Managing Security for a Hybrid Workforce

A Guide to Ensuring Email and File Protection Across Platforms

The modern workforce is hybrid in almost every sense of the word:

- In-office and work-from-home
- Mac and PC
- Google and Microsoft
- Desktop and mobile
- Employee and contractor
- Work and personal devices
- On-prem and cloud-based

Meanwhile, enterprise technology ecosystems are becoming increasingly complex: A 2021 report from Okta found that its average customer deploys 88 distinct applications, with tech companies averaging 155 apps.

Perhaps the most ubiquitous kind of enterprise application is email, with the average employee sending over 10,000 emails every year. With so much data flowing in and out of your organization, it's critical to safeguard the data that's shared, whether via email or a collaboration application.

How can technology leaders protect the sensitive data being shared across dozens, or even hundreds, of applications and platforms? This guide will help you examine your holistic security strategy across users, platforms, and apps to help you sustainably safeguard your organization's most important data.

Complete Security Strategy

- **Protect the data, not just the perimeter.** Because the modern workplace involves extensive collaboration, multi-cloud environments, and many different people and systems interacting with a network at any given time, protecting the perimeter alone is no longer enough. By protecting the data itself, it can move more freely across recipients and systems while still remaining secure.

- **Select a flexible tech stack that supports interoperability and data-centric security.** Flexibility and interoperability should be key priorities for those managing a hybrid workforce. Ensure your security solutions support a range of platforms and user configurations. A key benefit of a data-centric approach to security is that it sets you up for greater flexibility in the future. Evaluating your tech stack vendors and partners through the lens of data-centric security may lead you to make different decisions, and ultimately you will optimize those partners who will give you full control of your own data, throughout its life cycle.

- **Prioritize data by sensitivity.** Not all data is created equal. Do an analysis and audit of the types of data you are entrusted to protect, and gauge what your most critical data assets are. Determine whether the methods you use today provide you with the visibility of who the data is being shared with and how the data travels. Once you do, ensure that you are adequately safeguarding that data.

- **Manage identity.** Take a Zero Trust approach to all network traffic (whether devices or people): Never trust, always verify. Ensure you're using a strong method of authenticating users and devices, ensuring they are who they say they are. Better yet, connect identity to attribute-based access controls to validate those accessing vital data.

- **Govern access.** Not every employee needs access to your most sensitive data. Examine whether those with the greatest access actually need that level of information to effectively do their job. Revisit access regularly, as roles, projects, and responsibilities can shift and evolve. If someone no longer needs access to your most vital, sensitive data, revoke their access to mitigate risk.

- **Ensure you have granular audit and visibility.** Closely monitoring the flow of information into and out of your organization requires you to have both a holistic and detailed view of what's being shared, by whom, and when. A 2020 Tessian report found that, for organizations with more than 1,000 employees, the average IT leader estimated 720 unauthorized emails were sent every year. However, Tessian found an average of 27,500 unauthorized emails were actually sent: 38 times more than estimated. Ensure you have visibility into where data is traveling and how it's being accessed—as well as the ability to take action on that data at any time.

- **Build breach readiness.** In case of a breach or incident involving your data, you want to be able to act quickly. Take, for example, the 2021 Microsoft Exchange Server attack, where thousands of organizations had to wait for a software patch to secure their systems. If those organizations were hosting and managing their own encryption keys and policies according to a Zero Trust framework, they could immediately take action by rotating the keys, mitigating data loss and "stopping the bleeding" until a patch was developed. Additionally, these attacks are not one-time incidents: It can take months to assess the damage and ensure systems are appropriately secured.

- **Evaluate the supply chain.** Regardless of your industry, data needs to be shared across a supply chain. That supply chain can be physical (such as manufacturing, retail, or ecommerce), or digital (including your business partners, investors, or technology vendors). Often the nature of this shared data is sensitive—related to financial information, intellectual property, or business agreements. Ensure that data can remain under your control, even after it's been shared.

