GarbleCloud

Zero-Trust Data Security for Cloud-based Sharing & Collaboration Platforms

Contacts:

Bijit Hore (bijit@garblecloud.com)

Akhilesh Verma (akhilesh@garblecloud.com)

David Poger (david.poger@garblecloud.com)

Sharing & Collaboration workflows in DoD moving to the Cloud

Google Workspace and **Microsoft 365** are a great way for **information sharing** and **real-time collaboration** in a distributed and hybrid work setting.

Hugely useful even for secure data sharing with troops deployed in hostile territory -- at the **Tactical Edge***

Concern for DoD:

How to ensure the end-to-end security (confidentiality & integrity) of the data being shared between troops deployed in enemy territory?

*Source: https://taskandpurpose.com/news/air-force-afghanistan-airlift-kabul-google-doc/

Securing Controlled Unclassified Information (CUI) in the Cloud

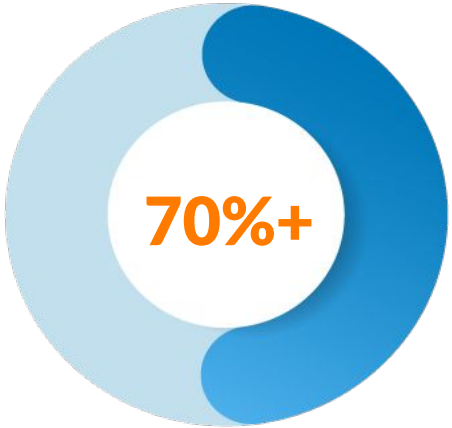
How to ensure data security when sharing with contractors outside DoD

CUI protection is a major challenge for the small and medium sized contractors in the Defense Industrial Base (DIB).

Concern for DoD:

Ensuring the security of the CUI data being **generated, shared and stored by its contractors in the cloud**, without requiring prohibitive investments to meet the CMMC requirements.

How Safe are your Files in these Cloud Platforms?



70%-80% of corporate data is unstructured, residing as files & documents. **60%+ of this data is now in the cloud.**

- [Malicious Exposure] **Docs and Files are the easiest form of data to compromise & exfiltrate** because they are easy to download, share, copy, forward, and print.

- [Accidental Exposure] As users share documents via different SaaS applications **chance of accidental exposure of sensitive documents is very high**.

You are NOT in Control of your Files at all times

Securing files-and-documents across SaaS platforms is a big challenge

- Easy to lose control of files replicated across various SaaS platforms - **Data Sprawl**!
- **Rights Management** is difficult, error-prone & limited by controls that the platform provides.
- **No control** over file access by **Server-side Entities**.

Sources of Threats to Sensitive Data in the Cloud

Threats from Agents

- **Person or non-person entities that have access to sensitive data can leak the information intentionally or by accident.**

Threats from Environmental Factors (dependent on CSPs & SaaS vendors)

- **Application features & functionality have unpredictable consequences;**
- **Secure code implementation (supply chain security);**
- Server-side security (access control, BC/DR, hosting service);
- Company culture, Business ownership changes;
- Outsourced support, technology/maintenance partnerships etc..

[Question]: How to achieve Zero Trust Data Security in the Cloud

How to enforce <u>Zero-Trust Security for Data</u>

Never Trust, Always Verify

<u>Without entrusting CSPs</u> with your sensitive Data?

- **Secure data from the cloud to the edge** - *at rest, in transit &* ***<u>in use</u>***.
- **No loss of functionality**.
- **Negligible effect on performance**.

[Key]: Make Sensitive Data Opaque to the Cloud Platforms

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

OMB Memorandum M-23-02
(Nov. 2022)

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

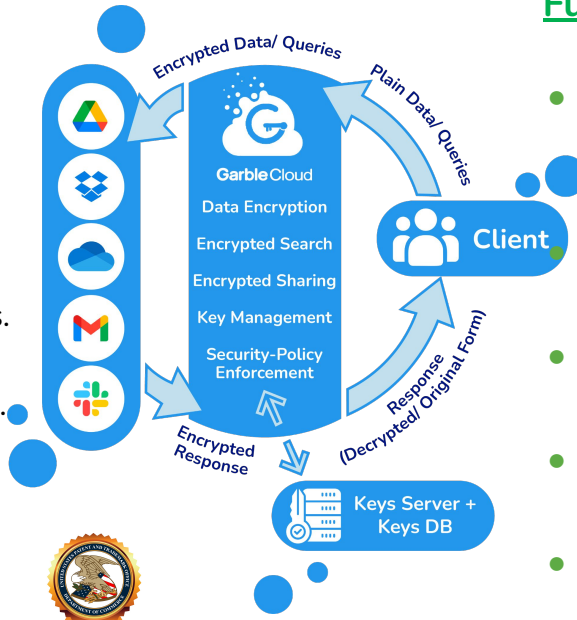
Federal agencies are moving to a zero trust architecture, ...

