

# Future-Proofing Email Security

Can hybrid security deliver the best of appliances and SaaS?

Spearphishing, cost concerns, exploding spam rates, increasing compliance requirements, and new cloud-based deployment options may have you reevaluating your current email security solution. Your best solution may be a hybrid solution, one that gives you all the advantages of both appliances and SaaS, without forcing you to pay twice for your privileges.

Like a growing number of IT teams, you may discover a hybrid solution serves all of your business requirements, eliminating the need to choose one approach over another. By keeping your options open, you can both optimize and future-proof your email security.

Traditionally, on-premises solutions, including appliances, software, and virtualized environments, have dominated the email security space. Recently, though, security Software-as-a-Service (SaaS) solutions have become much more appealing and enterprise-worthy, especially as organizations look for areas to trim capital and operational costs. Both options, on-premises and SaaS, can even be used together to implement a hybrid approach to email security. This solution is attractive to large organizations under pressure to outsource expenses and those looking to tier or layer services or scale to more users.

Each option has its pros and cons, and one organization's "pro" might be a "con" for your business. Weighing the factors as they relate to your business will help you determine your best email security deployment option.

Some questions to consider:

- Does your current solution's performance and spam detection meet expectations?
- How would you improve it?
- Does your current solution fit within your upcoming budget?
- What are your email security priorities today? How will they be different in a year? In two years?
- Does your organization need email filtering to do more than anti-spam and anti-virus? What about data loss prevention (DLP) and archiving?
- Can you demonstrate the control that regulations demand, generate the reports you need, and quickly locate lost emails or archived files?

Your best solution will balance your needs for protection—both inbound and outbound inspection—against budgetary, organizational, and regulatory constraints. These considerations will help you compare the advantages and tradeoffs of today's deployment options, unfettered by the built-in bias of a single product vendor. Like a growing number of IT teams, you may discover a hybrid solution serves all of these factors, eliminating the need to choose one approach over another. By keeping your options open, you can both optimize and future-proof your email security.

McAfee can be neutral about deployment choice because we offer email security that works any way you prefer, as an appliance, a virtual appliance, SaaS, or any hybrid combination thereof. Our per-user pricing eliminates premiums for multiple delivery options. This simplicity eases your purchasing choice, so your deployment decision can be determined by today's business needs. The deployment flexibility keeps all of your options open as your business requirements change.

### Cloud-based: How Much Time Do You Want to Devote to Managing Email Security?

Cloud-based security (SaaS) allows organizations to offload some or all of the implementation and management to a service provider. Service offerings vary, but most include spam and malware filtering at a minimum. Some vendors offer continuity services, email encryption, archival, and other premium value-added services such as content filtering for compliance and policy enforcement.

Administration of SaaS solutions is performed through a web portal and can include fairly limited to fairly flexible options for managing policies, spam settings, and content controls. Simple installations and defaults that apply “best practice” settings make it easy to get email protection started.

#### Play keep away

Because it filters out spam and harmful email before it reaches the corporate network, SaaS enhances overall security. It keeps malicious content away from your hosts, network, and email servers. Historically, SaaS has appealed to smaller businesses that do not have in-house security experts or sufficient IT resources. With the increasing sophistication of threats, there is increasing value from the service provider’s security expertise, constant vigilance, and automated updates to the service and protections.

#### Pay as you go

Instead of the up-front licensing and capital expense traditionally associated with on-premises equipment, SaaS solutions offer a predictable subscription that can typically be treated as an operating expense. Day-to-day maintenance and updates are handled by dedicated security experts and are built into the subscription, eliminating additional ongoing expenses. Because service updates are instantly available—no manual product updates—organizations receive a faster time to value on innovative new features. Cloud-based services also help you save on bandwidth costs and storage by eliminating processing of unneeded content.

#### Expand on demand and “go green”

For growing companies and those with “go green” goals, the absence of appliances or servers running in the data center can offer instant savings and instant expansion. A SaaS-based solution is always the right size without worrying about extra equipment requirements or increases in operational overhead like power consumption and data center space.

Since SaaS services initiate easily, they are ideal for companies that need quick access to new capabilities or higher capacity. For example, to facilitate disaster planning and compliance goals, you can add in specialized options such as continuity and multi-year archival services. Because these services are hosted, your business can have greater confidence that its email application and data will be available during an emergency or an audit. These services can be added to any deployment configuration, foreshadowing the hybrid configuration we will discuss later in this guide.

### Onsite: How Much Control is Critical to Your Organization?

SaaS is not the answer for everyone. Many organizations are attracted to SaaS solutions, but desire a higher level of control over their email security infrastructure than the policy set traditionally provided by SaaS solutions. You must weigh its convenience against your needs for hands-on oversight, integration with other on-site technologies, and more granular rules. The insistence on control may be due to the existence of complex policies for handling and routing email or a corporate culture that prefers ownership of security solutions in order to avoid compliance violations, such as the escape of confidential data. There may be financial reasons as well. For example, some companies want to use virtualized systems to extract more value from their existing hardware and software investments. Every company has different priorities, and some of these concerns will anchor you in at least a partially on-premises solution.

#### Make your own rules

Direct management of physical systems can make it easier to define, meet, and maintain policies for changing regulations and business requirements. At a financial institution, for example, governance policies and regulations may demand long-term retention of logs for audit, or service level guarantees that are cost prohibitive for a service provider to meet.

