SilverSky
SECURITY FROM THE CLOUD

White Paper

What to Look for in Cloud-based Email

Summary

The cloud is more than a buzzword these days. Companies large and small are looking skyward for critical business functions that were once seen as untouchable—and they're doing it for the time-honored reasons of reducing cost and complexity. The prevailing wisdom not long ago was that a critical application like email had to be housed in a company data center where teams of expensive IT staff members could babysit it and do little else. But that's all changed in the past few years

As companies look to focus on what they do best and leave certain tasks such as email and other resource-intensive activities that aren't a core part of their business to experts in the cloud.

That doesn't mean companies can just shake hands with a cloud email provider and leave the driving to them. In addition, there are (sometimes) unfounded concerns about security and the cloud.

So there are a number of issues buyers need to talk with providers about, including:

+ **Cost:** What are the risks, what are the all-in costs (and what costs are hidden)?
+ **Backing Up:** Is backing up encrypted, is it onsite or offsite, do you have compliance issues, is it indexed and can it be easily searched, can you connect seemingly disparate conversations, and how easy is it to use?
+ **Monitoring:** Who's watching your systems, data and services and ensuring that your information is kept safe?
+ **Uptime, SLAs and Compliance:** What safeguards are in place to ensure 24/7 operations and high availability, will the shutdown of one data center automatically failover to another, are data centers geographically distributed, will the provider work with you on your specific needs, and is the network protection from DoS? Will the provider ensure compliance with internal company policies and regulatory requirements?
+ **Data Protection:** Can the provider encrypt sensitive data, is there granular encryption policy enforcement, is encryption manual or automated, do keywords or key data trigger encryption, what algorithms are in place, and how does the provider handle key management? Does cloud email work seamlessly existing security investments like DLP technology?
+ **Spam and Malicious File Protection:** How does the provider keep inboxes clear, what kinds of filters and are in place, what are the false positive/negative rates?
+ **Mobility and Enterprise Collaboration:** Will the provider provide access for mobile devices, and is there a way to administer the system via a mobile device? Does the provider enable integration between email and collaboration applications?
+ **Industry Experience:** Does the provider have case studies of companies like yours, how experienced is the provider with implementations like this, and what's their experience with maintenance.

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

Contents

It's the Economics, Stupid 4

What's the Real Cost? 4

What's Included? 4

What Else do You Need? 4

Hidden Cost of Hosting on Your Own 4

Letting Go (and Holding On) 5

Archiving 5

Creating the Right Policy 5

The Right Backup Strategy and 100% Availability 5

Who's Minding the Store? 5

Availability, SLAs and Compliance 5

Your Right to Audit 7

Data Protection 7

What to Ask Your Provider 7

Spam and Malicious File Protection 8

Don't Panic; Just Ask the Right Questions 8

Mobility and Enterprise Collaboration 8

Collaboration Shouldn't Miss a Beat in the Cloud 9

Industry Experience 9

What to Get from Your Provider 9

Takeaway 10

About SilverSky 10

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

SilverSky
SECURITY FROM THE CLOUD

It's the Economics, Stupid

Cost is often the primary factor anyone considers when making a big purchase. But, as one learns more about the product (whether it's a car or cloud email) cost becomes an important factor among many.

In your evaluation of cloud email options, you should know your budget and consider cost as an important driver of your decision. But it shouldn't be the only one. Nonetheless, there are a number of considerations you need to examine.

What's the Real Cost?

In a 2009 report , Forrester showed that executives often underestimate how much existing systems costs. Those executives often lowball costs such as software maintenance and support, storage and archiving, staffing, operating systems, power and data center, and financing. Forrester notes that cloud-based email is cheaper, even for mid-sized companies.

What's Included?

But just what do cloud email providers cost—and what does the cost include? Often, a provider will give you a quote that accounts for only the bare necessities. It's important to understand everything you get for the quoted price—as well as what you don't get. But it's also helpful to understand what you're paying now with your on-premises system.

What Else do You Need?

For example, are there any additional levels of security you'll need to purchase (or subscribe to)? And what about firewalls, patch management, compliance and archiving? Check to see if this kind of functionality is included in the price you get from a provider. If it isn't, and if yours is like most companies, you'll need at least a few of the options from that list. And more than likely you'll need all of them. Like many technology initiatives, choosing a cloud email provider is all about balancing cost with risks (perceived and real) such as project failure and compromised data. If you can save considerable money by using cloud-based email while, at the same time, minimizing your risks, it's probably worth exploring. Risk is a relative thing, though. Some companies can handle more than others. So gauge your ability to handle risk (and think not just about your propensity for business risks, but your emotional willingness to take risks) as you examine your cloud email options.

Hidden Costs of Hosting Your Own

Labor and complexity are the most significant costs underestimated by companies that run their own email systems. Companies know what they pay their employees but rarely factor it in when they examine the cost of an email infrastructure. With cloud email, the costs should be easy to figure out.

