CHECK POINT

Cybersecurity for banks

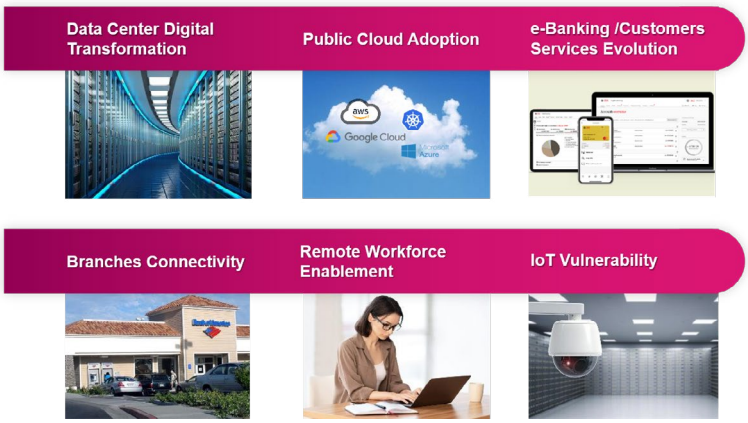
Deliver advanced digital services with the highest levels of security and stringent adherence to compliance

Introduction: the bank's security mandate

During the past year, financial organizations and banks in particular, have suffered increasing rates of cyberattacks coming in from every possible threat vector. According to Check Point Research, a financial organization was attacked on average 700 times every week during 2021, a 53% increase year-over-year, and according to IBM the average cost of a successful breach was $5.85 million. From phishing to supply chain attacks, and everything in between, what we have seen is just the tip of the iceberg.

Banking technology trends that increase cyber vulnerability

- Growing adoption of new technologies spurred on by **digital transformations**
- Widespread migrations to **public cloud** for multiple applications
- **Hybrid data centers** becoming the norm
- Increased use of **online and mobile channels** for banking needs
- The ongoing state of **remote work** due to a pandemic that's not going away
- Extensive deployment of **SD-WAN** connectivity for remote branches
- Accelerating proliferation of **IoT devices**



As the cyber threat landscape continues to evolve and become more dangerous every year, protecting a bank's IT infrastructure will only continue to become more and more challenging. In this paper we will present real-life stories from banks from all over the world, the specific challenges they faced, and the Check Point solutions they leveraged to overcome the challenge and bolster their security posture.

1. The challenge: securing growing datacenters and high frequency trading platforms

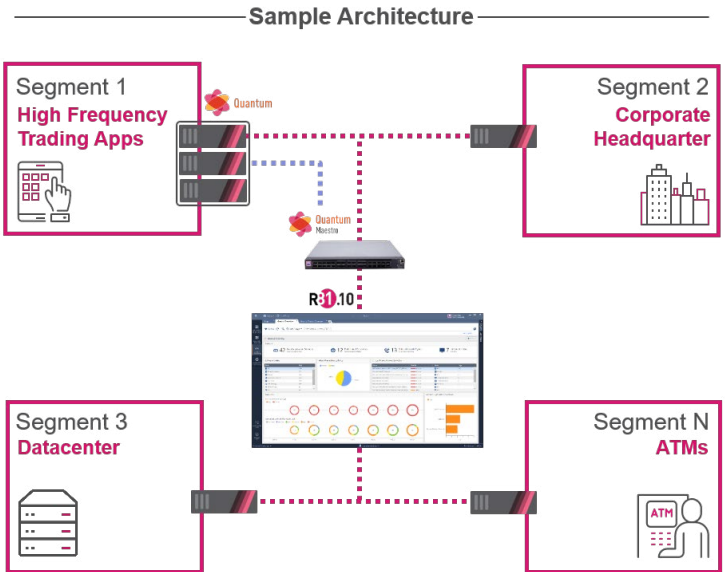
Banks need network security that performs at the speed of business. This is the key to transferring hundreds of terabytes of data securely and in minutes, as well as to providing low latency for high-frequency financial transactions, and for scaling security on-demand to support a hyper-growth business such as online commerce.

The main challenges to achieving these goals include assuring:
- **Zero trust,** granular network segmentation to prevent lateral movement
- The **secure transfer** of hundreds of terabytes
- **Low latency** for ongoing high-frequency financial transactions
- **Simplifying** cumbersome management and gaining **visibility** across on-premise and cloud datacenters

Customer story: US Big 4 bank

This US bank was seeking to achieve datacenter hypergrowth. The strategy was to execute gradually with flexible time slots for upgrades. It was also looking to centralize management, reporting, analysis, and visibility. To assure robust datacenter protection throughout the journey and to meet all related goals, the bank deployed an architecture with zero-trust segmentation and simple network, granular micro-segmentation.

Segmentation architecture for protecting the datacenter during hypergrowth



Taking this approach enables banks to:

- Secure high-speed workloads, backups, and data transfers at an 800 Gbps line-rate firewall throughput
- Protect high frequency trading apps at 3µSec ultra low latency
- Support hyper growth with scalable throughput, at a scale of up to 3.0 Tbps of firewall performance
- Achieve centralized management with automated operations

Solution for bank network security

Check Point's Network Security solutions simplify the bank's security posture management and streamline and scale operations for continued business growth. Specifically, the Quantum Network Security solution provides ultra-scalable protection against Gen V cyber-attacks on the network, cloud, data center, IoT, and remote users.

