CASE STUDY

Global Pharmaceutical Company Fills its Detection and Remediation Gaps

cybereason

THE CUSTOMER

One of the world's largest pharmaceutical companies, with annual revenue in the billions of dollars.

THE PROBLEM

The company had limited visibility into the source of security incidents and was unable to detect advanced, never-before-seen threats.

THE CYBEREASON SOLUTION

- Immediate detection of signature-based threats, including several malware programs that the company's top-tier antivirus software failed to stop.
- Provided detailed attack context to enable a remediation plan in fewer than 10 hours.
- Less time spent re-imaging infected computers, freeing up the IT department to work on more critical tasks and decreasing interruptions to users.

One of the world's top pharmaceutical companies was struggling with gaining greater endpoint visibility. The company, which has to protect an intellectual property portfolio worth billions of dollars, had limited endpoint protection.

Top-tier antivirus software was installed on all its endpoints and a well-maintained SIEM configuration as well as a stack of network security tools were in place. However, malware was still getting through. The security team couldn't identify the malware's source or determine the incident's severity and its impact on the organization.

AN EXTREME APPROACH TO REMEDIATION

Since the company didn't fully understand what was happening on its endpoints, it had difficulty gathering context around the threats it faced. This lack of visibility forced the organization to take an extreme approach to remediation: it re-imaged any machine that was detected as infected. In a global organization that wiped 1,500 computers every day, this process had several drawbacks. With so many machines offline, business continuity suffered, worker productivity declined and incident response costs skyrocketed. And the company's IT department had more meaningful tasks to handle besides re-imaging machines.

The organization approached Cybereason looking for a solution that could help it continuously know what was happening on its endpoints, provide context around detected incidents and lead to a smarter, scalable remediation strategy.

KEEPING THE COMPANY SAFE WHEN ANTIVIRUS SOFTWARE FAILS

The company decided to deploy the Cybereason platform on 4,000 endpoints in one of its business units. A few days after roll out, Cybereason picked up several signature-based threats that the organization's antivirus software failed to detect. The antivirus software vendor, according to our customer, had fallen behind in manually adding newly discovered malware to its signature database. Cybereason, though, automates this task, meaning the platform will always contain the latest known malware.

Additionally, Cybereason gave the organization's security team a complete picture of the attack and provided them with details including what machines were infected, when and how the adversaries infiltrated the company and the extent of the damage. Having access to this data supercharged the company's security team and provided junior analysts with the information they needed to shut down a threat.

COMPUTER RE-IMAGING PLUMMETS AFTER ANALYSTS GAIN MORE CONTEXT ABOUT ATTACKS

With Cybereason, workers no longer had to surrender their computer to the IT department when a threat was detected. Instead, having a full attack picture helped analysts better judge if a machine really needed to be wiped. After a threat was detected, an analyst was able to remotely view what was happening across the company's IT environment and immediately take action using the Cybereason Incident and Response Console. In most cases analysts were able to carry out a remediation plan in fewer than 10 hours and remotely remove the malicious executable without shutting down the device.

In fact, soon after deploying the Cybereason platform the company reported a 90 percent drop in the number of machines that were re-imaged. In an organization with approximately 100,000 employees, this easily translates into freeing up a year's worth of time for several IT workers. Additionally, **the number of incidents in which the security team said it understood the full context of an attack increased from 35 percent to more than 90 percent.**

"The savings in time and the savings on re-imaging transformed the way our SOC operates," said the manager at one of the company's regional SOCs.

The decrease in re-imaging also had benefits for employees. Workers were able to continue using their computers and maintain business productivity instead of shipping them off for re-imaging.

EASING CONCERNS OVER THE DISCOVERY OF A POSSIBLE APT

A few weeks after deploying Cybereason in another business unit, the company's analysts discovered advanced malware in their network. The company's security management team feared that they were the victims of a sophisticated APT and decided to roll out Cybereason on several thousand more endpoints in this network to understand the attack's magnitude and how it spread.

Deployment only took a few hours, enabling immediate threat detection. The platform quickly discovered that several machines in Asia-Pacific and a few computers in Europe were infected and proved that the threat was not an APT. Cybereason showed the security analysts that even though the malware was a sophisticated program, it was not specifically targeting the company. Also, the malware infection was a confined event. Cybereason did not see any other related malicious activity. Armed with this information, analysts used Cybereason to immediately launch a remediation plan.

Given the complexity and novelty of this attack, even the most experienced analysts would most likely not have discovered it until months after it had infiltrated their organization. But by using behavioral analysis, Cybereason spotted and linked together seemingly disparate activities to reveal this never-before-seen attack.

The pharmaceutical company soon realized that Cybereason's ability to detect malware exceeded the capabilities offered by its antivirus program. To enhance its protection program, the security team implemented a new procedure: when Cybereason detected malware, its signature was added to the antivirus program. This additional benefit allowed the organization to supplement its existing security products with Cybereason.

ABOUT CYBEREASON

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and active monitoring services. Founded by elite intelligence professionals born and bred in offense-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioral patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

cybereason