proofpoint.

CUSTOMER STORY

Global Chemical Company Uses Proofpoint to Gain Visibility Into Insider Threats

The Challenge

- Prevent the improper use of the company's technology systems
- Gain visibility into user activity to know when insider threat incidents take place
- Increase security while respecting employee privacy

The Solution

- Proofpoint Insider Threat Management

The Results

- Enabled more efficient and proactive incident investigations
- Removed guesswork around what happened during a potential insider threat incident
- Provided complete context around both accidental and malicious insider threats

The Company

This global specialty chemical company is part of the American Fortune 100 and employs over 14,000 people. A very established player in its industry, this company serves various fields, including transportation, construction, consumer products, healthcare and more. With more than 50 locations around the world, this company earns billions every year.

The Challenge

The chemical company sought to prevent the intentional, accidental and otherwise improper use of their technology systems. When an insider threat occurred, the company would typically conduct forensics on insider threat incidents after the fact.

However, the company recognized the importance of building a comprehensive insider threat program to prevent fraud and misuse of its systems. The security team wanted to take a more proactive approach to detecting, investigating and responding to incidents—while respecting the privacy of their employees.

"If we can conclude efficiently that a concern is not substantiated, we can exonerate people," said an IT security architect from the company. "If, on the other hand, wrongdoing has taken place, we can take action with full context and proof of what happened."

The main goal of implementing an insider threat program was to gain visibility into user activity, allowing the company to know when real insider threat incidents took place, investigate them, and take appropriate action.

"We started out with some major visibility problems around insider threats. With Proofpoint, we have dramatically improved visibility into user activity on our systems."

IT security architect, global chemical company

The Solution

Recognizing that insider threat security is a team sport, the company's IT security partnered with global business conduct groups to find a solution. Many of the legacy tools they researched and tested were not up to the task and required far too much hands-on work and fine tuning.

The company chose Proofpoint Insider Threat Management, which provides deep visibility into user behavior without infringing upon user privacy. The platform enables detailed investigations into potential insider threat incidents—including fraud and misuse—with the full context needed to understand what really happened before, during and after an incident.

The Results

With Proofpoint, the team was able to dramatically improve visibility, increase efficiency of investigations, and exonerate innocent employees, all while preserving user privacy.

The company is now able to conduct investigations quickly and effectively, as compared to time-consuming forensic review based on the use of difficult to parse logs. With Proofpoint, there's no more guesswork as to what happened during a potential insider threat incident; it is immediately clear upon investigation.

The company is also able to be more proactive about insider threat investigations, no longer relying only on reactive forensics. They have also increased awareness around specific threat vectors, such as USB device usage and exfiltration to cloud services. In fact, USB misuse has become a vital area of focus for this company when it comes to identifying and stopping data exfiltration by insiders.

They're also able to maintain employees' and other users' privacy—one of the company's key considerations when developing an insider threat program. With better ability to pinpoint threats, the company can provide education and training to employees who do something out of policy because they do not understand the repercussions. And not punish them for accidents that are usually the result of trying to do their jobs well. At the same time, the team has enough context to prosecute real, intentional threats and conduct thorough investigations with full proof around what happened before, during and after an incident.

"We started out with some major visibility problems around insider threats," said an IT security architect from this global chemical company. "With Proofpoint, we have dramatically improved visibility into user activity on our systems."

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0612-004-01-01 11/21