INCEDO INC. TRANSFORMS SECURITY DEFENSES AND BECOMES A HIGHLY RESILIENT ORGANIZATION WITH CHECK POINT

INCEDO

Customer Profile
Incedo Inc. is a U.S.-based digital transformation consulting, data science and analytics, and technology services and solutions firm.

Challenge
- Consolidate multiple point solutions from different security vendors
- Unify cloud security defenses and management across multi-cloud architecture
- Gain better run-time visibility into endpoints to reduce risk

Solution
- Check Point Quantum Security Gateways
- Check Point Harmony Endpoint
- Check Point CloudGuard Posture Management
- Check Point CloudGuard Network Security
- Check Point R81 Security Management

Benefits
- Consolidated and automatically orchestrated defenses across platforms enterprise-wide
- Gained automated protection from ransomware and other zero-day attacks
- Unified endpoint protection, threat-hunting, email security, and mobile security in a single solution
- Orchestrated network, application, and cloud security and governance across multiple clouds
- Increased resiliency with automated threat detection, investigation, and remediation

"By consolidating our security defenses with Check Point, we're far more agile and flexible than we could have been before. Check Point has helped us become a highly resilient organization."

- Archie Jackson,
  Senior Director and Head of IT and Security, Incedo Inc.

Overview

Incedo Inc. helps clients achieve competitive advantage through end-to-end data science, analytics, and technology services and solutions. By combining strong engineering, data science, and design capabilities with deep domain understanding, the company helps clients in financial services, telecommunications, life sciences, healthcare, and product engineering maximize business impact from emerging technologies.

Business Challenge
Securing a Complex Global Environment

Protecting data and service offerings is integral to Incedo Inc.'s reputation and service quality. As a consulting firm, it works with large volumes of clients' proprietary data and intellectual property. Incedo Inc. also processes data for customers, providing it in packaged information services. Finally, Incedo Inc. generates its own product development data and Internet and application-based services. Everything must be secured.

With a global presence, the company supports multiple, distributed cloud environments. Some are pure cloud, while others are hybrid models that share data and workloads between the cloud and on-premises data centers. Incedo maintains separate environments for

itself in addition to segregated environments for each client.

Until recently, each environment was protected by traditional perimeter, and endpoint solutions from multiple vendors. As the global threat environment quickly evolved however, interoperability issues made it difficult to orchestrate policy and visibility across the different security solutions.

"Identity and access management quickly became complex and unknown endpoints deployed via shadow IT introduced risk," said Archie Jackson, Senior Director and Head of IT and Security for Incedo Inc. "We needed a better, faster way to gain visibility into endpoints, detect threats, and consolidate management."

> "Check Point was a trusted partner from the very beginning. It was remarkable how the Check Point sales and implementation teams are so well integrated. They completely focused on helping us solve our challenges."
>
> - Archie Jackson, Senior Director and Head of IT and Security, Incedo Inc.

SOLUTION
Proactively Defending the Network

Jackson had experience with multiple security solutions and vendors, so when Incedo Inc. decided to consolidate its security infrastructure, he had two specific requirements. In addition to delivering industry-leading protection, he looked for a vendor that supported the company's zero-trust approach to security. He also wanted a trusted partner. He chose Check Point.

"Check Point was a trusted partner from the very beginning," said Jackson. "It was remarkable how the Check Point sales and implementation teams are so well integrated. They completely focused on helping us solve our challenges."

Incedo Inc. deployed Check Point Quantum Security Gateways to protect its networks from advanced, multi-vector attacks. Quantum Security Gateways deliver the highest-caliber, integrated threat prevention with SandBlast zero-day protection. Check Point Threat Prevention includes firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known cyber attacks and threats. It also provides SandBlast™ Threat Emulation (sandboxing) and Threat Extraction, a Content Disarm & Reconstruction (CDR) technology, for complete protection against the most sophisticated threats and zero-day vulnerabilities.

Quantum Security Gateways are part of the Check Point Infinity Architecture, which provides a comprehensive approach to implementing a zero-trust security model to secure an organization. With Check Point Infinity, a threat seen and prevented in one part of the organization becomes an indicator of compromise (IoC), signaling the need to secure the whole organization. The Infinity Architecture unifies security management and applies zero-trust security principles to secure networks, people, devices, data, and workloads.

"Quantum Security Gateways made it easy to consolidate our defenses with autonomous threat prevention across all of our network points.They almost orchestrate themselves. They immediately configure themselves and automatically update policies."

