SPB Relies on Forcepoint to Block Illegitimate Email Traffic to its 1,800 Employees

Spam, ransomware, sandboxing URL, phishing: the European leader in insurance and affinity services reduces unwanted emails by more than 20% thanks to Forcepoint's cloud-based solutions.

Malicious emails, including spam and phishing attempts, represent a significant threat to businesses in terms of both cyber risk and in lost efficiency of employees dealing with the influx. Insurance broker-manager SPB Group decided to tackle this threat and empower its employees with a centralized, easy-to-manage, cloud-based email security platform from long-time cybersecurity partner, Forcepoint.

CUSTOMER PROFILE:
SPB is the European leader in insurance and affinity services.

INDUSTRY:
Financial Services

HQ COUNTRY:
France

PRODUCT(S):

- Forcepoint NGFW
- Forcepoint Web Security
- Forcepoint Email Security Cloud
- Forcepoint Advanced Malware Detection (AMD)

Fraudulent emails are the first vector of attack against companies, thus embodying a real threat for companies that are the target of data theft or scam attempts. The latest example is the "Varenyky" malware that spreads through emails with deceptive labels—"billing," for example—containing an archived attachment. Once installed, the malware can save the screen of the victim, steal passwords, or send phishing spam from the infected system. In 2018, a study by Altospam1 showed that one in a hundred emails was malicious; in the first half of 2019 spam and phishing emails accounted for 65% of total email traffic. Avoiding these attacks, the consequences of which can be disastrous, has become a major issue for businesses, including SPB.

Protect employees from fraudulent emails

SPB is a leading European broker-manager in insurance and affinity services with a presence in 17 countries and 50 million policyholders in Europe. SPB is distinguished by its ability to combine assistance with the design and management of insurance programs, warranty extensions, and services associated with mobile telephony, nomadic, banking and provident products, business events and life, travel, leisure, household goods, mobility, energy, or health. An independent family business founded in 1965, SPB has a gross turnover of € 290 million and employs 1,800 people.

In order to address the challenges of email attacks, SPB wanted to strengthen its approach to securing the messages of its 1,800 employees. IT managers also desired a solution that was easy to use and allowed for centralized management for the group that operates across Europe.

A long-time Forcepoint customer, SPB chose Forcepoint's proposal for Email Security Cloud and Advanced Malware Detection due to the centralized management console, the effectiveness of its deployment, its operational maintenance and its innovative security approach. With its easy-to-integrate and use platform, Forcepoint allows end-users to become autonomous when it comes to unlocking emails, a major advantage of the solution.

Zero-day threat protection, effective immediately

The relationship of trust between SPB and Forcepoint goes back almost 10 years. The Forcepoint NGFW solution was implemented in 2011 to ensure the security of corporate networks and the detection of intrusion attempts. In 2014, SPB deployed the Web Security solution for URL filtering to extend web security to mobile workers. The Forcepoint Email Security solution implemented in 2017 has enabled the migration of part of the infrastructure to the cloud and constitutes a third layer of security. It was first implemented in France before being rolled out to all 17 of the group's subsidiaries in Europe and the Maghreb.

The Forcepoint Email Security solution controls incoming and outgoing email traffic and detects the most advanced threats. It enables real-time protection using a unique blend of discovery technologies, including machine learning, sandboxing, and predictive analytics to effectively stop complex threats such as ransomware.

With Forcepoint Email Security, SPB can encrypt sensitive email conversations and improve mobile security by controlling access to attachments on each device. "With its integrated features, Forcepoint offers the most comprehensive inbound and outbound defense solution on the market right from the moment it is acquired. This allowed us to limit the complexity of deployment while reducing costs," said Johann Kuster, Head of Operations at SPB.

On the technical side, zero-day threat protection is provided by advanced malware detection (sandboxing) through a complete sandbox emulation system. In-depth content inspection uncovers unknown threats and minimizes false positives. By ranking incident risks, activities are correlated across multiple events to identify true cumulative trends in risks and activities. In addition, the solution systematically assigns a risk score to help SPB's security teams identify the most important risks based on real-time activity and thereby save time by focusing on real threats.

Challenges

Have a centralized and easy-to-use email security solution.

Approach

Detect threats through predictive analytics and provide better service to employees by empowering end-users.

Forcepoint Email Security's Phishing Education feature helps SPB employees adopt best practices while identifying those who need additional training to improve their security practices. Nearly a year after the implementation of the solution, SPB has chosen to allow end users to get their hands on blacklists. Employees can now access blocked emails without having to query the IT department, giving them greater autonomy. This initiative is fully in line with the desire to improve the user experience in order to provide a better service to employees. At the same time, this choice reflects Forcepoint's vision of enhancing security while giving the user greater confidence.

Finally, the flexibility of deployment allows SPB to choose from a range of physical and virtual devices to use the full potential of existing hardware, cloud deployment or hybrid environments.

> "Forcepoint's technical team support was very responsive during the POC and greatly helped us configure the solution."

JOHANN KUSTER, HEAD OF OPERATIONS, SPB

Technical support determines decision

Before choosing the Forcepoint Email Security solution, SPB completed a Proof of Concept (POC): "Forcepoint's technical team support was very responsive during the POC and greatly helped us configure the solution," explained Johann Kuster. "The role of Forcepoint support was all the more critical as the deployment of the solution allowed the migration of part of our infrastructure to the cloud."

"In addition to technological aspects, we highly appreciated the financial benefits of Forcepoint solutions. The results are there: in July 2019, out of a total of 524,466 emails on all of the group's email domains, 108,007 were detected as spam (spam, virus, sandboxing URL)," he said. "The Forcepoint tool was used to block a little over 20% of illegitimate email traffic, including ransomware, upstream of the infrastructure. We are more than happy."

20%

reduction of unwanted emails during July 2019

Results

SPB now has tremendous efficacy against phishing and modern attacks, with all the benefits of the cloud.

20% reduction of unwanted emails during July 2019.

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.