Point SASE platform reduces operational friction and closes security gaps that are common to fragmented stacks.

[1] Flexera, "Cloud computing trends: Flexera 2024 State of the Cloud Report," 2024, https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/

[2] Robert Half, "Remote Work Statistics and Trends for 2025," 2025, https://www.roberthalf.com/us/en/insights/research/remote-work-statistics-and-trends

[3] Microsoft, "AI at Work Is Here. Now Comes the Hard Part," 2024, https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part

Blazing-Fast Secure Internet Access

Check Point SASE Internet Access delivers 10x faster performance by fundamentally redesigning how traffic is secured. Unlike traditional SASE solutions that suffer from cloud backhauling, our **hybrid architecture** can inspect traffic locally on the device, thereby optimizing speed and privacy while maintaining rigorous security enforcement.

- **Hybrid Architecture:** Delivers on-device inspection to bypass unnecessary cloud processing for blazing-fast browsing, and a localized experience that respects data residency requirements and privacy
- **Comprehensive Threat Prevention:** Delivers unified security including web filtering, malware protection, and advanced threat prevention that moves with the user, offering consistent protection regardless of location
- **Browser security:** Integrated protection against phishing, malicious downloads, corporate password reuse, and risky search results

GenAI Protection

GenAI adoption is growing fast as individual workers, teams, and organizations look to maximize their productivity through automated processes and workflows. But this also presents a critical security threat requiring significant attention to protect against data leakage and compliance violations.

GenAI Protection from Check Point SASE prevents critical data from leaking out of your organization and provides detailed intelligence on generative AI usage by your workforce. Gain prompt-level visibility, risk scoring for platforms and user sessions, and real-time data loss prevention.

- **Identify and monitor:** See how employees are using sanctioned and shadow GenAI apps
- **Risk Scoring:** Understand user intent and assess risk
- **Use AI to secure AI:** Accurately discover and classify data within conversational prompts with AI-powered analysis
- **Use case categorization:** Uncover what GenAI is used for within your organization
- **Set Policies:** Restrict or allow GenAI platforms with granular policies and copy/paste restrictions
- **Coach Users:** Check Point's interactive user experience can advise users when they are about to take a risky action or block it outright

Full Mesh Zero Trust Access

Check Point SASE Private Access replaces legacy VPNs and fragmented access tools with a Full Mesh Zero Trust architecture. Instead of just connecting users to apps, Check Point SASE creates a global, software-defined network in minutes connecting users, sites, clouds, and resources with effective Zero Trust access policies.

- **Identity-Centric Access:** Apply least privileged access to any enterprise resource by integrating your existing Identity Providers (IdP) to enforce policies based on user role, groups, and context that accommodates employees, contractors, and partners alike
- **Agentless & Managed Access:** Secure BYOD, partners, and consultants with frictionless agentless web access
- **Contextual Device Posture:** Validate device health (OS version, antivirus status, and more) before granting access and during connections, ensuring only safe devices are allowed on the network
- **Reliable, high-performance connectivity:** Delivers a superior user experience with low-latency connectivity over a full mesh global private backbone of 80+ PoPs
- **Seamless deployment:** Create networks and bring them online quickly to interconnect your sites, data centers, clouds, and users via an intuitive cloud console

SaaS Security

Check Point SASE provides comprehensive visibility into your SaaS (software as a service) applications ensuring complete coverage of your cloud environment. It automatically discovers and maps your SaaS ecosystem, eliminating the manual work of discovering and securing hundreds or even thousands of third-party integrations.

- **Shadow SaaS Discovery:** Expose hidden risks by creating a complete mapping of your organization's SaaS interconnectivity, including every application, plugin, and API
- **Risk Remediation:** Shrink your attack surface by continuously monitoring SaaS configurations with alerts and remediation for security gaps, misconfigurations, and compliance violations
- **Application Control:** Allow or disallow access to specific SaaS applications based on corporate policies and compliance requirements
- **Extensive reporting** covering services, integrations, users, and tokens, with actionable insights and recommendations to enhance your security posture
- **Identity & Anomaly Detection:** Leverages AI to detect data theft, supply chain attacks, and account takeover by analyzing behavioral indicators, threat intelligence, and historical data on SaaS activity within and across organizations
- **Automated Compliance:** Maintains continuous regulatory adherence with alerts and fixes for compliance mistakes as well as changes in your supply chain, ensuring tight regulatory adherence and an audit-ready posture

Advanced Threat Prevention

Check Point SASE blocks known and unknown threats before they reach your users or data. By leveraging Check Point's ThreatCloud AI we deliver the industry's best catch rate (99%) with near-zero false positives.