Email and File Protection Best Practices

- **Protect emails and attachments with end-to-end encryption.** Whether your users are using Microsoft 365 Outlook or Gmail (or a combination of both), you want to ensure that emails and their attachments are fully encrypted from end to end—in transit, in use, and at rest—and across the entire lifecycle of the data, from creation to sharing and beyond. While many organizations think that native email security is enough to protect their data, this is not usually the case—and this is especially true for highly regulated industries.

- **Ensure compliance with industry regulations.** For industries with specific data protection regulations, such as healthcare (HIPAA), law enforcement (CJIS), education (FERPA), and manufacturing (ITAR), it's critical that the data shared via email is adequately secured, so you don't compromise sensitive data or incur noncompliance fines—civil fines for an ITAR violation can total $1 million, and a GDPR violation can cost as much as €20 million (or 4% of annual global revenue from the preceding financial year, whichever is greater). Evaluate whether your data protection solutions offer the level of security and granularity you need to meet these requirements.

- **Optimize for consistency across platforms.** You want both your Gmail and Microsoft 365 Outlook users to have consistent, thorough controls that equip them to protect the data they're sharing. Ensure that the email protection solutions you adopt don't present any security gaps across different users in your organization. Also examine any differences in user experience across devices, platforms, or interfaces (such as browser vs. desktop) to ensure seamless deployment across teams.

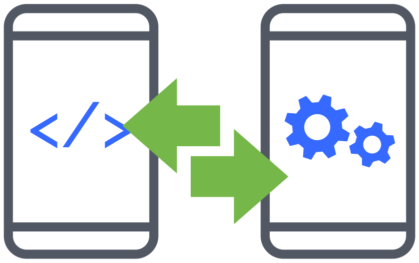
- **Use access controls to ensure business privacy.** Different types of data have different privacy needs. Ensure that your administrators and end users alike have the access controls they need to manage access to shared data, including the ability to revoke access, restrict sharing/forwarding, and watermark sensitive documents.

- **Select tools that are easy to use (and therefore more likely to be adopted).** Security solutions are only effective if they're actually being used, so you want a solution that makes it simple and seamless for users to protect the data they're sharing. Understand whether an email protection platform requires users to take additional steps, remember specific keywords, or navigate to another application.

- **Host your own encryption keys.** For total control of your data—whether it's hosted on premise, in the cloud, or a combination of the two—ensure that you have the option to manage your own encryption keys separately from your data. By doing this, you ensure that none of your vendors, and not even your cloud provider, can access encrypted information. For organizations that need to maintain data sovereignty, this is essential.

- **Set Data Loss Prevention (DLP) rules.** Every organization needs a safety net for human error, and DLP rules enable you to detect and automatically encrypt sensitive data before it's shared. Look for solutions that give you granular controls over DLP rules and that allow you to continuously adjust, tailor, and monitor those parameters in ways that best serve your organization.

Data Sharing Platforms and Other Applications



- **Secure your collaboration apps (such as Google Drive).** Often, colleagues and partners will collaborate using shared documents on platforms such as Google Drive. Ensure that shared documents remain protected as they're created, edited, downloaded, and shared.

- **Safeguard SaaS apps that intake and disseminate data.** Don't forget about securing email and files that are transmitted through SaaS applications such as Salesforce, Zendesk, Workday or any other application that is used to communicate with your consumers, partners or employees.

About Virtru

Virtru is a global leader in data security and privacy. Virtru's email encryption for Google Workspace (Gmail and Google Drive) and Microsoft 365 Outlook complements and enhances your native email experience with the secure, data-centric protection you need. Virtru also offers encryption for enterprise SaaS apps like Salesforce, SAP, Zendesk, and Workday. Whether you're in a highly regulated industry like healthcare, manufacturing, or government that requires meeting compliance needs—or you want to safeguard customer and company data from the escalating number and frequency of data breaches, Virtru can help you ensure your data is protected everywhere it's shared.

Learn how Virtru can help protect your organization's data, everywhere it's stored and shared. Contact us to schedule a demo. virtru.com/contact-us

virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection.