proofpoint.

CUSTOMER STORY

Defense Contractor Hones Monitoring on Insider Threats With Proofpoint

The Challenge

- Avoid exfiltration of sensitive intellectual property and data, including by nation-state actors infiltrating their ranks
- Enrich alerts from other security tools to build context and speed investigations
- Improve security speed and performance without sacrificing context
- Meet requirements of a highly regulated industry

The Solution

- Proofpoint Insider Threat Management

The Results

- Gained visibility into risky events to assemble a more complete picture
- Mitigated insider threats before they spread and put the organization at risk
- Provided security team ability to explain what happened during an incident
- Facilitated faster investigations with rapid contextualization

The Organization

This U.S.-based company is a defense and aerospace contractor, as well as providing information technology services to a variety of fields. It develops a range of services, software and products, including avionics and electronic systems, for government, defense and commercial usage. It also specializes in technology and various types of weaponry. With a broad portfolio of offerings and massive customer base, this company is one of the largest defense contractors in the world.

The Challenge

Due to its industry and customer base, this company handles a massive amount of sensitive data and information in the course of business. Its primary concern was avoiding exfiltration of sensitive intellectual property and data, including by nation-state actors. They found USB drives and other removable media in particular to be a common exfiltration channel. They also needed a way to enrich alerts from other tools to build context and speed up investigations in the event of an insider threat incident.

Previously, the team had used a traditional data loss prevent solution to attempt to monitor and respond to data loss scenarios. While the security analysts liked the granular detail provided by the tool, it was difficult to set up and maintain, and the IT team and CISO were frustrated with the product.

"Our team felt they were sacrificing performance and user frustration for data collection, and the balance between those concerns was tenuous at best," said the cybersecurity architect.

The Solution

At the outset, the team decided to test out ObserveIT (now Proofpoint Insider Threat Management) in their environment to determine how it stood up to their current tooling. Quickly, they found that it could be used for nearly twice as many relevant use cases as their legacy toolset.

After a six-week pilot, the company brought Insider Threat Management on board to augment their insider threat program with increased visibility and context into security events. "This solution has now been an integral part of our insider threat program for several years," said the cybersecurity architect.

With Insider Threat Management as part of the company's security arsenal, it now has user visibility into risky events in one place. Previously this data was dispersed across disparate tools, and it was difficult to reconcile the information to build a complete picture.

> "Insider threat investigations that used to take days now take 15-20 minutes on average. I receive good, solid alerts. The information is relevant and doesn't waste my time with searching."
>
> Senior vice president of information technology, Defense Contractor

At enterprise scale of over 30,000 endpoints, a single source of truth on user-driven events is an absolute requirement to mitigate insider threats before they spread and put the organization at risk. The easy-to-understand timeline of user activity, applications, endpoints, files and data associated with a security event in Insider Threat Management enables the security team to quickly demonstrate to stakeholders what happened, why it happened, and why it is concerning. The cybersecurity architect describes the Proofpoint solution as a "storyboard" that helps the company easily convey out-of-policy activity to legal, HR, and even authorities in extreme cases.

The Results

Rapid contextualization

Previously, when the team's endpoint detection and response (EDR) tool fired an alert, a security analyst had to dig in and study multiple processes. It often took 30 minutes to two hours for them to understand what had happened. With Proofpoint, this takes minutes.

Using Insider Threat Management, the team can search for user activity on the endpoint or using the process name in the EDR alert. The powerful Insider Threat Management search capability highlights users and any risky behavior on the endpoint, on applications and in files they've interacted with. Security teams can see the context of what the user did on that endpoint or application before and after the EDR alert fired.

All this is served in an easy-to-read timeline of events, so the security team knows the context in minutes without log analysis. Insider Threat Management serves as a diagnostic tool that enables the team to deep-dive into what happened before, during and after an alert was triggered. This gives them the rich context they need to determine how to respond.

Faster investigations

One of the key metrics that the team tracks is time to close an investigation; in other words, from the moment it becomes clear an investigation is needed to the moment it is officially closed.

Many cybersecurity teams focus on "mean time to detect" or "mean time to response." Both of these are useful metrics. However, resolution of insider threats in a timely fashion is very important and goes beyond a technical blog or mitigation. Hence the company's decision to prioritize the "time to close investigations" metric, an indication of a very mature security program.

The defense contractor has been able to dramatically decrease this metric using the increased visibility and context achievable through the Insider Threat Management platform. "We have found that the quality of security 'leads' and fidelity of alerts in general is much higher because the solution enables the team to avoid most false positives and to quickly get to the root of whether user activity was negligent or malicious in nature," said the cybersecurity architect. "It is indispensable to our efforts."

LEARN MORE

For more information, visit **proofpoint.com**.