CASE STUDY

proofpoint.

AKORN SELF-PRESCRIBES PROOFPOINT PROTECTION

EFFECTIVELY STOPS PAIN AND INFECTION CAUSED BY THREATS

CHALLENGE

- Stop malicious emails from getting into users' inboxes
- Maximize the small IT team's ability to fight threats effectively
- Increase situational awareness
- Integrate protection capabilities with its SIEM

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Information Protection Suite
- Proofpoint Threat Response

RESULTS

- Drastically reduced the number of suspicious emails coming through its network, compared to the previous solution
- Stops 4,500–5,000 malicious attachments and URLs per month from entering users' inboxes
- Stopped Cryptolocker attacks from recurring
- Eliminated hours of time spent investigating, cleaning, and resolving incidents

Akorn is no stranger to challenging requirements. The Lake Forest, Ill., pharmaceutical maker develops, manufactures, and markets generic and branded prescription pharmaceuticals. It specializes in difficult-to-make products, such as drops, topical preparations, inhalants, and sprays. When it came to cyber threats, Akorn had some challenging requirements of its own. Having a mature security posture is just part of being a publicly traded company with FDA oversight. The company has troves of data it needs to protect: trade secrets, market-moving financial data, personal information, and more.

Akorn's multi-level security architecture was doing a good job of containing threats before they caused much damage. But threats were growing more frequent and severe, and the security team wanted to block them from even getting in.

"We were blocking a significant amount of spam and malware," said Todd Gray, Director of IT Security at Akorn. "But we still saw a large number of malicious emails, attachments, and URL links. We began looking for a better solution."

TARGETING ATTACKERS

Attackers used malicious links, impostor emails (also known as business email compromise, or BEC), and weaponized malware to try and breach IT defenses, steal credentials, and take over endpoints. Akorn was targeted by fake emails, purportedly from top executives, sent to the financial department requesting funds. The few times that these emails made it through, the security team stopped them. Scrupulous backup processes also enabled the team to quickly isolate, clean, and restore several laptops attacked by Cryptolocker, a popular strain of ransomware.

Akorn regularly educates employees, reminding them not to click on suspicious emails and to be aware of fake emails that they might see. But attackers have gotten much better at creating legitimate-looking email that exploits human nature. Even under the best circumstances, employees might end up clicking on one.

"Email is attackers' primary vehicle to achieve negative intent," Gray said. "In addition to deploying endpoint and network security, we want to stop all infected email and mail with no business value from coming in."

> **"…If a company is starting to ramp up their fight against email, targeted attacks, and other threats, I'd tell them to look at Proofpoint. It will let them gain the protection they need with the headcount they already have."**
>
> Todd Gray, Director of IT Security, Akorn

DUE DILIGENCE FOR SUPERIOR DETECTION

The IT Security team researched its options, looking for a tool that did a superior job of detecting email that carried malware or included links that didn't match the context of Akorn's business. Gray had used Proofpoint solutions at a global research institute. He suggested that the team look into deploying the technology at Akorn.

The company chose Proofpoint Email Protection and Proofpoint Targeted Attack Protection (TAP) to help stop email-based attacks. Email Protection defends against unwanted and malicious email, while TAP protects from advanced threats that use malicious attachments and URLs. Akorn also chose Proofpoint Information Protection with Email DLP and Email Encryption capabilities to protect sensitive information from unintentional exposure.

"We moved to Proofpoint because of its reputation for best-in-class email threat detection and advanced threat protection," Gray said. "Proofpoint does a great job of blocking unwanted and suspicious emails from getting in. It's exactly what we were looking for."

NO ENTRY, NO CLICKS

With Email Protection, Akorn drastically reduced the number of suspicious emails coming through its network, compared to its previous solution. Potentially harmful emails are blocked, but legitimate emails get through. The solution has generated few, if any, false positives.

"When we stop non-legitimate emails, users can't click on them," Gray said. "Therefore, they aren't causing problems that require us to investigate, clean machines, or resolve a breach. We haven't had any significant fire drills. Proofpoint saves us a lot of time right there."

TURN IT ON, TURN THREATS AWAY

Gray reports that they just turned the Email Protection solution on, and the deployment was seamless to users. Now users receive a digest of blocked emails, and they can determine if any were actually legitimate. If so, they can release that email to their inbox.

TURNING THE TABLES ON MALWARE

Akorn uses TAP to help it detect and stop advanced malware and credential phishing attacks. TAP typically stops 4,500–5,000 malicious emails per month, and Akorn hasn't seen any recurrences of Cryptolocker.

"We haven't had many incidents since we deployed Proofpoint," Gray said. "If something does come in that's not legitimate, our users can identify it and send it to our team. We confirm if it's malicious or fake and block future emails from that source. Proofpoint makes it fast and easy."

NOTHING ESCAPES NOTICE

Proofpoint dashboard views also help Akorn increase its situational awareness. The IT Security team uses dashboards to validate malware trends, gather metrics for senior executives, and investigate incidents that are detected by other Akorn security tools. For example, if a network or endpoint security tool identifies a threat, the IT Security team can view consoles from those security tools—as well as the Proofpoint dashboard—to correlate information and better understand the incident and its impact. If the company receives a threat update from the FBI, notifications of new malware attacks, or an alert from one of its remote offices, the team can compare data more easily and increase protection as needed.

“I’m very happy with our Proofpoint dashboard configuration, “Gray said. “The views are great. I wish other products had dashboards that let you drill down into data like Proofpoint does.”

Akorn also uses Proofpoint Threat Response to automate and enrich threat data that it receives. Within Proofpoint Information Protection, the Email DLP capability gives the team a way to make sure that sensitive information, such as credit card data, isn’t accidentally leaked. Proofpoint Email Encryption enables employees to encrypt and securely send emails that contain sensitive data to external recipients.

UPPING THE ANTE

The Akorn team is evaluating new Security Information and Event Management solutions. When the new system is deployed, they intend to integrate Proofpoint with it—further increasing their abilities to detect, analyze, and proactively fight threats aimed at the company.

“There simply aren’t enough people to throw at today’s threat landscape,” Gray said. “If a company is starting to ramp up their fight against email, targeted attacks, and other threats, I’d tell them to look at Proofpoint. It will let them gain the protection they need with the headcount they already have.”

For more information, visit www.proofpoint.com.