- Archie Jackson, Senior Director and Head of IT and Security, Incedo Inc.

"Quantum Security Gateways made it easy to consolidate our defenses with autonomous threat prevention across all of our network points," said Jackson. "They almost orchestrate themselves. They immediately configure themselves and automatically update policies. We can implement best practices in a click to proactively defend against the latest threats."

Check Point CloudGuard Network Security extends the same industry-leading threat protection to the Incedo Inc. private cloud infrastructure. Automated security provisioning allows the company to protect assets with advanced security services wherever they are needed. Centralized management enables the team to configure and monitor all physical and virtual security instances.

Check Point R81 Security Management provides Jackson with complete, unified visibility of his entire environment—simply and quickly. Policy installation is fast. Automation makes enterprise-wide configuration and deployment seamless. Consolidation makes everything visible from a single pane of glass.

"Check Point Infinity's consolidated, unified architecture is simple to implement," said Jackson. "The integrated Infinity architecture delivers organization-wide visibility with the ability to scale services up or down. Check Point R81—with policy management and integration with other Check Point services—gives us comprehensive next-generation threat protection."

Endpoint Protection Without Business Impact

To protect endpoints, Incedo Inc. initiated a proof of concept with Check Point Harmony Endpoint. Behavior-based detection protects against zero-day attacks such as ransomware, phishing, and malware. It identifies behaviors, like file encryption, and automatically restores ransomware-encrypted files. It blocks users from phishing sites and blocks malware from web browsing and email attachments. Files received via email are sent to the SandBlast Threat Emulation sandbox for inspection and sanitized without delay using Threat Extraction before being sent to users.

"Harmony Endpoint gave us the protection and visibility we needed without affecting business performance or productivity," said Jackson. "Unlike other end-point security solutions, Harmony provides browser security, remote access VPN, email security, and mobile security in addition to malware protection, anti-bot, URL filtering, anti-ransomware, disk and media encryption, anti-exploit, and Behavioral Guard. Harmony integrated with Check Point Infinity-Vision encapsulates extended detection and response (XDR) capabilities with ThreatCloud real-time threat intelligence. With automatic blocking, detection, investigation, and remediation—it's seamless. We expanded deployment to all endpoints and servers."

> "I'd recommend Check Point for multiple reasons. Its products are effective and speak for themselves. I doubt there is any other security product by any security vendor that offers such orchestrated security like Check Point Infinity."
>
> - Archie Jackson, Senior Director and Head of IT and Security, Incedo Inc.

Benefits

Increased Agility

With enterprise-wide visibility across the network and endpoints, Jackson has at-a-glance assurance that the infrastructure is being actively protected. Automated detection, investigation, and remediation capabilities do the work of an entire team.

"By consolidating our security defenses with Check Point, we're far more agile and flexible than we could have been before," said Jackson. "Check Point has helped us become a highly resilient organization."

Proven Protection

When ransomware attacks spiked in 2020 and early 2021, Incedo Inc. and its clients' environments stayed safe. Harmony Endpoint's threat hunting capabilities provide real-time visibility of all indicators collected from endpoints across the organization—with an event timeline and detailed information. During the ransomware spikes, it provided 100% detection across all tested, unique MITRE ATT&CK techniques.

"Harmony Endpoint threat hunting showed us a wider spectrum of the threat landscape," said Jackson. "Automated detection and detailed reports dramatically shortened our Security Operations Center (SOC) processes. Check Point took care of the monitoring and heavy lifting—and gave us actionable response options."

Incedo Inc. is continuing to consolidate its cybersecurity defenses. It recently implemented Check Point CloudGuard Posture Management for a client's AWS cloud deployment. CloudGuard Posture Management provides a broad set of security and compliance controls, deep visualization, multi-factor authentication, and policy automation for verifiable security management. The company is also evaluating Check Point CloudGuard to protect its internal application development assets in the cloud. CloudGuard Automated DevSecOps features enable security posture management and workload protection across the development, CI/CD, and runtime lifecycle.

"I'd recommend Check Point for multiple reasons," said Jackson. "Its products are effective and speak for themselves. I doubt there is any other security product by any security vendor that offers such orchestrated security like Check Point Infinity. It secures the enterprise from end to end. Second, I recommend Check Point for its culture. Throughout our evaluation, implementation, and upgrade processes, the sales and project implementation teams are strongly aligned with our needs. Check Point is truly a trusted partner for Incedo Inc. and our clients."