This paradigm shift relies in part on the ubiquitous use of strong encryption throughout the agencies.

[Solution]: Function-Preserving Data Encryption controlled by Owners

Technical Challenges

- **Strong encryption** for all kinds of unstructured data.
- Highly **scalable key management**.
- **Control of master keys** with data owners.
- **Fast search** & **retrieval** of encrypted data.
- Information **rights management** that works across platforms.
- **Secure file-sharing** with internal and external parties.
- **Secure collaboration** in the cloud without exposing content to platforms.



US Patent #9,825,925: *Method & apparatus for securing sensitive data in a cloud storage system.*

US Patent #10,013,574: *Method and apparatus for secure storage and retrieval of encrypted files in public-cloud computing platforms.*

Function-Preserving Data Encryption

- NIST approved **AES-256 encryption** for files & unstructured data; User-controlled and easy-to-use. Robust **enterprise-grade encryption key management** based on NIST guidelines.
- Support **CRUD operations on encrypted files** across popular SaaS platforms.
- Support **Fast cross-platform, full-text search on encrypted files** [**Patented**].
- Enable **sharing & collaboration on encrypted documents** between people using **PKI** and **client-side encryption**.
- Platform-agnostic, **encryption-based file security & rights management** policies.

GarbleCloud

Demo Outline

End-user features

- GarbleCloud UI overview
- **File Encryption & Decryption**
- **Encrypted Search**
- **Encrypted Sharing & Information Rights Management**
- Policy-based restrictions -- **DLP capability on encrypted docs**
- Audit trail

Admin capabilities snapshot

- Password Reset & Account Transfers
- **Bulk Encryption**
- **Lockdown**

Client-Side Encryption for **Secure collaboration at the tactical edge**

- **Google Docs/Sheets/Slides encryption**
- Other applications -- **Google Calendar**, Meet, Gmail...
- CSE **Admin Console** -- **Sharing permissions**, audit trail, Key Management

GC makes Function-Preserving Data Encryption at Scale a Reality

Function-Preservation

- Enable operations on encrypted files and documents, such as **full-text search** [**Patented**].
- **DLP/IRM on encrypted files** (avoid opacity due to encryption from policy engine).
- Real-time collaboration on encrypted docs via **Client-Side encryption**.

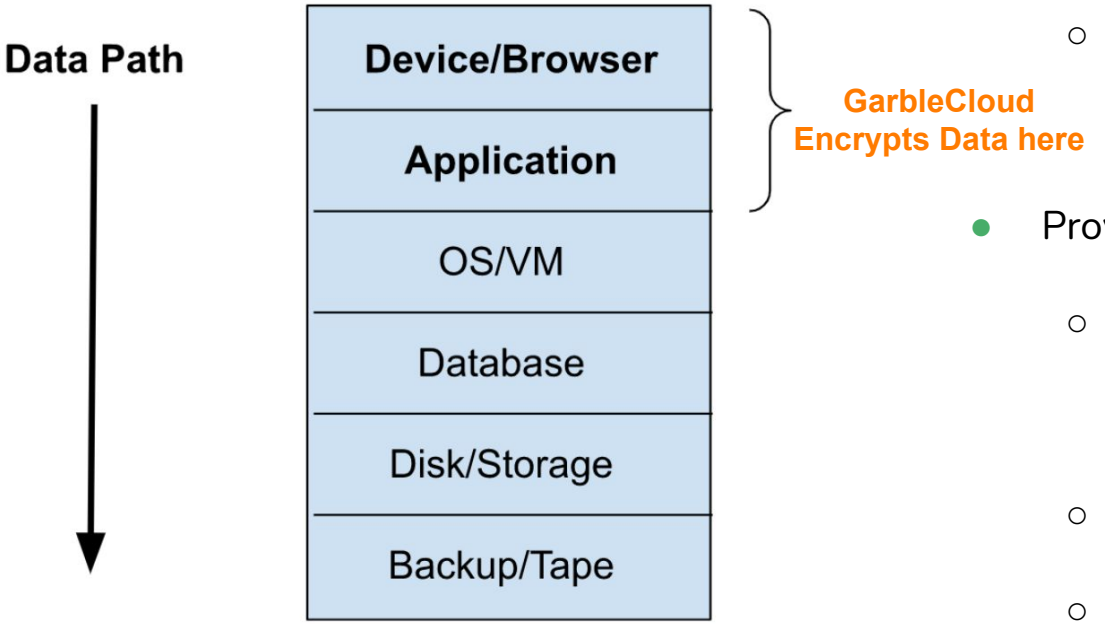
Reduce the Burden of Encryption Key Management

