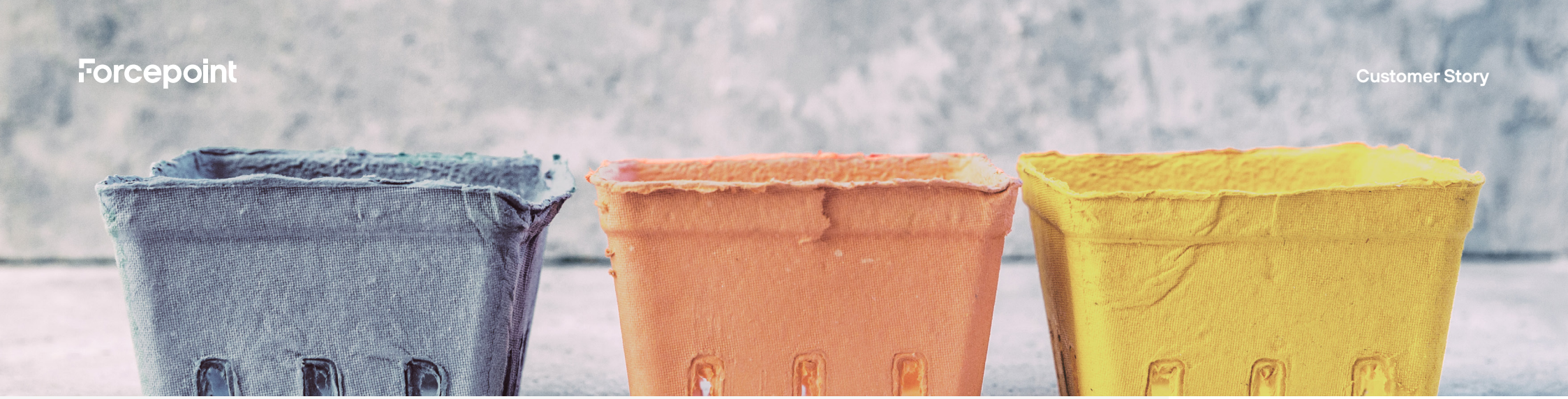

Global Packaging Company Increases Safety And Productivity on its Way to the Cloud

Forcepoint Web and Email Security gave this innovative packaging company an enterprise-wide security solution that perfectly fit their needs and strategy for moving to the cloud.

One of the world's leading providers of paper-based packaging knows how important it is to keep innovating in all aspects of their business. Its global brand is focused on delivering customer growth through smart insights. The company partnered with Forcepoint to make sure that its future is as safe as it is open as well as support its continued business growth and digital transformation.

CUSTOMER PROFILE:
Leading European packaging enterprise with 45,000 employees across 33 countries and billions in revenue.

INDUSTRY:
Manufacturing

HQ COUNTRY:
Netherlands

PRODUCTS:
› Forcepoint Web Security
› Forcepoint Email Security

This innovative packaging company believes that addressing the entire packaging lifecycle can make a difference—from the production line through to consumers. It partners with customers to develop new approaches that take packaging to the next level. For example, when a chemical company in Argentina needed to phase out usage of plastic cartons for chemicals in order to improve its sustainability credentials and reduce lengthy logistics processes, the company imported an idea from the French wine industry that is 100% recyclable and delivered a 30% reduction in packaging costs.

It's the kind of innovation and optimization the company expects across all its operations. So, when faced with underperforming and unwieldy web and email security solutions, the Infrastructure Operations Manager and his team found a solution that could not only address their challenges at the time of deployment but would also be flexible enough to support them into the future as they address challenges of moving to the cloud.

Consolidated management of web and email security across four continents

The company's size and high profile create a tempting target for attackers. In fact, C-level executives regularly received spoofing emails that asked them to execute "urgent" business wire transfers. If even 1% of these attempts proved effective, the company stood to lose millions of euros.

The infrastructure team is responsible for information security management and prevention of spam and malware at all of the group's 380 organizations. This includes managing 56 email domains and 532 DNS servers, preventing spam, malware, and data theft or loss incidents while also administering servers and domains in data centers in Europe. This created a significant management burden for the company's IT Infrastructure division.

Adding to that burden, the company's previous web and email security products were generating an average of 350 incidents each week, including false positives, that required staff time to investigate. With the overall workload, this created far too much need for maintenance and continuous monitoring. The manager realized that his organization needed a new solution that could reduce the number of necessary investigations through better efficacy, thereby generating fewer false positives. In addition, centralized management and reporting capabilities would make investigations more efficient and reduce staffing needs.

"We wanted one solution for proxy, content categorization, and virus scanning," he explained. And it needed to be flexible and easy to manage—a tall order for a security solution for such a large and distributed organization.

Finding flexibility, performance, and productivity in a single package

The company started with a Forcepoint Web and Email Security proof of concept and found a solution that answered all their needs. "The pilot was so successful that we decided to opt for the full solution," said the manager. The highly customizable solution allows continuous tuning to specific business needs, including secure and open collaboration among global employees and support for digital transformation.

Forcepoint delivered flexibility through deployment options. The company chose a cloud deployment for email to stop threats sooner. Web Security recently transitioned from a hybrid deployment to cloud-only to support their continued shift away from on-premises appliances.

"The kind of flexibility that we got from Forcepoint was not offered by our previous products," the manager said. "We can hold many threats outside of the door at our data centers, before they even have a chance to enter."

Because the team is also responsible for data protection and compliance, Forcepoint's integrated DLP, which protects against data infiltration, exfiltration, and people-based vulnerabilities, helps further reduce risk. They're now better able to comply with relevant data regulations like GDPR.

Challenges

Underperforming and inflexible web and email security products.

Investigation and maintenance burden on IT staff.

Compliance with relevant data security regulations.

Secure transition to the cloud, including Office 365.

Approach

Implement a highly tunable Forcepoint Web and Email Security solution.

Flexible deployment for digital transformation support.

Dedicated technical account manager.

Immediately after deployment, the company saw the benefits of its decision. First of all, ease of management has been a boon to optimizing IT staff time. The globally applied solutions can be simply managed from a single console, and built-in incident risk ranking facilitates prioritization and reduces false positives to improve response time.

It didn't take long to notice an increase in efficacy. The new solution identified and quarantined an exceptionally high number of emails containing unsafe or unauthorized content that the previous products had missed. "With Forcepoint we fulfilled our need for email protection so that our end users can work safely in a highly secure email environment," the manager said.

He continued, "Forcepoint has increased both productivity and safety. The fact is we are now optimally protected against phishing attempts and hackers because of Forcepoint."

Calibrated to adjust to brand-new attacks for disruption-free environments

Over the last several years, the company has come to rely on Forcepoint as a trusted security partner. "We work well with their security team because of consistent, open, two-way communication," Michel Le Belle, a Forcepoint account manager, explained. The company's team recently noticed email attacks that have become more sophisticated. When something slips through, they provide detailed information to their dedicated Forcepoint technical account manager.

10yr

trusted partnership

01

single console provides global management

> **"We're able to adjust quickly to these brand-new attacks in just two to three days with our adaptable email security."**
>
> **MICHEL LE BELLE,** ACCOUNT MANAGER, FORCEPOINT

"We're able to adjust quickly to these brand-new attacks in just two to three days with our adaptable email security," explained Le Belle.

The company also relied on Forcepoint when continuing its transition into cloud computing. The team sees moving servers to the cloud as a must for ROI and key to their roadmap for the next five years. Part of this plan includes the recent migration to Office 365 to better support global collaboration and communication. Though Office 365 has some built-in security measures, the company retained Forcepoint Email Security to add a critical protection layer against inbound threats and outbound data loss.

Happy with Forcepoint's partnership and the quick technical response that cultivates a safe working environment, the company is considering the next step in their security journey.

"We conduct quarterly business reviews with Forcepoint's senior-level team," said Le Belle. "We also make it a point to meet regularly with their C-level executives to talk about their security vision for the future and how we can help them build a roadmap for how to get there."

"Whatever new challenges appear on the horizon, Forcepoint will be there," said Le Belle.

Results

Identified and quarantined emails not caught by previous solution.

Reduced false positives and prioritized events to reduce investigation.

Global management and maintenance from a single console.

Improved ability to comply with regulations like GDPR.

Ability to adjust to brand-new attacks in 2 to 3 days.

10-year trusted partnership.