But the cost of omplexity can be a hard one to nail down. Think about the services that surround email, such as encryption and antivirus, which often come from different vendors. They require a lot of babysitting and expertise to manage properly. And when a problem comes up it can often be hard to track down and then even tougher to get a vendor to admit the problem and work with other vendors to make it right. With cloud email, a company can rely on experts to do what they're good at. And best of all, without multiple vendors to chase down, there's the proverbial single throat to choke when there's a problem.

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

SilverSky
SECURITY FROM THE CLOUD

Letting Go (and Holding On)

Tighter control does not always equate to better security. That's because most companies aren't email security experts. Moving email to the cloud can, in fact, increase security and give a company more peace of mind

The key is to strike a balance. A good cloud email provider should give you the control you need, while taking on tasks that you don't need to control.

You should determine what falls on either side of the ledger and ensure that your cloud provider can accommodate you.

Archiving

Archiving email is one of those unglamorous but necessary chores that can lead IT managers to pull their hair out. But getting it right is critical. Federal Rules of Civil Procedure require organizations to be able to produce email relevant to a specific caseload in a timely and accurate manner, and a well-architected archival strategy can help you respond to eDiscovery requests faster. The net result is lower regulatory risk and less business disruption.

Carefully assess your current and future needs. Physical storage is cheap these days, so some companies save everything. And some companies save everything because they have to.

Creating the Right Policy

To ensure you have a sound archiving policy in place with your cloud provider, you need to understand the following issues:

+ Will the provider help build and roll out a lifecycle policy that you can adjust as needed?
+ Do you have any forensic needs?
+ Do you need to be ready for e-discovery?
+ Are the backups and archives searchable and indexed?
+ Are conversations connected so that subjects remain intact?
+ How easy is it to use the backup functionality?

The Right Back-up Strategy and 100% Availability

Ask the cloud email providers you're evaluating whether they offer a continuity archiving service.

This kind of service delivers redundancy that covers all downtime, which enables a provider to offer 100% availability in an SLA.

Who's Minding the Store?

This is a question that some people overlook. But it's important to know who's watching your systems, data and services and ensuring that your information is kept safe. Threats are everywhere these days. They come from inside your company via often-inadvertent slip-ups from employees. They come from outside your company, from the bad guys who are looking for a way to make a buck — or just trying to wreak havoc.

When you make the decision to move important parts of your computing infrastructure to the cloud, you need to be assured that it will be monitored by a top-flight security operations center, with certified, experienced employees who can quickly analyze threats and neutralize them.

Knowing how your provider protects your data should be central to your decision-making. Trusted providers have a security monitoring service that continuously watches their cloud infrastructure — and your data. Expect your provider to collect, aggregate and monitor security events from your key workload servers, security devices and authentication systems. To prevent an intrusion, your provider should follow best practices from the Center for Internet Security (CIS), SANS Institute and other authorities to harden servers and networking infrastructure. And if a potential breach occurs, your provider should immediately send you an alert.

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

Availability

Uptime is something every provider talks about. Many brag about offering five-nines availability. That means the service is available 99.999% of the time, which equates to 5 and a half minutes of downtime a year. Will your provider really be able to keep your email up and running 525,554.5 minutes a year? That's what it takes for five-nines.

SLAs

But no matter what your provider says, one way to assure you get the service you need is to have an SLA that spells it out.

To get a glimpse into whether the provider can give you the availability you need, ask questions:

+ What is the provider's mean time between failures?

+ How will the provider ensure availability?

+ What safeguards are in place?

Your SLA should set down hard and fast rules for the availability you'll get. And it should extract penalties from the provider if it misses the target. In addition, you should have a very clear escalation path and minimum response times for certain types of events (i.e., a data breach or a loss of data) with a clear reporting path to you. Perhaps more importantly, you should have a single contact (the "throat to choke" we mentioned earlier) at the provider.

The SLA should also make clear how the provider tracks server availability and how it can trace problems that crop up. Don't accept the first copy of the SLA the provider sends. Make sure it is customized to your needs.

Every company is a bit different, and although the challenges we all face are similar, you should ensure that the cloud provider writes your SLA in plain English with your business needs in mind.

Compliance

Whether an internal company standard or a regulatory requirement, compliance is about knowing your email and data are protected to a specified standard—and having proof.

The external requirements can be tricky, and you don't want to run afoul of them. If you can't comply with regulations, fines and bad press could be in your future. But, ultimately, the biggest loss could come to your business.

Here are some questions you need your provider to answer about compliance and cloud email.

+ Will you secure my information from loss and unauthorized access?

+ Can I run compliance checks when I need to?

+ Do you encrypt data in transit?

+ Are you EU Safe Harbor certified?

+ Are you FFIEC-reviewed?

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

+ Are you HIPAA-compliant?

+ Will you sign a business associate agreement?

+ Can I see your last audit?

There are other compliance issues that are generally not relevant to cloud email (such as PCI compliance, which is for electronic payments). But compliance isn't a gray area, so your provider should be able to answer these questions and show compliance. If they can't, it might make sense to keep looking.

