proofpoint

FOCUSING ON THE NEXT LEVEL: PROACTIVE, CORRELATED DEFENSE

BANK TAKES THE OFFENSE AGAINST THREATS WITH STRATEGIC APPROACH

CHALLENGE

- Fighting a growing flood of diverse threats without unlimited resources
- Take bank security posture to the next level
- Streamline multiple systems to reduce the security footprint
- Gain strong data correlation capabilities

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection and integration with Palo Alto Networks Wildfire
- Proofpoint Information Protection, Email Encryption

RESULTS

- Improved protection, catching 99% of malicious email threats
- Consolidated and leveraged capabilities for data correlation through integration
- Saved hours of time each week investigating and remediating threats
- Built a strategic foundation for taking the bank's security posture to the next level

Pinnacle Financial Partners is currently the second-largest bank in Tennessee and growing. Strong client relationships drive every decision—from the leadership team to the deepest levels of IT and security. The bank's laser focus on protecting clients and employees led it to adopt a strategic approach to fighting cyber attacks. Deploying a combination of Proofpoint and Palo Alto Networks solutions, Pinnacle has gone on the offensive, proactively fighting threats in email and on the network.

"We're seeing attacks and more sophisticated email campaigns daily," said Randy Withrow, Chief Information Officer for Pinnacle Financial Partners. "So we tightened our reins, working hand in hand with best-in-class partners."

Pinnacle deployed Proofpoint Email Protection in 2015. It quickly got better visibility into malicious attachments, impostor emails, ransomware, and other threats targeting the bank, and the team watched the tide rise. In January 2016, Proofpoint caught 5,000 messages with malicious attachments. By May, the number had risen to 20,000 per month, and in August it stopped more than 31,500.

"Our Board, shareholders and executives are very progressive in regard to information security," Withrow said. "Just meeting compliance requirements is not enough. Our Board actively understands our information security posture and wants to be laser-focused and strategic. Quite honestly, that's what you should expect from a bank."

The entire bank is committed to protecting its clients and data. When the security team needs to teach employees a new tool, the training and management teams provide crucial backing. In Early 2016, Pinnacle brought in industry expert Jeremy Hopwood of Five Iron Technologies to provide consulting and managed services. Hopwood worked directly with Withrow to understand the Board's direction and implement best-in-class infrastructure. With support from the top down, Hopwood and his team worked to take the bank's security posture to the next level. They wanted to streamline their security solution and leverage the most powerful capabilities.

STREAMLINING AND INCREASING PROTECTION

Hopwood's team moved its Proofpoint Email Protection solution to the cloud, deployed Palo Alto Networks Wildfire, and began migrating to Microsoft Office 365. Proofpoint Email Protection defends against unwanted and malicious email while providing

"Proofpoint data is as valuable as its detection and protection features. We have a new level of visibility at our fingertips, and we're actually getting aggressive—rewriting policies, training, and adapting our approach."

Jeremy Hopwood, Chief Information Security Officer, Pinnacle Financial Partners

granular visibility. Deployed in the cloud, it filters email directly in front of Office 365. If Office 365 mail servers become unavailable, Proofpoint Email Continuity lets Pinnacle continue to send and receive email.

"We're very comfortable with Proofpoint, and it's user friendly," Hopwood said. "It doesn't require a lot of extra effort to make things work together. Every time we add a Proofpoint capability, we add value."

Next, the security team added Proofpoint Targeted Attack Protection (TAP) to its arsenal. Proofpoint TAP detects, mitigates, and blocks advanced known and unknown email threats. It also integrates with Palo Alto Networks Wildfire. Now, potential malicious email attachments are automatically delivered to both companies' cloud-based malware analysis offerings to align protection and enhance network, cloud, email, and endpoint security.

"Integrating Proofpoint TAP and Palo Alto Wildfire lets us correlate data and gain context for stronger protection," Hopwood said. "Integration literally took five minutes—point and click—and it was done."

INTEGRATION FOR BETTER PROTECTION

Within the first 30 days, Proofpoint TAP automatically synchronized suspicious findings with Palo Alto Networks Wildfire more than 2,000 times. Together, the tools caught 50 pieces of malware that otherwise would have evaded detection. Integrating both systems caught 99% of malware attacks.

"Correlating data is critical to us," Hopwood said. "We'll also feed Proofpoint data directly into our SIEM so that we don't have to follow individual data trails. All the data will correlate."

POWERING A PROACTIVE STRATEGY

"Proofpoint data is as valuable as its detection and protection features," Hopwood said. "We have a new level of visibility at our fingertips. We're actually getting aggressive—rewriting policies, training, and adapting our approach."

Proofpoint TAP delivers visual insight into threats and campaigns. In addition to knowing how many threats were stopped, attempted, and caught, now Pinnacle can identify sophisticated campaigns—such as one email sent to 60 different employees every other day at 1 p.m. Integration with Palo Alto Networks delivers data at an even more granular level. Now the team knows the precise type of threat, how it attempts to enter, and targeted users. They can see how widespread the attack is from a global perspective, intended targets, and attack progression, and they also get forensic data.

"With better heuristics, we can make better decisions," Hopwood said. "We've used this data to tune our firewalls, make changes in our workflow, and communicate to our Learning and Development team how threats are morphing."

SAME TEAM, HIGHER EFFICIENCY

Pinnacle's team already has saved dozens of hours a week. They don't have to dive into multiple systems, gather data, and try to piece together an accurate threat snapshot. And the more threats caught, the fewer endpoints the team has to remediate. Hopwood estimates that the bank's new level of detection and prevention enables it to avoid hiring additional staff for its security operations center.

Pinnacle also deployed Proofpoint Information Protection, Email Encryption to encrypt outgoing messages. In the past, employees often used Dropbox to share large files with external partners. That created a huge security hole. Proofpoint Email Encryption solved the problem of enabling users to easily share files while maintaining security visibility. Proofpoint will identify sensitive information in files dropped in shared folders and automatically encrypt them and assign an expiration date.

"We're using the built-in automated encryption and other features," Hopwood said. "Again, we plan to minimize risk from every possible angle and attack vector, which is how we leverage Proofpoint."

CORPORATE-WIDE BUY-IN

"Proofpoint gives us the ability to communicate effectively to the rest of the business," Withrow said. "When we can tell our Board and executives that we had 31,500 email messages with malicious attachments trying to attack us so far this month, it drives conversation to tactical and strategic initiatives. We can discuss the real issues that we are facing rather than subjective thoughts. Real data puts us all on the same team, all buying into the importance of security investment."

"We're focusing on the next level," Withrow said. "The better we can integrate solutions and correlate information, the stronger and more agile we are as a security team. And the more effective we are for the bank, our clients, and shareholders."

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.