cybereason® | CASE STUDY

PIONEER TELEPHONE COOPERATIVE

Pioneer

INDUSTRY

Telecommunications

NUMBER OF ENDPOINTS

1,400

USE CASE

Centralized detection and response across operating systems, endpoints, email, identity, productivity suites, network, and cloud.

THE CHALLENGE

- Provide Pioneer's information security team with access to the relevant information needed to predict, understand, and end attacks on a global scale.
- Monitor all potential system security incidents in a centralized manner and prioritize based on the required level of data protection.
- Deploy an enterprise-wide solution that integrates all the operating systems, devices, workstations, and servers of the organization seamlessly.
- Measure cost-effectiveness of the solution against company requirements, thereby saving money and other resources in the long run.

THE SOLUTION

- Cybereason XDR correlated data across endpoints, applications, the cloud, and identities and provided analysts with an actionable attack story.
- Cybereason XDR provided integrations with leading firewall and MDR vendors to consolidate alerts, correlate network context with user and asset activity, and enable automated and guided response actions from within the XDR console.

CYBEREASON XDR IMPROVES DETECTION AND RESPONSE FROM ENDPOINT TO ENTERPRISE

Pioneer Telephone prides itself as an industry leader in rural telecommunication services and products. With almost 600 employees, this Oklahoma-based company has more than 140,000 customers. Chad Kliewer, Pioneer's Information Security Officer, describes the company as "a big little company," that provides a wide range of solutions from local telephone and cellular services to high-speed internet in rural Oklahoma.

Infrastructure evolution and the global shift in the threat landscape over the years has significantly increased the need for better visibility into the company's cybersecurity posture. This also meant that the company was employing a large number of endpoint devices and a variety of operating systems, including iOS, Microsoft Windows, and Linux. In addition, standard cloud protection solutions, such as Microsoft Defender, don't have the capacity to log and inspect issues over a larger scale without additional licensing cost.

The solution, therefore, had to provide a unified investigation and response experience that correlates telemetry across remote endpoints, mobile devices, cloud platforms, and applications to predict, prevent and end malicious operations.

THE CHALLENGE

Being in the telecommunications business, Pioneer Telephone has spent years connecting people's homes with fiber and wireless internet services, providing worldwide long-distance calling, and gaining their consumers' trust. It makes for an attractive target for cybercriminals that can significantly damage the company's reputation.

Previously, the company satisfied their security needs using traditional antivirus for their devices. However, as the company grew, its assets became more critical and a higher level of protection became mandatory. Many popular options failed to equip Pioneer with company-wide monitoring and threat defense solutions.

Pioneer was looking for a solution that afforded them the flexibility to use a large number of servers and workstations across all employees and offices.

"My number one goal was to find a solution that would protect all the pieces of the system, so MacBooks are as secure as Windows devices," Kliewer said.

Finding a solution that would protect Linux servers, Android, iOS, Microsoft, and all other devices proved to be tricky. The company wanted a centralized logging and monitoring system, along with native integrations with all employee emails, productivity suites, and management platforms.

THE SOLUTION

Pioneer reached out to Cybereason to provide a solution that would correlate data across endpoints, applications, the cloud, and identities as an actionable attack story.

Cybereason XDR provided Pioneer with a platform that integrates with leading firewall and EDR vendors to consolidate alerts, correlate network context with user and asset activity, and enable automated or guided response actions from within the XDR console.

Cybereason XDR gave Pioneer the ability to protect all of its employees with effective security far beyond the endpoint. Through native integrations with email, productivity suites, identity and access management, and cloud deployments Pioneer was able to find undetected signs of compromise and end malicious operations.

THE OUTCOME

The Cybereason AI-driven XDR Platform delivered Pioneer diverse and deep integrations, and enhanced correlations across Indicators of Compromise (IOCs) and Indicators of Behavior (IOBs) to detect the more subtle signs of network compromise.

The XDR console helped the company save on cloud storage and third-party analysis expenses, by providing an all-in-one solution. It also improved Pioneer's response time from hours down to a few minutes, with very few false positives.

According to Kliewer, Pioneer has come to regard Cybereason as more of a partner than a vendor. By understanding Pioneer's business model, Cybereason was able to break down their data silos and reduce their response time to only a few minutes.

> "I was in search of something that would work on all the different operating systems and bring everything back to one central place. That's what I was looking at with Cybereason. Even to this day, I'm still not aware of any other products that will touch every different OS in all the different pieces."
>
> **CHAD KLIEWER**
> **INFORMATION SECURITY OFFICER**
> Pioneer Telephone