

Bilfinger Protects Supply Chain Email Communications with Proofpoint Email Fraud Defense

Restores confidence in email and prevents brand misuse through authentication



BILFINGER

THE CHALLENGE

- Prevent fraudulent emails that misused Bilfinger's legitimate domains
- Restore trust in the supply chain, as it was not certain that an email obviously coming from Bilfinger was really genuine
- Eliminate CEO fraud

THE SOLUTION

- Proofpoint Email Fraud Defense
- Proofpoint Managed Services

THE RESULTS

- Gained transparency across all legitimate email flows
- Prevented domain spoofing in email traffic
- Protected the brand in email communications and secure trust in the supply chain

The Company

Bilfinger is a leading international industrial services provider. The company increases the efficiency of industrial plants, ensuring high availability and reducing maintenance costs. Its portfolio covers the entire value chain: from consulting, engineering, production, assembly, maintenance, plant expansion and general overhaul to environmental technologies and digital applications. The company provides its services from two business units: Engineering and Maintenance and Technologies. And its customers in the process industry come from the chemical and petrochemical, energy and utilities, oil and gas, pharmaceutical and biopharmaceutical, metallurgical and cement sectors, among others. Bilfinger upholds the highest standards for safety and quality, and has about 34,000 employees. It generated €4.327 billion (\$5.17 billion) in sales in 2019, and does most of its business in Europe, North America and the Middle East.

The Challenge

Cyber criminals use fraudulent emails to target people, not infrastructure. One method of doing this is identity theft, where the company's real domain is used for phishing attacks—often within the company itself or within the supply chain. Known as business email compromise (BEC), this type of attack is not only costly but it also leads to loss of confidence in email communication.

Bilfinger was faced with this challenge. Integrated into complex and multilevel value chains, Bilfinger set itself the goal of ensuring that every email that was apparently sent by Bilfinger actually came from the company. And this was particularly true when it came to emails from the leadership team.

With other Proofpoint solutions already successfully deployed, the company decided to test Proofpoint Email Fraud Defense. Proofpoint quickly found evidence that the Bilfinger name had indeed been used to attempt to spread malware via email. "The trust of all parties in our supply chain in our email communication must not be put at risk," explains Mr. Lauterbach, CIO, Bilfinger and Bilfinger Global IT GmbH. "So the decision to go ahead with this project with Proofpoint was a logical solution for us."

The Solution

With Email Fraud Defense, companies are able to stop BEC attacks that abuse their domains at their source. It authenticates all incoming and outgoing emails at the company. And it protects employees, customers and business partners from attacks with a fake identity. This restores trust in emails.

“Ultimately, it was the outstanding expertise of the Proofpoint team that made the project possible.”

Andreas Pfau, head of CIO office, Bilfinger Global IT GmbH

This is made possible by the open DMARC standard. Achieving a DMARC reject policy can often be a costly and lengthy process, since the inadvertent blocking of legitimate emails needs to be eliminated before the reject policy is actually established.

Email Fraud Defense is also available as a managed service. This involves Proofpoint working with the customer to address this process. Bilfinger chose this approach and was assigned a dedicated consultant who quickly identified all email senders that are legitimately allowed to send email on behalf of the Bilfinger domain. This included external services such as email dispatch service providers who send legitimate emails on behalf of Bilfinger.

With Email Fraud Defense, the Bilfinger security team gained valuable insights that accelerated the authentication process and ensured that legitimate emails were not blocked.

The Results

The implementation of such a project may seem simple in theory. But in practice it's highly complex. At Bilfinger, various divisions had started to commission their own email service providers to send email advertising and newsletters. “On the IT side, there was no longer any transparency as to who was sending legitimate emails with the Bilfinger domains. And without this knowledge, no rejection policy for DMARC can be achieved. Many, many legitimate emails would also be blocked with the corresponding negative consequences for the business,” explains Mr. Graser, infrastructure specialist at Bilfinger Global IT GmbH. “Proofpoint has provided us with exactly this transparency.”

As a B2B company, it was particularly important for Bilfinger that Proofpoint was also able to provide fully GDPR-compliant transparency on B2B email flows. “This is a criterion that all companies working with other companies should look for when selecting a provider. Having transparency over this data can make all the difference to the success of such a project,” Mr. Graser continues.

“Ultimately, it was the outstanding expertise of the Proofpoint team that made the project possible,” concludes Mr. Pfau, head of CIO office, Bilfinger Global IT GmbH. “Not only did our consultant understand the technology, he also dug deep into our organisation to capture all legitimate email flows. He then worked with our third-party vendors to achieve the correct configuration and email authentication.” Armed with the insights the team gained through Proofpoint, Bilfinger can now consolidate external service providers in the email delivery arena—and save time and money.

“Now if one of our business partners receives a Bilfinger email from our CEO, he can be sure that it really comes from our CEO,” explains Mr. Lauterbach, addressing the success of the project. “This ensures good and close cooperation in the supply chain and improves trust in our business relationships.”

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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.

©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.