January 2017

Ensuring Secure Endpoint Content Collaboration in the Cloud

How do you ensure secure endpoint, email and document collaboration in the cloud?

Pervasive Threat of Document Leakage

Balancing the need for document/file sharing and collaboration with enterprise security and control to protect information against breaches, non-compliance, hacks and intellectual property theft from any mobile or desktop device represents the most significant challenge for organizations of all sizes in all industries in today's digital-centric, mobile society.

Public cloud services deliver a solution for anytime, anywhere collaboration—half of the equation. They provide the ability to collaborate on the go, but without a private key, they don't provide secure collaboration—the second half of the equation. According to a Gartner survey, "security/privacy" concerns continue to be the major reason why organizations choose not to adopt a public cloud service[1]. As the capabilities and boundaries of networks expand with new device platforms and increasingly complex applications, the number of pathways susceptible to unauthorized access to information continues to increase. With the new normal requiring mobile access and collaboration inside and outside the enterprise, secure collaboration through a private cloud is a top priority.

The risk level for email and document leakage is very high due to the deployment of public cloud services and the trend of "Bring Your Own Device" (BYOD) to the office, and everywhere. The ability to protect against data attacks and employee mistakes is mission critical. The challenge is how to secure email and documents in the cloud—anytime, anywhere, on any device and any platform, and anyone-to-anyone.

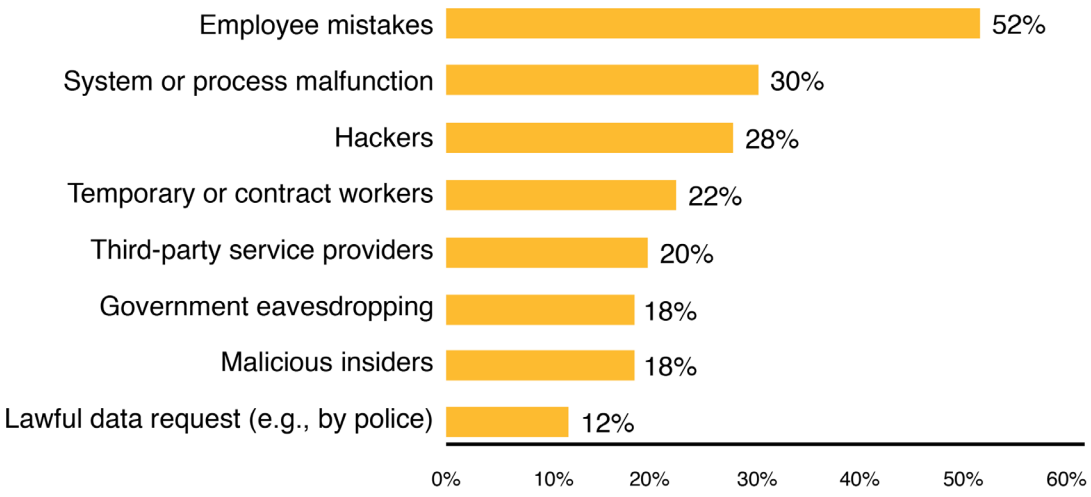
[1]Deshpande, Sid; MacDonald, Neil; Lawson, Craig. "Emerging Technology Analysis: Cloud Access Security Brokers", Gartner (September 2014)

Proliferation of Data Breaches and Hacks

Several recent studies have confirmed the rise in security and data breaches over the last few years. Two 2016 Ponemon Institute reports reveal current data breach costs and trends.

- Cost of Data Breach Study: Global Study
  - Average cost of each lost or stolen record with sensitive and confidential information is $221 in the U.S.
  - Average worldwide cost is $158 per record—a 29% increase since 2013
  - 26% probability for a company data breach involving 10,000 lost or stolen records
- Global Encryption Trends Study
  - Employee mistakes identified as most significant threat to sensitive data (see Figure 1)

Figure 1. Most Salient Threats to Sensitive or Confidential Data



Source: 2016 Poneman Institute Global Encryption Trends Study

Data breach and hacking threats are driving the need for robust content protection and compliance with regulatory standards. Almost every day, the news is filled with headline-making, data-breach incidents including WikiLeaks, LinkedIn, Target, and Sony. With persistent email and document protection at rest, in transit, and in use, incidents like these would not have occurred:

- The hacking of the Democratic National Committee in 2016 and the release of confidential emails to the public.
- The copying of thousands of classified NSA documents by Snowden in 2013 without prior authorization.
- The downloading of 250,000 classified government documents smuggled out of the office in a CD case Corporal Manning titled Lady Gaga in 2010.
- The data breach in the Veterans Affairs (VA) Department in 2006 when a VA employee took home records of more than 26 million veterans on a laptop PC, which was subsequently stolen.

