SOLUTION OVERVIEW

GigaCloud™ for DoD Supply Chain

Protecting Controlled Unclassified Information (CUI)

The clock is ticking on the latest cloud compliance mandate: NIST Special Publication 800-171, otherwise known as DFARS (Defense Federal Acquisition Regulation Supplement). Any organization or contractor that holds or processes unclassified Department of Defense (DoD) data must ensure that they comply with this new DFARS clause.

December 31, 2017 is the final deadline by which to prove compliance—so action is recommended as soon as possible.

Organizations working with the DoD are already used to applying stringent controls to systems that manage classified data, but with DFARS guidance this now extends to unclassified systems that are owned, operated by a contractor that process, store, or transmit covered defense information. This can have wide-reaching consequences for the contractor who now must extend the security controls across a larger number of systems than in the past.

This mandate is designed to protect sensitive government information from being destroyed, compromised, or stolen while residing in or transiting through Information and Communication Technology (ICT) systems as it's shared between federal agencies and vendors. This mandate applies to organizations that create, process, store or transmit CUI, or that provide security protection for these components.

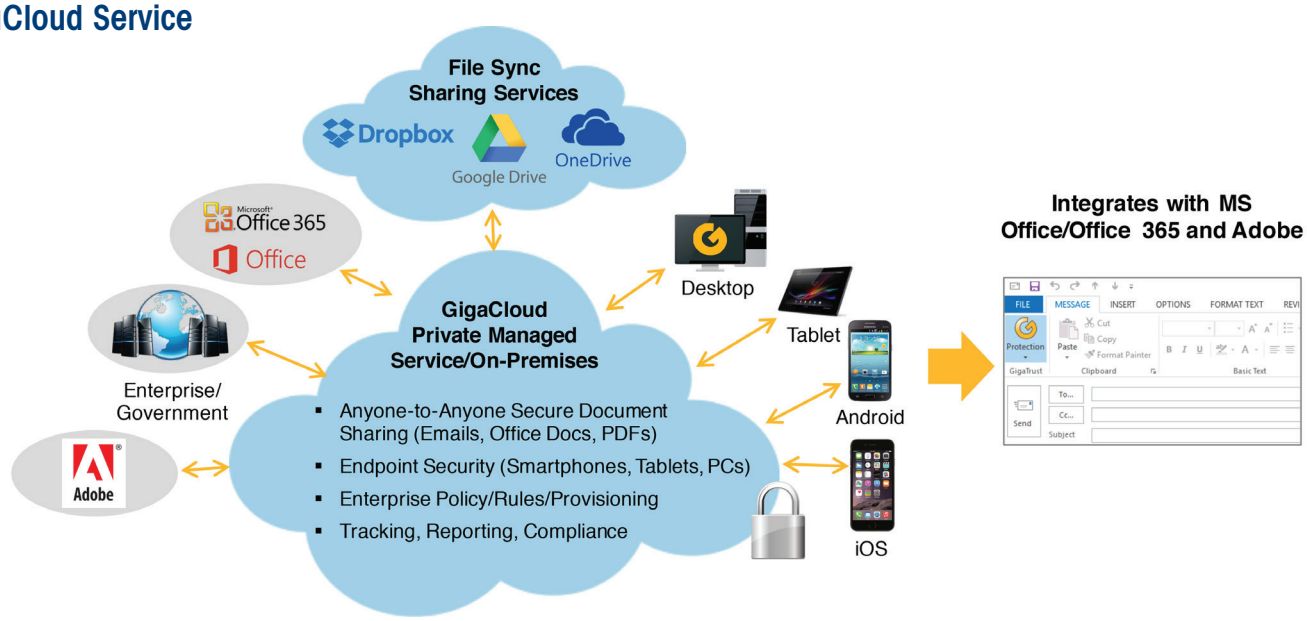
NIST is a very important piece of document and email security compliance in a time when cyberattacks are becoming more and more prevalent.

GigaCloud for DoD Supply Chain Delivers Secure Collaboration on Virtually any Device

The GigaTrust™ GigaCloud for DOD Supply Chain for secure endpoint email and document collaboration provides numerous features and functions to enterprise and government users. With GigaCloud for DOD Supply Chain, a redundant infrastructure is provided to persistently protect content (at rest, in transit, and in use) no matter how or where the content travels or is stored. GigaCloud for DOD Supply Chain is FIPS 140–2 compliant. Documents are protected with a 256-bit AES key. All communication between applications and the GigaCloud server are encrypted using a 2048-bit RSA key.