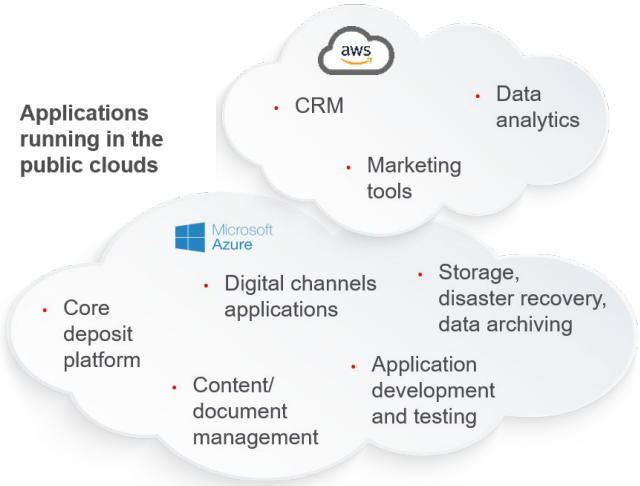
2. The challenge: assuring a secure & compliant cloud migration

As banks move data and workloads to the cloud, they need to assure that cloud assets and data are secured and meet compliance with regulations such as those from the US's Federal Financial Institutions Examination Council **(FFIEC)** and the European Banking Association **(EBA)**.

But modern cloud deployments are tremendously complex, typically spanning multiple clouds. So, while public cloud providers do invest extensive efforts into security, the bank still remains the one who is accountable for assuring the organization's cybersecurity.

Achieving this goal entails multiple challenges:
- **Unified security management** across clouds and an on-premise datacenter
- Detecting and remediating **misconfigurations** in real time
- Streamlining and assuring **governance**
- Meeting stringent **compliance** and privacy regulations

How the public cloud is serving banks today



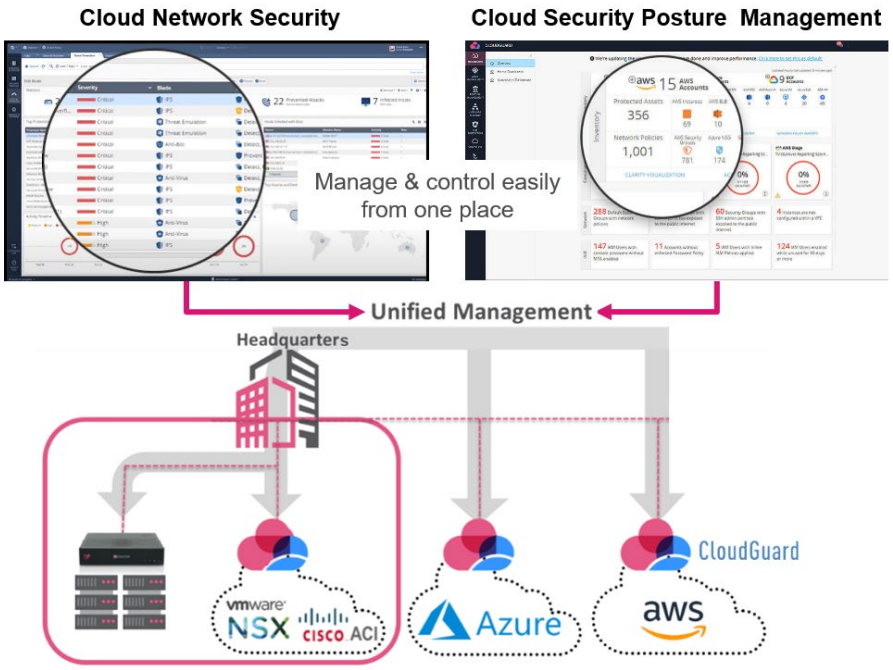
Customer story: a large South American bank adopts multi-cloud securely and efficiently

To support the effort to expand its Microsoft Azure and AWS cloud, the bank selected CloudGuard Network Security, and CloudGuard posture management, Check Point's unified and **cloud-native security solution** for posture management and compliance with regulations such as NIST CSF/800-53, PCI DSS. The solution provides the bank advanced threat prevention and automated cloud network security through a **virtual security gateway** and with **unified security management** across all multi-cloud and on-premises environments.

Benefits achieved by the South American bank with CloudGuard

- A single cloud-native security solution on-prem and hosted cloud, multi-cloud (Azure, AWS, NSX, and more), with unified security and posture management
- Automated compliance & best practices for enforcement of compliance frameworks, e.g., PCI DSS, NIST CSF/800-53, etc., and detection of misconfigurations and enforcement of policies
- Improved performance: low latency for business apps, easily create rules and profiles
- Reduced costs: easy integration with multiple systems, 50% TCO reduction vs. other solutions
- Real-time threat prevention: threat emulation and extraction, zero-day, antivirus, anti-bot, URL filtering, DLP, anti-spam

CloudGuard unified and cloud-native network security



Solution for cloud migration security and compliance

Check Point offers comprehensive security and compliance solutions for financial service organizations' multi-cloud environments. With CloudGuard Network Security they get advanced, multi-layered cloud network security across public and private clouds.

