Q&A WITH RYAN KALEMBER

SVP, CYBERSECURITY STRATEGY, PROOFPOINT

Ryan Kalember is the senior vice president of Cybersecurity Strategy for Proofpoint, a next-generation cybersecurity company. Proofpoint provides cloud-based solutions that protect the way people work today across email, mobile devices and social media channels. Backed by ongoing innovation, Proofpoint enables organizations to protect their users from advanced attacks, protect the information their users create from loss and compliance risks, and respond quickly when incidents occur. More than 50% of the Fortune 100 trust Proofpoint.

Q) WHAT DIFFERENTIATES PROOFPOINT IN THE MARKETSPACE?

A) Right now there is a hurricane of messaging in the advanced threat and advanced malware product market. In essence, the messages are all variations of each other and many sound similar. I'm happy to say that no startup in 2016 is getting funding to create a mail gateway product, which is our core offering, and no other company protects how people work across all communication platforms.

Our secure mail gateway is not only a security product, but also a fundamental piece of company infrastructure. As advanced threats increase in frequency and sophistication, email has become the number one threat vector. Proofpoint uniquely combines a world class email gateway solution with the industry's leading Targeted Attack Protection technology, catching and stopping cyber threats from malicious links and attachments hours or even days before traditional defenses.

Another differentiator for us is getting our product into the market by having people test it out in their own organizations. More than 50% of the Fortune 100 use our products simply because they work. If you want to do anything correctly in security, you cannot rely on lab tests, PowerPoint presentations, or company messaging to make good technical decisions. You have to test to clear the clutter. You have to test because your environment is unique and the way the threat landscape affects your environment is unique. At the bottom line, there is no substitute to actually seeing how it performs in your environment.

Q) HOW DOES PROOFPOINT HELP CISOS PROTECT THEIR ORGANIZATIONS?

A) We help CISOs at both a technical and strategic level.

Let's look at security as a funnel of threats either targeting people or infrastructure, that come in through various vectors such as email, web, social media and mobile. All attacks are fundamentally targeting people and if you pair those with set of attacks on infrastructure side, you have a whole universe of inbound threats you are facing. If these threats get through the gateway they become problems for other layers, and for your security's defense in depth infrastructure to solve. If you go back to the gateway and reduce the funnel by stopping the email from getting through in the first place, you are in a much better position. In terms of broader architecture, the value of stopping threats at the gateway, where the attack is maximally exposed, allows you have the best chance of stopping it before damage is done.

Q) HOW DOES PROOFPOINT HELP CISOS SPEAK TO THEIR BOARDS?

A) Proofpoint identifies who incoming attacks are targeting, something most Boards want to know about, especially when targets are the C-suite.

There are two types of C-suite attacks, first are malware attacks sent to the C-suite over email. The second type of attacks are spoofing, where a fake email appears to be sent from the CEO asking for something such as a wire transfer to be approved by the CFO. CISOs can use our solution to create reports on how the C-suite and Board are being targeted and protected, which turns into a very compelling story.

Q) HOW DOES PROOFPOINT KEEP UP WITH GROWING TRENDS?

A) We are growing over 40% as company and more than 20% of our revenue is reinvested back into R&D, one of the highest rates in the industry—and our threat team is growing even faster. We are trying to stay ahead of threat landscape by giving customers visibility into areas they might not have previously examined.

For example, we are seeing the same threat actors now target social media and mobile devices, in particular apps on smartphones. I was recently talking to the CISO of a large university who encountered a professor who studied politically sensitive matters. Even with numerous password changes on his laptop, someone continued to have access to his sensitive emails. The CISO discovered that a malicious app on the professor's iPhone was able to go in and steal his password. It is stories like this that demonstrate the need for us to continue to stay one step ahead.