CUSTOMER CASESTUDY

SmartWave Technologies Secures IP Everywhere with Robust Endpoint Protection

Customer Profile

SmartWave Technologies customers benefit from low-cost manufacturing while also enjoying world-class design and a single source of accountability via professionals in North America

Challenge

- Prevent IP and customer data from theft and tampering
- Protect employee endpoints in the most dangerous cyber environments
- Defend and track documents on removable media

Solution

- Check Point Harmony Email & Office
- Check Point Harmony Endpoint

Benefits

- Encrypted USB devices and documents to prevent unauthorized access or use
- Secured remote access to bypass unreliable public WiFi networks
- Gained ability to stop end-point threats coming from cloud-based email and online downloads

> "Check Point Endpoint Protection gives us advanced protection without impacting our users. We gained robust defenses that protect IP consistently—wherever it travels."
>
> - Dhevan Yogeswaran, System Administrator, SmartWave Technologies

Overview

SmartWave Technologies

Smartwave develops, designs, and manufactures electronic and electromechanical systems that enable hands-free or autonomic operation. The company's customers include many Fortune 500 companies that use SmartWave solutions in hands-free soap, air freshener, water faucet, and paper towel systems. SmartWave technology also powers industrial systems such as brake cleaner fluid dispensing, chemical proportion mixing, and flushing systems. Headquartered in Toronto, Canada, SmartWave has manufacturing associates in North America and Asia. Protecting proprietary IP is the company's security priority, and it turned to Check Point to protect company endpoints.

Business Challenges

Increasing Endpoint Security for IP Protection

Each SmartWave customer has unique applications for the company's technology. Sensing, verification, and dispensing capabilities are proprietary to customers' specific needs, often resulting in IP and patented designs that must be protected.

SmartWave employees travel frequently to manufacturing facilities in China and Malaysia, which significantly increases the risk of cyberattack. Travelers are subject to threats and data theft attempts via spam email, hotel WiFi networks, email hacking, and stolen devices. SmartWave employees typically returned home with laptops infected with malware, viruses, and other threats.

"We were looking for a better way to prevent engineering drawings, product information, documents, and other files from falling into the wrong hands," said Dhevan Yogeswaran, System Administrator for SmartWave Technologies. "We also wanted the ability to track document movement, such as from a laptop to a USB device or vice versa."

As Yogeswaran and his team began evaluating endpoint security solutions, they had three primary requirements. First, running a Proof of Concept (PoC) was essential to their decision. They wanted to ensure that the new solution fit well with the company's environment. Next, they wanted a solution vendor who would listen and understand their unique needs and then be able to deliver deep technical and product knowledge. Finally, the new solution had to be robust.

"We needed much more than just an antivirus," said Yogeswaran, "We also needed the ability to track document usage, tailor policies to usage requirements, and provide encryption without requiring a separate infrastructure to support it."

SmartWave's technology solutions provider, CDW, suggested several potential solutions, including Check Point. As the SmartWave team evaluated each, they quickly narrowed down their choice.

"The Check Point PoC was invaluable," said David York, CFO at SmartWave. "The product speaks for itself, and the Check Point team stood with us the entire way to help fine-tune policies. Check Point delivered the highest value of the solutions we considered."

-Dhevan Yogeswaran, System Administrator,

Solution

Securing Data at Rest and in Motion

SmartWave conducted a PoC of Check Point Endpoint Security, using company executives as the test users. Check Point Endpoint Security enables organizations to secure data at rest, in use, and in transit on corporate laptops and PCs. It provides data security, network security, advanced threat prevention, forensics, and remote access VPN capabilities to defend vital data anywhere it is used.

During the PoC, the Check Point team transferred product knowledge, provided security expertise, and helped SmartWave maximize the capabilities of Check Point features. It quickly became clear that Check Point Endpoint Security delivered the robust capabilities SmartWave wanted, along with a strong vendor relationship and maximum value.

“The Check Point PoC was invaluable,” said David York, CFO at SmartWave. “The product speaks for itself, and the Check Point team stood with us the entire way to help fine-tune policies. Check Point delivered the highest value of the solutions we considered.”

Results

Protecting Removable Media

SmartWave endpoints can be secured with Check Point Full Disk Encryption, but the Media Encryption capabilities are critical to Yogeswaran. Company policy requires all documents to be encrypted. When documents are copied to removable media for use onsite with customers or while traveling, the media itself is encrypted by Check Point. This makes it impossible to open the drive or documents on any endpoint that does not have Check Point Endpoint Security deployed.

Check Point also gives Yogeswaran centralized management of all endpoint ports. He can set and enforce encryption policy and control device access settings. Device activity and file movement logs are stored for centralized auditing and reporting.

Stopping Threats at the Border

Check Point SandBlast Agent defends endpoints against zero-day malware, bots, and ransomware. SandBlast Threat Emulation detects potential threats and sandboxes them for analysis. SandBlast Threat Extraction removes malicious content and reconstructs the document before sending a clean, safe version to the user.

“We’ve seen several incidents where SandBlast Agent detected and removed embedded malware in files downloaded from the Internet,” said Yogeswaran. “We also rely on Check Point CloudGuard SaaS to protect Office 365 email traffic and prevent account takeovers.”

Check Point CloudGuard SaaS protects SmartWave data by preventing targeted attacks on SaaS applications and cloud-based email. It also defends email attachments and shared files, protecting SmartWave data all the way from email.

Centralized Management Simplifies Everything

Yogeswaran uses Check Point R80 Security Management to control all endpoints from a single pane of glass. Integrated threat management provides centralized logging, monitoring, event correlation and reporting. A visual dashboard provides full visibility at a glance, while unified policy makes it easy to tailor policies with granular control.

“Check Point Endpoint Protection gives us advanced protection without impacting our users,” said Yogeswaran. “We gained robust defenses that protect IP consistently—wherever it travels.”

For more information, visit: https://www.checkpoint.com/products/ mobile-threat-defense/