Forcepoint

Customer Story

Italian Equipment Manufacturer Guards Against Insider Threats with Forcepoint

The metal manufacturing equipment maker is countering the rising threat of internal data loss with Forcepoint DLP and Insider Threat.

A global leader in building factories and equipment for the biggest manufacturers of metal products must safeguard not only its own sensitive data but the intellectual property of its customers as well. With its digital transformation and move to the cloud in full swing, the company first partnered with Forcepoint to protect against external threats. Now the company is focusing on countering potential data loss caused by insiders, teaming up with Forcepoint for an integrated, centralized solution.

CUSTOMER PROFILE:
One of the world's top 3 suppliers of equipment and physical plants to the metal industry.

INDUSTRY:
Manufacturing

HQ COUNTRY:
Italy

PRODUCTS:
- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint DLP
- Forcepoint Insider Threat

The old ways of stealing valuable data and damaging organizations—hacking into networks and computer systems, malware infections, and other ways of breaking down defenses from the outside—are becoming less successful against companies which invest in sophisticated tools to stop such external threats. But that doesn't mean the bad guys have stopped trying. In fact, there is growing recognition that exfiltration of data by an employee or compromised system from within an organization can do at least as much damage as infiltrations by external actors.

This Italian manufacturer is one of the three largest global suppliers of industrial plants and equipment for the metal industry, with a list of customers that includes the world's leading steelmakers. The company's IT security team is well aware that rogue insiders, negligent end users, and hijacked systems could compromise the valuable trade secrets and intellectual property (IP) belonging to the company and its global customers.

The manufacturer produces a host of products for metal manufacturers, ranging from customized tools and equipment to entire manufacturing plants complete with automation and process control capabilities. The company's 11,000 employees work with and share valuable, sensitive data that includes confidential internal and customer documents stored in digital, analog, and unstructured formats. This includes IP like technical drawings in 2D and 3D CAD formats that may be stored and shared via internal networks, USB devices, CD/DVDs, and printed hard copies, as well as in the cloud.

The Italy-based manufacturing giant maintains 25 design, manufacturing, and service centers around the world, including its seven primary production facilities in Italy, Austria, China, Germany, India, Russia, and Thailand. The company wanted to better detect and prevent data loss and insider threats at all of those locations.

It also needed to be able to manage its data loss prevention (DLP) solution from a central console and sought to train its employees about security best practices to make them additional assets in the effort to protect data.

Creating a unified security framework

The company has relied on Forcepoint Web Security and Email Security for more than a decade, growing its number of licenses from 400 to 4,000 over the past ten years. As the company began addressing the threat of data loss by exfiltration, its IT security team decided it would be best to integrate additional data protection solutions with the existing security framework.

"IT security must be deployed as a unified perimeter where each department is aligned at the same level of defense, in order to maintain consistent, viable protection. If security is conducted differently throughout the different departments, there is a danger that the least protected department becomes a target and possibly a victim of an attack," said the company's IT Security Manager.

The company's rollout of Forcepoint DLP and Forcepoint Insider Threat (FIT) was done in coordination with the year-long rollout of Office 365. The company is also transitioning to the cloud for some of its file-sharing, collaboration, and other key IT operations. As a part of the cloud transition, the company has deployed the hybrid versions of Forcepoint Web Security and Forcepoint Email, which give the IT team the ability to combine on-premises and hybrid (cloud or security-as-a-service) policy enforcement.

Challenges

Safeguard data against rising risk of internal threats.

Build a centrally managed, platform-based security solution.

Train employees to become security assets.

Approach

Deploy Forcepoint DLP and Insider Threat on a unified platform also including Forcepoint Web Security and Email Security.

The newly integrated Forcepoint security platform with Forcepoint DLP and FIT was designed to protect against internal and external threats, in the cloud and across older file-sharing and storage formats and technologies. The company also enabled the Phishing Education feature in Forcepoint Email Security to give feedback to employees as they use email, helping them to better learn and understand safe email best practices.

Catching and fixing data leaks faster with DLP and FIT

The company checked off all of its main goals in implementing its new data protection solution. By integrating Forcepoint DLP and FIT on its existing Forcepoint security platform, the IT team is able to manage all aspects of cybersecurity from one centralized and unified console. Forcepoint DLP and FIT are now part of a total solution which easily extends the same level of security across all geographic locations around the globe.

Forcepoint Web Security and Email Security continue to safeguard against external, advanced threats, while performing other key tasks like blocking non-business-related websites to reduce risk and promote productivity. Forcepoint DLP and FIT provide protection against data exfiltration, including user and system risk scoring, as well as FIT's forensics capabilities for determining how data leaks happen and more quickly fixing vulnerabilities.

The company is able to easily adjust its data security polices to comply with regulations in different geographies, thanks to Forcepoint DLP's extensive library of regulatory policies. Forcepoint FIT helps comply with privacy regulations, providing granular control over when to collect data and what to specifically gather to protect users' privacy. Fully integrated with Forcepoint DLP, FIT helps the IT team make smarter, faster remediation decisions after detecting risky user or system behavior that could lead to data exfiltration.

The company has also found a way to use its Forcepoint tools to train employees about security best practices. The IT security team now uses FIT-identified examples of user data-handling mistakes to teach all employees how to better avoid such mistakes in the future.

"Thanks to DLP and FIT, we have significantly increased the degree of awareness and attention across the whole company to the possibility of data loss by exfiltration," the manager said. "We can more easily and more quickly discover mistakes by employees that can lead to data loss. This has allowed us to highlight these accidents as examples and use them to educate employees to be better about security."

Results

Centralized control over a unified, integrated security framework protecting against external and internal threats.

More rapid response to internal threats reduces risk of data loss.

Employees now trained in best practices for data protection.