A SaaS-based solution is always the right size without worrying about extra equipment requirements or increases in operational overhead like power consumption and data center space.

It is common to augment on-premises systems with additional policy-based controls and configuration options, such as alerting, re-routing, quarantining, message altering, blocking, and encryption, creating custom policies for each. For instance, encrypting sensitive data before it leaves your site helps to ensure that restricted information does not leave the network unprotected. Encryption may also be required to comply with regulations.

**Play nicely with others**

For larger or more heavily regulated companies, hands-on contact with your email security system may also allow integration with other security and compliance management systems, user directories, reporting processes, and compliance auditing. Local, technology-based integration can enhance the accuracy and efficiency of these inevitable tasks. Integrated monitoring across protections, for example, enables increased visibility across your organization’s overall risk posture.

**Support an organizational philosophy of control**

Finally, on-premises systems are best for ultra-secure organizations and those with an ingrained requirement for control. Beyond the simple solace of blinking color-coded status lights, when you implement and maintain your own system, you control instant access to detailed logs for troubleshooting and forensics, usage analysis, audits, and other data-intensive requirements that would be less feasible with cloud-based solutions.

Some organizations prefer to perform outbound filtering and policy-based encryption of sensitive data on their site. This provides hands-on control and accessibility to avoid potential business and compliance risks, without worry about accidental data loss once it leaves the controlled environment of their network. A SaaS solution alone may not work for these organizations, but both on-premises appliances and hybrid deployments are well suited to address these requirements.

Direct management of physical systems can make it easier to define, meet, and maintain policies for changing regulations and business requirements.

Priority	Ideal Solution
Reducing management costs	SaaS
Stopping nuisance traffic and spam before it hits the network	SaaS
Email continuity and archival	SaaS
Controlling data loss at the gateway	On-premises appliance
Encrypting sensitive data	On-premises appliance
Fine-tuning policy controls	On-premises appliance
All of the above	Hybrid

**Hybrid: Can You Take Advantage of Both?**

Many companies create multi-layered security by using a mixture of solutions. This hybrid email security combines the attractive parts of cloud-based SaaS solutions with the advantages of on-premises systems for maximum flexibility.

In the most common hybrid email deployments, inbound email filtering for anti-spam and antivirus is handled in the cloud. The cloud-based component handles the bulk of the security work and only filtered email actually makes it to the corporate network.

Once the email arrives on site, appliances (physical or virtual) can provide additional filtering for inbound email, usually to filter policy-controlled content and support complex routing and policy development. The email is then handed off to the email server for distribution.

For outbound traffic, an on-premises system will scan outgoing emails and attachments to identify sensitive content. It can then take policy-based action (such as encryption) on sensitive content before it leaves the corporation.

Beyond hosted spam and malware filtering, any company can consider using hosted email continuity and archival services, since they provide unique availability advantages at a low implementation and maintenance cost. Hybrid services help companies who want to tier the controls and protections applied to different sites or user communities, for instance differentiating the email policies for different groups within the organization, such as distinct rules for “executives” and “manufacturing.”

### Time to Choose

You owe it to the future of your business, your budget, and your own productivity to explore some of the hybrid and cloud-based options in the market. The chart below compares the chief distinctions for each deployment option we have discussed. The hybrid option depends on the SaaS services you choose, so we provided answers based on the most common hybrid deployment option described above. We included the McAfee® Email Protection solution for comparison. Review your preferences and requirements, and then consider your options. Learn more at [www.mcafee.com/emailsecurity](http://www.mcafee.com/emailsecurity).

*“The hybrid approach offers the cost savings and management ease of a cloud-based solution that reduces unwanted email before it hits the corporate gateway. It allows for custom policies, data loss prevention, and integrated encryption capabilities that are best provided by an on-premises appliance.”*

—Brian Burke, IDC

Consideration	SaaS	On-premises	Typical Hybrid	McAfee Email Protection
<b>Cost Model</b>	• Subscription	• Upfront purchase	• Varies	• Subscription, optional hardware purchase*
<b>Management and policy options</b>	• Web-based portal with built-in policy defaults	• Extensive granular rules	• Varies	• Built-in defaults with sophisticated customization capabilities
<b>Maintenance requirements</b>	• Maintenance built into the subscription	• Hardware lifecycle management	• Combination	• SaaS maintenance built-in, optional hardware lifecycle management
<b>Integration with existing infrastructure</b>	• Low	• High	• Possible	• Tight integration with complementary McAfee portfolio solutions, DLP, Web, Archiving, etc.
<b>Support for Green Initiatives</b>	• High	• Low	• Possible	• Energy-saving SaaS and virtual appliance options
<b>Scalability</b>	• Instant	• Requires additional resources	• Varies	• Instant
<b>Detailed reporting, logs, and forensics</b>	• Sophistication varies with service provider	• Yes	• Possible	• Yes
<b>Spam filtering and threat prevention</b>	• Cloud—before your network	• At the network edge (gateway), with fine-grained control	• Either or both (for layered protection)	• Either or both (for layered protection)
<b>Outbound filtering and encryption before data leaves your network</b>	• No	• Yes	• Yes	• Yes
<b>Offsite continuity and archival</b>	• Yes	• No	• Yes	• Continuity included, archival optional

\*The McAfee Email Protection Service uses a subscription-based licensing model, with a per-user price regardless of the delivery platform used (SaaS, virtual appliance, standard appliance, or any combination thereof).