- **Threat Emulation (sandboxing):** Identifies unknown malware by running suspicious files in a controlled virtual environment
- **Data Loss Prevention (DLP):** A unified DLP engine prevents sensitive corporate data from being uploaded to unauthorized web or cloud environments
- **Anti-Bot Protection:** Detects and blocks outbound traffic from infected devices to botnet command-and-control servers, neutralizing botnet threats
- **Optimized Performance:** Fast, seamless protection that preserves performance even for remote workers

Mobile Security

Mobile Security extends the power of Check Point SASE to smartphones and tablets, closing the security gap for your most vulnerable endpoints. Consolidate Zero Trust Access and Mobile Threat Defense (MTD) into a single, lightweight app optimizing the user experience while ensuring consistent security policies across all devices.

- **Zero-Phishing Protection:** Blocks phishing across all applications preventing credential theft, including from zero-day threats
- **Safe Browsing and Anti-Bot:** Prevents access to malicious sites and C2 servers
- **Comprehensive App & File Protection:** Leverages ThreatCloud AI and sandboxing to detect malicious apps and block malware downloads before they reach device storage
- **Wi-Fi and DNS Security:** Detects man-in-the-middle (MitM) attacks and enforces safe DNS policies, ensuring users are protected on public Wi-Fi
- **Device Posture Validation:** Automatically blocks access from compromised or non-compliant devices to protect corporate data
- **Zero-Touch Deployment:** Deploys via your MDM (Mobile Device Management) or UEM (Unified Endpoint Management) platform for seamless management
- **Privacy-First Design:** No performance impact or personal data collection
- **Secure Remote Access:** Secure Zero Trust access to corporate resources from company- or employee-owned mobile devices

Enterprise Browser

For organizations that require secure access and advanced protection for unmanaged devices, Check Point Enterprise Browser solves this "BYOD Gap" by creating a secure, isolated workspace on any device. It eliminates the need for a persistent agent allowing you to safely onboard contractors and partners while still enforcing security posture, controlling data, and preventing lateral movement.

- **Data Isolation & Auto-Wipe:** Isolates corporate apps and data from the host device, preventing unauthorized data transfers. When the session ends critical corporate data is wiped from the device
- **Agentless Posture Validation:** Verifies the security posture of unmanaged devices before granting access, despite the absence of a persistent agent
- **Integrated DLP Controls:** Prevents unauthorized data exfiltration via downloads, copy-paste, printing, or screen captures, with options such as on-screen watermarks
- **Full Session Recording and Auditing:** Provides complete visibility and reporting for user actions within the browser

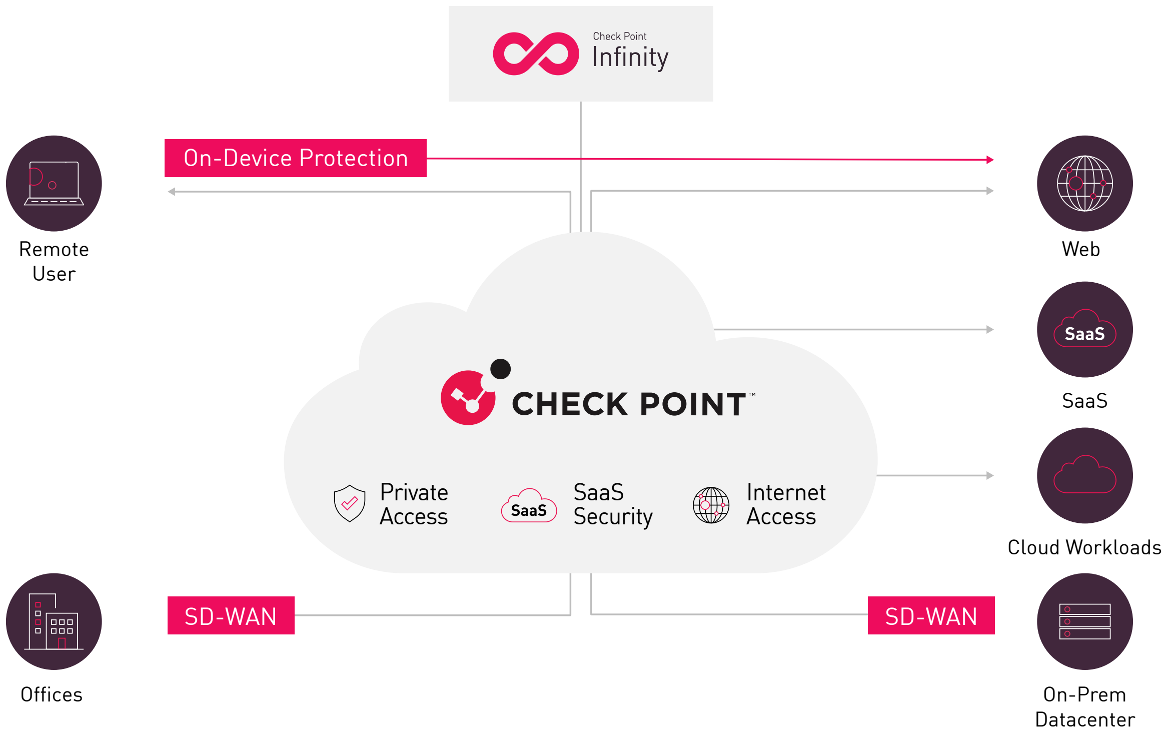
SD-WAN Unified with Industry-Best Security

