GUIDE TO NETWORK SECURITY FOR THE AI ERA

Securing Today's Hyperconnected Enterprise

CHECK POINT™

TABLE OF CONTENTS

CHECK POINT

INTRODUCTION

The only constant in cyber security is change. Cloud-first strategies, globally distributed, hybrid workforces, hyperconnectivity, and the ubiquity of encrypted traffic are now normal considerations for security leaders as they plan and evolve security strategies. But the challenges don't stop there. AI-driven threats are escalating in speed, scale, and sophistication, outpacing traditional defenses and reshaping the risk calculus for enterprises around the world.

This change has impacted network security and the firewall as well. No longer just a gateway between internal networks and external threats, the modern firewall has evolved into a foundational element of distributed Zero Trust architectures. But to remain effective, firewalls must now operate as intelligent, scalable nodes within a hybrid mesh: a dynamic, cloud-aware security fabric capable of defending an increasingly fragmented digital environment.

This eBook explores the evolution of network security, examining how the firewall has been redefined for today's security demands, and why legacy approaches fall short in a world of decentralized applications, hybrid clouds, and advanced threats. We'll share insights into what modern security leaders should demand from their firewalls and how hybrid mesh firewalls are enabling end-to-end protection across users, devices, and workloads, wherever they reside.

Whether you're reassessing your current infrastructure or planning for future resilience, this guide is designed to help you better examine the firewall's role in your broader cyber security strategy.

CHECK POINT™

01 THE DISTRIBUTED THREAT LANDSCAPE

The cyber security landscape is evolving faster than most organizations can react. Attacks are no longer isolated or opportunistic. They are persistent, multi-pronged, and increasingly automated. Nation-state actors and cyber criminal groups now leverage AI, deepfakes, and disinformation to manipulate environments both digitally and socially. At the same time, ransomware groups have become more agile, shifting from large-scale encryption to data theft and extortion. Infostealers are flooding underground markets with stolen credentials, and cloud misconfigurations continue to leave doors wide open.

This rapidly expanding threat landscape demands more than just incremental improvements in security—it calls for a foundational shift in how we defend our networks. That's where next generation firewalls come in.

Traditional firewalls were never built to manage the complexity of today's hybrid, cloud-connected, and edge-driven environments. They can't see or stop modern threats that span cloud APIs, IoT devices, encrypted traffic, or AI-generated malware.

Next generation, AI-enhanced firewalls are designed to be intelligent, adaptable, and context-aware. They're not just filters—they're decision engines that bring visibility, control, intelligence, and threat prevention to the heart of your network architecture.

Insights from our State of Cyber Security Report 2025 underscore the changes in the threat landscape, including the rise of AI-powered disinformation campaigns, ransomware groups that now specialize in data exfiltration, and infostealers that exploit unsecured devices and stolen VPN credentials to quietly infiltrate networks. These trends reveal a growing need for security solutions that go beyond basic traffic inspection to provide deep behavioral analysis, real-time threat detection, integrated response, and automated cross-vendor exposure remediation .

DOWNLOAD REPORT

CHECK POINT

We explored the current state of cloud security in our annual Cloud Security Report and found similar issues with complexity, advanced threats, and a lack of preparedness from cyber leaders.

DOWNLOAD REPORT

Over 65% of organizations experienced a cloud-related incident in the past year, yet most still struggle with delayed detection and tool sprawl. The average organization uses over 10 different cloud security tools—and half receive more than 500 alerts per day. This alert fatigue not only overwhelms teams, it creates dangerous blind spots, especially as adversaries now use automation to orchestrate multi-vector attacks that blend cloud, endpoint, and IoT exploits.

AI-enabled firewalls are uniquely positioned to close these gaps. With capabilities like intrusion prevention systems, encrypted traffic inspection, application-layer filtering, integrated threat intelligence, sandboxing, threat extraction, and Zero Trust policy enforcement, modern firewalls provide the visibility and control security teams so clearly need . When deployed effectively, they help consolidate tools, reduce alert noise, and provide a unified front against threats that span users, devices, cloud environments, and remote endpoints.

CHECK POINT™

02

THE ARCHITECTURAL SHIFT DRIVING THE NEXT GENERATION OF FIREWALLS

CHECK POINT

The digital transformation (sparked by the growth of public and private cloud networks) that gained momentum some 15 years ago has fundamentally reshaped enterprise IT, and with it the structure and function of corporate networks. Once built around centralized data centers and relatively predictable traffic flows, today's networks are highly dynamic. Cloud workloads span geographic regions and providers. Every large organization is multi-cloud. Applications and data continuously move between private data centers, SaaS platforms, and the edge.

And the way we work has also shifted considerably, with employees and contractors working from coffee shops, home offices, and airports and accessing enterprise resources with a variety of managed and unmanaged devices. In this highly distributed model, the network perimeter no longer exists as a fixed location. It now expands and contracts, truly moving at the speed of business.

From Centralized Infrastructure to a Borderless Network

Enterprise security has historically been focused on protecting a well-defined perimeter. Firewalls could be placed at key network choke points to inspect traffic and enforce policies. But in today's hybrid and cloud-first environments, this approach is far too limited. Modern networks are fluid, operating beyond the guiderails of the past. Users and workloads appear and disappear dynamically. Identities shift and with 90% of internet traffic now encrypted, visibility and control is more complex and challenging than ever.

THE LIMITS OF TRADITIONAL NEXT GENERATION FIREWALLS

Context Awareness: They lack the ability to understand who the user is, what application they're using, or where they're located.

Inconsistent Policy Enforcement: With environments spanning on-prem, cloud, and hybrid networks, traditional firewalls can't apply uniform policies across all platforms.

Lateral Movement Blind Spots: Once attackers breach one part of the environment, they can move laterally undetected. Older firewalls weren't built to inspect internal traffic patterns or encrypted east-west traffic.

Encrypted Traffic Inspection: With encryption now the default, firewalls must inspect traffic at scale without compromising performance. This weak point is a particular challenge for many legacy platforms.

Our new reality demands a more comprehensive approach to security. Even traditional next-generation firewalls can fall short. Often architected to inspect traffic at centralized locations, relying on static IPs and fixed infrastructure, they no longer provide a full picture of user behavior and traffic.

