Starkey Hearing Technologies Amplifies Visibility into Advanced Threats

Company extends advanced threat protection to laptops and improves security posture with Check Point Harmony Endpoint

INDUSTRY	HEADQUARTERS	COMPANY SIZE
Manufacturing	Eden Prairie, Minnesota	5,001-10,000 employees

OVERVIEW

Starkey Hearing Technologies is a world leader in advanced hearing solutions

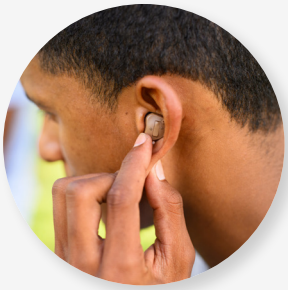
and the largest U.S. manufacturer of hearing aids. Its evidence-based design process results in products that make a dramatic difference in people's ability to hear the world around them.

OUR SOLUTION

Harmony
Secure the Workspace

Hearing care professionals worldwide order Starkey products through the company's online ordering and payment system. Starkey must meet Payment Card Industry (PCI) compliance requirements in addition to securing its business with other solutions, such as Data Loss Prevention (DLP), antivirus, and other network security tools.

"Technology changes quickly, which makes it a real challenge to keep up," said Joe Honnold, IT Manager of Network Services at Starkey Hearing Technologies. "We're trying to minimize the impact of change and still provide a secure environment for employees and customers."



> Since we deployed Harmony Endpoint, we have not had a single advanced malware or ransomware incident in almost a year.
>
> *Joe Honnold, IT Manager of Network Services, Starkey Hearing Technologies*

CHALLENGE

Honnold's job became even more challenging when Starkey was hit by an unknown advanced malware attack that started communicating with a command and control server. The team later learned that the malware was Gatak, a type of Trojan. Gatak hides data in image files. When it installs on a computer, it tries to download an image from any number of URLs that are hard-coded into the malware. The image contains encrypted data in pixel data. Next, Gatak deploys a lightweight capability that performs detailed fingerprinting on the infected machine and can also install additional payloads. A second Trojan component persists on the machine and steals information.

That persistence led to three or four advanced malware incidents per week. The attacking malware gathered valuable data that enabled it to escalate access privileges to network assets and spread laterally. It infected 2,000 machines in just two weeks. Under external control, the data could have been exfiltrated or encrypted and held for ransom. When employees took their laptops home and were no longer behind the corporate gateway, they became much more vulnerable. It was obvious that Starkey's antivirus solution was no longer enough.

"Modern malware changes every day," said Honnold. "We needed more advanced capabilities to protect our laptops and other edge devices. We called Check Point and asked how we could better leverage our Check Point Quantum Gateway infrastructure to increase our protection."

OVERVIEW

Starkey chose Check Point Harmony Endpoint to protect the company's desktops and laptops. Harmony Endpoint uses a complete set of advanced endpoint protection technologies—both on-premises and remote—to defend endpoints against zero day malware and targeted attacks. Starkey deployed Harmony Endpoint on

> Our Check Point SmartEvent event management console consolidates monitoring, logging, reporting, and event analysis to correlate data and give us actionable attack information. Our security analysts can see malicious events, attack entry points, the scope of damage, and data about infected devices so that we can respond quickly.
>
> *Joe Honnold, IT Manager of Network Services, Starkey Hearing Technologies*

4,000 systems across 34 facilities worldwide.

Harmony Endpoint detects and blocks attacks from email, removable media, spear phishing, watering holes, and command-and-control communications, even when users work remotely. Harmony Endpoint also stops data exfiltration to prevent sensitive information from leaking, and it quarantines infected systems to prevent malware from spreading. Starkey gains valuable protection across enterprise file types, such as Microsoft Office, Adobe PDF, Java, and multiple Windows operating system environments.

"We use Harmony Endpoint's threat emulation capability to discover malicious behavior," said Honnold. "It even uncovers new types of malware and threats hidden in SSL and TLS encrypted communications."

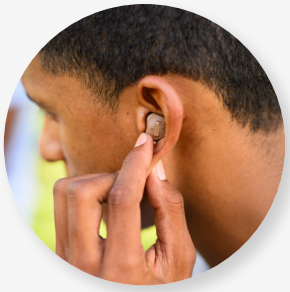
Harmony Endpoint threat emulation quickly inspects files in a virtual sandbox. Suspicious-looking files are flagged for deeper analysis, and then threat emulation sends a signature to the Check Point Infinity Platform Services ThreatCloud AI database, which documents and shares information on newly identified malware.

Harmony Endpoint's automated forensics capability gives Honnold's team a deeper understanding of security events faster. When a malware event occurs, a combination of advanced algorithms and deep analysis of raw forensic data in Harmony Endpoint builds a comprehensive incident summary with a complete view of the attack flow.

"Our Check Point SmartEvent event management console consolidates monitoring, logging, reporting, and event analysis to correlate data and give us actionable attack information," said Honnold. "Our security analysts can see malicious events, attack entry points, scope of damage, and data about infected devices so that we can respond quickly."

OUTCOME

Deploying Harmony Endpoint on desktops and laptops extended protection across the organization. When mobile users take laptops home, Harmony Endpoint, with its advanced protection, goes with them. The result is better, more effective protection no matter where users are working. At the same time, more secure endpoints help Starkey continue to meet its PCI compliance goals.



> Check Point helps me meet the challenges I face every day.
>
> *Joe Honnold, IT Manager of Network Services, Starkey Hearing Technologies*

"Since we deployed Harmony Endpoint, we have not had a single ransomware incident in almost a year," said Honnold.

The Starkey team keeps up with change by bringing new technologies in, deploying them quickly, and minimizing management and maintenance tasks. With Harmony Endpoint and its forensics capabilities, Starkey can immediately drill down into the details of a malware attack and remediate a device or situation quickly and easily. Now, the team can view the threat landscape from both Starkey's Check Point gateway and endpoint perspectives. All logs are consolidated into SmartEvent summaries for easy review.

Since Harmony Endpoint was deployed, the Starkey team has made some interesting discoveries. For example, they found that a certain version of Chinese Pinyin—which translates Chinese characters to English characters in email—actually records users' keystrokes and sends them off to command and control sites. Without the visibility they now have, the team would have been vulnerable to unknown bad actors and potential security vulnerabilities.

Harmony Endpoint has saved the team a great deal of time. In the past, they would have to quarantine an infected computer and often ship it to a central location, where it was isolated from the network. Now, they can isolate a device at the site of the incident and work with local staff to identify and remediate an issue. The IT team saves up to a day and a half of time per incident, and employee productivity is not affected.

"Check Point helps me meet the challenges I face every day," said Honnold. "It gives me a common platform, support structure, and log and event management system that a very small team can manage easily. I would recommend Check Point Harmony Endpoint to anyone."

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Platform Services for collaborative security operations and services.

LEARN MORE

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

www.checkpoint.com

July 2024