Check Point SD-WAN unifies the best security with optimized internet and network connectivity, ensuring uninterrupted web conferencing thanks to seamless link failover and an automated steering policy, combined with robust management and site protection.

- **Uninterrupted User Experience:** Ensures smooth web conferencing with sub-second WAN link failover with support for broadband internet, 5G cellular, and MPLS connections
- **Intelligent Path Optimization:** Routing for 10,000+ applications and users, with auto-steering based on link health including jitter, packet loss, latency
- **Unified Branch Security:** Zero-touch provisioning with a full branch-level security stack and industry-leading threat prevention

Unified SASE Architecture

Optimizing Security and Connectivity



Check Point SASE Feature Overview

FEATURE	DESCRIPTION
Zero Trust Network Access / Private Access	
Network access	Supports all protocols, full mesh access in any direction, all connections subject to policy with posture and identity
Agentless web access	Supported with reverse proxy, option for URL alias and customer certificate
Agentless enterprise browser	Zero Trust access for unmanaged devices with corporate data sandboxing and DLP protections including session recording and watermarking
Agentless RDP access	• Web Interface (HTML RDP), or native RDP agent (configurable options) • Support multiple screens, local printing • Security control option to limit copy-paste and printing • Configurable RDP security mode and authentication
Agentless RDP with dynamic access control	Use a single access rule, to establish a dynamic access policy that determines which specific RDP host is assigned to each user, based on IDP attribute
Agentless VNC access	Web interface
Agentless SSH access	Web interface
Device posture validation checks	Endpoint Security, Certificate, Disk Encryption, File exists, registry key, process running, windows security center, domain membership
Posture validation profiles	Multiple profiles, support all OSs
Continuous validation	Yes, configurable intervals
Additional zero-trust validations (access context)	Geo-location, Date and Time, OS, Browser
DNS filtering	Cloud resolver with DNS filtering
Firewall	Identity-based Firewall-as-a-Service
Secure Internet Access	
Malware protection	Scan all downloaded files and web components
Sandbox protection	Utilizing Check Point Threat Emulation technology and ThreatCloud AI (1)
Content Disarm and Reconstruction (CDR)	Utilizing Check Point Threat Extraction technology and ThreatCloud AI (1)
Zero-day phishing protection	Utilizing Check Point Zero-Phishing technology and ThreatCloud AI (1)
URL reputation protection	Utilizing Check Point Anti-Bot and ThreatCloud AI
URL filtering	Utilizing Check Point's URL categorization with 110 categories
HTTPS inspection	Yes
DLP	
Predefined data types	700+ including PCI, PII, HIPAA, source code and many more (1)
Supported data object types	Pattern, Keyword, Dictionary, Weighted Words, Template, File attribute (1)
Microsoft Purview sensitivity labels	Supported (1)
OCR analysis	Supported (1)

Requires the following license: (1) Browser security. (2) SaaS security. (3) Collaboration security.

