CANON SOLUTIONS AMERICA

WHITE PAPER

EMAIL SECURITY FOR LAW FIRMS WITH CLOUD STORAGE AND MXHERO

SMART CHANGE STARTS HERE.

CANON SEE IMPOSSIBLE

How best of breed cloud content storage with mxHero Mail2Cloud can help secure every email sent by your firm—in one hour!

> “May you live in interesting times” *- **Ancient Chinese curse***

Law firms are living in interesting times. With near total reliance on email, one of the least secure and hardest to manage technologies, firms face the multifaceted challenges of protecting information entrusted to them by their clients, strict observance to an increasingly stringent regulatory environment, and the rapid rise of cyber-attacks targeting law firms as “soft targets.” As if this weren’t enough, legal firms need to contend with significant internal resistance to change and new ways of working.

The good news is all is not lost. A combination of emerging technologies provides a surprisingly easy solution for many of these challenges. By combining best of breed technologies, law firms are able to not only mitigate many of the aforementioned challenges but also surpass the value single-point solutions have been able to provide up to today. Several years ago, mxHero predicted that the emerging class of powerful cloud content management platforms, led by Box, would be the future of content management and collaboration. Based on industry trends over the last several years, their vision seems prophetic. By connecting existing email systems with leading cloud storage (e.g. Box™, Egnyte®, OneDrive™, or Google Drive™), mxHero Mail2Cloud is able to present an innovative solution that has resonated with the legal vertical, whether that be law firms or legal business units within larger organizations.

> “Last year was the year of law firm hacks. *Law firms are soft targets*; this is the world we are living in.”
>
> ***- Andrew Tannenbaum****, IBM’s Chief Cybersecurity Counsel*

mxHero Mail2Cloud and Cloud storage is the perfect platform to achieve new levels of email security without requiring significant implementation investment or effort towards end user adoption.

EMAIL IS NOT SECURE

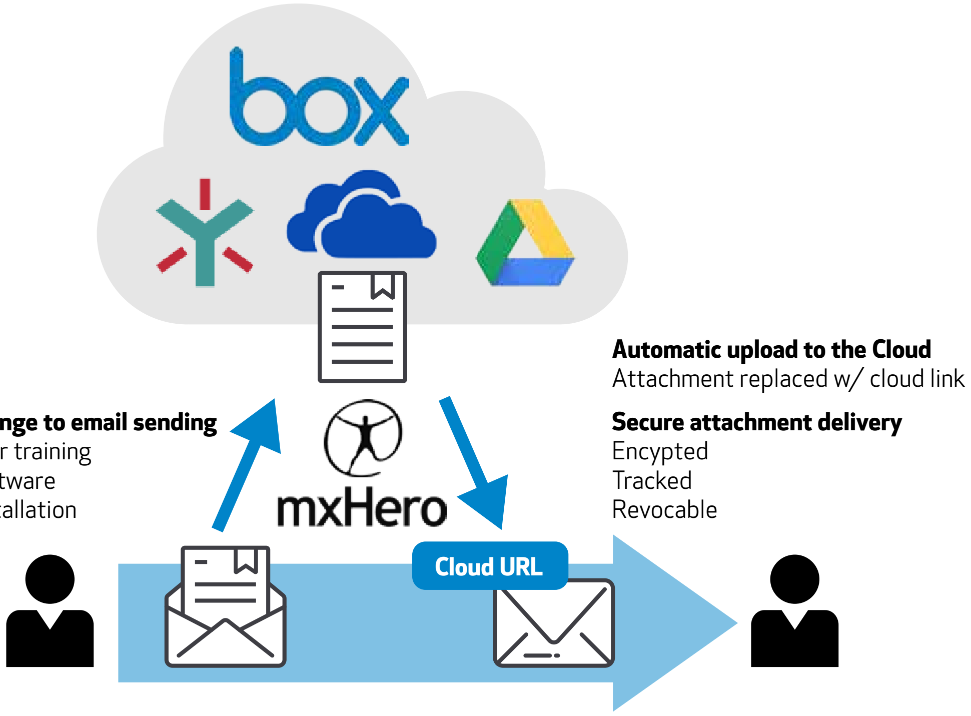
Admittedly the bar for email security is not high. Native email sends full, unencrypted copies of attachments to anyone (even accidental recipients) without any downstream protections. Once delivered, the sender has no visibility or control over what happens with files sent through email—are they opened? If opened, when and by whom? Have the attachments been forwarded? Where was the recipient when they opened the files? Furthermore, no easy option exists to revoke access once an email attachment has been sent.

