proofpoint. corelight

CUSTOMER STORY

Corelight Improves Visibility to Transform Data Security With Proofpoint

Challenge

- Increase visibility into Corelight's cloud data and cloud environment risk posture
- Enhance security capabilities to protect data and cloud systems
- Empower security team to detect and effectively respond to potential security incidents

Solution

- Proofpoint Data Security Posture Management (DSPM)

Results

- Proofpoint assessments instantly identify sensitive structured and unstructured data
- Context-aware data security insights drive better security decision-making
- Proofpoint determines relevant attack paths that place data at risk

The organization

When organizations need to know about malicious activity within their networks and clouds, and also gather the remnants of that activity as evidence, they turn to Corelight. Corelight's customers include Fortune 500 companies, major government agencies and large research universities. Based in San Francisco, this open-core security company was founded by the creators of the widely used network security technology, Zeek.

The challenge

Acquiring comprehensive visibility for better security

Data security is so challenging that even sophisticated security companies like Corelight need external support for diligent, complete security strategies. Bernard Brantley, CISO of Corelight, needed to develop the company's data security strategy and vision, and strengthen its ability to execute that strategy.

Brantley's primary objective was to ensure visibility into the risk posture of Corelight's data capabilities to protect its data and cloud environment.

"Not only would this help us to reach and maintain effective security and systems, but it would also enable us to detect and effectively respond to potential anomalies when necessary," said Brantley. This visibility would also let Brantley's team accurately provide executives with the details needed to communicate the value of their security program and regulatory compliance efforts.

The organization sought a complete view of all its sensitive data and business-technology assets, as well as the access and configurations of their cloud access. Although the team could gather the data manually from their engineering, operations and application teams and scour through their access logs and security and operations dashboards, the process would be inefficient and time consuming.

The team also considered open-source tools, but those posed challenges as well. "The reality is that we don't have the size or team composition necessary to dedicate to building and maintaining the open-source solution," said Brantley. "I needed to know how we could scale into such a platform, and I didn't have an answer for that."

Cloud security posture management tools were another option, but they lacked the customization capabilities the team required. Brantley and his team sought a complete solution that could help the team identify structured and unstructured data, assets and security configurations.

The solution

Exceeding expectations for data insight

After considering their options, Brantley and Corelight chose Proofpoint Data Security Posture Management (DSPM). DSPM offers a data-first approach to security that provides comprehensive visibility and control over sensitive data across an organization's entire digital ecosystem. It lets organizations maintain continuous awareness of their data assets and protection status.

"The business and engineering teams weren't convinced that we could deliver comprehensive insights regarding our data and the entire structure of our cloud systems, all correlated to risks those systems face. But we did it, and there's a big 'wow factor' because these capabilities didn't exist before."

BERNARD BRANTLEY,
CISO, CORELIGHT

To begin their use of Proofpoint, Brantley started by assessing the critical cloud infrastructure that supports the services Corelight provides. Proofpoint provided much more insight quickly than expected. The initial use case was such a success that Brantley will soon deploy Proofpoint DSPM across its entire Amazon cloud infrastructure.

One of Brantley's most significant benefits from Proofpoint is the knowledge graph that powers the platform. Based on the findings from the Proofpoint one-pass scanner, it connects all enterprise data with its associated assets, identities and their access to that data, as well as misconfigurations and vulnerabilities that place that data at risk.

With the Proofpoint graph, organizations such as Corelight and their security teams can continuously discover sensitive information, determine relevant attack paths and automate the necessary remediation efforts to secure their data. In addition to finding structured and unstructured data, organizations can also use predefined compliance profiles within DSPM to detect personally identifiable information (PII), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and more to ensure sensitive data never leaves their cloud environments.

The solution is equally valuable to the CISO as it is to the security engineer, analyst, DevOps professionals and more as a way to discover data, classify its risk and attack paths, and remediate risks. The Proofpoint data-first cloud security platform operates in three essential phases:

- Proofpoint builds an intelligent graph with deep context and transitive trust relationships that represent all the data stores, applications, identities and infrastructure resources in all clouds and understands how they connect. The Proofpoint agentless data scanner then determines what data-stores house sensitive information and automatically maps it to specific security policy and regulatory compliance profiles.
- The Proofpoint prioritization engine identifies risk paths discovered through the graph and prioritizes them based on the sensitivity of the data at risk and the attack's impact.
- Proofpoint integrates with various external tools for notification, ticket creation, workflow triggering and more, so that users can automate remediation through their orchestration engine.

The results

Proactively understanding and mitigating data risks

Following the deployment of Proofpoint DSPM, Brantley quickly identified the locations of Corelight's sensitive data, and he could even spot data in areas they did not anticipate it existed. "We were able to review with the data owners the nature of the data that was making it to certain cloud storage locations," said Brantley. "The data being there turned out to be a surprise to the team."

"The identification of sensitive data in places we did not know it was before is a testament to Proofpoint's capabilities," he added. "Now when asked how teams are storing data and what controls they have for deleting or removing that data, we can see if they are following policy, and we will know if sensitive data shows up somewhere it shouldn't. And we can then go work with the team immediately to remediate that."

Furthermore, with Proofpoint's timed data assessments, Brantley and the team will know whenever a weakness surfaces that could lead to a data breach and automatically dispatch a service ticket to ensure that situations that place data at risk are fixed swiftly.

Perhaps most important to Brantley is how the Proofpoint graph capabilities provide him with the comprehensive insights he needs into where sensitive data resides and how well it's protected throughout their cloud environments.

"It's one of those tools that enables me to focus on defending and protecting data and systems rather than respond, which is much better from a risk perspective. The more efficiently I'm running my program, the more we stay ahead of potential issues in our interaction throughout the business," he said.

"There are two extremely important things that Proofpoint solves," explained Brantley. "The first is: Do I know where everything resides and how the systems are configured? Second: Do I clearly understand the risk facing that data and systems? Proofpoint presents me with these views."

In the near future, Corelight will increase its use of Proofpoint. "I'm going to ensure everybody who owns a cloud account or manages resources within a cloud account has the knowledge that Proofpoint exists and fully understands its value," he said.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →

0607-002-01-01 3/25