DARKTRACE

CASE STUDY

CordenPharma

Overview

Industry

- Healthcare & Pharma

Challenge

- Needed to protect valuable intellectual property
- Customers had stringent data protection requirements
- Lacked comprehensive visibility into all network traffic
- Small security team

Results

- Real-time alerts allow security team to be proactive in threat detection
- 100% visibility into network activity
- Machine learning technology safeguards critical data
- Early threat detection satisfies customers' requirements

Business Background

CordenPharma began as a technology-based contract manufacturing business in 1946. Over the last 70 years, the organization has contributed important technological advancements to Active Pharmaceutical Ingredients (API) manufacturing, becoming a highly trusted contract manufacturer. Acquired by International Chemical Investors Group (ICIG) in 2006, CordenPharma is now ICIG's largest manufacturing site. Today, the organization produces pharmaceuticals for many of the world's leading pharmaceutical and biotechnology companies.

> It was eye-opening to witness the capabilities we had with Darktrace. It lets our small security team of four look like we are a team of 20.
>
> **Brandon Frontz**
> **IT Systems and Network Administrator**

Challenge

In recent years, the pharmaceutical industry has been increasingly targeted by sophisticated cyber-attackers. Given that drug development often takes years and billions of dollars, companies are particularly concerned with the security of their proprietary drug formulas. Tasked with storing the sensitive intellectual property of numerous major companies, CordenPharma's reputation relies on its ability to protect this data.

Many of CordenPharma's largest customers have their own stringent security requirements to prevent the theft of their valuable intellectual property. CordenPharma needed a tool that could provide early threat detection, prevent data breaches, and accommodate its customers' myriad requests.

Additionally, as the company continued to grow, the lean security team struggled to keep track of activity across its complex network infrastructure and lacked visibility. Without the ability to prioritize threats or distinguish genuine anomalies from network noise, the security team was concerned they would not be able to act quickly enough to prevent damaging attacks.

Solution

These concerns led CordenPharma to deploy Darktrace on its network for a four-week Proof of Value (POV) period. After a one-hour installation, Darktrace began learning the activity of every user and device on the network, establishing a 'pattern of life' for all devices and users. Now the Enterprise Immune System's evolving understanding of 'normal' allows it to identify threatening anomalies on CordenPharma's network as they emerge. Darktrace's unique early threat detection capabilities prevent potential threats from escalating into crises.

Soon after its deployment on CordenPharma's network, the Enterprise Immune System detected a serious anomaly that had gone undetected by legacy tools. Darktrace alerted the security team to late-night traffic flowing from the company's networks to a foreign country. Given that CordenPharma had no business connections to the country in question, the security team cut off the connections and was able to avoid further network compromise, preventing damaging data loss.

Later in the POV, Darktrace alerted CordenPharma to a potential incidence of malicious insider activity: sensitive information was transferred to a USB device and then uploaded onto multiple computers. The use of a USB device was a violation of company policy, and not a malicious insider. Darktrace's detection enabled the security team to identify the users in need of additional security training and better enforce company policy in the future.

> We could immediately understand how Darktrace would improve our security posture and how valuable the technology would be for data loss prevention.
>
> **Brandon Frontz**
> **IT Systems and Network Administrator**

Benefits

One of the major benefits of Darktrace's technology is its ability to notify CordenPharma to threatening incidents early – before they can become damaging attacks. For example, armed with Darktrace's capabilities, if a file containing customers' names moves anywhere off the corporate network, CordenPharma's security team is instantly alerted. These alerts can be the difference between a minor threat and a serious breach, and allow both CordenPharma and its customers to feel confident in the security of their data. "This is a massive selling point for our customers," Frontz noted. "Darktrace's unique alerting system is something no other tool has been able to provide."

Additionally, Darktrace's Threat Visualizer provides CordenPharma with an interactive and comprehensive view of its network. Within a single screen, the IT team can observe and engage with every corner of the network. "The Threat Visualizer put in perspective the traffic flow across our network, including the traffic in and out of our firewall," commented Frontz. "The user interface has also been simple to pick up and understand."

"We're such a small team that we don't have the resources to constantly monitor the logs and look for anything unusual," said Frontz. "Darktrace's machine learning only brings what we need to see to our attention. With Darktrace it is: here's the activity, here's a red flag, and here's why."

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010

info@darktrace.com
darktrace.com