ExtraHop

Global Telecommunications Provider Uses ExtraHop to Monitor External Connections to Improve Compliance and Security

Case Study: Global Telecommunications Provider

> "You can't secure what you can't see. With ExtraHop, we've got eyes on every interaction that takes place on our network. That is the first step to protecting our environment."
>
> – *Senior Cyber Security Engineer, Large Wireless Telecommunications Company*

Executive Summary

This global telecommunications provider connects tens of millions of consumers and business customers with wireless voice, messaging, and data services.

In order to deliver these services, they partner with numerous third-party vendors to maintain their internal and external-facing systems. In order to ensure security, compliance, and performance quality, the telco needed a way to monitor and manage connections coming into their environment.

With performance management and cybersecurity analytics from ExtraHop, they can hold partners accountable to their high security standards.

Challenge

Working with over 30,000 third-party vendors to maintain their internal and external-facing systems, this telecommunications provider needed a way to monitor and manage the connections coming into their environment to ensure security, compliance, and performance quality.

Solution

With performance management and network security analytics from ExtraHop, the telecommunications provider eliminated a blind spot and gained the visibility they needed to monitor these third-party connections.

Benefits

- Discovered over 650 connected machines not yet registered in CMDB
- Avoided millions of dollars in potential PCI violation fines
- Detected and halted use of unencrypted traffic
- Gained the ability to monitor third-party connections and behavior internally and independently

The Beginning

This telecommunications provider offers voice, messaging, and data services to tens of millions of individuals and business customers across the globe. They work with well over 30,000 vendors and partners to maintain the technical and physical infrastructure required to deliver top-quality service. Many of these third parties need to connect to the corporate network of the wireless telco and tracking these connections to assure secure and appropriate use required broad visibility across the infrastructure.The company's security team used a configuration management database (CMDB) to keep track of assets in their environment, as well as configuration details and the internal owner of each asset. While the CMDB was good in theory, in practice it required cumbersome manual updating, rendering information outdated almost immediately. During a routine audit of third-party connections coming into their environment, the telco's security team learned that the CMDB had no record of several hundred systems accessed by their vendors. In order to maintain the security of systems accessed by third-party vendors, the telco's security team needed a way to keep the CMDB updated in as close to real-time as possible.

The Transformation

As the telco's security team found out, they already had such a technology in place. The telco's network team was already using ExtraHop for performance management, and the platform's ability to automatically discover both the presence of machines on the network and their configuration details in real-time, was exactly what the security team needed. Better yet, that information could be automatically populated into the CMDB, saving significant time and resources.

The Benefits

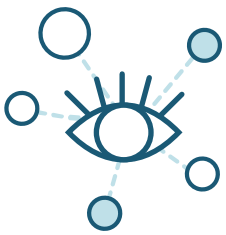
The Age of Automation

Using ExtraHop, the security team discovered over 650 machines connecting to their network that were previously unaccounted for in their CMDB system. Many of these machines had access to company data, as well as the ability to move data into and out of the main company network. Getting these machines registered in the CMDB without manually checking ARP tables and tracing cables saved a huge amount of time and resources, and provided the team with visibility into a significant and previously opaque source of risk.

Insight that Prevents Oversight

In the process of discovering unregistered machines, the security team found a third-party vendor sending unencrypted data using the Telnet protocol. This posed a security risk of which neither the internal security team nor the responsible third party was aware. While the vendor thought they were using HTTPS, ExtraHop discovered that they were transmitting personally identifiable information (PII) as cleartext using Telnet, a legacy protocol that should not have been in use anywhere in the company's IT systems.

This risked a PCI compliance violation and left the door open to a potential data breach. With ExtraHop, they were able to identify the issue and provide the relevant data to the vendor to quickly remediate the problem, before it resulted in a PCI violation that could have resulted in millions of dollars in fines.



Independent Investigations at Last

The security team knew they needed total visibility into third parties connecting to their production network, but the process of having to manually reach out to over 30,000 third parties to ask for details on their machines simply didn't scale.

With ExtraHop, the team could begin with an internal investigation that automatically exposed the connections between external services and internal resources. With that data, they were no longer reliant on the accuracy of vendor information or the manual processes required to obtain updates.