D. C. Law firm future-proofs security across network, cloud, and mobile security threat vectors with Check Point Infinity Architecture

Customer Profile

This law firm represents clients in complex, high stakes regulatory, litigation, and transactional matters. Its clients range from fortune 500 corporations to trade associations and individuals.

Challenge

- Meet clients' security requirements across all threat vectors
- Prevent SaaS application account takeovers
- Maximize attorney productivity and availability (uptime)

Solution

- Check Point Infinity

Benefits

- Gained complete visibility into threat landscape
- Future proofed firm's defenses through on-going, real-time access to all Check Point technologies
- Achieved predictable spend through Check Point Infinity Total Protection subscription model

> "We're thrilled with Check Point Infinity Architecture. It delivers a single solution that protects our entire attack surface—from endpoint and mobile device to cloud—today and into the future."
>
> — Director of Information Security

Overview

D.C. Law Firm

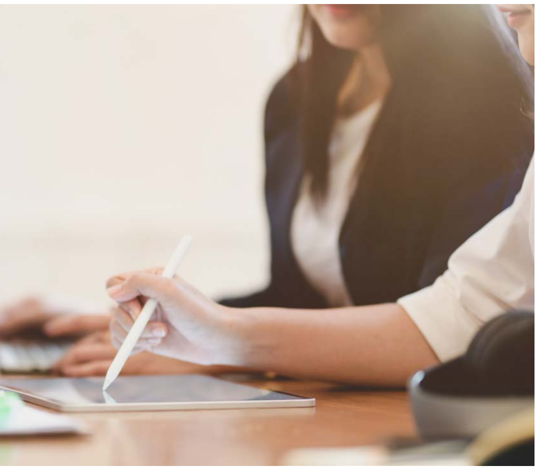
This law firm represents clients in complex, high-stakes regulatory, litigation, and transactional matters. Its clients range from Fortune 500 corporations to trade associations and individuals. To secure highly sensitive data and comply with clients' security requirements, the company secured its expanding environment with the Check Point Infinity architecture.

Business Challenges

The Need for Multi-Vector Defense

The firm's clients span organizations from agencies and large enterprises to international organizations and foreign companies. Attorney-client data is always privileged and confidential. The international scope and high visibility of clients make security business-critical.

Attorneys often travel internationally. When they returned home, their mobile devices were frequently infected and had to be totally wiped and re-installed. Clients trust the firm with data that is essential to their businesses. Some is intellectual property and trade secrets.



> “We must properly secure client data in compliance with their requirements and ensure that it stays secure as cyberthreats and tactics evolve. That’s why we chose the Check Point Infinity Architecture.”
>
> — Director of Information Security

Other data relates to potential mergers and acquisitions. Whether data is related to commerce or national security—it must be protected against leakage or loss. The firm also must protect its attorneys’ productivity. Cyberthreats cannot be allowed to disrupt client engagements or reduce the attorneys’ availability.

“We must defend all potential attack vectors,” said the Director of Information Security. “Our attorneys are mobile and some work across international borders. Many clients collaborate using cloud platforms. And of course, we need to protect everything within the four walls of our company.”

Most clients collaborate with attorneys and staff using Office 365. In the past, there were several times when clients’ Office 365 email systems were hijacked and used to send malicious emails to the law firm—unbeknownst to the client company.

Because attorneys use their own mobile devices, the information security team must secure sensitive, work-related data and email content while preserving user privacy. The firm’s Mobile Device Management (MDM) platform provides some cybersecurity protection, but the security team needed better visibility into the device posture. They also wanted features that could alert users to malicious websites and block installation of rogue apps.

“We have strict terms of engagement, which include security requirements, for each client,” said the Director of Information Security. “We must properly secure client data in compliance with their requirements and ensure that it stays secure as cyberthreats and tactics evolve. That’s why we chose the Check Point Infinity Architecture.”

Solution

Simpler, Predictable Payment Model

To simplify administration and budgeting, the law firm purchased its Check Point solution through the Check Point Infinity Total Protection subscription model. It is an all-inclusive, per-user, per-year consumption model. It provides comprehensive security architecture, Check Point Infinity, through one simple subscription payment plan.

