THREE KEYS TO SELECTING THE RIGHT EMAIL SECURITY VENDOR
INTRODUCTION
ADDRESSING THE THREAT LANDSCAPE
MOVING TO A MORE PROACTIVE SECURITY POSTURE
MAKING A STRONG BUSINESS CASE
CONCLUSION
Email is one of the most established delivery methods used by cyber criminals. Who among us has not been told (multiple times), “Don’t open email from senders you don’t know”? Yet it’s also demonstrably the top method used by cyber criminals to successfully enter organizations and install malware.

Email security is a mature market with many available choices. There are still “pure-play” email security vendors, security vendors offering broad portfolios and suites, and even infrastructure companies that offer solutions. Regardless of vendor type, the three things a CISO should be sure to consider when approving a strategic partner for email security are whether the solution will:

- Address the risk posed by a constantly changing and accelerating threat landscape
- Help you move from a reactive to more proactive security posture
- Provide a quantifiable return on your investment
When selecting a strategic vendor for email security, you need to make sure it’s able to deliver protection against a fast-changing threat landscape. This includes having:

- A strong and substantial threat research team that has the ability to stay abreast (and ideally ahead) of the fast-paced email threat landscape. This team is critical in identifying the latest techniques being employed by cyber criminals to get past established email security controls. It is also responsible for the intelligence that identifies established and emerging campaigns.

- A correspondingly expert and properly resourced development team to continually deliver and improve the necessary email security features to address the latest cyber-crime techniques and apply that threat intelligence from the research team to the production environment. In the case of email, those advanced technologies include sandboxing, content disarm and recovery, impersonation analysis, and more.

- Independent validation of effectiveness. While it’s recommended to test a solution in your own environment to ensure fit, such tests typically only last 30 to 90 days. Looking for vendors with an established commitment to independent testing, such as participation in ICSA Labs Advanced Threat Defense Certification for Email, can provide a credible data series on security effectiveness for a much longer period.

**EXPERT TIP:** Assess the expert resources a vendor has in the area of email security, along with the capabilities in the offering to be sure they match the latest threat landscape. But at the end of the day, look for proven and quantified security effectiveness over an extended period of time.
Simply blocking the latest email attacks (while necessary) leaves the organization constantly on the defensive and frankly ignores a wealth of information that is increasingly available to the organization. Whereas the traditional secure email gateway was a proverbial “black box” applying various rules to discard unwanted and malicious email, times have changed with the inclusion of new capabilities like sandboxing.

- Consider that, in many cases, the email received is often the first stage in a multistage effort to not only reach the end-user but also entice them to click a URL, visit a site, download an additional component, and/or take other action. All of this follow-on activity is typically uncovered during sandbox analysis, offering insight into associated cyber-criminal infrastructure that may be used in future attacks, for those who take the time to look.

- Further, given how busy everyone is on the security team, solutions that present intelligence from that sandbox analysis and make it available to inform other security controls are highly valuable.

- Better still, the ability for the security controls to integrate and share intelligence automatically, from email security, to sandbox, to the rest of the security infrastructure including network, endpoint, and other security components is ideal.

**EXPERT TIP:** Look for email security solutions that offer insight beyond the initial email attack, creating intelligence about the supporting cyber-criminal infrastructure through the attack life cycle and automatically sharing that threat intelligence across the attack surface.
Of course we all know that time and money, especially for security, can be scarce. Justifying security spend on the latest, often detection-oriented products can be tough. The good thing about email security is:

• There is an acknowledged problem. Gartner\(^1\) notes that advanced threats are easily bypassing traditional techniques used by secure email gateways.

• There are established costs. The FBI estimates that business email compromise cost the industry $5.3 billion from 2013 to 2016 and ransomware cost another $5 billion in 2017 alone.

• The brand new attacks you see with email security are ones you can stop. Unlike network or endpoint security where any delay is visible to the end-user, minor delays in email security (to hold, inspect, and then decide whether to deliver) are often unnoticeable.

**EXPERT TIP:** Conduct a proof of concept with the prospective email security solution behind what’s currently in place to see what would otherwise have happened without a change. Use available costs of attacks like ransomware, business email compromise, and more to calculate a financial ROI (in addition to other benefits) for increased security.

CONCLUSION

In such a mature category as email security, many options (at various price points) abound. And with 49% of malware installed via email\(^2\), having the right email security in place is critical.

Be sure to look for vendors that offer a leading feature set that has independently demonstrated its security effectiveness over time. But then go one step further by selecting a vendor that offers insight beyond the initial email entry and intelligence sharing about later-stage components across your attack surface. In doing so, and by testing it behind your current email security solution, you will move from reactive to a more proactive security posture and have a strong business case for doing so.

This is the approach that Fortinet has taken with its email security solution within the broader notion of a security fabric. Specifically, Fortinet Email Security:

- Benefits from a leading threat research team and email security development group that deliver solutions with the latest features to earn ICSA Advanced Threat Defense certification and Virus Bulletin’s top VBSpam+ rating for years.

- Includes the option to integrate with FortiSandbox to not only block the latest spear phishing, ransomware, and other attacks, but also uncover intelligence about the full intended attack life cycle and share it across your security fabric for a more proactive security posture.

- Routinely blocks a wide range of attacks, offering the opportunity to assess and submit a quantified business case, when tested behind legacy email security products and solutions.
