Email & Endpoint Protection: Today’s Threats Require a New Approach

Attackers are using more sophisticated ways than ever to get into networks, and organizations need advanced toolsets to defeat the threat actors. Email and endpoint protection are solutions that you should be offering to your customers, however the tools of yesterday aren’t going to protect against the threats of today. We talked to Ingram Micro’s Jacob White, Technology Consultant II, to learn more about the importance of email & endpoint protection, and what to look for in the tools you’re choosing to deploy.

According to the 2021 Verizon Data Breach Investigation Report, email remains the #1 threat vector that attackers use to breach customer networks

Email continues to be a main pain point for customers. They may feel protected with current tools, and they may trust their users to make good decisions when it comes to opening attachments and clicking links, however this is not always the case. Customers are apt to have endpoint security tools in place, but they tend to be out of date, and they don’t deal with current threats well, or don’t provide visibility into the endpoints.

How do today’s email threat vectors work? How do they differ from the past?

Today’s email threat vectors can be considered metamorphic, meaning that attackers make small changes to code to evade older signature-based detection tools. Once users activate the malware that arrives via email either by clicking on a link or downloading an attachment, it runs on the endpoint carte blanche. The older endpoint protection tools look for a specific signature, which has now been slightly edited and will no longer be caught. Overall, customers need a “one-two punch” solution that can block attacks before they arrive in the inbox and stop malware from activating if it sneaks past email controls or arrives via the web or external jump drive.

Email and endpoint need to work together to create a holistic solution

As we learned previously, many customers are likely to have endpoint controls that are aged and don’t perform well with the most current set of threats. Consider a holistic refresh on your customer’s control set that combines email controls with new, advanced endpoint controls that deal with modern threats like ransomware or other adaptive malware.

What action should resellers take?

Review your customer base and determine the last time their security tools were updated. Have a conversation about how past solutions won’t keep up with what today’s hackers are doing and introduce the idea of a holistic email & endpoint security refresh. It’s imperative that customers are protected with tools that take today’s threats like malware, metamorphic malware, and ransomware into account.
Ingram Micro’s Cybersecurity Delta Force is here to help connect you to the endpoint & email security solutions that make the most sense for your specifically desired business outcomes. Leverage our team to help work through available options that meet your needs! Contact us at cybersecurity@ingrammicro.com to learn more.