cybereason | CASE STUDY

Retail Industry

INDUSTRY

Retail

NUMBER OF ENDPOINTS

11,300

USE CASE

Network and data protection at retail superstores, corporate offices, and the home networks of employees' now working remotely due to the COVID-19 pandemic.

THE CHALLENGE

- Protect corporate technical assets against a variety of cyber threats in big box stores, data centers, and home networks for remote working employees.
- Eliminate false positives, allowing the SecOps team to focus on critical risks and incidents.
- Deploy a flexible and scalable cybersecurity solution that grows as the company expands.

THE SOLUTION

- Cybereason Enterprise and MDR provide state-of-the-art SecOps protection for employees and customers.
- Corporate cybersecurity analysts became more efficient and productive due to the elimination of false positives as well as the actionable intelligence on every malicious operation provided by Cybereason's MalOp™ detection engine.
- The company now benefits from a proactive SecOps approach including NGAV, ransomware, and malware protection, as well as mobile endpoint security.

CYBEREASON PREVENTS BUSINESS DISRUPTION AND PROTECTS CUSTOMER DATA BY PROVIDING EXCEPTIONAL DETECTION AND RESPONSE

A French-based home improvement and gardening retailer for nearly a century boasts big-box superstores all over the world. Like other modern retail establishments in the eCommerce era, protecting against network intrusions and other cybercriminal activities at the company is critical. Additionally, cybersecurity became even more important as the company recently transitioned to mobile point-of-sale systems in lieu of an older PC-based approach.

In addition to ensuring customers enjoy a secure in-person shopping experience, the company needed to protect their employees working remotely due to the COVID-19 pandemic. Increasing the number of endpoints in this fashion requires a proactive SecOps approach, focusing on threat prevention as well as quickly detecting and remediating any suspicious network activity.

Confronted with this scenario, the company's CISO turned to Cybereason. After a side-by-side comparison with Microsoft Defender, the CISO chose Cybereason because of its superior behavioral-based prevention and detection features.

"Cybereason detects and prevents things that are completely missed by other solutions," he said.

THE CHALLENGE

The COVID-19 pandemic forced companies across the globe to close offices, requiring their employees to work from home. This situation exponentially increased the number of potential threats to the organization's technical assets, including customer data and network infrastructure. Ultimately, being able to protect IT assets both at home and in the office remains critical for any business.

Many SecOps experts agree that ransomware is the greatest cybersecurity risk currently confronting businesses and governmental agencies. Not immune to this issue, the company required flexible ransomware protection

as part of its enterprise SecOps solution.

Given the global footprint of its IT ecosystem, the company needed a cybersecurity solution that provides a high signal-to-noise ratio. False positives only serve to dilute the efforts of cybersecurity analysts. Eliminating these distractions ensures the cyber team is able to focus on only the real threats to the organization's technical infrastructure.

THE SOLUTION

The CISO's SecOps team selected Cybereason and Microsoft Defender for a proof of concept project. The POC revealed Cybereason as the clear winner, with superior behavioral-based prevention and detection functionality, as well as flexible support for hybrid enterprise network architectures. This flexibility ensured the company easily transitioned to a remote working model for their employees as branch offices closed due to the pandemic.

At the heart of the cybersecurity solution resides Cybereason Enterprise. The company also leveraged Cybereason Managed Detection and Response Complete (MDR), a robust SecOps tool leveraging state-of-the-art behavioral-based prevention and detection. MDR also includes the MalOp™ detection engine, providing security analysts with actionable intelligence for any malicious attack on the network; ensuring their valuable time is no longer wasted chasing down false positives.

Each report from the MalOp™ also includes tailored instructions with best practices for handling similar network security issues. Analysts see at a glance all aspects of the event, including affected users and systems as well as the timeline of the attack. More importantly, these SecOps analysts can now completely remediate any incident with minimal impact on the company's business operations.

Other components within the Cybereason Enterprise solution include multi-layered AV, NGAV, an endpoint detection and response (EDR) server add-on, and MDR Mobile. That service played a big role as the company transitioned to mobile point of sale systems at their big-box retail locations. It ensures customers are able to shop without worrying about their private data being stolen by cybercriminals.

THE OUTCOME

Ultimately, the Cybereason Enterprise solution protects the company's 11,300 endpoints from any malicious operation. It supports a SecOps approach to ensure both customers and remote employees enjoy trusted access to the network assets they need. The inherent flexibility of the MDR platform also provides the critical scalability to expand protection when necessary.

The cybersecurity team now works more efficiently and effectively with the actionable intelligence provided by the MalOp™. Notably, the CISO shares

> "The MalOp gives us the capability to proactivly protect and the possibility to see what we don't know. The team is now alerted to events in realtime that we may not see otherwise "
>
> **CISO**
> Retail Industry

information about cyber incidents from within the Cybereason Platform with other CISOs within their family of companies. This approach improves the standard of protection across the entire enterprise.

The CISO commented that Cybereason detects cyber threats missed by other SecOps solutions. The platform provides SecOps analysts with enhanced visibility into the entire network. Visibility into this infrastructure grew much more complex with employees accessing corporate technical assets from their home networks.

Cybereason also offers significant protection against fileless attack vectors. The company had a machine attacked with the Emotet malware, and MDR prevented attempts to use PowerShell to propagate that malware throughout the rest of the network.

This behavioral detection approach also expands to ransomware protection. This functionality is one of the most valuable features provided by Cybereason Enterprise. Ultimately, Cybereason offers peace of mind to any CTO worried about this form of malicious attack.

The company's brick and mortar retail establishments also benefit from Cybereason's MDR Mobile. The company's sales and credit processing systems and data stay protected from the prying eyes of cybercriminals. As a result, customers now enjoy a state-of-the-art secure shopping experience with their mobile devices.

Cybereason provides the company with a cybersecurity solution that protects the full range of corporate technical assets – on-premises, cloud, hybrid, and mobile. Everything from a cloud-based virtual server farm to an iPad running a point of sale app falls under the Cybereason security umbrella.