TOPRX ROTECTS BUSINESS CONTINUITY WITH CHECK POINT HARMONY ENDPOINT

TopRx

Customer Profile

TopRx is a leading national supplier of generic pharmaceuticals, over-the-counter drugs, vitamins, and home health products.

Challenge

- Extend robust protection to remote endpoints
- Further enhance security posture with better visibility into threats
- Simplify endpoint security management

Solution

- Check Point Harmony Endpoint
- Check Point Next Generation Security Gateways

Benefits

- Gained continuous protection for all endpoints whether on or off the corporate network
- Proactively detect, identify, and remediate threats with awareness of suspicious tactics, techniques, and procedures
- Simplified endpoint security management while improving overall security posture

> I highly recommend Harmony Endpoint. It's very robust and has proven highly effective. TopRx has greatly improved its security posture with far less time invested in maintaining endpoint software."
>
> - Michael Catanzaro, Lead Information Security Engineer, TopRx

Overview

TopRx distributes generic pharmaceuticals, over-the-counter drugs, vitamins, and home health products from 90 manufacturers to more than 7,000 pharmacies in 50 U.S. states. As an Authorized Distributor of Record (ADR), the company provides customized services and outstanding support for its customers and manufacturing partners. TopRx is based in Memphis, Tennessee with sales offices and remote employees across the U.S.

Business Challenge

Maintaining Uninterrupted Operations

IMillions of patients rely on their pharmacies for prescriptions and other healthcare products. To meet those needs, TopRx's priority is ensuring nonstop operations. Having a strong security posture is integral to this goal. Until the COVID pandemic, most of the company's users and endpoints were on premises, defended behind Check Point Next Generation Security Gateways. When the pandemic forced employees to work from home, TopRx needed to extend protection to their systems.

"It became critical to implement stronger safeguards with deep visibility into remote endpoints," said Michael Catanzaro, Lead Information Security Engineer at TopRx. "We wanted to replace our previous signature-based detection solution with one that used behavior-based techniques."

The TopRx team compared potential solutions from Check Point, VMware

"Not only did Harmony Endpoint detect and stop every threat we tried, it's cloud-based and easy to use"

- Michael Catanzaro, Lead Information Security Engineer, TopRx

Carbon Black, and CrowdStrike. After throwing a variety of malware, ransomware, and phishing attacks at the platforms, only Check Point Harmony Endpoint* stopped all of them.

Harmony Endpoint is a complete endpoint security solution built to protect remote workforces from cyber threats. It prevents ransomware, phishing, and drive-by malware from affecting endpoints while minimizing breach impact with autonomous detection and response. Harmony Endpoint is the only endpoint protection solution that automatically remediates the entire cyber kill chain.

"Not only did Harmony Endpoint detect and stop every threat we tried, it's cloud-based and easy to use," said Catanzaro. "We also like the compliance blade. It scans endpoints to be sure they have the latest Windows service packs and updates—not allowing them to join the network until they are properly patched."

SOLUTION

Deployed Easily, Immediately Indispensable

The TopRx team reports that deployment was fast and easy. They packaged Harmony Endpoint capabilities to implement the specific protections needed for their desktop systems, laptops, and servers. Using the built-in deployment policies, the team protected all endpoints in about two days.

"The deployment was seamless," said Catanzaro. "Once deployed, Harmony Endpoint is very low maintenance. If we need to upgrade, it's simple from the cloud and we don't have to install a complete new package."

TopRx remote endpoints use the full capabilities of Harmony Endpoint—threat emulation and extraction, threat prevention, remote access VPN, anti-ransomware, anti-malware, and URL filtering. Windows servers are protected by anti-malware, anti-ransomware, and behavior guard features, and Linux servers use the threat prevention capabilities. Harmony Endpoint also is integrated with the Check Point Infinity architecture for effective detection and prevention of imminent threats.

"The threat emulation and threat extraction features have been really helpful to securing our users," explained Catanzaro. "Anytime a user downloads a file from a website, Harmony Endpoint assumes the file is sensitive and runs it in a sandbox. If it detects anything malicious, it blocks the file, removes the malicious elements, and sends back a clean copy of the file."