FEATURE	DESCRIPTION
Cloud Service	
SLA	99.999%
Cloud Points-of-Presence (PoPs)	80+ global POPs, privately owned
Cloud backbone	Private backbone consisting of at least dual tier-1 providers at each PoP for fast connectivity across our network
Multiple cloud networks per customer	Support for multiple networks per account for more flexible network architectures and faster M&A consolidation
Full mesh connectivity in any direction	Full mesh cloud-based networking enables seamless private access connectivity in any direction (e.g. data center to branch, branch to user, etc.)
Network-to-Site connection	Connect from any device using IPsec, or connect with Connector software
Network-to-Site protocols	IPsec IKEv1, IPsec IKEv2, Wireguard, OpenVPN
Redundancy	Support for redundant tunnels to separate availability zones or regions
User-to-Site protocols	Agent: Wireguard, OpenVPN
Dedicated cloud IP per customer	Standard for all customers, enables IP-whitelisting for zero-trust access to SaaS
SD-WAN integration	Integrated with Check Point SD-WAN. Connect with 3rd party SD-WAN via IPsec
Dynamic Routing	Yes, using BGP
Data residency	United States, European Union
SASE Agent	
Supported platforms	Mac, Windows, Linux, iOS, Android, Chromebook
On-device network security - Hybrid SASE	Network security controls for Internet Access (SWG) are enforced within the agent (optional), and subject to customer policy, are routed directly to the internet service without cloud routing. This capability enables users to experience their native internet speed and delivers internet performance that is double that of traditional SSE/SWG services which force all traffic through the cloud.
Split tunnelling	Yes
Disconnect when in trusted networks	Yes
Connection protocol	Wireguard or OpenVPN - configurable
Prevent user sign-out	Yes, option to issue one-time disconnect code
Connect on launch	Yes, Configurable
Connection notification	Yes, Configurable
Control agent upgrade	Yes, Configurable per OS
Automatic Wi-Fi security	Yes, Configurable
Automatic log-out	Configurable
Identity Management	
Supported IDPs	Microsoft Entra ID, Okta, Google Workspace, Active Directory, Generic SAML (OneLogin, JumpCloud, etc.)
Authentication	SAML 2.0
Identity Management	SCIM
Multiple IDPs	Yes
Local user database	Yes
Reset user password	Yes

Requires the following license: (1) Browser security. (2) SaaS security. (3) Collaboration security.

FEATURE	DESCRIPTION
SaaS API Security	
SaaS application catalog [3]	10,000+ SaaS applications Display per application: Name, Description, Publisher/Vendor, Category, Website, Risk Assessment, Certification, Privacy Policy, Terms
SaaS application discovery	Discovered SaaS applications are categorized, monitored and assigned a risk score
SaaS visibility and monitoring [3]	Extensive reporting covering services, integrations, users, and tokens, with actionable insights and recommendations
SaaS Anomaly Detection [3]	Yes
Supported SaaS apps: Threat Prevention and SSPM [3]	Asana, Atlassian, AWS, BambooHR, Bitbucket, Box, Dropbox, Freshdesk, GitHub, GitLab, Google Workspace, HubSpot, Jira, Microsoft OneDrive, Microsoft SharePoint, Microsoft Teams, Monday, Okta, OneLogin, Ping Identity, Salesforce, ServiceNow, Slack, Smartsheet, Zendesk, Zoom
Supported SaaS apps: DLP and Threat Prevention[2]	Microsoft OneDrive, Microsoft SharePoint, Microsoft Teams, Google Drive, Dropbox, Box, Slack, Citrix ShareFile [3]
SaaS Security	
SaaS Application Control	Identifies HTTP/S application traffic and enforces allow/drop actions.
Logs and reports	
Log retention	3 months by default, extended period available at an additional cost
Event forwarding to SIEM	Supported using syslog
Activity monitoring	Active sessions, User activity, Web and remote access and threat prevention, Audit Logs
Certification	
SOC2 Type 2 Compliance	Certified
ISO 27001, ISO 27002	Certified
ISO 9001	Certified

Requires the following license: (1) Browser security. (2) SaaS security. (3) Collaboration security.

Discover Check Point SASE

Don't compromise on an excellent user experience to secure your shift to hybrid and cloud.

To see the latest alternative, sign up for a demo of Check Point SASE.

To learn more visit: https://www.checkpoint.com/