GigaCloud for DOD Supply Chain 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, sharing integration services including Dropbox, OneDrive and Google Drive, secure document management systems such as SharePoint®.

GigaCloud Service



GigaCloud for DoD Supply Chain Features
Anyone-to-Anyone secure messaging — IMAP and Exchange email support
Document Protection (Office, PDF and more)
Endpoint Security (tablets, smartphones, PCs)
Secure Collaboration (Protected emails, cloud storage services, thumb drives)
Users are provided with set of predefined policies/templates that make the service simple and easy to use
Customize policies/templates for protection and consumption of documents suitable to your organization and environment down to the individual user level
Document tracking, reporting and compliance
Revoke document permissions instantaneously
Data analytics allowing administrators to monitor usage in real time to identify potentially suspicious activity
Easy subscriber provisioning allows sharing protected documents with both internal and external users
Internal users can send protected content to external users once the external user has been invited by a GigaCloud administrator — this oversight prevents unauthorized content leakage by users attempting to sneak sensitive content out by protecting it

GigaCloud for DoD Supply Chain Endpoint Security Components

GigaCloud for DoD Supply Chain is available for both mobile and desktop users.

Service Available for:	
Mobile (Android, iOS)	Protect/View/Edit Microsoft documents and emails. Protect and View PDF, text and images files. Provides a similar desktop experience with full file fidelity.
Windows Client	Protect/View/Edit Office documents and emails in native Office applications. Protect/View PDF documents in Adobe Reader/Acrobat, and other non-Microsoft file formats in native applications. Provides policy management, rules and automatic protection at the user level.

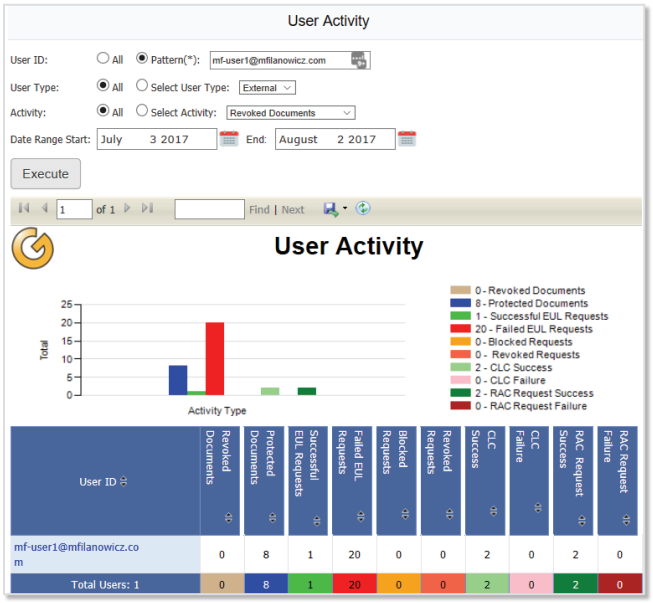
Data OverWatch

GigaCloud for DoD Supply Chain includes our Data OverWatch service. It is a cloud-based set of capabilities that provide measurement, auditing, tracking and analytics of data content. Specifically, the analytics shows ROI and user adoption, and enables users to better manage people, devices, content and policy. It allows them to know what is protected and where that content resides, and all the retained information is configurable and location sensitive. Data OverWatch "events" provide information about user, device, content and policy. Events are captured from applications interacting with the secure content and extensive analytics data is captured for each event.

Data OverWatch enables:

- Tracking and usage reporting of sensitive emails and documents.
- Automatic protection of emails and attachments based on content or destination.
- Revocation of sensitive emails and documents, even after distribution and use.
- In Use protection, not just In Transit, enabling the limitation of functions such as Print, Edit, Reply, Reply All, Forward, Copy/Paste, Screen Capture.
- Email and document expiration dates and prevention of usage until start dates.
- Each DoD supply chain vendor to have control of their sensitive emails and documents, separate from the controls provided to other supply chain vendors.
- Security Audit of policy changes.
- Alert notification of events (example: if one user opens an unusual number of documents, system will send an email to security/administrator).
- Data OverWatch events provide information about user, device, content and policy, and enables customers to better manage people, devices, content and policy.

