CYREN

Email and Web Security Buyer's Guide

CRITICAL QUESTIONS

The decision making process for purchasing an email and web security solution is complex. This document outlines some of the questions you should be asking yourself and the vendors you are speaking with at each stage of the process.

What are the prevalent threats and how do they impact my business?

- Do we have full visibility of all information and applications in use?
- What specific information does the business possess that could be at risk?
- Where does it reside and how is it protected?
- Who can access it, how are they authenticated and authorized?
- Are we operating a least privilege policy – can people access information who don't need to?
- What are the risks to each information type (e.g., the result of stolen intellectual property, lost information, leaked information)?
- How do we mitigate the risk from each specific threat type? Are the controls applied adequate and proportionate to the level of associated risk?

Do we understand any risks associated with specific business processes and how we operate?

- Are we in an industry that is targeted by specific threats because of the way we do business (e.g., real estate businesses process high-value transactions, logistics businesses have extensive supply chains)?
- Are there specific projects underway that are leaving us exposed in an exceptional manner?
- Does line of business have the freedom to deploy unsanctioned applications?
- Do we have a large number of mobile users who are more at risk than non-mobile users?
- Are users using their own devices and how are they secured?
- Do we limit access to high-value information in higher risk situations (e.g., mobile users, BYOD)?
- Are we regulated and do we understand the impact of non-compliance?
- What web properties do we have a presence on and what would the impact of them being compromised be (e.g., social media accounts, web site)?
- Are our users IT savvy and educated about information security?
- Do we have operational technologies or a high number of connected devices (IoT) and how are they secured?
- Do we have a complex supply chain and do we understand the security posture of third parties that access our systems and information?
- Do we understand the implications for our business partners of an attack on our business?

What are key things we should consider before drilling down into technology and products?

- What budget do we have and where should we focus it to best protect our most valuable assets and information?
- What are the potential results of a successful attack (e.g., competitive disadvantage, lost reputation, lost business, fines from regulatory bodies)
- What technology security controls do we already have and are we realizing maximum value from them?
- What cyber security skills and expertise do we have in-house and are we using them to best effect?
- What is the anticipated number of IT/IT security staff and what skills levels will they possess?
- If we are investing in a long-term solution, will it evolve to meet the changing needs of the business (e.g., an increase in numbers of users, email volumes and web traffic)?
- How will it protect from future, as yet unknown threats?

Should we choose on-premises software/appliance or a cloud email and web security service?

- Do we have a no cloud policy?
- Do we prefer capital or operating expenditure?
- How complex a cost model are we prepared to accept and what do our procurement and finance teams prefer?
- Do we understand the total cost of ownership of the cloud security service or appliance, or do we only know the cost of acquisition?
- What are the additional costs of high-availability and disaster recovery?
- What is the cost of deployment and ongoing management of each cloud security service or appliance?
- Do we have staff on the team with the relevant skills and time to do ongoing tuning and management, and how much dedicated time does a cloud security service or appliance need?
- Have we considered intangible costs like the cost of bandwidth to download spam emails to an email security appliance or backhaul traffic from remote users to a web security appliance?
- Will the cloud security service or appliance scale with the business in a linear manner or will we need a "forklift" upgrade at some point?
- Do we need to offer web security to mobile users and do not want to backhaul their traffic to an appliance?
- Do we use many cloud applications and need to control access to them for mobile users who are not behind an appliance?
- Can a cloud services provider actually help us achieve higher levels of security, compliance and information protection than we could ever hope to achieve with our budget and resources?
- Will an integrated email and web cloud security service or appliance provide technical and/or cost benefits and can we achieve them by building our own?

How do we get the best possible detection and the fastest time-to-protection?

- Is the cloud security service or appliance using more than just signature-based AV?
- Is it using multiples layers of detection and are they integrated or does each just provide a binary decision on its own?
- Is the cloud security provider or appliance vendor using their own detection technologies or is it just

an aggregator of third party technologies?

- Does the threat detection capability sit in the cloud and have access to enough information to quickly detect new threats?
- How often are security updates applied or is the protection instantaneous as soon as a new threat is detected?
- For appliances, what is the impact on performance of adding new detection capabilities?
- Does the cloud security service or appliance provide multiple sandbox environments to detect unknown and evasive threats?
- Is the web security proxying and scanning all content or simple doing DNS or URL filtering that just prevents access to known malicious sites and webpages?
- Does it scan SSL traffic with no impact on performance?
- Does the web security provide visibility and allow control of cloud applications?

How do I determine which vendor I choose and if they sell through an indirect partner network, which of their partners I purchase from?

- Is the cloud services provider or appliance vendor financially stable?
- Is the cloud services provider or appliance vendor going to continue to fully support the service or product?
- Will we get a benefit from purchasing from a specific type of organization, what is the benefit and do we fully understand all implications (e.g., if we receive cost benefits from purchasing from our IT generalist is the product really as good as that from a specialist?)?
- How much specialist help do we need to understand the pros and cons of each cloud security service or appliance?
- If we want to purchase integrated email and web security, does the cloud security service provider or appliance vendor offer it?
- Can we purchase through our preferred reseller, MSP or CSP and how beneficial is this to us?
- Does the cloud security provider or appliance vendor offer a free trial?
- Can they do a live comparison with our current email security?