Starkey Hearing Technologies Amplifies Visibility into Advanced Threats

Company Extends Advanced Threat Protection to Laptops and Improves Security Posture with Check Point SandBlast Agent

> "Since we deployed SandBlast Agent, 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

Customer Profile

Starkey Hearing Technologies is the leading developer and manufacturer of hearing aids worldwide.

Challenge

- Increase protection against zero-day threats and ransomware attacks
- Protect laptops of mobile users
- Gain better visibility into incidents without increasing management and maintenance tasks

Solution

- Check Point SandBlast Agent with Threat Emulation and Automated Forensics

Benefits

- Detected and blocked ransomware, reducing incidents to zero
- Gained full visibility into threats to minimize unknown vulnerabilities
- Accelerated incident review and remediation while simplifying management
- Saved significant time every week by not having to remediate ransomware attacks

Overview

Starkey Hearing Technologies

Starkey Hearing Technologies is a world leader in advanced hearing solutions, as well as the largest U.S. manufacturer. Its evidence-based design process results in products that make a dramatic difference in people's ability to hear the world around them.

Getting—and Staying—a Step Ahead

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."

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.

Check Point SOFTWARE TECHNOLOGIES LTD

April 11, 2017

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 gateway infrastructure to increase our protection."

Solution

Protection That Lives on the Edge

Starkey chose Check Point SandBlast Agent to protect the company's desktops and laptops. SandBlast Agent 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 SandBlast Agent on 4,000 systems across 34 facilities worldwide.

SandBlast Agent detects and blocks attacks from email, removable media, spear phishing, watering holes, and command-and-control communications, even when users work remotely. SandBlast Agent 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 SandBlast Agent'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."

SandBlast Agent 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 ThreatCloud database, which documents and shares information on newly identified malware.

SandBlast Agent'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 SandBlast Agent builds a comprehensive incident summary with a complete view of the attack flow.

"Our Check Point SmartEvent 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."

> "Our Check Point SmartEvent 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, scope of damage, and data about infected devices so that we can respond quickly"
>
> — Joe Honnold, IT Manager
> of Network Services,
> Starkey Hearing Technologies

Check Point
SOFTWARE TECHNOLOGIES LTD

Benefits

Extending Advanced Protection

Deploying SandBlast Agent on desktops and laptops extended protection across the organization. When mobile users take laptops home, SandBlast Agent 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.

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

Giving IT Management More Visibility

The Starkey team keeps up with change by bringing new technologies in, deploying them quickly, and minimizing management and maintenance tasks. With SandBlast Agent 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 SandBlast Agent 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.

Successfully Meeting Every Challenge

SandBlast Agent 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 SandBlast Agent to anyone."

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

For more information, visit
www.checkpoint.com/sandblast

Check Point SOFTWARE TECHNOLOGIES LTD