Tool Fragmentation and the Siloed Security Dilemma

In the race to solve some of the above-mentioned limitations, many organizations have created a patchwork of specialized tools to help keep them protected. This tool sprawl, combining endpoint detection, email gateways, cloud security brokers, SIEMs, and dozens of platforms, has made it common practice for IT leaders and operations teams to be managing a multitude of disparate solutions all with the aim of creating a "seamless" security strategy.

But rather than solving the problem, this approach has created an ecosystem of operational silos. Each tool has its own policies, data feeds, and identity sources. Synchronizing these systems is time-consuming and error-prone. Zero Trust principles, including enforcing least-privilege access and continuous verification, have become difficult to implement consistently across so many disconnected platforms. Policy conflicts go unnoticed, compliance suffers, and incident response is time intensive, taking away from higher priority work.

The result: fragmented security that cannot respond effectively to modern threats.

Security Operation Center (SOC) teams have now become overwhelmed by the volume and complexity of alerts (a particularly acute challenge given the global cyber security skills shortage), while NOC teams struggle with poor visibility, manual troubleshooting, and extended downtime.

CHECK POINT™

Security Gaps and Threat Response Challenges

When one enforcement point doesn't share threat intelligence or vulnerability exposure insights with another, gaps emerge. An endpoint solution might block a file, but that intel doesn't inform cloud or email systems, especially if those are other vendors' products.

This fragmented architecture allows attackers to find the weakest link and exploit it, very often gaining access through a single misconfigured or outdated system. Once attackers have gained access, they can move laterally and escalate privileges before detection.

Without a unified threat detection and prevention layer, organizations are left with incomplete visibility into attacks, increased dwell time, inconsistent remediation efforts, and SOC team burnout from alert overload and manual response fatigue.

CHECK POINT™

03

FROM PERIMETER GUARD TO HYBRID MESH SECURITY FABRIC

CHECK POINT

The modern IT estate is sprawling, dynamic, and constantly adapting to the changing demands of business. For cyber security to keep up, it must protect across a hybrid landscape where on-prem data centers, multiple cloud environments, branch offices, and remote workers interweave. To protect this environment next generation firewalls have evolved beyond perimeter gatekeepers into identity-aware enforcement points, embedded throughout your infrastructure.

No longer confined to network edges, modern firewalls are engines of Zero Trust, designed to apply micro-segmentation, inspect traffic (even encrypted with TLS 1.3), and prevent threats in real time, not just detect them. They understand who is connecting, from where, on what device, and why. They decrypt and inspect traffic at scale, enforce least-privilege access control, and keep threats at bay before they spread laterally.

Introducing the Hybrid Mesh Firewall

What has emerged to protect the modern network is the hybrid mesh firewall. The hybrid mesh is a fabric of enforcement points—physical devices, virtual firewalls in the cloud, and firewall-as-a-service (FWaaS)—all united under a centralized, cloud-based orchestration plane. Policy updates, threat intelligence, and enforcement happen seamlessly, regardless of location.

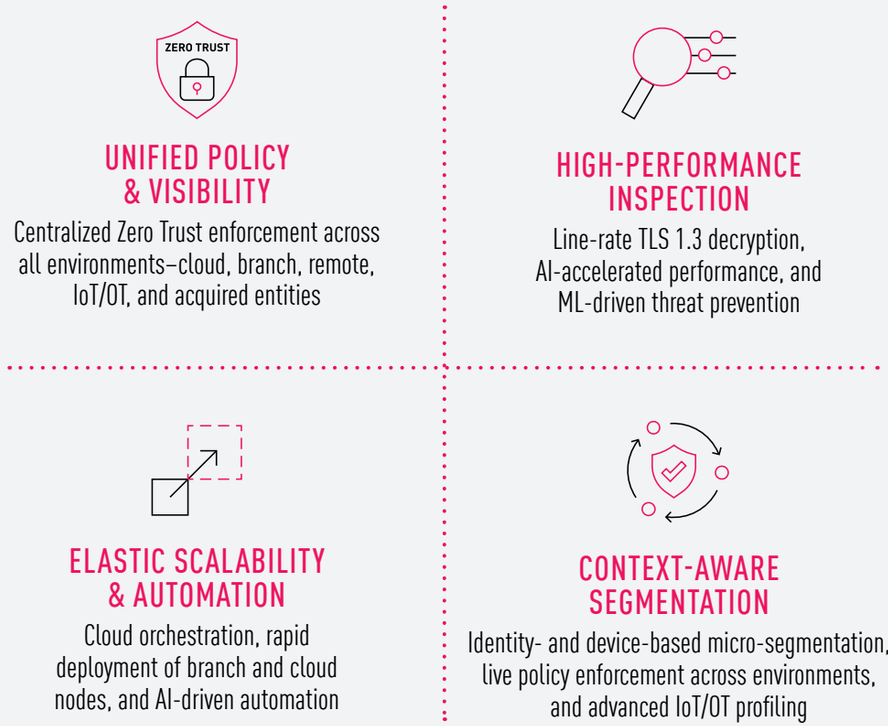
Core Capabilities of the Hybrid Mesh Firewall

- Consistent Zero Trust enforcement, regardless of where users and workloads reside
- Scalable TLS 1.3 decryption and inspection
- Micro-segmentation and identity-based controls, tying policy to users and devices, not IPs
- Real-time threat prevention powered by AI/ML across edge, cloud, and FWaaS deployments
- Central orchestration, offering a single dashboard and unified policy engine across environments
- Elastic scalability, using virtual instances and cloud orchestration to meet demand dynamically

CHECK POINT™

Building a Cohesive Hybrid Security Fabric

By combining these capabilities, enterprises can construct a hybrid mesh security architecture with four key attributes:



Hybrid enterprises demand security architectures that go with the flow, maintaining agility while protecting complexity.

By architecting a cohesive security fabric—integrating SASE, branch SDWAN security, cloud-native firewalls, IoT/OT defense, and rapid integration for seasonal scalability or acquisitions—organizations can deliver consistent, high-performance Zero Trust security without sacrificing speed or visibility.

Check Point Quantum: A Modern On-Premises Firewall for a Modern World

Consider Check Point's Quantum firewall line as a benchmark for what modern, on-prem next-gen firewalls can achieve. Powered by more than 50 AI engines and real-time threat intelligence from the Check Point ThreatCloud AI, Quantum gateways block 99.9% of zero-day attacks—far outpacing the industry average.

