

# Industrial Engineering Leader Aims to Protect Data

## People-centric Security Helps Control Risk of Data Loss



### THE CHALLENGE

- Protect data and intellectual property against attacks
- Master access management and information sharing in different environments, including Microsoft Office 365
- Support employees with best practices and security solutions

### THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Internal Mail Defense (IMD)
- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Security Awareness Training (PSAT)

### THE RESULTS

- Protected against 95% of phishing attacks and malware infections in Office 365 in one year
- Enhanced visibility into account compromise risks through alerts and analysis dashboards
- Reduced time spent searching for, understanding, and neutralising active threats
- Controlled costs

### The Company

Fives is an industrial engineering group, headquartered in Paris, France. It designs and manufactures machines, process equipment and production lines for the world's largest industrial players including steel, aeronautics, aluminium, automotive, cement, energy, logistics, glass and more.

In 2019, Fives achieved a turnover of 1.99 billion euros. And it employed nearly 8,400 people across 80 companies in some 30 countries.

### The Challenge

Supporting global industry leaders at every stage of their production cycle requires solutions to prevent identity theft and data loss to protect industrial and intellectual property. As massive ransomware attacks began to hit the world, Fives realised it needed to strengthen the security of its Office 365 messaging system. It also needed to support its employees with security best practices.

Attackers use social engineering techniques to get employees to open a fraudulent attachment or click on a malicious link. And there's a constant evolution of threats in work environments, which includes an increase in malicious URLs. This has accelerated the organisation's commitment to implement a truly people-centric defense strategy.

"The legacy solution we were using to protect our messaging was not working to our satisfaction. Following several peer recommendations, we decided to conduct a proof of concept with Proofpoint to compare the performance of the two solutions," explains Kélig Dugué, director of cybersecurity at Fives.

## The Solution

### Increased visibility

The proof of concept for Proofpoint Cloud App Security Broker (CASB) was decisive. “We quickly realised the full potential of this solution. Its ability to give us visibility into users and data, generate alerts and navigate in analytics dashboards, convinced us. We were particularly fond of its user interface,” explains Kélig Dugué.

“The scale of the 2017 WannaCry and NotPetya ransomware attacks led to a real awareness of cyber risks. Protecting email became a priority for us.”

**Kélig Dugué**, director of cybersecurity, Fives

### Tailor-made project management

The project gained momentum and took on a new dimension when Fives decided to federate the company’s intranet with Office 365. The transition from an application-based intranet to a collaborative solution, a Digital Workplace, had to be done without compromising security. In fact, it had to improve security while simplifying the user experience by reducing the number of required passwords.

A new proof of concept was then launched with Proofpoint CASB and Ilex Sign&Go. This was to ensure that the authentication environment had the right configuration.

Proofpoint was the leader on this project and highlighted its flexibility, responsiveness and ability to quickly deploy its solution in complex environments. It took less than five months to complete the Fives Digital Workplace federation project.

### A stronger last line of defense

In addition to its infrastructure protection, it’s a key mission of the Fives security team to support employees in implementing good security practices.

Fives recognised that a security-conscious employee can be the last line of defense against an attack. The company deployed Proofpoint Security Awareness Training (PSAT), which simulates phishing attacks and encourages its users to play a key role in identifying and blocking these attacks. Employees can simply click on a button to report suspicious messages. With these comprehensive features, Fives puts people at the heart of its security strategy. This helps to reduce the exposure to threats and effectively protects against attacks.

## The Results

With Proofpoint, the entire risk management process is optimised. There’s faster identification of potential account compromises, enabling instant, accurate reporting to the monitoring team. They can then make informed decisions quickly, such as changing a password, revoking OAuth tokens and more. And now it only takes a few minutes from detection to neutralisation of active threats.

## LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations’ 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 organisations 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](https://www.proofpoint.com).

©Proofpoint, Inc. Proofpoint is a trade mark of Proofpoint, Inc. in the United States and other countries. All other trade marks contained herein are property of their respective owners.