A Solution for Every Vector

The Check Point Infinity architecture is a fully consolidated cybersecurity architecture that provides unprecedented protection against today’s mega attacks across all vectors—network, endpoint, mobile and cloud.

For the firm's networks, Check Point Next Generation Security Firewalls provide application control, URL filtering, anti-bot, antivirus, antispam, content awareness, VPN, mobile access, IPS, identity awareness, and data loss prevention (DLP) capabilities. Check Point SandBlast Network provides complete protection against the most sophisticated threats and zero-day vulnerabilities. Its Threat Emulation capability detects potential threats and sandboxes them for analysis while Threat Extraction features remove malicious content and reconstruct documents before sending clean, safe versions to users.

Check Point Infinity architecture makes it easy for the firm to extend the same protections to endpoints with SandBlast Agent and to mobile devices with SandBlast Mobile. Consistent defenses simplify the user experience and protect privacy, no matter where the attorney is working.

To protect the firm's sensitive data while its being stored and used on SaaS applications, Check Point CloudGuard SaaS prevents attacks on Microsoft Office 365 email. CloudGuard SaaS protects against the most sophisticated malware and zero-day threats while easily preventing account breaches. The Check Point Infinity architecture makes it easy to defend other assets in its Azure cloud environment. There, CloudGuard IaaS extends Gen V cyberthreat protection with dynamic scalability, intelligent provisioning, and consistent control across physical and virtual networks.

"We're thrilled with Check Point Infinity architecture," said the Director of Information Security. "It delivers a single solution that protects our entire attack surface with the Zero Trust Security model —from endpoint and mobile device to cloud—today and into the future."

Check Point R80 Security Management provides centralized management control across the network and cloud environments. It enables the security team to manage security globally with threat prevention and full threat visibility in a single pane of glass. A single policy for users, data, applications, and networks gives the team in-depth control, while allowing them to easily segment policy to align with network or business functions and see everything in a unified console.

The Check Point ThreatCloud collaborative network and knowledge base delivers real-time threat intelligence to the firewalls. If an attack is detected and blocked on one vector, it automatically updates all other platforms and activates security protections accordingly

> "Check Point CloudGuard IaaS gives us visibility that we previously lacked, It also provides assurance that as we gradually move more applications and capabilities to the cloud we have the right protection and the right governance in place."
>
> — Director of Information Security

Results

Strong Governance, Great Protection

The law firm has not had a data security event since implementing the Check Point Infinity architecture. With Check Point preventing malicious actors from infecting devices, attorneys' mobiles stay clean and safe. Attorneys can stay productive and the IT team no longer has to continuously restore devices to a known, safe state. Clients' data stays secure and so does their cloud-based collaboration with attorneys.

At the same time, the firm has more visibility and better governance into its security posture. The security team is working to ensure that they have the right level of access controls to specific types of data, and once those are in place, they plan to automate processes as much as possible.

"Check Point CloudGuard IaaS gives us visibility that we previously lacked," said the Director of Information Security. "It also provides assurance that as we gradually move more applications and capabilities to the cloud we have the right protection and the right governance in place."

Increased Engineer Efficiency

Check Point R80 security management enables the team to set technical and administrative policy controls. With Check Point SmartLog, engineers can access log records across the infrastructure from a single console. SmartLog provides centralized tracking of log records and security activity with instant visibility over billions of log records, saving valuable time.

"Check Point R80 and SmartLog have been a huge improvement for our engineers," said the Director of Information Security. "Before, they had to log on to three or four different consoles, which was challenging. This makes it so much easier."

Simplicity with Cost Predictability

The Check Point Infinity Total Protection model also simplified security budgeting and spending. The law firm has flexibility to protect the firm's assets against today's most advanced threats and the ability to adapt defenses as threats evolve. The security budget stays predictable, making it easier to manage costs and plan for the future.

The security team's goal is to consolidate most of the firm's existing security solutions under the Check Point Infinity architecture. By eliminating multiple point solutions and expanding control under the Check Point Infinity umbrella, they can further simplify management while freeing the company's endpoints to be lighter and more efficient.

"Check Point gives us partnership with a trusted company that provides real protection," said the Director of Information Security. "We have assurance, and we can extend that assurance to our clients as well, so they know that their data is protected."

For more information, visit:
https://www.checkpoint.com/products/