Our Quantum R82 software release added four more AI engines, blocking an additional 500,000 attacks per month, and introduced post-quantum encryption capabilities. Quantum appliances also deliver 99.999% resiliency through automated clustering and scale to terabit-level throughput with NVIDIA-powered acceleration.

Stacked against competitors in third-party comparative testing, Check Point was the threat prevention leader:

CHECK POINT
99.74%
phishing URL block rate, surpassing Palo Alto (98.69%), Fortinet (97.39%), Zscaler (91.12%), and Cisco (55.87%)

CHECK POINT
99.9%
malware block rate in SASE environments, ahead of Cisco (96%) and Fortinet (84%)

CHECK POINT
98%
block rate against high-severity CVEs in intrusion prevention tests—significantly higher than Cisco (42.6%) and Zscaler (72.5%)

Check Point's Quantum architecture presents the case for what's possible when firewalls are reimagined—built to be so much more than static gatekeepers, but as proactive, AI-enhanced guardians of the modern enterprise.

CHECK POINT™

04 EVALUATING YOUR FIREWALL READINESS

CHECK POINT™

Is your Firewall Built for 2026 and Beyond?

The network security trends that are shaping modern cyber security strategy—an elastic perimeter, an emphasis on cloud deployments and multi-cloud configurations, and the extensive use of encryption—mean that security leaders need to think differently about protecting the network.

As digital transformation accelerates and threats become more sophisticated, simply patching or adding tools to legacy infrastructure isn't enough. Firewalls that were once positioned at the network edge are now expected to defend a much broader and more complex digital terrain—including the cloud, remote users, SaaS applications, and IoT/OT environments.

CHECK POINT

If you're considering a firewall upgrade, here's where to begin:

Understand Your Risk Surface

Today's enterprise isn't defined by a data center, it's a hybrid mesh of cloud workloads, branch locations, remote employees, and connected devices.

Key Questions:

- **Where does sensitive data live and travel?**
- **Who is accessing what—and from where?**
- **Are IoT/OT assets visible and protected?**
- **How much of your traffic is encrypted, and can you inspect it effectively?**
- **How are you managing vulnerabilities across your multi-vendor security stack?**

Align to Zero Trust and Distributed Enforcement

Upgrading your firewall isn't just about performance or throughput—it's about architecture.

Modern security strategies must move beyond perimeter-centric thinking. Instead, you need distributed enforcement, where policies are enforced consistently across every location—on-prem, cloud, remote, and edge.

This is the essence of a Zero Trust architecture: always verify, never trust.

What this looks like in practice:

- **Identity-aware enforcement:** Policies based on user, device, and context—not just IPs or zones
- **Cloud-native integrations:** Firewalls that extend into AWS, Azure, and SaaS ecosystems
- **Unified policy management:** One console to define and deploy Zero Trust rules everywhere
- **Real-time AI-driven prevention:** Block threats across all environments—not just detect and log them

CHECK POINT

Four questions to help evaluate your firewall readiness

1

Can your firewall enforce Zero Trust across environments?

Zero Trust isn't just a framework—it's a necessity. If your firewall can't apply identity-based access controls consistently across cloud, branch, remote, and on-prem environments, your defenses are already behind. Modern threats pivot between users and workloads. Only context-aware firewalls that tie policy to identity, device posture, and real-time access decisions can enforce Zero Trust effectively.

2

Can it decrypt and inspect encrypted traffic (TLS 1.3)?

With most modern attacks hidden inside encrypted traffic, firewalls must inspect TLS 1.3 sessions without compromising speed or user experience. If your firewall can't decrypt and scan at scale—or does so at the cost of latency—it becomes a blind spot. Modern firewalls built for 2025 need hardware acceleration and intelligent TLS handling to stay both fast and secure.

3

Does it provide AI-powered threat prevention or just alerting?

Detection alone isn't enough. By the time alerts reach the SOC, damage may already be done. Firewalls must now prevent threats in real time, using AI and machine learning to block zero-day attacks before they spread. Check Point's Quantum Force firewalls combine real-time threat intelligence with AI-driven engines to automatically block advanced attacks, including those targeting encrypted channels or using lateral movement.

4

Is policy centrally managed and identity-aware?

Managing siloed firewall policies across clouds, offices, and virtual networks leads to drift, misconfigurations, and gaps. Firewalls must now be part of a hybrid mesh architecture, allowing centralized policy enforcement that adapts dynamically to users, devices, and workloads—wherever they reside.

CHECK POINT™

05 CHECK POINT'S HYBRID MESH FIREWALL

What enterprises need today isn't just a better firewall. They need a smarter, more adaptive approach to security—one that's built for complexity, speed, and scale.

Check Point's Hybrid Mesh Firewall is more than just a firewall. It's an enterprise-wide security framework built for the complexities of a hybrid world. Whether your focus is Zero Trust, encrypted traffic inspection, scaling into cloud, or protecting remote teams, Check Point gives you the confidence to move fast, and do so with the highest level of security efficacy.

A Smarter, More Adaptive Firewall for Modern Enterprises

Check Point's Hybrid Mesh Firewall unifies multiple firewall form factors into a single, cloud-delivered management system. It supports on-premises, virtual, cloud-native, and firewall-as-a-service (FWaaS) enforcement points, making it ideal for organizations with hybrid networks and diverse security needs.

Security teams get reduced complexity, better scalability, and unmatched threat prevention, all managed with simplicity through a single pane of glass.

AI-Powered Threat Prevention for a Fast-Moving World

The modern threat landscape is evolving rapidly, characterized by highly disruptive zero-day exploits, AI-generated phishing schemes, and ransomware that spreads at machine speed. Traditional firewalls often rely on detection and alerting after threats are already in motion.

At the heart of Check Point's Hybrid Mesh is ThreatCloud AI, a real-time threat intelligence engine powered by over 50 AI engines and data from 150,000+ networks. This powerful AI delivers a prevention-first approach that blocks threats before they enter your network, with a proven 99.9% malware block rate and 99.7% phishing prevention.

Check Point shifts the paradigm from reactive defense to proactive protection, empowering security teams to prevent attacks instead of just mitigating them.

Encrypted Traffic Without Blind Spots

More than 95% of all internet traffic today is encrypted. While this protects privacy, it also creates blind spots where attackers can hide malicious payloads.

Unlike legacy firewalls that degrade performance when inspecting SSL/TLS traffic, Check Point offers full SSL/TLS inspection, including support for TLS 1.3 and HTTP/3, without sacrificing speed or stability. Enterprises gain deep visibility into encrypted traffic—without latency, broken apps, or performance trade-offs.

