CUSTOMER STORY

proofpoint.

SCALAR ENHANCES EMAIL THREAT VISIBILITY

PROOFPOINT INTEGRATION WITH PALO ALTO NETWORKS WILDFIRE DELIVERS MORE DETAIL

THE 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 visibility and enhance prevention

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Information Protection, Email Encryption
- Palo Alto Networks WildFire threat analysis

THE RESULTS

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

THE COMPANY

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 email protection and gain next-generation security capabilities, it found the protection, performance, and visibility it wanted with Proofpoint and Palo Alto Networks WildFire.

THE CHALLENGE

Scalar has more than doubled in size in the past two years, migrating its email systems along the way. Email security is a joint effort of Scalar's security operations center (SOC) and IT services teams. The SOC team wants as much data as possible about the wide range of threats trying to get into the company through email. The IT services team wants to make sure that email is delivered quickly and correctly.

Before adopting Proofpoint, Scalar 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 delivery," said Sean Murphy, national team lead, IT services at Scalar. "A torrent of alerts delayed email delivery and jeopardized our service level agreements with customers."

Email delays of 10 to 15 minutes were common, and sometimes they stretched as long as 45 minutes. When the team reviewed trace logs to identify the problem, log data was 15 minutes—or more—late. The tool vendor was frustratingly unresponsive. It was time for a change.

"We started down the path of conducting a proof of concept for Proofpoint and another product," Murphy said. "A new solution had to work effectively, give our SOC team all the technical detail they want, and do it without compromising email delivery performance. The Proofpoint results were so compelling that it easily stood apart."

THE SOLUTION

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.

Scalar also had deployed Palo Alto Networks WildFire cloud-based threat analysis for its managed services environment. Proofpoint TAP integrates easily with WildFire. When TAP receives a malicious email, it uses Attachment Defense to inspect the full message and attachments. At the same time, Palo Alto Networks Wildfire also receives the attachment for analysis. Either TAP or WildFire

"As a Managed Security Services Provider, our SOC and IT services teams not only protect customers, we proactively work on their behalf. The integration of Proofpoint and Palo Alto Networks WildFire is a great example of how you can gain more 'muscle' against threats with more information sources. Together they deliver incredible visibility."

Gerard Dunphy CISSP, GCFA, GCIA, director of cyber security operations, Scalar Decisions

can condemn the message based on their respective analyses. Either way, the user is protected. Forensic reporting includes data from both platforms and is presented on the TAP dashboard.

Comprehensive protection reduces risk

Both teams love the breadth and depth of the integrated Proofpoint and WildFire coverage. Proofpoint makes sure that the mail is delivered on time, helping Scalar maintain SLA agreements with customers. In addition to blocking spam, Proofpoint also validates recipients, encrypts sensitive data, provides reputation filtering, supports regulatory compliance, and enables the teams to quickly apply rules and policy on the fly.

"It's a real benefit when one of our vendors offers integration with another market-leading product." said Gerard Dunphy, director of cyber security operations at Scalar. "The integration of WildFire into Proofpoint delivers invaluable insight. The more we know, the more proactive we can be at reducing risk."

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. With Proofpoint, any issue that arises can be instantly scrutinized and acted on.

"There are so many facets of information that we can collect about threats," said Murphy. "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 the message out of email if we need to delete it."

THE RESULTS

More muscle to fight threats

Together, Proofpoint and Palo Alto Networks Wildfire deliver detailed views of threats to help inform incident response and shape policy. Having complementary capabilities is important to Scalar's mission because "no single vendor does everything."

"As a managed security services provider, our SOC and IT services teams not only protect customers, we work proactively to defend," said Dunphy. "The integration of Proofpoint and Palo Alto Networks WildFire is a great example of how you can leverage more 'muscle' against threats with more information sources. Together they deliver incredible visibility to enhance prevention."

LEARN MORE

For more information, visit 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.

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