User Activity Summary with Selectable Filters



CUI Document/Email Activity Summary for User

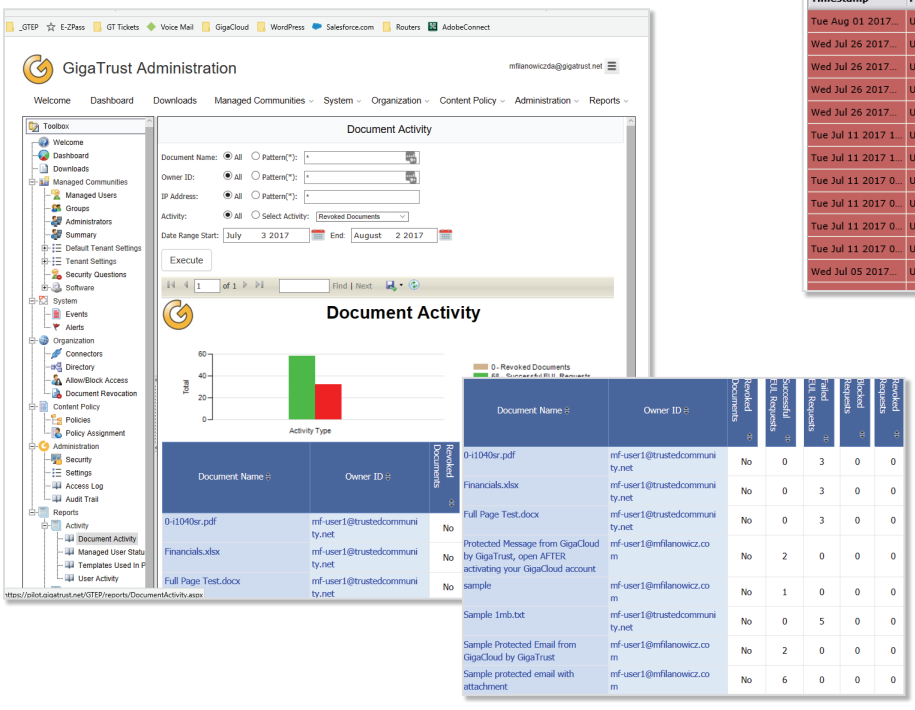
Enterprise Administrator Rights

One of the mandates of the NIST controls is to have content protection that tracks the usage of the CUI data, as well as audits what was viewed and by whom. As part of the GigaCloud for DoD Supply Chain service, an Enterprise Administrator can set policies for protection and consumption of documents suitable to their organization. The data analytics features of GigaCloud for DOD Supply Chain allow the Enterprise Administrator to monitor usage and to set up alerts for any suspicious activity. They are also able to produce reports for management review and regulatory compliance needs.

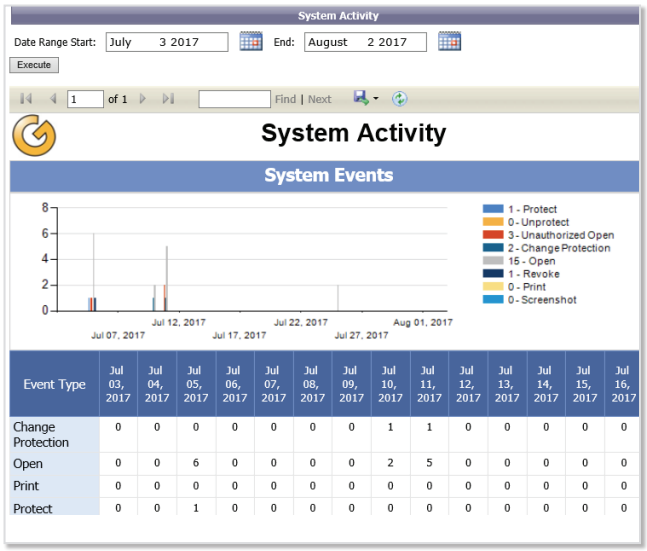
The supplier's Enterprise Administrator sets up the new tenant account with an enterprise customer domain name in GigaCloud. The designated Enterprise Administrator will be given rights to manage their account.

The supplier's Enterprise Administrator then creates enterprise user accounts quickly and easily in a GigaCloud DoD Supply Chain directory. The enterprise account is then ready for operation using default security policies, which can be modified by the Enterprise Administrator. The Enterprise Administrator can push out the GigaCloud DoD Supply Chain Desktop Client software to its users with SMS or another similar service. The GigaCloud Android and iOS Apps are available for download from Google Play and Apple's App Store. The Enterprise Administrator can also distribute the Apps directly to its enterprise users.