Zero Trust Enforcement at Every Layer

Today's enterprise is perimeter-less. Users and workloads move dynamically, requiring access policies based not on IP addresses but on identity, posture, and context.

Check Point's Hybrid Mesh Firewall delivers true Zero Trust enforcement with identity-based controls that integrate seamlessly with identity providers like Azure AD and Intune. Whether segmenting applications, securing remote access, or enforcing device compliance, organizations can reduce lateral movement and prevent privilege abuse across all environments.

Securing IoT and OT (Because Everything Is Connected)

From smart HVAC systems to industrial sensors, modern enterprises rely on countless IoT and OT devices. There are also many more devices tied into their wireless or physical networks, including streaming audio devices, personal cameras, mini refrigerators, printers, personal AI assistants, and other devices that are not authorized or secured. Firewalls must include automatic scanning and detection to analyze and secure all IoT devices to maintain protection.

Check Point's Hybrid Mesh Firewall brings these blind spots into view with automatic discovery, classification, and segmentation of connected devices. With protocol-aware policies and compliance templates, even legacy or industry-specific devices can be secured—no forklift upgrades required.

CHECK POINT™

Hyperscale Security for Expanding Enterprises

As organizations scale, opening new branches, migrating to the cloud, or integrating acquisitions, their security must be flexible and intelligent enough to meet the demands of growth.

Check Point delivers this scalability through Maestro Hyperscale Orchestrator and ElasticXL, enabling you to increase performance and capacity with a few clicks. When paired with Quantum Force appliances, offering up to 1.5 Tbps of threat prevention, enterprises get seamless growth without rearchitecting their security infrastructure.

Unified Console, Unified Strategy

One of the biggest challenges in enterprise cyber security is security sprawl and fragmentation, juggling multiple consoles, tools, and policies across various environments.

Check Point solves this with the Infinity Platform, offering:

- SmartConsole for unified policy management (available for on-prem)
- Infinity XDR and Playblocks for automated incident response and ready-made with playbooks with 100+ security vendors
- AI-driven tools for threat hunting, compliance auditing, and health monitoring
- Multi-vendor automated threat remediation for consistent virtual patching and IoC sharing across multi-vendor security stacks/environments

This unified approach not only boosts visibility but also enables faster, more confident decision-making—across remote offices, data centers, clouds, and mobile workforces.

Integration with Cloud Orchestrator

Integration with cloud and on-prem orchestrators offer dynamic, automated policy enforcement across your entire environment. As cloud workloads spin up or change, the firewall automatically applies the right security controls without manual intervention. This "set-and-forget" model simplifies administration and ensures consistent protection across all cloud assets.

WHY CHECK POINT LEADS IN HYBRID MESH FIREWALL

Security Built for Now—and What's Next

The Check Point Hybrid Mesh Firewall i sn't just a new firewall—it's a new model for enterprise defense. It meets today's challenges head-on: encrypted traffic, policy sprawl, visibility gaps, and performance bottlenecks. But more importantly, it's built for where your business is going.

From real-time threat prevention to Zero Trust enforcement and hyperscale readiness, Check Point empowers your organization to operate confidently in a distributed world.

Industry-Leading Threat Prevention

- Highest-rated malware and phishing block rates (Miercom 2025 Benchmark)
- Global threat intel shared across all enforcement points within 2 seconds

Agility to Scale Anywhere

- High-throughput Quantum Firewalls for on-prem needs
- Harmony SASE for cloud-delivered FWaaS and agentless access
- CloudGuard Network for dynamic policy enforcement in hybrid clouds

Unified AI-Powered Platform

- Infinity Portal: a single interface for managing security operations, compliance, and threat intelligence
- Infinity XDR and Playblocks for streamlined SecOps workflows
- Automated threat exposure remediation across multi-vendor security stacks
- AI Copilot reduces security administrative task time

Predictable, Flexible Pricing

- Infinity Platform Agreement includes all hardware, software, services, and support under one annual per-user model
- Easily transition between enforcement points without license restrictions

CHECK POINT™

Core Components of Check Point's Hybrid Mesh Firewall

ENTERPRISE NETWORKS

Hyperscale data centers, SD-WAN, industrial-grade appliances, integrated DDoS & IoT protection

HYBRID WORKFORCE

FWaaS, agentless access, Zero Trust enforcement, mesh connectivity

HYBRID CLOUDS

Cloud network security, WAF, cloud detection & response, per-workload policy enforcement

SECURITY OPERATIONS

ThreatCloud AI, XDR/XPR, AI Copilot, MDR/MPR, incident response, training

CHECK POINT™

06 REAL-WORLD SUCCESS STORIES

CHECK POINT

CASE STUDY

BOTSWANA POWER CORPORATION SECURES ITS INFRASTRUCTURE, ITS BUSINESS, AND ITS MANAGEMENT'S CONFIDENCE WITH CHECK POINT

Overview

In the past five decades, Botswana Power Corporation (BPC) has played an integral role in developing Botswana. The organization provides energy transmission and distribution across the country. Moving forward, BPC is increasing the use of renewable energy in its mix as it continues to bring electricity to underserved rural areas and empower citizens.

Business Challenge

Evolving Security for Digital Transformation

From lighting up classrooms and connecting students to the world through the internet, to powering the plants that provide clean water, BPC has helped build the nation of Botswana. Digital transformation is shaping its next steps into the future. As part of a larger digital transformation strategy, BPC undertook a security assessment to align its cyber security posture with its business goals and the current threat landscape.

Power organizations like BPC operate and maintain strategic infrastructure, which has increasingly come under cyber attack. Making matters worse, organizations in Africa are targeted more than those on any other continent. According to Check Point Research, an average of 1,848 attacks per week target an organization in Africa compared to 1,164 attacks per week for organizations globally. Ransomware attacks lead the pack, with email as the most prevalent attack vector.

"From our initial security assessment, it was clear BPC needed to evolve its security posture," said Godfrey Mathumo, IT infrastructure and Operations Manager for BPC. "Previously we had used multiple security vendors and solutions, but they were not keeping pace with digital transformation and the evolving threat landscape."