> “Email was built for a different time, one in which cyber threats were few and far between. It should come as no surprise that email is the number one threat vector facing organizations today.”
>
> ***- Chris Ross****, SVP - International at Barracuda*

CLOUD STORAGE IS SECURE

By contrast, content uploaded to cloud storage and delivered as a cloud storage link is secure. Files distributed through cloud storage are delivered over encrypted connections that in themselves can require authentication, be automatically revoked, and contain restrictions on download, deletion, and alteration. Furthermore, any action over a file in enterprise class cloud storage services, like Box, are fully tracked with detailed audit trails.

By replacing email attachments with shared links to files saved in the cloud, a firm instantly benefits from a more secure delivery and control over its attachments. No longer are the firm's emails "soft targets." A hacker accessing an email that has cloud storage links is denied immediate access to content he or she would have enjoyed if there had been traditional attachments.


box
mxHero
Automatic upload to the Cloud
Attachment replaced w/ cloud link
Secure attachment delivery
Encypted
Tracked
Revocable
No change to email sending
No user training
No software
No installation
Cloud URL

BUT WE HAVE ALWAYS DONE IT THIS WAY…

If you are like most people reading this, you're probably thinking, "Of course, adopting a secure technology like Box would greatly improve the security over a technology like email that has no security, but let's be real, old habits die hard."

If you agree with the above statement, you are absolutely correct. Even though sending an attachment as a cloud link is simply a matter of copy & paste, that is an extra step and an extra step that might be hard to do in certain contexts, like on a mobile phone (copy/pasting between phone applications with your thumb isn't fun). Furthermore, users already must deal with too much complexity in their work; why ask them to learn new tricks and jump through more hoops?

COMBINING CLOUD SECURITY AND EMAIL ATTACHMENTS WITHOUT USER EFFORT

Recognizing the reality that additional steps needed to leverage a powerful content security technology are unlikely to be easily adopted, mxHero developed a seamless process that automatically exchanges email attachments for secure cloud links. The process is completely systemic, requiring no effort by the end user, nor any software installation on the user's devices. Whether sending an email from their laptop or mobile phone, mxHero will ensure that attachments are stored to the cloud and automatically delivered as secure links. Finally, for recipients, the links are easy to follow and do not require special software to access file content.

Hermetically Sealed Protection
Full email domain protection
Centrally controlled
Always-on security
All device

At the flip of a centrally controlled switch on mxHero's dashboard, every email sent from the law firm is protected. The type of cloud storage protection, whether requiring authenticated or self-expiring access, is easily configured by the firm, which helps to ensure the appropriate security gets applied depending on the file's content and context. For example, email attachments sent internally can be automatically set to "organization access only," thereby allowing for easy access to the content by employees but denying access to files in the event an email gets forwarded outside the organization or if an attorney misplaces their mobile device.

BEYOND SECURITY, LET'S LOOK AT COMPLIANCE

Beyond ensuring that content is delivered securely by replacing attachments with cloud links, firms will be aided in their compliance efforts around regulations like HIPAA that stipulate that PHI need be delivered via encrypted channels. Content saved in the cloud is always delivered through HTTPS encrypted links. With mxHero helping to ensure that all attachments are accessed securely from the cloud, inadvertent transmission of sensitive HIPAA regulated files via email is no longer a risk.

OTHER BENEFITS

What is so powerful about this solution is the simplicity of the model, the ease of end user adoption, the immediacy of deployment (1 hour in most cases) and the meaningful, positive impact on overall security. Of course, security, governance, and compliance are only some, albeit important, benefits of content saved in the cloud. To the degree that content moves out of hard-to-manage email and into powerful Cloud Content Management (CCM) platforms, the firm benefits from greater productivity powered by the potential of workflow automation, artificial intelligence, machine learning, eDiscovery, boundary system integrations, and expansive innovation tools all powered by their cloud storage service. mxHero provides the non-user impacting technology pathway between email and cloud content storage. It's the future of work and will drive the next wave of digital innovation for the law firms and the legal business units of tomorrow!

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

Neither Canon Inc., nor Canon U.S.A., Inc. nor Canon Solutions America, Inc. represents or warrants any third party product or feature referenced herein.

Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment.