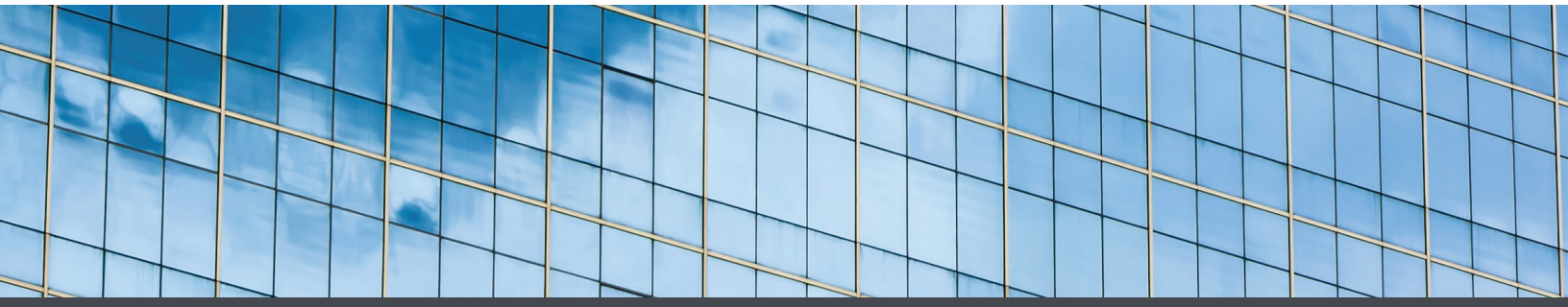


How safe is your email?

If you use a cloud-based email service like Google Gmail or Microsoft Office 365 – or are considering moving to one – it's tempting to believe that all your bases are covered. They take care of the hardware, upgrades, availability, and more, so that email "just works" without any of the headaches and hassles of on-premises software.

Microsoft, Google, and their competitors, of course, do what they can to foster this illusion. But don't be fooled: the promise of an email "one stop shop" is, in fact, an illusion – and falling for it may put your business at serious risk. When your business' security and reputation are on the line, you can't afford to compromise on email protection.

CLOUD-BASED EMAIL: VULNERABILITIES AND RISKS

No software solution is perfect, no matter where it lives. If you used to run Microsoft Exchange on-premises, for instance, there is a very good chance that you enhanced its performance with third-party add-ons to meet your specific needs around security, monitoring, backup, etc. Cloud-based products are no different, and require the same level of attention, but administrators often assume that everything they need is built-in.

That is decisively not the case. Let's look at three ways that cloud-based email can introduce risk into your organization and how Aurea Messaging Solutions can help.

Security

Every business is concerned about cybersecurity – rightfully so – but not every organization takes the necessary steps to protect itself. The question is not "if" but "when": you will have a security breach at some point, in your own data center or via one of your cloud services. When it occurs, will you be ready?

While major cloud email providers certainly take security seriously and have a variety of protection mechanisms in place, they simply cannot account for every type of attack. Microsoft's and Google's developers may move fast, but hackers are faster. From the basics like spam and malware to incredibly sophisticated threats like phishing, impersonation, ransomware, DDoS, and more, the number, complexity, and severity of attacks increase every day.

SECURITY:
All your eggs in one basket: The problem with a security monoculture

Further, the big vendors are prime targets for the most dramatic of these attacks. Breaching Microsoft or Google provides huge bang for the bad guys' buck, and they only have to figure it out once to impact millions of users. Both solutions operate as a security monoculture: a multi-tenant email solution monopoly backed by a single security solution code base designed to protect every tenant. This is akin to putting all of your security eggs in one, very large basket – never a good idea.

Protection from these attacks isn't automatically included in every email plan, either. While your email plan likely contains basic anti-spam and anti-malware coverage, safety from more recently discovered or involved threats often comes as an

add-on. These add-ons, although helpful (if you know to ask for them), come with their own trade-offs. They increase your total cost of ownership and can also diminish performance. Microsoft's Safe Attachments feature, for instance, puts attachments into a "sandbox" to ensure that they're safe. This can delay receipt of the email by as much as 30 minutes.

EMAIL SECURITY FROM AUREA MESSAGING SOLUTIONS

Es

Email Security from Aurea Messaging Solutions (AMS) adds a powerful layer to your email system for complete, trustworthy protection. Like Gmail and Office 365, AMS is cloud-based with no upfront hardware or software costs, virtually no maintenance, and it can be deployed in days. When you combine Email Security from AMS with your cloud-based email platform, you essentially eliminate the risk of inbound and outbound threats, providing comprehensive protection against spam and viruses and industry-leading uptime guarantees.

Email Security from AMS is your backup plan when – not if – your primary email system comes under attack. It fully protects your organization with features like:

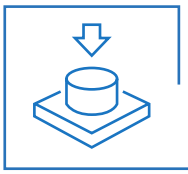
- **Inbound and outbound antivirus protection:** Antivirus engines offer double scanning of all incoming and outgoing email and automatically update to minimize management while maximizing protection.
- **Multi-layered spam analysis:** A comprehensive layered approach ensures the highest continuous levels of spam detection accuracy. These include Sender Policy Framework (SPF) and recipient verification; SURBL and RBL validation; and keyword, header and body text analyses. Email Security from AMS also integrates customized scoring algorithms which deliver an overall per-email score to determine if each message is safe.
- **End-user spam management:** With Email Security from AMS, you can delegate daily spam management. End users have full visibility to all blocked email and can release required email without having to resort to the company helpdesk.
- **Comprehensive reporting suite:** Gain real-time access to graphical reports to keep email secure and under control. Reports include top spam recipients and senders along with full search capabilities to get a deeper understanding of issues affecting your enterprise email.

Email Security from Aurea Messaging Solutions essentially eliminates the risk of inbound and outbound threats, including comprehensive protection against spam and viruses and industry-leading uptime guarantees.

Archiving

Once a nice-to-have, stored on tapes never to be seen again, archived data has recently become a major organizational concern. From law firms to healthcare orgs to small businesses – for legal, regulatory, or compliance reasons – reliable eDiscovery, assured data retention, and point-in-time recovery are now a critical part of your email operations.

Solutions like Office 365, however, aren't built for serious archiving. The on-premises version of Exchange relies on third-party solutions for enterprise-grade data archiving and so does its cloud cousin. The solution offers a weak built-in archiving feature as well as some add-ons targeted towards legal use cases, but none of these band-aids come close to supporting the data archiving needs of the modern enterprise. They do, however, bog down your infrastructure with inefficient storage that not only struggles with availability and accessibility but also adds a significant performance burden.



ARCHIVING:
Enterprise-grade archiving not included: When band-aids aren't enough

Perhaps most importantly, if Microsoft or Google faces a data loss situation in their data center(s), they do not offer point-in-time recovery. This is, and should be, a deal-breaker for many businesses. If you're facing a lawsuit or an audit, you can't risk the security, availability, and integrity of your archived data.

EMAIL ARCHIVAL FROM AUREA MESSAGING SOLUTIONS

Ea

Email Archival from Aurea Messaging Solutions addresses these challenges and more. Built as a best-of-breed long-term storage solution for the Microsoft environment (either on-premises Exchange or Office 365), it combines continuous archiving of all your email messages and attachments with fast, comprehensive search and discovery. And because it's SaaS, Email Archival from AMS frees IT from managing additional systems and storage while providing true enterprise-grade data archival services.

What makes Email Archival from AMS different from the big vendors' out-of-the-box archiving features?

- **Scalable, secure cloud storage:** Email Archival from AMS is built on Amazon Web Services (AWS) and takes full advantage of the capabilities that make AWS the most reliable, secure, and dominant cloud platform in the world.

Archived email is also stored with customer specific encryption to ensure the highest security standards.

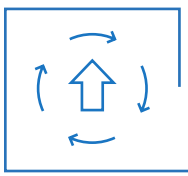
- **Flexible retention policies:** Set as many retention policies as you need to meet compliance and business needs. Email Archival's flexible retention criteria ensure policies can be as granular as required. Legal hold capabilities let you identify messages that shouldn't be purged at all, and with our long-term retention capabilities, you can even continue to archive emails previously deleted from user accounts.
- **Attachment stubbing:** Email Archival from AMS can stub-out attachments based on age, size, file type, and more. Stubbing policies can also be associated with users, mailboxes, and groups. This massively reduces storage requirements by up to 80%.
- **Import historical email:** Securely upload pre-existing email using the import manager application, which can be easily installed and accessed with any internet connection. With its managed import service, Email Archival from AMS also enables and simplifies large bulk imports.

If you're facing a lawsuit or an audit, you can't risk the security, availability, and integrity of your archived data.

Business Continuity

The third use case where cloud-based email solutions typically fail is business continuity. Whether Microsoft, Google, or another vendor, no matter how many 9s are in their guaranteed uptime, all cloud services will at some point go down. It's up to you to ensure that you have a backup in place when they do.

What if a hurricane or other natural disaster hits? What if hackers launch a DDoS attack? What if maintenance or migration issues shut down the system? As services like Gmail and Office 365 become de facto for businesses, they also attract more risk. If your email system is brought down by Mother Nature, user error, or more insidious human agents, you need to ensure that your business can return to productivity as quickly as possible.



BUSINESS CONTINUITY:
Will offline email put your business on the line?

It's worthwhile to consider the cost and impact of downtime:

- 72% of companies will experience unplanned email outages in a year.
- IT downtime reduces companies' ability to generate income by more than 22% annually.
- Companies lose about 300,000 hours annually through unplanned downtime.
- 54% of companies have experienced downtime from a single event lasting more than 8 hours.
- Information and communication technology downtime costs North American organizations $700 billion per year, largely through lost employee productivity.

Given these facts, an email business continuity solution begins to seem not only worth it, but like a bargain.

EMAIL CONTINUITY FROM AUREA MESSAGING SOLUTIONS

Email Continuity from Aurea Messaging Solutions delivers always-on failover for instant, reliable, and secure access to your email during a planned or unplanned outage. It enables users to send and receive email through mobile devices, web browsers, or Microsoft Outlook – and can be activated in less than 60 seconds. That means that no matter what happens, an email outage will never shut down your business.

How does it work? As email is sent and received, a copy of each file is compressed, encrypted, and transmitted to the AMS cloud for secure storage. When an outage strikes, Email Continuity from AMS can be activated in seconds for full access to recent and incoming email, contacts, and calendar entries.

Additional features and benefits include:

- **Fast failover, completely under your control:** Users can continue to send and receive email, while IT staff focuses on restoring primary systems. With Email Continuity from AMS, users have complete access to email, calendars, contacts and distribution lists, even during an outage.
- **Seamless mobile access:** Automated failover ensures that users don't even realize the switch. During a primary system outage, employees using Apple and Android mobile devices can continue to send and receive messages without interruption.
- **Automatic reconciliation:** Easily reconcile all activity completed during an outage after the event is resolved.

Your primary system remains completely up-to-date with sent and received email, including timestamps and read/unread status.

- **Intuitive Outlook integration:** Seamlessly switch users to the backup email system upon activation, making outages virtually invisible.
- **Total data-loss prevention:** Ensure 100% data-loss prevention in your email environment. Unlike high-availability solutions based on replication, clustering, vaulting and log shipping, AMS is not vulnerable to database corruption. If messages are ever lost or corrupted in the primary email system, you can easily locate and restore the missing messages.
- **Right-sized and cost-effective:** Manage costs by controlling the amount and duration of email history stored in user backups, so you can ensure high data continuity at the lowest possible cost.
- **Enhanced security:** Because Email Continuity from AMS is built on Amazon Web Services (AWS), users benefit from increased performance, scalability, built-in redundancy, and lightning-fast disaster recovery.

Conclusion

Cloud-based email platforms like Microsoft Office 365 and Google Gmail offer a variety of benefits over traditional on-premises systems. They can be excellent solutions for organizations looking to streamline operations, cut downs, and/or scale their business.

Cloud-based email, however, isn't perfect or all-encompassing. Like their on-premises predecessors, these platforms come with meaningful gaps and vulnerabilities that should be ignored at any organization's peril. They are powerful tools with critical risks that can only be addressed by a true enterprise-grade email continuity, archiving, and security solution.

With Email Continuity from Aurea Messaging Solutions, no matter what happens, an email outage will never shut down your business.

Learn more about how Aurea Messaging Solutions helps protect your organization with targeted solutions for all of your email needs.

Aurea

AMS Email Archival >

AMS Email Continuity >

AMS Email Security >