Upgrading security involved taking many factors into consideration. As a power company, BPC endpoints include not just desktops, laptops, and servers—they also include supervisory control and data acquisition (SCADA) and operational technology (OT) systems located in substations and power plants. BPC's environment had become even more complex when the pandemic forced many employees to work remotely, relying heavily on mobile and BYOD devices, cloud access, and internet connectivity. The security operations team needed to ensure comprehensive security and visibility across all of its environments—enterprise, endpoints, cloud, collaboration, SOC, and OT.

BPC had also adopted National Institute of Standards and Technology (NIST) and ISO 27001 as governance frameworks for monitoring security posture. It needed an easier way to measure progress and compliance performance against these standards.

> "With Check Point, we're able to quantify our security. Our management team is very enthusiastic because they can actually see the control we have. We can show where a vulnerability might exist, or report that we're 100% compliant. Reporting visibility is invaluable for executive decision-making and planning."
>
> - Godfrey Mathumo,
> IT infrastructure and Operations Manager, Botswana Power Corporation

Solution

A Strong Defensive Framework

BPC's security assessment spanned every area of the organization, from endpoints and mobile devices to cloud and virtual environments. In addition to upgrading security infrastructure, the team wanted to improve security controls and manageability.

Check Point Quantum Security Gateways in high-availability clusters form the network security infrastructure cornerstone. They provide ultra-scalable protection from sophisticated Gen-V cyber attacks against networks, data centers, OT, and users. Quantum is powered by Check Point ThreatCloud, which combines AI technology with big data threat intelligence to prevent the most advanced attacks while reducing false positives.

"Check Point Quantum Security Gateways are not just firewalls," said Mr. Mathumo. "They deliver everything—IPS, application control, threat emulation and extraction, identity awareness, and more. We can see our applications across the organization. We can see VPNs and how they are secured. We can even see compliance with our governance frameworks."

CloudGuard Network Security protects BPS assets and workloads to, from, and across the organization's Azure and AWS public clouds, as well as in its VMware ESXi virtual environment. Industry-leading advanced threat protection and single-pane-of-glass management make it easy for the BPC team to ensure they have the same comprehensive security protection in the cloud as on premises.

Protecting Users and Devices

The BPC team manages more than 1,300 endpoints. They deployed Check Point Harmony Endpoint to prevent the most advanced threats from affecting users and devices. Harmony Endpoint automates 90% of attack detection, investigation, and remediation tasks. It identifies ransomware behaviors and safely restores ransomware-encrypted files automatically. Zero-phishing technology identifies and blocks the use of phishing sites in real time. BPC is also protected from malware, file-less attacks, and credential theft.

"Check Point Harmony Endpoint is one of the most brilliant solutions we've seen," said Mr. Mathumo. "With endpoints under management, we can ensure they are compliant with our policies. We can dictate which devices and software versions can connect to our network to minimize the risk of threats entering through endpoints."

Check Point Harmony Mobile also is applied to all mobile devices. It delivers the same granular visibility in managing device security and isolating any device that might be compromised. Check Point Email & Collaboration extends visibility and protection into BPC's Office 365 and Microsoft environments. It blocks advanced phishing, malware, and ransomware attacks before they reach the inbox, and it prevents sensitive business data from leaving the organization.

> "We chose Check Point for our upgrade. Not only did Check Point address all of our environments, it provided specific control capabilities that we needed combined with the visibility to see everything, everywhere."
>
> - Godfrey Mathumo,
> IT infrastructure and Operations Manager, Botswana Power Corporation

"Check Point Infinity SOC also has been great for us," said Mr. Mathumo. "Now, our SOC team can see any vulnerability across our network, clouds, endpoints, mobile, and OT environments. Infinity SOC allows them to quickly expose, investigate, and shut down attacks."

Benefits

Infrastructure. Secured.

The new security infrastructure has dramatically improved BPC's security posture. Prior, the BPC team was dealing with thousands of malware and phishing attempts. With Check Point automatically handling prevention, as well as detection, investigation, and remediation, threats have dropped to almost zero.

"Central management has greatly simplified everything," said Mr. Mathumo. "We can manage all of our gateways deployed in multiple places in one pane of glass. We can manage all policies in one place. Check Point enables us to ensure consistent protection everywhere."

Securing the Business

Maintaining IT compliance with NIST and ISO 27001 benchmarks is an ongoing objective, but ensuring high security standards for all parts of the business is just as critical. Harmony Email & Collaboration and CloudGuard defend the company's Microsoft cloud-based solutions. Integration with enterprise platforms has been a huge benefit as well.

"We've integrated Check Point with our SAP ERP environment," said Mr. Mathumo. "Now we can ensure that our devices and users are secure—especially in the finance area—and we can see the posture at a glance. This has been one of the biggest benefits of our Check Point solutions."

Earning Management's Confidence

Check Point reporting capabilities have enabled the BPC IT team to document vulnerabilities, threat activity, and compliance gains. They know what's going on and can confidently report status to upper management to demonstrate that the company is operating securely.

> "We needed to manage and monitor user identities as they accessed our cloud from outside the network. With our Azure cloud, AWS cloud, and VMware ESXi environments connected to CloudGuard, we can see everything. CloudGuard makes it easy to monitor and manage our cloud security posture."
>
> - Godfrey Mathumo,
> IT infrastructure and Operations Manager, Botswana Power Corporation

"With Check Point, we're able to quantify our security," said Mr. Mathumo. "Our management team is very enthusiastic because they can actually see the control we have. We can show where a vulnerability might exist or report that we're 100% compliant. Reporting visibility is invaluable for executive decision-making and planning."

Growing Forward

Check Point Professional Services helped BPC map its security architectural requirements and identify the most optimal solutions for today and tomorrow. The Check Point team transferred knowledge and best practices to the BPC team and continues to provide monthly updates and assistance.

"I would give Check Point Professional Services and support a 10 out of 10," said Mr. Mathumo. "Whenever we need assistance—24x7—we call and they respond immediately. Check Point delivers a secure environment and has done well for us. We would definitely recommend them."

"Shift left capabilities are critical going forward," said Nix. "We're monitoring code now with CloudGuard and plan to make code security automatic and part of the normal DevOps pipeline."

"CloudGuard is great," he continued. "Some products out there focus only on compliance, some on posture, and some only on DevOps. CloudGuard does it all, and it was the key determinant for us."