Your Right to Audit

One key point that many companies forget is the right to audit. You should be able to visit the data center with a third-party auditor to ensure the provider is meeting the targets. You should also have insight into the audits (i.e., SOC 2 Type 2 and PCI) the provider has undergone as well as its certifications (i.e., Verizon Cybertrust). You'll also want a bit more than a list of checked boxes; ask your vendor for a due diligence package that includes the actual audit results and financial statements.

Data Protection

How many times in the last few years have we read a story about critical data going missing? In the hands of an unauthorized user, rich stores of data can be a goldmine. The same is true of data in transit with a cloud email provider, so they need to provide data protection.

What to Ask Your Provider

Ask your cloud email provider the following questions:

+ Do you provide granular encryption policy enforcement?

+ Is the encryption process manual or automated?

+ Do keywords or key data trigger encryption?

+ What kinds of algorithms do you employ?

+ How do you handle key management and what's the lifecycle for refreshes?

+ Do you have a third-party key distribution policy?

+ Do you practice a layered approach to data protection?

+ What are your data loss prevention and content filtering practices?

+ How do you handle archiving?

+ What kind of network security monitoring do you have in place?

+ How often do you perform vulnerability testing and how do you conduct it?

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

Spam and Malicious File Protection

Few things are more aggravating than an inbox full of spam. But spam can be more than a mere irritant. It often carries malicious software. And, in the guise of seemingly legitimate offers from real companies, spam can direct unknowing users to a website that silently deposits a malicious file that enlists the victim PC in one of many global botnets. Botnets may sound like something out of science fiction, but they are a real phenomenon.

Don't Panic; Just Ask the Right Questions

Don't panic though. Just ask your cloud email provider the following questions:

+ How do you keep inboxes free of spam?
+ Do you utilize more than one spam detection engine?
+ What kinds of filters do you have in place?
+ Do you provide intelligent monitoring?
+ What is your false positive rate—and what's the impact?
+ What is your false negative rate—and what's the impact?

Mobility and Enterprise Collaboration

Name a businessperson who doesn't carry a smartphone and we'll show you Don Draper. It's not 1966 anymore. Now everyone has a smartphone. Mobility is growing and is a core function for just about every business, so the ability of a cloud email provider to accommodate mobility is critical.

Mobilizing enterprise email is easier than is used to be, but it still requires a staff member to babysit the Exchange or BlackBerry Server—and figure out how to get multiple devices to work with it.

With cloud email there should be no hassles. Mobility should be a no brainer. Click a few buttons and you should be set. But IT should also be able to manage the cloud implementation (or at least certain aspect) from their mobile devices while they're on other business (or the 14th tee on a Saturday morning).

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

Collaboration Shouldn't Miss a Beat in the Cloud

Collaboration via intranet-type functionality and IM that are both connected to the email system is critical for most companies. So it's not something you should abandon or continue to host once you go with a cloud email provider.

Ask the provider the following:

+ Can you support this kind of collaboration in the cloud alongside email? And will it to work seamlessly?
+ Can we control policies from a single point?
+ Can we control consumer (i.e., iOS and Android) as well as traditional (BlackBerry) devices?
+ Can you enforce password complexity?
+ Can you perform remote wipes on devices?

Industry Experience

A provider's experience is a good indication of their capabilities. It's not a guarantee the company will shine when it rolls out your cloud email, but you'd be a fool not to ask a few questions (and expect straight answers).

What to Get from Your Provider

+ Ask for references and talk to them
+ Get case studies of companies like yours, in similar verticals
+ Ask the company how experienced they are with implementations and get examples
+ See what the company's experience is with maintenance

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461

Takeaway

+ Figure out the real costs of your existing email system—and don't underestimate the costs of labor and complexity.
+ Understand whether you'll need to purchase or subscribe to additional levels of security or add functionality such as firewalls, patch management, compliance and archiving.
+ Remember that cloud email can give you more control, not less. Plus, you get to focus on the things you do best.
+ Ensure you can create the right policies for archiving.
+ Get an SLA that spells out everything you should expect from your provider. Don't accept the first copy your provider sends and make sure it is customized to your needs.
+ Ensure you have a "single throat to choke" at the provider.
+ Remember you have a right to audit the provider, including visiting the provider with a third-party.
+ Make sure your provider can give you the data protection you need to keep your data safe and comply with regulations.

About SilverSky

SilverSky is the expert cloud provider of information security solutions. We deliver the industry's only advanced Security-as-a-Service platform that's simple to deploy and transformational to use. For years, SilverSky has been recognized as a leading managed service provider of business email and network security services. We have hosted, secured and monitored the information assets of thousands of large enterprises and regulated businesses utilizing our proprietary security software. By tirelessly safeguarding our customers' most important information, we enable growth-minded leaders to pursue their business ambitions without security worry.

If you would like to learn more, please do not hesitate to call at 800.234.2175 Option #2 or visit our web site at **silversky.com**.

Corporate Headquarters SilverSky 440 Wheelers Farm Road Suite 202 Milford CT 06461