Continuous Protection and Recovery

In the past, blocking malicious URLs required all endpoints to be

"Check Point Infinity ThreatCloud™ enables us to proactively search for potentially malicious tactics, techniques, and procedures (TTPs)."

- Michael Catanzaro, Lead Information Security Engineer, TopRx

connected to an on-premises dedicated gateway. With Harmony Endpoint, a browser plug-in implements policies and protects endpoints. Now, all remote systems are continuously protected, whether they are connected to the LAN, via VPN, or off the company network and using a home Wi-Fi network.

Harmony Endpoint's powerful anti-ransomware features provide full attack containment and remediation to quickly restore any infected systems. Anti-ransomware capabilities create small backups of users' files as they work. If the software detects ransomware starting to encrypt files, it kills the encryption process and instantaneously recovers files that would have been lost.

Finding and Remediating Threats

"I discovered Harmony Endpoint's threat hunting features through the Check Point Infinity ThreatCloud™ portal," said Catanzaro. "It enables us to proactively search for potentially malicious tactics, techniques, and procedures (TTPs). The dashboard is great—we can see any scripting occurring on endpoints to discover threats that might otherwise go undetected."

Threat hunting is powered by enterprise-wide visibility and globally shared threat intelligence from hundreds of millions of sensors collected by ThreatCloud. Predefined queries make it simple for the TopRx team to identify and drill down into suspicious incidents. The MITRE ATT&CK© dashboard also provides additional queries for identifying specific TTPs and mitigations. All activity is rolled up into the Harmony Endpoint dashboard in an easy-to-use view.

"I get on the threat hunting dashboard first thing every day," said Catanzaro. "I can instantly see botnet traffic, infected assets, remediated infections, and running scripts. Harmony Endpoint threat hunting capabilities give us really deep visibility into threats and our defenses."

Working hand in hand with threat hunting are Harmony Endpoint's forensics capabilities. When threats are proactively uncovered through threat hunting, forensics processes take over to automatically monitor and record endpoint events—including affected files, processes launched, system registry changes, and network activity.

Catanzaro said that the forensics have been really helpful. In the past, the team had to do lots of manual digging and event correlation between multiple sources to find out if an event was truly malicious or if legitimate software was behaving in a way that simply looked suspicious.

"Now we just go into forensics and see all of the processes and applications running," he said. "If it's truly malicious, we can do further analysis. If it's legitimate, we can whitelist the application. It eliminates false positives and saves us a lot of time."

"The MITRE ATT&CK© integration has helped us further strengthen the company's security posture. Prebuilt queries and direct access to the MITRE TTPs and mitigations make it quick and easy to identify suspicious behaviors and dig deeper"

- Michael Catanzaro, Lead Information Security Engineer, TopRx

Benefits

Keeping Everyone Safely Connected

TopRx remote employees are staying safely connected to the resources they need for serving customers and partners. Harmony Endpoint's VPN and compliance features not only keep users protected, they also help ensure that threats don't enter the corporate network through endpoints.

Preempting Threats with Deep Visibility

Daily threat hunting allows the team to proactively monitor traffic from endpoints to servers for unusual behaviors. Integration with the MITRE ATT&CK© Framework delivers additional visibility and guidance for mitigating any suspicious events.

"The MITRE ATT&CK© integration has helped us further strengthen the company's security posture," said Catanzaro. "Prebuilt queries and direct access to the MITRE TTPs and mitigations make it quick and easy to identify suspicious behaviors and dig deeper."

Making Strong Security Simpler

Catanzaro says that Harmony Endpoint's effectiveness and Check Point support have been key to strengthening the TopRx security posture. Cloud management makes upgrades and everyday use seamless. Integration with the Check Point Infinity architecture delivers fantastic visibility and advanced capabilities that TopRx couldn't find with other solutions.

"I highly recommend Harmony Endpoint to other security professionals," he said. "It's very robust and has proven highly effective. TopRx has greatly improved its security posture with far less time invested in maintaining endpoint software. It's great."

* - formerly known as SandBlast Agent