To prevent another breach of any type, VA took immediate action by setting restrictions—providing only the author of the content or someone given full-control permission to the content the ability to remove the persistent protection from emails, attachments and documents. To provide this high degree of security safeguarding against data leakage, VA was an early adopter of email and document security using in-use protection on mobile devices and desktops with GigaTrust—and has not experienced a breach since.

The GigaCloud Solution

GigaCloud™ is GigaTrust's new SaaS (Software as a Service) offering providing secure document protection—delivering email and document collaboration services anytime, anywhere, on any device and any platform with real-time data analytics, reporting and administrative tools. GigaCloud is the first and only secure email and document protection, consumption, and collaboration service that is an easy-to-use, easy-to-deploy cloud service powered by the Microsoft – Active Directory Rights Management Services (AD RMS) security ecosystem. A soon-to-be-released Linux OS interface (beginning 2Q '17), will deliver scalability and broad device support to open, view and persistently protect documents at all times no matter where they are stored. This is why GigaTrust was not included within Gartner's Market Guide for Cloud Access Security Brokers (CASBs) published in October 2016 and herein included in this newsletter.

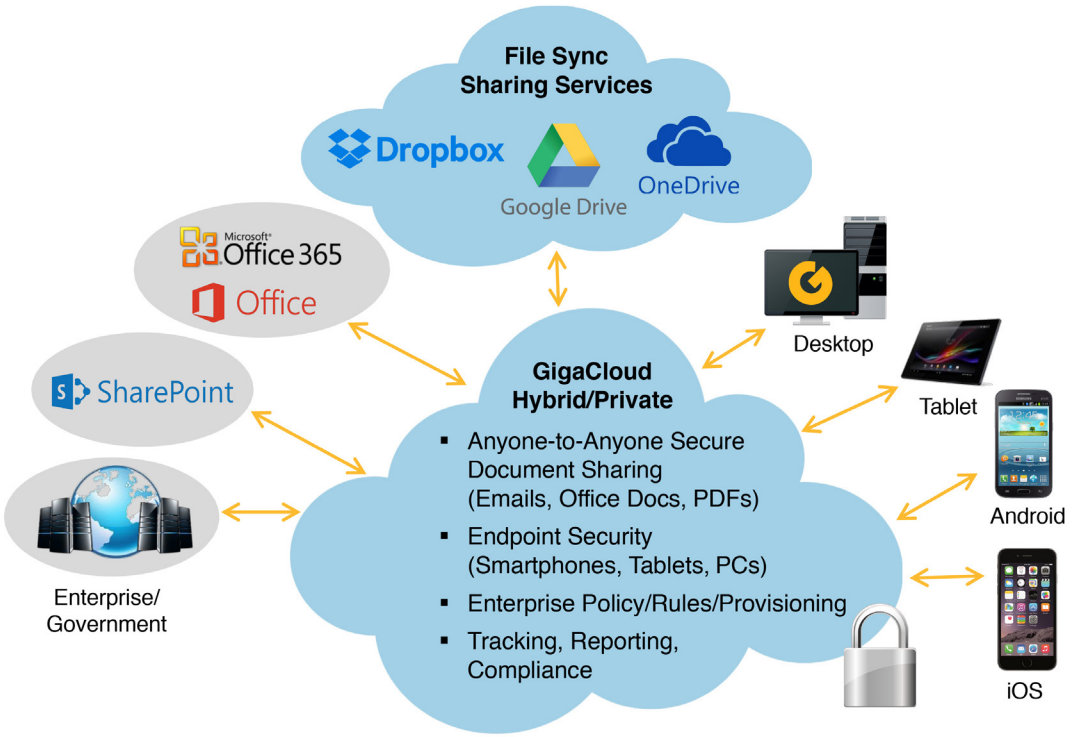
GigaCloud offers the following configuration: a fully managed SaaS solution hosted in Microsoft Azure, as well as on-premises, such as Azure Stack, Hyper-V, etc. and cloud installations in Microsoft Azure and other public clouds.

The GigaCloud service provides a secure email and document collaboration platform for enterprises and government organizations with protection that persists for the content's entire lifecycle. GigaCloud delivers optimum document protection by providing secure collaboration through a private key delivering full control on who can print, forward or edit information. It applies and enforces security permissions (or rights) down to the digital content (emails, documents, pictures) level, resulting in content being

protected from misuse while at rest, in transit, and most important, in use—even when opened by any permitted recipient—on any mobile device or PC, and is always synchronized. GigaCloud, with the Linux interface, allows for easy integration with CASBs, thus providing a more comprehensive threat protection, data security, and compliant solutions by including in-use protection directly on mobile devices and PCs. This will allow for GigaCloud, in addition to Windows Server, to be integrated with any of the Linux-based CASB providers listed herein the Gartner report presented in this January 2017 newsletter.

