Balancing Cloud-Based Email
Benefits With Security

White Paper

Balancing Cloud-Based Email Benefits With Security

Symantec

Balancing Cloud-Based Email Benefits With Security

CONTENTS

Brought to you compliments of

As organizations try to take advantage of the business benefits and cost savings afforded by cloud offerings, email software as a service (SaaS) stands as one of the easiest first paths toward cloud adoption. Generally simple to set up and maintain, cloud email often is the first win for organizations that may not yet have the wherewithal for more complex cloud deployments.

TechTarget Custom Media

A TECHTARGET WHITE PAPER

Unsurprisingly, statistics show that 58% of businesses today have already migrated to cloud email.[1] And the enterprise is also quickly catching up. Gartner estimates that between 2014 and 2017, the percent of email seats based on a cloud or SaaS model will triple.[2]

Many reputable cloud email providers do offer some fundamental security controls bundled into their services. Nevertheless, organizations struggle to find the right balance of ease of use for their employees and cloud cost savings. After all, they must still maintain the same level of security their organization came to expect when email was hosted on internal infrastructure in their on-premises environments.

Trouble Spots in Cloud Email Security

Whether delivered on-premises or through the cloud, or a hybrid model email these days is ground zero in the struggle to manage corporate risk. Its ubiquity as a business communication tool and the stability of its presence in the business environment over the last two decades makes it a prime candidate for abuse. Cybercriminals and fraudsters of all types set their sights on email as the first line of attack when working criminal campaigns online. And internally, uneducated or fraudulent users further add risk to the equation by using email to share or even steal some of the most sensitive information a business cares for—at least when proper protections aren't in place.

The statistics bear out the fact that email is usually the Achilles' heel of cybersecurity today:

Phishing: According to Symantec's research, one in 965 emails sent today is a phishing email attempting to steal user credentials. These emails use various forms of bait, such as promises to view juicy news videos after logging into a social account or even posing as fake security updates that require logging into corporate accounts before loading.

Malware and malicious URLs: Even more troubling is the fact that one in 244 emails sent today contain some form of malware. Approximately 12% of those are delivered as malicious links, with attackers frequently using URL shortening services to mask their fraudulence. The link then redirects, to bounce from a legitimate site to a bad URL.

Targeted and advanced attacks: Symantec security researchers report that attackers are continually upping their game to single out specific high-value victims and try to infect them using sneakier, more

1 "State of IT," Spiceworks, 2014

2 "Gartner Says Cloud Office Systems Total 8 Percent of the Overall Office Market and Will Rise to 33 Percent by 2017," Gartner, June 2013

targeted emails, tricking spear phishing victims into divulging information or downloading malicious malware. For example, attackers frequently use stolen email accounts from one corporate victim to spear phish their next corporate victim. The number of active spear phishing campaigns online has nearly doubled since 2012.

Insider threats: Email can be a veritable sieve for sensitive corporate information. One recent survey showed that 84% of employees today are using personal email to send classified or confidential information as attachments.

With all of these email attack trends coming to a head, the increased adoption of cloud email can further complicate data protection if security is not appropriately designed into the cloud email architecture.

Many cloud email services are simple by design. That's what makes these systems so attractive to organizations, as this simplicity is what makes cloud email so easy to deploy and maintain. But cloud email's biggest selling point can also be one of its biggest security downfalls.

Simplistic design means it is difficult to offer controls over when and how emailed data is encrypted. Similarly, it is difficult to keep tabs on data as it flows in and out of corporate bounds. In many instances, there simply aren't enough controls available to administrators to offer a way to consistently manage what kind of data goes to whom via cloud email accounts.

Additionally, cloud email can seriously limit security visibility. Many organizations also find that, from a visibility perspective, once email goes to the cloud it is much more difficult to keep tabs on security incidents that start with email. This means that all of those phishing attempts, targeted attacks, malicious links and advanced malware fly under the radar much more easily through cloud email accounts than on-premises accounts. Without the context offered up by advanced email monitoring, it is much more difficult to act early within the attack kill chain and catch attacks before they do real damage.

What to Look for in Cloud Email Security

This is why it is so important for organizations large and small to evaluate hosted email services not just from a convenience perspective, but also from a security point of view. Cloud email has evolved a great deal over the past several years and it is possible to find services that still extend the benefits of easy deployment and use without compromising on data protection and security compliance.

As an organization considers potential hosted email providers, it should be prepared to evaluate based on several critical criteria. First and foremost, an organization should seek a platform that can offer protection against advanced malware attacks and phishing. Even more than just protecting within email, an organization should seek a provider that can also connect email intelligence into threat analytics for better security visibility across the organization. For good measure, it might also be important to evaluate how well the platform handles gray mail like newsletters, in addition to whether it can effectively stop spam with a low false-positive rate.

Additionally, it will be important to find out how well the email provider can help prevent sensitive information from being accidentally or intentionally shared through email. Data loss prevention can provide a key barrier to costly insider threat incidents through the email channel.

Another crucial point to consider is how well the platform enables encryption policy enforcement. With regulatory demands increasingly requiring encryption for important classes of sensitive information, it is critical for organizations to be able to automatically ensure that users are applying encryption to email in all the right situations.

There are other considerations regarding compliance: is the email provider certified by third-party organizations such as ISO to prove its security processes? This question bears answering.

Finally, organizations need to come at the evaluation with the understanding that the migration to the cloud is a gradual process. The cloud email provider should be able to support a gradual transition from on-premises systems to cloud systems.

Symantec™ and Cloud Email Security

As a global leader in information security, Symantec™ is a natural partner to help organizations overcome security challenges when migrating to hosted email. Symantec Email Security.cloud provides the perfect balance between security and convenience in the cloud email environment.

The Email Security.cloud platform is designed from the ground-up with data protection in mind. This includes data loss prevention (DLP) capabilities baked into the system, customizable policy templates and the ability to block messages that violate policy. It also offers encryption through TLS from the get-go, along with the option to add on policy-based encryption that will force users to encrypt data when corporate policies dictate that data be protected in this way.

Not only do all of these features offer added security and peace of mind, but they can also help keep auditors at bay. Email Security.cloud is designed to help organizations comply with numerous regulatory demands, including PCI and HIPAA requirements.

Meanwhile, Symantec's intelligence backs up Real-Time Link Following to help ensure that users are protected from advanced attacks and malicious links.

Symantec Email Security.cloud is both highly scalable and flexible, giving organizations the option to use it with mailboxes in the cloud, on-premises or a hybrid model as cloud adoption progresses. All of this is easily managed from the Web, and more importantly it is designed to work together with a host of other security products to provide greater context about the entire corporate environment's security posture.

More Information

Visit our website

www.symantec.com/email-security-cloud

To speak with a Product Specialist

North America: +1(866) 893-6565 or +1(520) 477-3135; SSL_EnterpriseSales_NA@symantec.com

To speak with a Product Specialist outside the U.S.

To speak with additional product specialists around the world, visit our website for specific offices and contact numbers.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions.Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems.Our industry leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world.More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com