CASE STUDY

proofpoint

SCALAR REDUCES RISK AND TRANSFORMS INCIDENT RESPONSE

GAINS INCREDIBLE EMAIL THREAT VISIBILITY AND COMPREHENSIVE PROTECTION

CHALLENGE

- Lacked comprehensive visibility into incoming threats, affecting the ability to mitigate them
- Experienced unacceptable email delays due to a flood of alerts
- Needed to integrate event data with SIEM to improve overall security posture

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Information Protection, Email Encryption

RESULTS

- Gained comprehensive coverage against range of email-based threats
- Improved email delivery performance
- Transformed incident response with unmatched visibility and control
- Implemented new capabilities ahead of schedule

Scalar Decisions Inc. is one of Canada's top IT solutions providers, providing expert understanding and delivery of security, infrastructure, and cloud technologies. When the company decided to improve its own email protection posture, it found the protection, performance, and visibility it wanted with Proofpoint.

Scalar has more than doubled in size in the past two years, migrating its email systems along the way. Recently, Scalar migrated to a new email system and looked for a way to increase protection for its email infrastructure. Email security is a joint effort of Scalar's security operations center (SOC) and IT services teams. The SOC team focuses on threats, and they want as much data as possible about the wide range of threats trying to get into the company. The IT services team manages email flow to make sure that it is delivered quickly and correctly. They had deployed an email gateway tool to defend against malicious attachments, phishing attacks, spoofing, impostor emails, and ransomware. But it didn't take long to realize that the tool wasn't delivering the mail—or visibility into threats—as well as they needed.

"Email represents a significant threat vector, but protection has to be balanced with timely email delivery," said Frederic Dorré, Chief Information Security Officer at Scalar. "A torrent of alerts delayed email delivery, which also jeopardized our Service Level Agreements (SLAs) with customers."

The teams frequently saw email delays of 10 to 15 minutes and sometimes experienced delays as long as 45 minutes. When they reviewed trace logs to find out what was happening, log data was 15 minutes—or more—late. When the team called the tool vendor for assistance, they were frustrated by a lack of responsiveness and poor communication. The combination of an immature product and poor customer service dictated a change.

"We started down the path of conducting a proof of concept for Proofpoint and another potential solution," Dorré said. "We needed a solution that worked effectively and also integrated well with our other security tools. And it had to give our SOC team all the technical detail that they want without compromising performance for our email users."

Scalar first launched a proof of concept (POC) with Proofpoint. Dorré said that the Proofpoint results were so compelling that it easily stood apart from other solutions under consideration.

"Our security posture is stronger because Proofpoint catches more and tells us when it catches it. We've reduced risk to the company by implementing Proofpoint, and that equals return on investment."

Frederic Dorré, Chief Information Security Officer

A SOLUTION THAT WORKS

Scalar deployed Proofpoint Email Protection to defend against unwanted and malicious email while providing granular visibility. They also implemented Proofpoint Targeted Attack Protection (TAP) to detect, mitigate, and block advanced known and unknown email threats. Deployed in the cloud, Proofpoint sits in front of the company's email solution to detect potential threats in inbound and outbound email traffic.

"Proofpoint is a much more mature product than the previous tool," said Craig Seidler, National IT Manager for Scalar. "It integrated smoothly with our email infrastructure and other solutions."

COMPREHENSIVE PROTECTION REDUCES RISK

Both the SOC and IT services teams love the breadth and depth of Proofpoint coverage. More than just detecting and blocking spam, it validates recipients, offers encryption, provides reputation filtering, supports regulatory compliance, and enables the teams to apply rules and policy. And those are just scratching the surface. Proofpoint also makes sure that the mail is delivered on time, offering SLAs for email delivery to help Scalar maintain SLA agreements with customers.

"ProofPoint has been very effective at helping us gain a strong foothold in the control of spam coming into our network," said Gerard Dunphy, Senior Security Specialist at Scalar. "It has significantly reduced risk to our company."

"Our security posture is stronger because Proofpoint catches more and tells us when it catches it," Dorré adds. "We've reduced risk to the company by implementing Proofpoint, and that equals return on investment."

CLEARER VISIBILITY TRANSLATES TO EFFECTIVE ACTION

According to the SOC and IT services teams, the previous tool 'sat there and did things,' but they couldn't tell exactly what it was doing. For example, it would notify them that it found advanced malware—but that was all.

"There is so much evidence and so many facets of information that we can collect about a threat or group of threats," said Sean Murphy, IT Administrator at Scalar. "We can correlate data—for example, why did nine different people get the same message today, why did it come from nine different email addresses, and what did that threat look like? I can go pull it out of the email solution if we need to delete it."

Newfound visibility has changed incident response workflow. In the past, users would continually add the sender of spam email to the Junk Senders list, and the system would learn slowly over time. With Proofpoint, any issue that arises now can be instantly scrutinized and acted on. A team member can quickly see why a message behaved a certain way, know where it came from, and understand how it got in the front door. They know who else got that mail and can block it. They know immediately if they need to deal with it, change a rule, add a rule, or adapt a policy.

"Proofpoint gives us incredible visibility and flexibility to deal with incoming threats," Seidler said. "And that volume of inbound threats is always just going to grow. Proofpoint lets us tackle threats from different angles, which is really impressive."

The same in-depth visibility also makes it easier for teams to report up to C-level management. They now can present easy-to-read graphics that help teams clearly communicate the benefits that Proofpoint is delivering to Scalar as a company. Technical audiences can go deeper—seeing actual logs, and what was blocked and why.

GIVES TEAMS THE CONTROL THEY NEED

Scalar gains a clearer picture of threats with Proofpoint. They have more granular control to finetune settings, which they didn't have with the previous tool. The SOC team has detailed views of each threat. Scalar even gained capabilities that were previously unforeseen.

"The built-in email digesting functions above and beyond what we'd had before," Murphy said. "Initially we focused on inbound threats. Because Proofpoint also provides email encryption we could solve several issues at the same time."

BENEFITS PAID FORWARD

Scalar now recommends ProofPoint to its clients who require advanced threat protection against inbound and outbound malware, phishing, and other advanced email or web threats. Scalar clients that choose ProofPoint typically see a drastic reduction in actual malware and phishing-related emails that make it to users' inboxes.

Scalar's own teams are moving forward with Proofpoint Information Protection Email Encryption capabilities, which will be used to protect sensitive data and for HR hiring processes. Next stop is SIEM integration. Proofpoint's ability to integrate with multiple vendors' products will enable the SOC to have security events flow from Proofpoint into the SIEM with its other security solutions.

"One of the biggest benefits of our engagement with Proofpoint—from sales to professional services—is that every time we come in with a question, the answer is 'yes,'" Dorré said. "The product is excellent, and beyond the product itself, the people have been fantastic. We get 'here's how' and why that way delivers value to us. The answer is never 'no'."

For more information, visit www.proofpoint.com.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.