The prevalence of the current BYOD environment has driven adoption of in-use protection to secure documents created and consumed outside the firewall. Built into GigaCloud, subscribers avoid the burden of setting up this costly infrastructure and the complexity of managing it and with the ability to enroll online, reduce the time and capital requirements of traditional deployments, with service available immediately to all users.

Figure 2. GigaCloud Service



Source: GigaTrust

Mobile and Desktop Protected Content and Collaboration

GigaTrust enables secure anyone-to-anyone collaboration whether inside or outside an enterprise's network on any device. No matter where content travels, it is persistently protected—on smartphones, tablets, PC laptops and traditional Windows desktops. GigaTrust provides support for Microsoft Office or Microsoft Office 365 cloud subscribers with a comprehensive security solution for native Microsoft Office documents and PDFs and additional file formats through our mobile solution for Android and iOS devices and Windows OS, providing decryption keys and allowing users to consume and protect confidential information anywhere, anytime, to anyone.

Android and iOS GigaTrust apps are available to download free from the Google and Apple app stores and the Desktop Client is available from GigaTrust. Users only have to install the GigaCloud endpoint security software and they are up and running.

Endpoint Security for Persistent Protection

GigaCloud includes a suite of patented security content management services that provides the benefits of encryption plus the ability for authors to control the use of assets—even after they have been delivered and opened. It meets enterprise document security requirements for external cloud-based file sync and sharing integration services including Dropbox, OneDrive and Google Drive and secure document management systems such as SharePoint®. It also enables secure anyone-to-anyone collaboration with persistently protected content—keeping sensitive data private with the security protection invoked staying with the content—no matter where or how it travels. System administrators can be alerted of potential security breaches. Data OverWatch analytics provides tracking, monitoring and compliance reporting.

Governance and Compliance

Within the enterprise, governance is based on the establishment of Acceptable Use Policies (AUPs) that pertain to the organization's content and information technology only, and compliance relates to government

Figure 3. GigaCloud Service Offering

PRODUCTS	GIGACLOUD PRIVATE i.e., Azure Stack	GIGACLOUD HYBRID Azure	SELECT PRODUCT FEATURES
Mobile Solutions (Android, iOS apps)	✓	✓	Protects/Consumes/Edits native Microsoft Office documents, PDFs, emails, text and images
Desktop Client	✓	✓	Protects/Consumes/Edits native Office documents, Adobe PDFs, emails, text and images, Policy Management, Rules, Automatic/Manual Protection
Data Overwatch	✓	✓	Endpoint Security Device Tracking (mobile and desktop), Monitoring, Auditing, Alerts and Data Analytics Services
Enterprise Policy Service	✓	✓	Policy Management, Rules, Automatic Protection

Source: GigaTrust

regulations. GigaCloud provides for policy delegation, management, distribution and assignment to integrate people, content and policies. It can manage and distribute corporate security policies enterprise-wide, down to the individual mobile device or desktop. The organization's administrator or delegated department-level administrators can control administration, policy creation and content management based on template rules. With GigaCloud, organizations can securely and persistently manage content both inside and outside the enterprise supporting corporate governance and compliance.

Find out how GigaCloud can secure your emails and documents with our 30-day free trial. Call (866) 868-7878 now to get started. It's too risky to wait another minute.

GigaTrust's flagship service, GigaCloud, delivers secure, persistent email and document collaboration for Android, iOS and Windows OS devices anytime, anywhere, anyone-to-anyone.

Source: GigaTrust

About GigaTrust

GigaTrust is a leading provider of endpoint security and document in-use protection for Windows, iOS and Android devices, offering fully managed SaaS solutions hosted in Microsoft Azure, as well as on-premises and hybrid cloud installations. GigaTrust is the largest and oldest provider that enhances and extends Microsoft's Rights Management Services (RMS) content security solution. Customers rely on GigaTrust's innovative next-generation content security technologies, combined with ease of use and deployment, to enable intellectual property protection and confidentiality.

The company's flagship offering, GigaCloud™, delivers secure email and document collaboration services anytime, anywhere, on any device and any platform with real-time data analytics, reporting and administrative tools. It applies and enforces security permissions down to the digital content level, protecting content from misuse throughout the entire lifecycle——while in transit, at rest and, most importantly in use, even when opened by any permitted recipient. GigaCloud is available in a secure private cloud configuration for enterprises and government entities requiring added security features and administrative control. For more information about GigaTrust, visit www.gigatrust.com.

Contact us

(866) 868-7878 (Sales)
sales@gigatrust.com