> "Check Point Harmony Endpoint is one of the most brilliant solutions we've seen. With endpoints under management, we can ensure they are compliant with our policies. We can dictate which devices and software versions can connect to our network to minimize the risk of threats entering through endpoints."
>
> - Godfrey Mathumo,
> IT infrastructure and Operations Manager, Botswana Power Corporation

CHECK POINT

CASE STUDY

VANQUIS' DIGITAL TRANSFORMATION: SECURELY PAVING THE WAY TO SCALABLE, AGILE BANKING

Overview

Vanquis Banking Group, a FTSE All Share company, is a leading specialist bank, established in 1880. Vanquis Banking Group lends responsibly, providing tailored products and services to 1.75 million UK customers through Vanquis, Moneybarn, and Snoop.

Business Challenge

West Yorkshire-based Vanquis Banking Group is amid a wide-ranging digital transformation to modernize its operations and enhance customer service. The transformation aims to streamline and consolidate its technology stack, enhance customer experience, and optimize internal operational efficiency.

As part of its transformation, Vanquis Banking Group has shifted to a cloud-first organization. The bank is carefully consolidating several discrete technology stacks into a single cloud infrastructure and set of applications. Until this transformation, the bank relied on several hybrid cloud environments that consisted of on-premises and cloud-based infrastructures.

> "We're thrilled that we chose Check Point. Check Point has a storied cyber security history. Check Point has the pedigree, and Check Point has the experience to meet our security needs."
>
> - John Rogerson, Senior Cloud and Infrastructure Manager, Vanquis Banking Group

While several technology stacks arose through acquisitions over the years, it meant operating, managing, and securing entirely different environments. "We wanted to remove these silos and to combine our technology stacks," said John Rogerson, Senior Cloud and Infrastructure Manager at Vanquis Banking Group.

When fully complete, the transformation will be enormously beneficial when managing its technology stack, making it more straightforward, practical, and agile when responding to changing business demands and evolving customer expectations. "Our data centers will probably disappear, and all those on-premises workloads will go into the cloud," said Rogerson of the transformation.

Rogerson knew a new consolidated technology stack would require a new security architecture, and a consolidation of the security tools used to defend those separate technology stacks. "When those organizations were running separately, and with their separate teams, they had different security tools because each team operated with their preferred technology," Rogerson explained. "But as we centralize, we don't want three different types of firewalls and other security defenses," he added.

Rogerson and the Vanquis security team set out to find the right security solutions to match the bank's new unified architecture and support its need for agility and responsiveness.

Solution

After thoroughly assessing available security platforms, Rogerson and the team selected Check Point Software Technologies to secure the bank's digital transformation and new cloud architecture. "Check Point has deep knowledge, expertise, and an understanding of cyber security. They are the trusted name people recognize within the cyber security industry," Rogerson said.

Rogerson and the team are deploying Check Point to gain a unified view and consistent policy management across all their networks. Quantum Security Gateway provides Vanquis access control and threat prevention for its on premises networks and CloudGuard Network Security protects the bank's cloud assets and workloads in Azure environments. CloudGuard Network Security provides Vanquis unified cloud-native capabilities for its cloud workloads and the same AI-powered threat prevention and access control capabilities as Quantum across Azure and other cloud vendor WANs.

Outcome

With Check Point, Vanquis is confident they can secure their consolidated technology stack with security capabilities that Check Point now unifies. "Previously, we had a mishmash of different products doing that. As new workloads migrate into the cloud, we can be confident they're secured," Rogerson said.

Now that Vanquis Banking Group is well underway consolidating the various on-premises systems and security from three business units into a single technology stack, they can enhance and transform their applications more rapidly, get new technologies to market more swiftly, and more readily respond to changing business conditions. "It's a given that we'll be working with Check Point going forward," Rogerson said. "Now that we are full pelt into our transformation journey, the ongoing approach will be to continue to migrate cloud and capabilities onto the new technology stack and secure it with Check Point."

> " Check Point has deep knowledge, expertise, and an understanding of cyber security. They are the trusted name people recognize within the cyber security industry."
>
> - John Rogerson, Senior Cloud and Infrastructure Manager, Vanquis Banking Group

"Having a robust level of security at the perimeter of our cloud environment and knowing that we mitigated potential weaknesses makes us more comfortable and confident that we have the right levels of security in place today," Rogerson said. "We're thrilled that we chose Check Point. Check Point has a storied cyber security history. Check Point has the pedigree, and Check Point has the experience to meet our security needs," Rogerson said.

CHECK POINT™

07 THE FUTURE OF FIREWALLS

AI-Powered, Autonomous Defense

As AI continues to become a larger part of our tech ecosystem and business strategies, the need for smarter, more agile network security will only grow. Traditional firewalls, while still essential, are no longer enough to stand against the velocity and sophistication of modern cyber attacks.

Technologies are already building even more advanced firewalls that are AI-powered, autonomous hybrid mesh firewalls. These systems represent a significant step forward, enabling real-time threat mitigation, policy adaptation, and environment-wide protection without constant human oversight.

Driven by AI, automation, and contextual awareness, our future firewalls will revolutionize how organizations secure their digital assets.

There are six core capabilities that will define this new paradigm of intelligent cyber security.

Self-Learning Defense

Tomorrow's firewalls will feature the ability to continuously learn from network behavior. Instead of relying solely on static rule sets or signature-based detection, self-learning defense systems apply machine learning to observe and understand traffic patterns. These systems identify anomalies, adapt to new threat vectors, and fine-tune policies in real time—all without the need for constant manual configuration. The result is a more responsive and intelligent defense posture that gets smarter and more effective over time.

This adaptive capability reduces both false positives and missed threats. And unlike legacy systems that require frequent updates and manual tuning, self-learning firewalls automatically evolve to detect and block zero-day exploits and previously unseen attacks. This proactive approach significantly reduces the time window in which threats can operate, giving security teams a powerful ally in the fight against cyber crime.

CHECK POINT™

Proactive Threat Hunting

The future of firewalls won't include waiting for threats to trigger alerts before taking action. The next generation flips this model with proactive threat hunting, where AI actively seeks out suspicious patterns using real-time analytics. By ingesting and correlating global threat intelligence feeds, these firewalls can identify subtle signs of malicious activity across vast networks. This enables early detection of coordinated attacks, ransomware campaigns, and insider threats before they cause significant harm.

Rather than relying solely on known indicators of compromise, these systems leverage behavioral analysis and predictive modeling to identify potential risks based on emerging trends. This shift from reactive to proactive dramatically enhances an organization's defensive capabilities. Security teams gain visibility into hidden or stealthy threats that might otherwise bypass traditional perimeter defenses, allowing for faster containment and remediation.

Autonomous Policy Optimization

One of the most time-consuming and error-prone aspects of firewall management is policy configuration. Autonomous firewalls solve this problem by employing intelligent policy optimization algorithms. These algorithms dynamically adjust rules and configurations to align with business needs, user behavior, and threat levels. The system ensures that policies are neither overly permissive nor unnecessarily restrictive, thereby reducing false positives and maintaining optimal network performance.

Keep in mind, automation does not sacrifice control. Security administrators retain oversight while the system handles the heavy lifting of continuous optimization. Manual policy tuning can, in turn, be minimized, freeing up IT teams to focus on higher-level strategic work.

With autonomous policy optimization, firewalls become self-regulating systems that can keep pace with both the threat landscape and the business's evolving needs.

Context-Aware Decisions

Modern security can no longer rely solely on IP addresses or port numbers for decision-making. Next-gen firewalls incorporate contextual awareness, taking into account user identity, device posture, application behavior, and even user intent. This enables granular, risk-based access control that adapts in real time based on the current context of the user and environment. For example, access might be permitted for a trusted user on a managed device but denied for the same user on an unknown or compromised endpoint.

Context-aware decision-making also enables more nuanced and intelligent security policies. It allows organizations to implement dynamic access models like Zero Trust, where access is continually assessed and revalidated based on evolving risk factors. This not only enhances security, but also improves user experience by minimizing unnecessary barriers for legitimate users. In an increasingly mobile and cloud-driven world, contextual intelligence is essential for ensuring secure, seamless access.

CHECK POINT

Zero-Touch Operations

Firewall management has historically involved manual tasks like rule cleanup, policy enforcement, and alert triage. Zero-touch firewalls automate these processes through advanced orchestration and AI-driven decision-making. They can automatically remove outdated rules, enforce compliance standards, and detect anomalies, all without human intervention. This greatly reduces the administrative burden on IT teams and helps maintain a clean, efficient rulebase.

Beyond efficiency, zero-touch operations also improve security posture by eliminating configuration drift and ensuring consistent policy enforcement across distributed environments. As organizations grow and adopt more hybrid and multi-cloud architectures, manual operations become untenable. Automated systems ensure that policies are not only applied correctly but also kept up-to-date and aligned with business goals. The result is a leaner, faster, and more reliable security infrastructure.

Adaptive Across Environments

Large organizations operate across diverse infrastructures—on-prem, public cloud, private cloud, and everything in between. Firewalls must be capable of adapting seamlessly across these environments, ensuring consistent protection without requiring separate rule sets or isolated management consoles. AI-powered firewalls provide unified visibility and control, automatically scaling and securing workloads no matter where they reside.

This adaptability is essential for businesses embracing cloud-native applications, containerization, and remote workforces. With centralized intelligence and distributed enforcement, these firewalls can apply policies uniformly while tailoring them to each environment's unique requirements. They can dynamically scale to meet cloud workload demands or extend protection to remote endpoints, all without manual reconfiguration.

Embracing Autonomous Cyber Security

The future of network defense is not just smarter—it's self-sustaining. Organizations that are planning for the future of firewalls today will be better equipped to handle tomorrow's challenges, achieving stronger protection, lower operational costs, and enable greater agility.

The question is no longer if this future will arrive. It's how quickly you will be ready for it.

CHECK POINT™

08 SECURING THE AI ERA

AI has quickly become a critical component of business operations, from copilots in productivity suites to autonomous agents that execute business processes. And we're only beginning to see the ways in which AI is being leveraged for efficiency and innovation.

Yet as enterprises scale AI to new heights, we must recognize that no business can innovate safely without securing the intelligence itself. Just as modern firewalls have redefined network defense through automation and contextual awareness, AI security is redefining enterprise protection for a world where language is the new executable.

Our research indicates that 1 in every 80 GenAI prompts exposes sensitive corporate data. Thirty-two percent of organizations have already faced AI-related prompt manipulation attacks. And the explosion of unsanctioned AI tools and integrations (aka, Shadow AI) creates unseen vulnerabilities across the enterprise.

Traditional security architectures can't meet this new security challenge. Protecting AI requires new capabilities that combine visibility, context, and prevention at machine speed without slowing the business or the pace of innovation.

This chapter explores the emergence of AI security capabilities and how organizations can secure their AI pipelines, applications, and agents end to end as we start to define the next era of digital trust.

New Risks Demand New Defenses

AI systems introduce risks that transcend traditional cyber security paradigms. In this new reality, *text itself* becomes executable code capable of altering model behavior, exfiltrating data, or manipulating downstream systems.

Common AI-specific threats include:

- Prompt injection and jailbreaks, which override safety controls or expose sensitive data
- Indirect attacks, where malicious inputs from one system exploit vulnerabilities in another
- Model inversion and data poisoning, where attackers manipulate or reconstruct training data
- Insecure output handling, where unsafe model responses trigger unintentional actions or data leaks
- Agent autonomy drift as AI systems act beyond intended scope without accountability

The emergence of these risks marks a dramatic shift in our perception of cyber protection.

Cyber security is becoming more than protecting infrastructure; cyber leaders must now think about how to secure the intelligence itself.

CHECK POINT

AI Security for the AI Transformation

Check Point is uniquely positioned to lead the push for security for the AI era. We have built a comprehensive AI Transformation Security Platform that can protect employees, applications, and agents through a unified, prevention-first architecture.

Our approach hinges on three primary AI security solutions:

1 Employee AI Usage Security—GenAI Protect

Most organizations are already using AI, very often without admin knowledge, visibility or control. Employees interact with copilots, chatbots, and online LLMs that process sensitive data every day, introducing significant risk to the business.

GenAI Protect enables enterprises to manage AI use and accelerate AI adoption safely. Key features include:

- Unified visibility into all sanctioned and unsanctioned AI usage
- Inline policies that prevent sensitive data exposure through real-time AI-based classification
- Granular controls that balance productivity and compliance
- Full inspection and data lineage for every AI interaction
- Seamless integration with enterprise DLP and threat prevention systems

Check Point helps transform AI usage from a visibility gap and potential risk vector into a managed, secure productivity advantage.

2 Application & Agent Runtime Security

As organizations build proprietary AI copilots, chatbots, and autonomous agents, security must move closer to the model itself.