- Highly granular encryption (per-file keys); **small "blast radius"** (in case of key compromise)
- **PKI** for robust key management as per NIST standards.
  - Key wrapping.
  - Secure key distribution/sharing.
- **HSM** for hardened master-key management.
- Enhanced Key lifecycle management to meet **KMIP** specs.

Comprehensive Encryption, with Visibility & Control

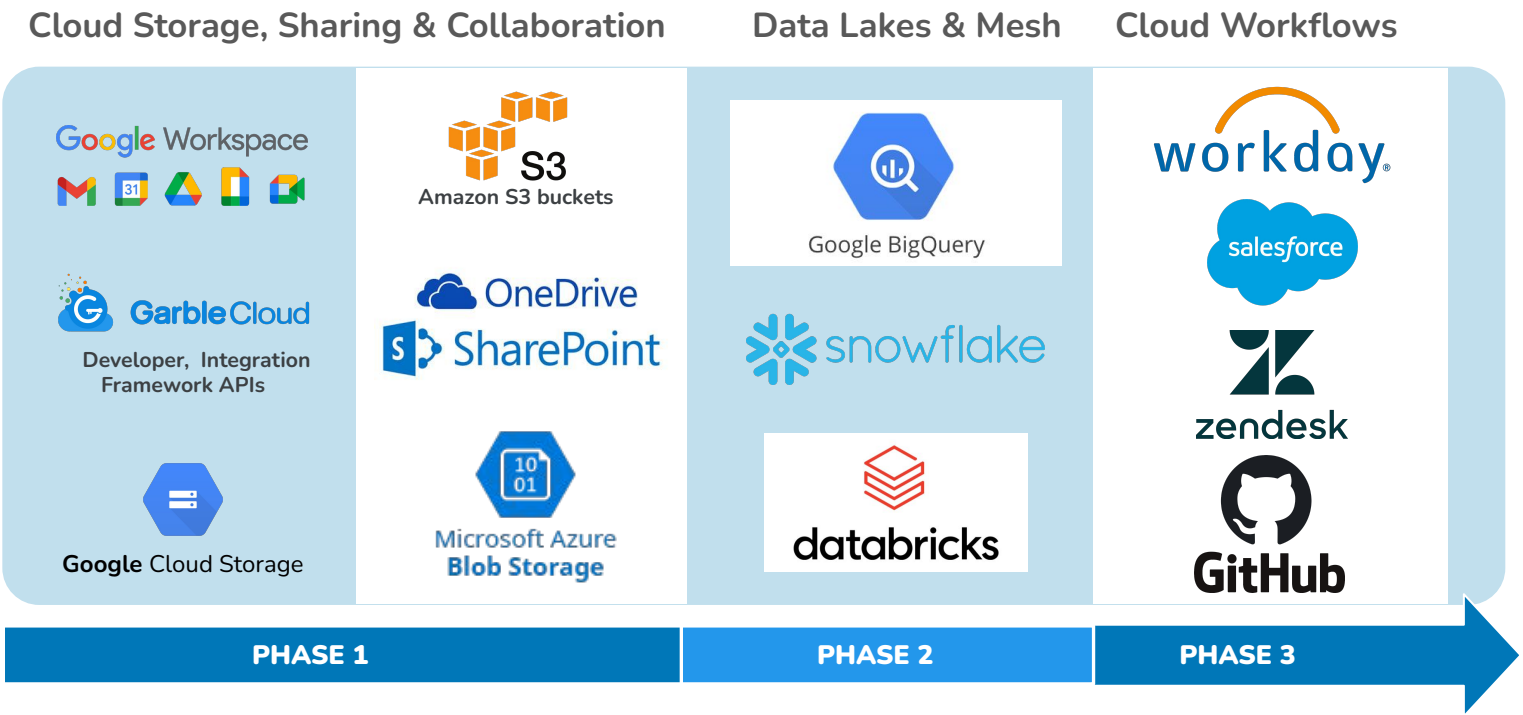
- Brings both **Admins & End-users** together to jointly determine data security posture.
  - Stakeholders who know what data is sensitive, can enforce encryption with ease.
  - Admins have tools to close gaps and enforce encryption policies at the org level.
- Centralized **Audit Trail** of every operation on encrypted data anywhere.