CloudGuard Network

3. The challenge: simplifying compliance and the complexity of security operations

Managing a bank's security operations is a complex undertaking entailing many tasks for keeping up with ever-changing security needs:

- Translating demanding industry regulations into **security frameworks**, easily and efficiently
- Defining, accelerating, and enforcing ongoing **policy update installations**
- Assuring operational efficiency amidst numerous time-consuming **manual processes**
- Delivering quick security system upgrades and security gateways updates with no impact to **business continuity**

Customer story: Banco del Pacifico increases security operations efficiency

Ecuador's Banco del Pacifico was seeking to bolster its defenses against cybercrime's escalating scale and growing sophistication. The bank turned to Check Point Infinity. The solution deployed includes a unified management console that delivers simplicity and consolidation across the bank's IT infrastructure, manages all corporate gateways, and integrates APIs with any application, for autonomous prevention.

The capabilities enabled include:

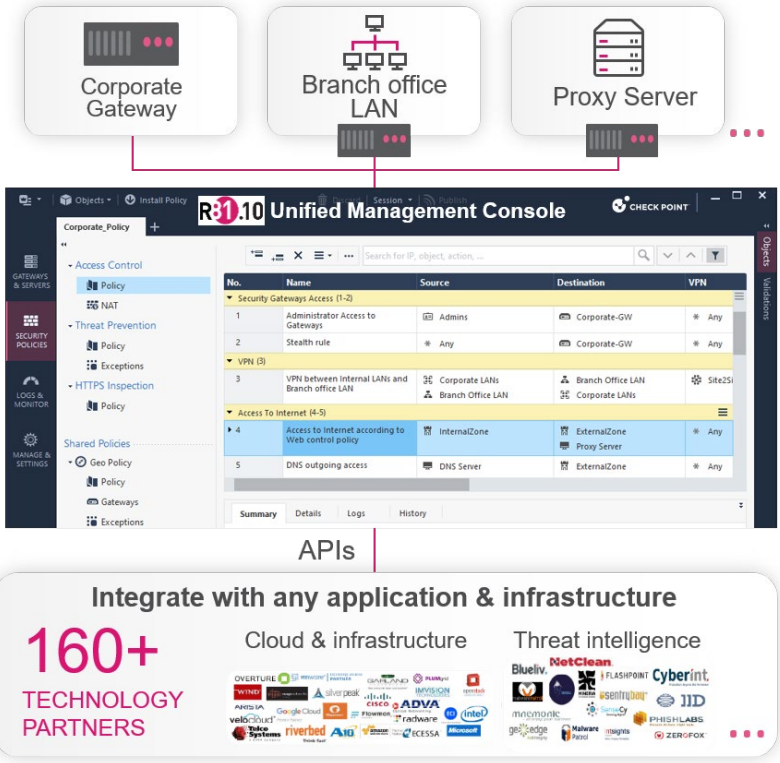
- Automated operations for improved efficiency, visibility, & control
- Consolidated security management with unified security policies
- Multi-layered protection with centralized threat emulation & extraction, and more

Banco del Pacífico

"We're constantly seeing new threats and examining the best technology on the market. We believe Check Point offers the best features in terms of solutions and security"

- Jose Luis Nath, Vice-President of Technology and Security, Banco del Pacifico

Banco del Pacifico's simplified security operations with Check Point



Customer story: EMEA bank improves security operational efficiency while boosting security & compliance with BASEL, SOX, NIST, GDPR, and more

The Check Point solution deployed enables continuous monitoring of the security infrastructure, gateways, blades, policies, and configuration settings, all in real-time. This way the bank can meet regulatory compliance and governance requirements while reducing security man-hours and driving increased security.

Solution for simplifying operational security complexity

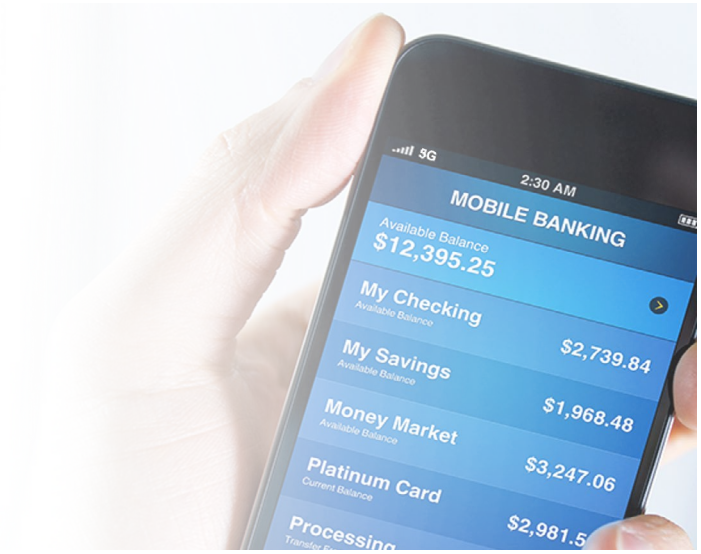
Check Point enables banks to cut operation management by up to 80% with unified security management across all cloud and network environments, as well as to centrally manage thousands of security gateways.

With the R81 Unified Cyber Security Platform, the industry's most advanced threat prevention and security management software, they get uncompromising simplicity and consolidation across the enterprise.