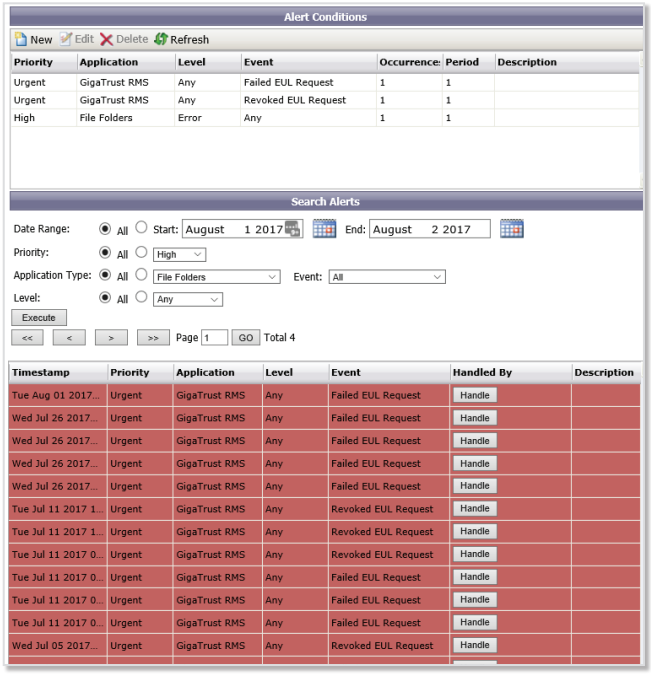
CUI Document Activity Detail with Selectable Filters



Summary System Activity



CUI Event Monitoring/Tracking/Alerts



Desktop Client

Protection for both Microsoft and non-Microsoft file types

GigaCloud for DoD Supply Chain for Desktop Client controls access to your data using our GigaCloud for DoD Supply Chain configuration when sending an Office document, PDF, JPG or other supported non-Office file format.

Desktop Client enables the opening of protected Office documents and supported non-Office rights-managed content directly on a desktop, tablet or smartphone device. This protection can also extend to other file-server sharing systems where emails are stored with attachments in different file formats. GigaCloud for DoD Supply Chain blocks over 250 screen capture/remote sharing programs from being launched with its blacklist support enabled for Office applications and non-Microsoft file formats. With GigaCloud for DoD Supply Chain Desktop Client, administrators can establish rules that automatically apply policies, track users and documents through the reporting function and revoke access instantly if a file is delivered into the wrong hands.

Desktop Client Requirements

- **Software Requirements**
  - Microsoft Office 2010 and above/O365
  - Windows 10 (x86, x64)
  - Windows 8.1 (x86, x64)
  - Windows 7 SP1 (x86, x64)
- **Supported Applications**
  - Microsoft Office Pro Plus 2010 and above/O365
  - Adobe Reader (v10.1.x, v11.0.04, DC)
  - Adobe Acrobat (v10.1.x, v11.x, DC)
  - Microsoft Notepad
  - Microsoft Paint
  - Microsoft Office Document Imaging
- **Supported File Formats**
  - Microsoft Office Suite — Word, PowerPoint, Excel
  - PDF — Adobe and Microsoft Format
  - TXT, BMP, GIF, JPG, JPEG, PNG, TIF, TIFF, MDI, DOC, XLS, PPT

Android and iOS Apps

The Android and iOS Apps bridge the gap between these mobile devices and secure content collaboration. Now your mobile user base can have persistent content protection and the convenience of mobility to send and receive protected content. Information sharing is greatly improved now that rights-protected content is accessible on mobile devices.

Unlike secure point-to-point messaging solutions that only protect content in transit, GigaCloud for DoD Supply Chain for Android and iOS protects content at rest, in transit and in use, allowing users to securely deliver and persistently protect emails and attachments while they are being read on the device. Android and iOS users can apply protection to outgoing email responses and messages, as well. If email permissions allow forwarding, attachments remain protected whether they are accessed on the desktop or on another mobile device.

Mobile Device Requirements

- **Software Requirements**
  - For Android — v4.4 and above
  - For iOS — v5.0 and above
- **Supported File Formats**
  - Microsoft Office Suite — Word, PowerPoint, Excel
  - PDF — Adobe and Microsoft Format
  - TXT, BMP, GIF, JPG, JPEG, PNG, TIF, TIFF, MDI, DOC, XLS, PPT

About GigaTrust

GigaTrust is a leading SaaS provider of endpoint email security and document in-use protection for on-premise private cloud or private cloud-based deployments for Windows, Android and iOS devices. 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 virtually 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. For more information about GigaTrust, visit www.gigatrust.com.

GigaTrust Headquarters 607 Herndon Parkway, Suite 302 Herndon, VA 20170 1.866.868.7878 sales@gigatrust.com www.gigatrust.com