More Secure Encryption & Crypto-Agility



- Encryption at higher level is **more secure**.
  - **Protects against data breaches at lower levels** of the stack (e.g., CSPs, 3rd party apps).
- Provides **crypto-agility**.
  - Cloud customers **stay in control of the encryption algos & encryption keys.** Become agnostic to encryption by CSPs.
  - Migrate to **PQC** faster & stay up-to-date.
  - Enable **Encrypted Sharing between parties using different KMS** such as PQC & non-PQC.

Roadmap



Other Solutions

- **Search as a Service on Encrypted Document Repositories**
- **Quantum-safe Encryption Key Generation** (via partnerships)
- **DLP, Data Classification** (integrations)

GarbleCloud

Key Value Proposition

GarbleCloud enables a powerful data-centric approach to enhance data privacy and security in the cloud.

How DoD Benefits

- Take **control** of your sensitive files across SaaS platforms without compromising functionality - Achieve **Zero Trust Data Security** in the cloud.
- Secure external and internal **sharing of sensitive documents without slowing down collaboration**.
- Become **crypto-agile** when it comes to encryption in the cloud and be able to stay on top of **PQC** as standards evolve.

Making multi-cloud environments more **functional**, **collaborative** and *'Zero-Trust Secure'*.

GarbleCloud

GarbleCloud

Thank you for your time.

Contacts:

Bijit Hore (bijit@garblecloud.com)

Akhilesh Verma (akhilesh@garblecloud.com)

David Poger (david.poger@garblecloud.com)

Mapping GC capabilities to DoD's Zero Trust Framework

DoD Zero Trust Capabilities (Target & Advanced Levels)

	Target		Target & Advanced		Advanced
User	**1.1** User Inventory	**1.7** Least Privileged Access	**1.2** Conditional User Access **1.4** Privileged Access Mgmt. **1.5** Identity Federation and User Credentialing	**1.6** Behavioral, Contextual ID, & Biometrics **1.9** Integrated ICAM Platform	
Device	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Mgmt.	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	**2.1** Device Inventory **2.2** Device Detection and Compliance **2.3** Device Authorization w/ Real Time Inspection	**2.4** Remote Access **2.7** Endpoint & Extended Detection & Response (EDR & XDR)	
Application & Workload	**3.1** Application Inventory	**3.3** Software Risk Management	**3.2** Secure Software Development & Integration	**3.4** Resource Authorization & Integration	**3.5** Continuous Monitoring and Ongoing Authorizations
Data	**4.1** Data Catalog Risk Alignment	**4.2** DoD Enterprise Data Governance	**4.3** Data Labeling & Tagging **4.4** Data Monitoring & Sensing **4.5** Data Encryption & Rights Management	**4.6** Data Loss Prevention (DLP) **4.7** Data Access Control	
Network & Environment	**5.1** Data Flow Mapping	**5.3** Macro Segmentation	**5.2** Software Defined Networking	**5.4** Micro Segmentation	
Automation & Orchestration	**6.3** Machine Learning	**6.6** API Standardization	**6.1** Policy Decision Point (PDP) & Policy Orchestration **6.2** Critical Process Automation	**6.5** Security Orchestration, Automation & Response (SOAR) **6.7** Security Operation Center (SOC) & Incident Response (IR)	**6.4** Artificial Intelligence
Visibility & Analytics	**7.1** Log All Traffic **7.3** Common Security & Risk Analytics **7.5** Threat Intelligence Integration		**7.2** Security Information and Event Mgmt. (SIEM)	**7.4** User & Entity Behavior Analytics (UEBA)	**7.6** Automated Dynamic Policies

EXECUTION ENABLERS	Doctrine	Organization	Training	materiel	Leadership & Education	Personnel	Facilities	Policy

NOTE: **Green** boxes show the capabilities we provide today; **Yellow** boxes show new capabilities and integrations we can deliver as per DoD's requirements around our core product.

GarbleCloud

GarbleCloud Short Demo Video

https://vimeo.com/766134607

The GarbleCloud Difference

Key Features; Patented Technology

Secure, encrypted external file sharing

Enables seamless sharing of confidential documents & files with entities outside your organization, without losing control. Enables platform-agnostic **Information Rights Management** capabilities.

Search over encrypted files

For the first time ever, allows **full-text search on encrypted files & documents** — offering enterprises a new level of functionality not possible before.

Bulk encryption

Ensures **long-term protection of cloud files** without compromising accessibility. Integrates with DLP engines and therefore does not depend on end-users to protect corporate data.