Quantum
Management Software

4. The challenge: securing advanced e-Banking services

A bank's applications drive the business. And as they evolve and grow they expose more APIs causing the attack surface to grow as well. Cybercriminals are exploiting this phenomenon, attacking web applications and APIs with advanced methods that include SQL injection, cross-site scripting, and deploying automatic scripts known as "bots." These attacks are damaging and costly, and the ability to secure applications has never been more critical.



But detecting and preventing these attacks is challenging, requiring the bank to implement app-specific security defenses, such as building security into their mobile apps from the get-go.

When they don't, the implications are dire, with great damage that can be incurred to customer security and the bank's reputation.

Customer story: a large European bank enhances security for e-banking web apps

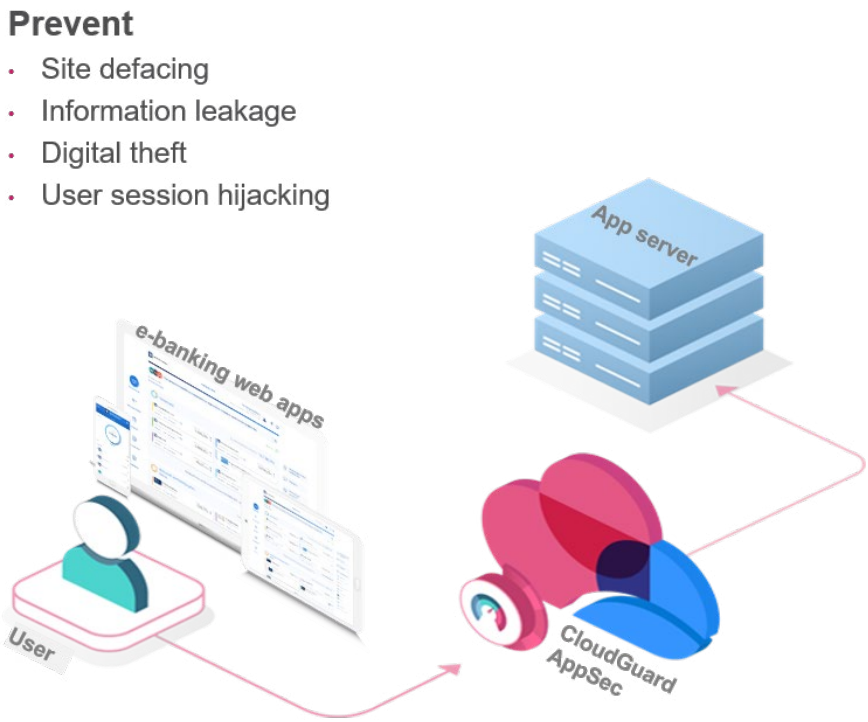
In the effort to overcome the challenges of securing its e-banking offering, a European bank was looking to enhance and automate the security of its customer-facing web applications' APIs.

With Check Point's CloudGuard AppSec, the bank can now prevent real threats such as those from the OWASP top 10, as well as zero-day API attacks and malicious bot traffic. And all this as it eliminates false positives.

Among the improvements made possible by the Check Point solution are:

- Improved security with automated application security and API protection using contextual AI
- Increased scalability with a fully automated solution for public clouds (AWS, Azure, Kubernetes, and more) and on-prem multi-apps, with protection for billions of annual application requests
- Reduced operational expenses by eliminating need for manual tuning and fully automating across multi-environments & apps

e-Banking services security with Check Point's CloudGuard AppSec



Customer story: large APAC bank releases mobile e-banking innovations to 1M+ customers quickly and securely

With Check Point's Harmony App Protect mobile SDK the bank has been securing its e-banking mobile apps from the start, achieving:

Apps secured out-of-the-box

- Runtime protection against malware, jailbreak/root, MitM attacks, and tampering attempts
- Detection of known and unknown threats and prevention of compromise

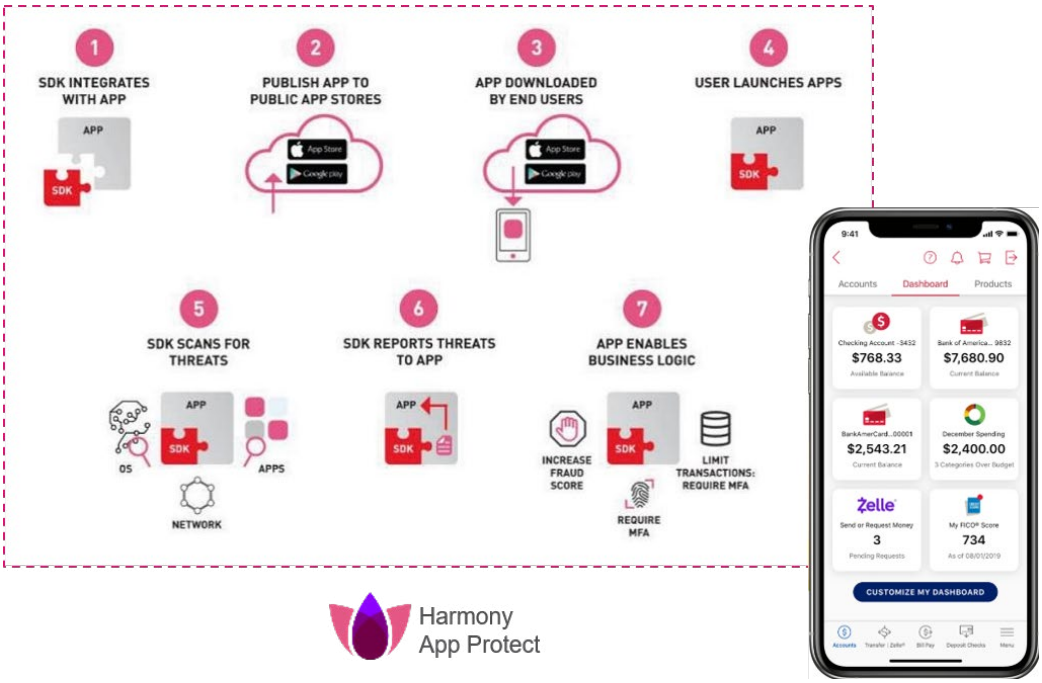
Faster version release

- Developers quickly and securely releasing new features
- A reduction in development and testing efforts

Automated compliance

- Apps compliant with financial regulations from day one, incl. FFIEC, PSD2, PCI DSS, and more

Secure apps with Check Point's Harmony App Protect



Solutions for securing advanced e-Banking services

Banks can protect web apps and APIs from cyber security attacks and build secure mobile apps from the get-go with Check Point's CloudGuard AppSec, which automate financial service applications and API protection, and with **Harmony App Protect** for securing e-banking mobile apps.

CloudGuard AppSec

5. The challenge: enabling the secure remote workforce

With remote users connecting to corporate applications more than ever, the organization's attack surface has never been wider.

To assure advanced protection of its remote workforce, a bank must secure:

- **All devices,** including tablets, mobile, BYOD, and managed devices
- **Users** while browsing the internet and using email and collaboration apps
- **Third parties,** including contractors, consultants, and partners accessing devices and applications

And, they must ensure **zero-trust access** to corporate applications from anywhere.

Customer story: RCB Bank enables employees to work securely using personal mobile devices

For its remote workforce protection RCB Bank selected Harmony Mobile, which enables the bank with:

- Complete protection from network attacks, incl. phishing, smishing, and others, blocking non-compliant devices and OS vulnerabilities
- Enhanced compliance with GDPR and full protection of user privacy
- Simplified management with visibility and remediation tips
- High scalability with MDM integration for zero-touch deployment for hundreds of employees

RCB BANK

"Harmony Mobile proved itself. It's an effectve, affordable solution that protects us in ways that our container solution alone could not accomplish."

- Stacy Dunn, Information Security Analyst, RCB Bank

Customer story: SEB Baltics protects thousands of endpoint devices with the highest level of security

With Harmony Endpoint SEB is benefiting from:

- Complete endpoint protection & EDR with a consolidated security architecture providing real-time threat prevention
- 90% automation of attack detection, investigation, and remediation tasks
- Ransomware protection with automated remediation and recovery from ransomware attacks
- High productivity with Content Disarm and Reconstruction (CDR)

- Reduced TCO with a single solution that includes advanced monitoring and reporting to ensure rapid problem solving

Customer story: Canal Bank protects hundreds of remote users of Office 365 email & collaboration apps with a seamless experience

Email and collaboration apps have become the most fundamental tools for businesses these days. Not surprisingly, it is also one of the most exploited channels by cybercriminals, with Business Email Compromise (BEC) attacks accounting for over 50% of losses caused by cybercrime.

To mitigate the risk and avoid the damage of BEC and other attacks to its remote workers, Canal Bank selected Harmony Email and Collaboration to achieve:

Improved security

Within the first year the bank stopped 1400 phishing attacks and defended against 800 malware attacks without impacting productivity.

Simple deployment & management

Deployment completed within minutes for instant protection,and reports provide ongoing visibility into threats.

Reduced TCO

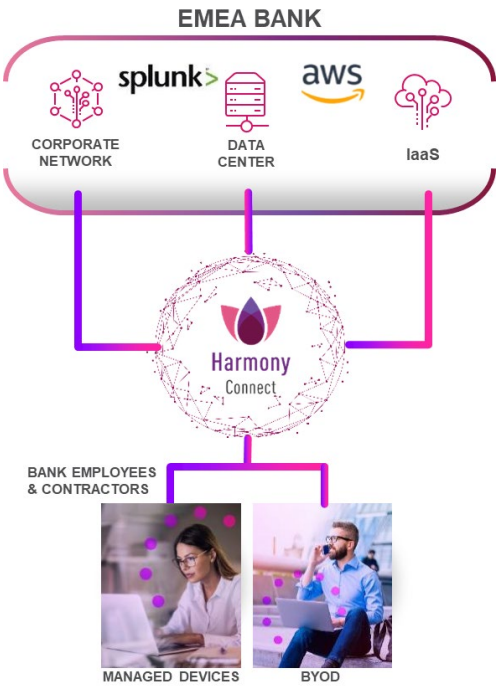
Only one solution is required for securing email, SharePoint, Teams, OneDrive, and more, including protection against malware, phishing, sensitive business data (DLP), malicious links, account takeover, and more.

canalbank

"Check Point Harmony Email and Office enable us to not only achieve our security goals, but discover other application issues that we had not been aware of"

- Erick Garay, CIO, Canal Bank

Customer story: EMEA bank enables secure access to corporate applications from any device anywhere



With Harmony Connect this EMEA bank is leveraging:

Zero-Trust Access

- With least-privilege access to web apps, secure Shell servers, remote desktops, and databases across multiple groups
- For Splunk, Internal WeApps, AWS resources, and more
- Enabling security admins to track user activity with fully recorded sessions and audit trails

Clientless Access

- Enabling hundreds of employees and contractors with access from any device via friendly UI

Cloud-delivered security

- That is highly available and scalable
- With no impact on the browsing experience

Solutions for securing remote workforce enablement

The Check Point Harmony family of products provides uncompromised protection and simplicity for the financial services sector and includes:

Harmony Endpoint

Harmony Endpoint for comprehensive endpoint protection at the highest security level, and for avoiding security breaches and data compromise.

Harmony Connect (SASE)

Harmony Connect for easily connecting any user to any resource, anywhere, without compromising security.

Harmony Mobile

Harmony Mobile for complete protection of the mobile workforce, with simple deployment, management and scale.

Harmony Email & Collaboration

Harmony Email and Collaboration for complete protection of Office 365, Teams, OneDrive, SharePoint, and Google Drive, using the Avanan technology.

6. The challenge: enabling secure SD-WAN connectivity for branches

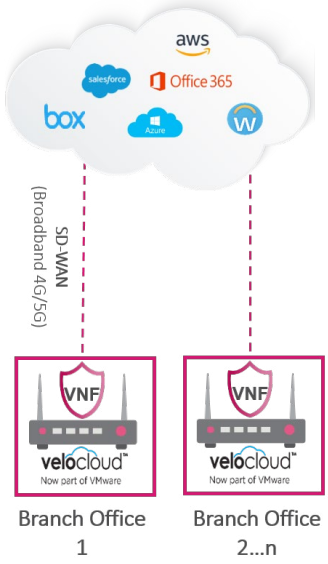
Connecting branches directly to the cloud significantly increases the risk of attack via malicious files, malware, zero-day, bots, viruses, APTs, and more.

To mitigate the risk, many banks are seeking to enable their branches with SD-WAN connectivity to the internet and cloud, and to do so gradually for assuring enhanced security.

Customer story: European investment firm connects dozens of branches with SD-WAN without compromising security

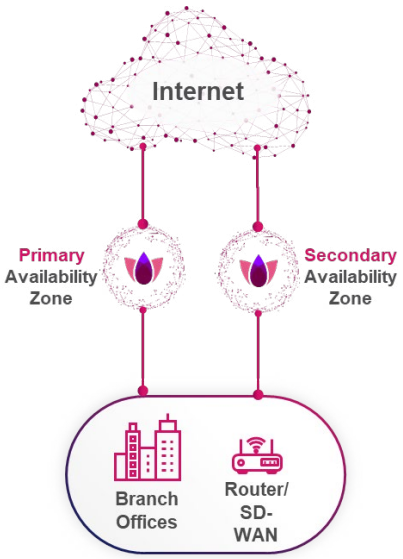
The European investment firm selected Quantum Edge, Check Point's on-premise virtual security gateway for high performance and privacy, which is deployed on the VeloCloud appliance. With this solution the bank is securing its connected facilities with top-rated threat prevention, having executed a simple deployment, and thereafter leveraging ongoing simplified management.

Virtual security gateway deployed on VeloCloud



Banks can also bolster SD-WAN connectivity protection with the Harmony Connect Firewall-as-a-service **(FWaaS) solution** from Check Point which:

- **Protects** branch-to-internet connections
- **Assures** consistent security
- **Enables** a fast setup
- **Offers** fully tested integrations with leading SD-WAN offerings

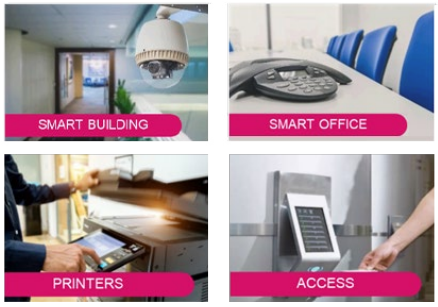


Solution for securing remote branches from the cloud or on-premises

Check Point solutions assure secure SD-WAN connections to the internet and cloud to protect the bank's remote branch offices from every threat. With Quantum Edge connected banks facilities on-premises are secured with top-rated threat prevention.

Quantum Edge

7. The challenge: securing bank IoT network & devices against attacks



From IP cameras and smart elevators to access devices and printers, IoT networked devices are constantly under attacks Though assuring protection is a great challenge for banks, requiring the ability to:

- **Identify** every IoT device on the network
- **Apply** and manage multiple and complex IoT policies
- **Protect** the network and as well as all IoT assets

Solution for securing the bank IoT devices to protect the network from attacks

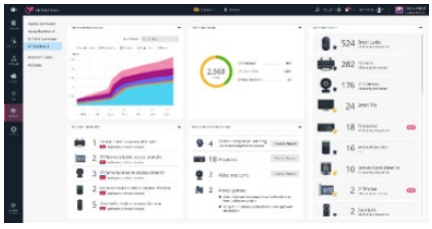
Check Point's IoT Protect enables banks to secure the IoT network against cyberattacks, from IP cameras to smart elevators, and so much more, delivering capabilities that include:

- An advanced discovery service that leverages a built-in discovery engine
- Seamless policy management that provides autonomous zero-trust segmentation and automation, with AI and behavioral learning-based analysis
- Real-time threat prevention with virtual patching and protection activation against device exploit, with continuous updates from ThreatCloud

Quantum IoT Protect

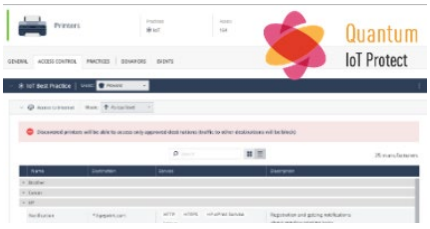
IoT network protection

Built-in discovery engine



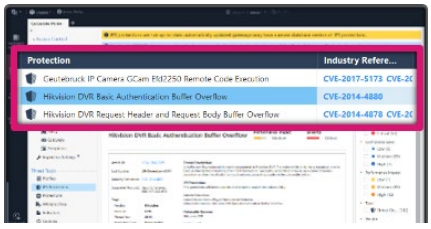
COMPLETE VISIBILITY INTO THE BANK IOT ASSETS

IoT security policy



AUTONOMOUS ACCESS-CONTROL POLICIES

Virtual patching



ACTIVATE PROTECTION AGAINST DEVICE EXPLOIT

8. The challenge: augmenting security with support from premier experts

One of the biggest challenges faced by almost every security organization, including the bank's, is the global **shortage in cybersecurity experts.** It is also very difficult to **stay up-to-date** and maintain **compliance readiness** with continually updated regulations. And running a **24/7 security** operation can be very demanding – requiring the orchestration of **siloed tools**, keeping the right **headcount**, providing right-time **training** to existing and new staff, controlling **alert fatigue**, and reducing **false positives**. The key to overcoming the challenge is to augment security design, deployment, operation, and optimization with the support of an industry leading **cybersecurity team of experts.**

Support for every phase of the security journey

This is where Check Point comes in. Our experts provide support for every phase and need along the cybersecurity journey. With dozens of cumulative years of Check Point **experience** the team executes superlative security **design**, seamless **deployments**, and any other **operations** and **optimization** related needs. We offer professional services with long and short-term engineers who make sure that your organization is always up to date, performing efficiently, and is compliance-ready, whether through manual execution or full automation.

Additional services include:

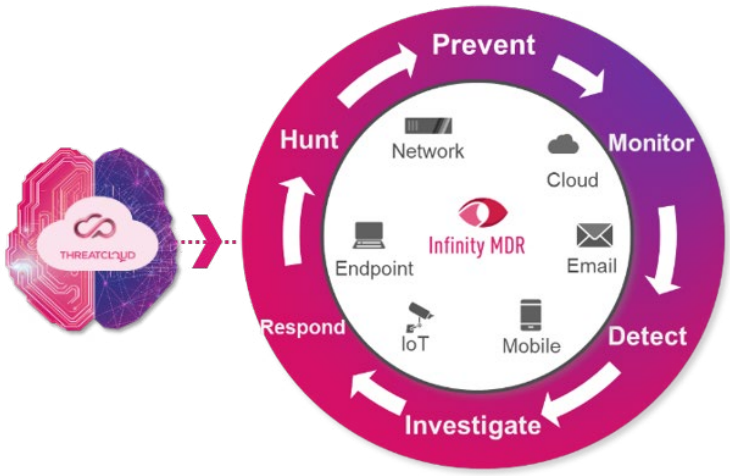
- Advanced Technical Account Management (ATAM)
- Cyber Resilience Testing (CRT)
- Lifecycle Management Services (LCMS)
- Incident Response provided by our Incident Response Team (IRT)
- Managed Services with managed detection & response (MDR)
- Security Consulting Services
- Security Training

Complete security operations as-a-service

Moreover, Check Point provides a complete **security operations as-a-service** that includes the Check Point Managed Detection & Response (MDR) service for detecting and responding faster to real attacks anywhere in the organization by leveraging our managed SecOps services.

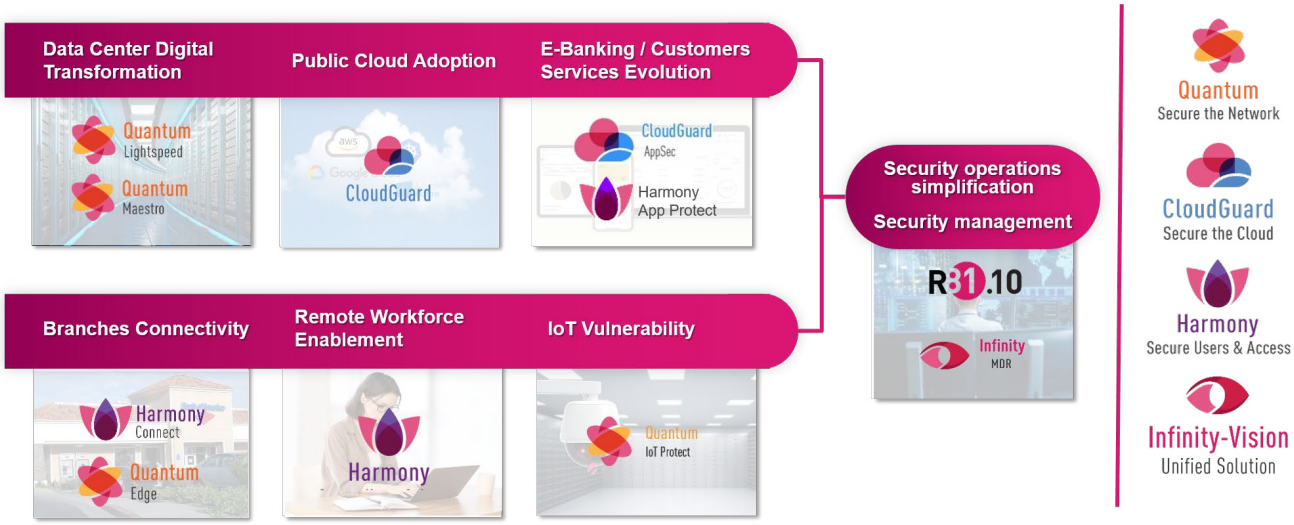
Managed detection and response

With Infinity MDR, the Check Point MDR team monitors, detects, investigates, hunts, responds, and remediates attacks on the environment, covering the entire infrastructure, including the network, endpoint, email, and more.

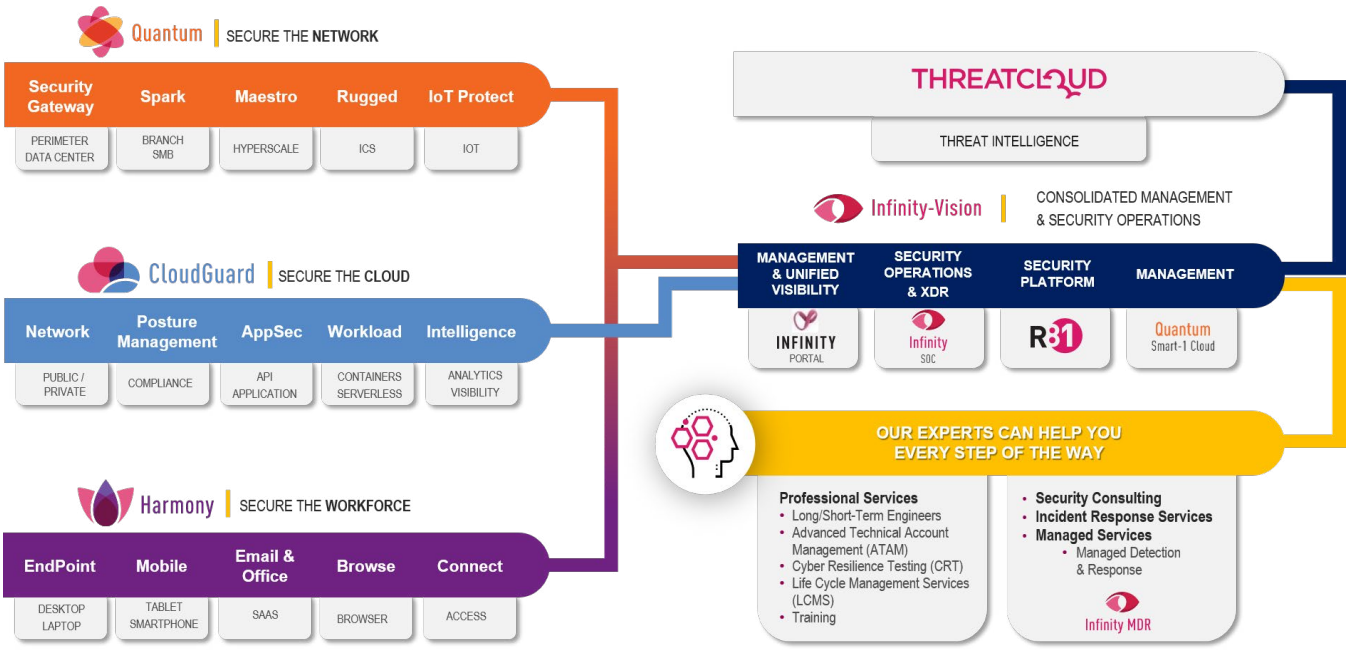


In conclusion

Check Point enable banks to provide advanced digital services to their customers with the highest level of security to their network, cloud, users, and access, with the Quantum, CloudGuard, Harmony, and Infinity families of products.



By adopting a consolidated security approach with **Check Point Infinity architecture and services,** banks realize preemptive protection against advanced fifth-generation attacks while achieving a **50% increase in operational efficiency** and a **20% reduction in security costs**.



This broad cybersecurity offering of solutions and services from Check Point is enabling 6,500 financial institutions around the world to overcome their toughest challenges today by:

- Protecting the bank's **network** and hybrid **datacenter**
- Assuring a secure and compliant **cloud migration**
- Simplifying **compliance** and the complexity of **security operations**
- Securing advanced **e-Banking** services
- Enabling a secure **remote workforce**
- Enabling secure **SD-WAN connectivity** for branches
- Securing the bank's **IoT network and devices** against attacks
- Augmenting security with the support of cybersecurity **experts**

To learn more about how Check Point is helping banks deliver superior digital experiences while assuring security and compliance, we invite you to contact us.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com