ExtraHop

Accolade Cuts Annual SIEM Spend by 60 Percent with ExtraHop

Customer Case Study: Accolade

"With ExtraHop and the SIEM we've built around it, our security guys have—at most—two windows they need to look at. One tells them what's going on, the other one tells them what has gone down and how to fix it. My goal is always to be within four clicks of any incident."

– Mike Sheward, Principal Security Architect

Challenge

For Accolade, providing top-notch service is a top priority. Indeed, it's what the company is known for. Accolade customers experience industry-leading engagement levels, satisfaction scores unseen in healthcare, better clinical outcomes and cost savings of more than 10 percent.

A major component of keeping customers happy is ensuring the security of their data.

When Mike Sheward joined Accolade in early 2016, he immediately saw an opportunity to streamline costs and improve the company's IT security posture. At the time, Accolade was using a managed security services provider (MSSP), which had deployed a commercial SIEM offering. Between the costs of the MSSP and the commercial SIEM, the company was spending approximately $200,000 a year. The team also had extremely limited visibility into the commercial SIEM solution, and depended entirely on the MSSP to monitor the security of their environment.

Solution

Working with his security team, Sheward set out to build a security solution that would better serve the needs of the business by keeping costs down and bringing control back in-house.

The result of that effort is FortifyHQ, a custom-built SIEM solution that uses wire data from ExtraHop, log data, and a third-party authentication platform to provide both real-time visibility and forensic analysis to keep Accolade and its customers ahead of emerging threat vectors. With FortifyHQ in place, Sheward and his team were able to terminate the contract with the MSSP and the commercial SIEM.

ACCOLADE®

Company Profile

Accolade is a leading provider of on-demand healthcare concierge services that help individuals and businesses navigate the often complex waters of the healthcare system, from identifying in-network providers to negotiating with insurers and healthcare providers over bills.

Challenge

As Accolade looks to broaden its technology and services offerings, the company needed a way to run lean while preserving the security of critical information and systems.

Solution

Built a custom SIEM solution leveraging wire data from ExtraHop to provide real-time, cross-tier visibility into all East-West traffic.

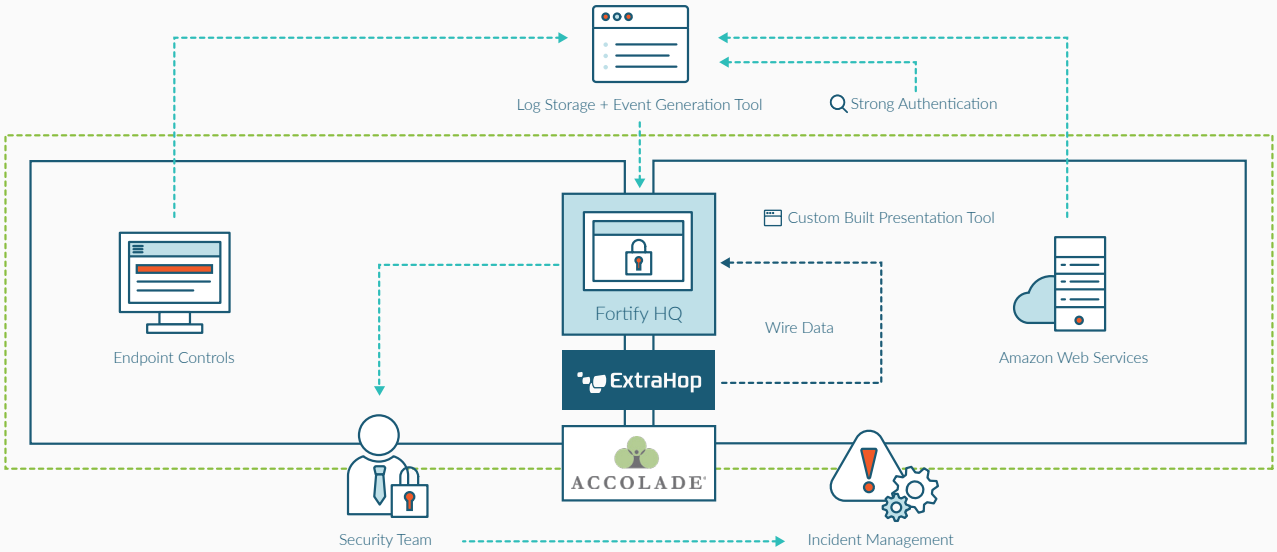
Benefits

Reduced annual IT security monitoring spend nearly 60 percent.

Gave in-house team complete oversight of IT security, allowing them to develop environment specific security knowledge.

Puts Accolade within four clicks of identifying and remediating any security incident.

Out-of-the- Box Threat Intelligence



By triggering a precise packet capture for suspicious events, and then sending that data to an open- source IDS solution using the ExtraHop Open Data Stream (ODS), Sheward and his team now have real-time intrusion alerting -- and the digital evidence needed to investigate incidents -- without requiring extensive customization.

"We can now answer questions like, 'Why are non-Accolade IPs trying to access the Admin page?' or 'Why are non-US IPs trying to login when all of our customers are in the US?'" said Sheward. "Not only does ExtraHop allow us to see and alert on that activity as it happens, we have the data we need to drill down to the source, get the answer, and protect our assets."

Benefits

Dramatically Reduced Costs

By building a custom SIEM solution using ExtraHop as the primary data source, the team at Accolade reduced annual spend on monitoring by around 60%.

Real-Time Security

Because FortifyHQ relies on wire data, not log files, as its primary data set, the team also has the ability to see, alert on, and react to security events as they happen.

"With wire data from ExtraHop, you don't have to wait for the event to happen, get written into the log file system, and then analyzed," says Sheward. "You see the traffic as it's hitting the wire, not when it's hitting the end-points. If you put an ExtraHop appliance in front of the firewall, you can even see what is hitting you versus what is actually getting through. It's incredibly powerful. We still use log files, but in a very limited way."

Four Clicks to an Answer

Before implementing ExtraHop and the FortifyHQ solution, the security team at Accolade had limited visibility into what was happening in their own environment. With the custom-built SIEM, not only do they have complete visibility across all systems and devices, they have a streamlined method for drilling down into potential anomalies.

Says Sheward: "What I really like about this is that our security guys have, at most, two windows they need to look at. One tells them what's going on, the other one tells them what has gone down and how to fix it. My goal is always to be within four clicks of any incident. The difference between wire data and log data is that wire data allows us to be highly prescriptive at the source, making it much easier to drill down quickly to get the answers you need."