Check Point delivers AI-native runtime protection that detects and blocks adversarial threats in real time. Capabilities include:

- High-accuracy, low-latency detection of prompt injection and topic manipulation
- Guardrails aligned to compliance policies and data loss prevention (DLP) standards
- Continuous monitoring of input/output streams to block malicious or non-compliant content
- Flexible deployment that can be integrated with Check Point CloudGuard WAF, embedded within applications, or via LLM gateways

By defending AI where it operates, enterprises protect both their users and their brand from emerging AI threats.

CHECK POINT

3

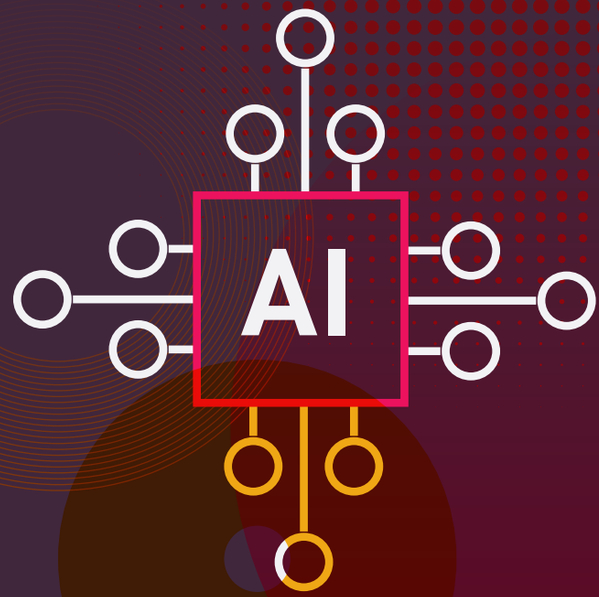
AI Safety & Security Scanning

Before deployment, AI systems must be tested and validated for security and robustness.

Check Point enables adversarial red-teaming against OWASP LLM Top-10 threats and beyond. Capabilities include:

- Automated stress testing for model robustness and bias
- Data lineage and poisoning analysis
- Actionable reporting for governance, compliance, and security-by-design readiness

Together, these capabilities establish an AI security lifecycle that helps your business stay protected across all phases of AI deployment, from development and training to runtime and continuous improvement.



AI Factories, Digital Intelligence and the New Security Frontier

Enterprises are now building what industry leaders call AI factories, sprawling compute and data environments where models are trained, fine-tuned, and deployed at scale. These environments represent the beating heart of enterprise AI strategy.

They also present a very prominent potential attack surface.

Securing AI Factories with NVIDIA

Check Point provides AI protection at the infrastructure level. Through our collaboration with NVIDIA, Check Point offers AI Cloud Protect, an integrated solution designed to secure AI factories, model development pipelines, and inference workloads with zero impact on performance.

Running on NVIDIA BlueField-3 DPUs and validated on NVIDIA RTX PRO Servers, AI Cloud Protect delivers full-stack protection across the AI supply chain from data center to cloud. Key capabilities include:

- Network-level defense against unauthorized access, preventing model exfiltration and data poisoning
- Host-level visibility via NVIDIA DOCA Argus, detecting and preventing malicious workloads and rogue processes within AI nodes
- Zero performance impact, as security functions are offloaded to DPUs, preserving GPU and CPU resources for AI computation
- Unified orchestration, enabling consistent policy enforcement across thousands of AI nodes

As AI factories become the new digital production lines, AI Cloud Protect ensures they are secure by design.

The Continuing Evolution of AI Security

AI is rapidly transforming from more than just passive copilots and productivity tools. Fully autonomous agents are being deployed and the advancements in AI use cases will increase exponentially in the coming years. Future AI systems will plan, decide, and act independently, interacting with APIs, modifying records, and executing workflows without human input.

Check Point's extended Agentic AI Security initiative brings control to this new frontier. Here are a few important elements of this new line of defense:

- Automatic discovery and inventory of all AI agents from third-party, internal, and managed frameworks
- Behavioral analysis for detecting anomalous or risky actions
- Policy guardrails that enforce least privilege and prevent unsafe automations
- Real-time runtime protection to block malicious prompts and actions

Just as modern firewalls introduced self-learning and contextual awareness, AI security is becoming autonomous, adaptive, and context-aware. It is continuously learning from interactions to strengthen protection without impeding performance or slowing innovation.

AI Security as a Business Enabler

Enterprises that embed security and governance into their AI operations can scale faster, ensure compliance with emerging regulations, and build trust with customers and partners by keeping them secure.

Check Point is helping to secure the AI era through a combination of powerful prevention-first architecture, AI-native guardrails, and NVIDIA's accelerated infrastructure protection. Combined, this approach helps organizations achieve:

- Comprehensive protection across data, models, and infrastructure
- Zero-latency performance, essential for large-scale AI workloads
- Unified management and visibility across every AI interaction
- Fast time-to-value, with lightweight deployment through APIs, extensions, or integrated WAFs

CHECK POINT™

09

CONCLUSION: HYBRID MESH IS THE FUTURE OF NETWORK SECURITY

CHECK POINT

At its core, a hybrid mesh firewall architecture delivers what modern enterprises need most: centralized orchestration of decentralized enforcement.

It gives you:

- **Visibility everywhere:** See users, devices, encrypted traffic, and cloud activity in real-time
- **Enforcement anywhere:** Apply consistent policies from headquarters to cloud workloads, branch locations, and remote endpoints
- **Adaptability at scale:** Expand capacity, coverage, and performance dynamically—without re-architecture or compromise
- **Security intelligence that acts:** Leverage AI-driven prevention to stop threats before they reach critical systems, reducing dwell time and response cycles

Check Point's Hybrid Mesh Firewall exemplifies this model, built from the ground up for the distributed enterprise, backed by the power of ThreatCloud AI, and unified through the Infinity Platform for seamless policy, visibility, intelligence, and operations.

Perhaps most critically, this shift transforms the role of the firewall from a performance trade-off to a business enabler. With robust encrypted traffic inspection, Zero Trust enforcement, and hyperscale readiness, your firewall no longer limits innovation, it supports it.

Your firewall should not be a relic at the edge. It should be a dynamic part of a distributed, intelligent security architecture—interwoven into your enterprise fabric.

Learn more about Check Point's Hybrid Mesh Firewall.

Ready to talk about how a Next Generation Firewall can help transform your business security?

Talk to one of our Global CISOs today!

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

CHECK POINT