SECURITY FACT SHEET

DataDefender by Cloud Storage Security

Prevent breaches and resource misuse through control of your storage layer.

Breaches involving cloud storage can cost organizations over $5.17 million/incident[1]. DataDefender, by Cloud Storage Security, offers environment-wide inventory, over 90 security checks on misconfigurations, and activity monitoring that answers the who, what, where and how much of all your data in cloud storage. The information below contains all the relevant facts surrounding the security of the DataDefender platform.

DataDefender Security Facts

1 | Certifications & Competencies

Cloud Storage Security is **SOC2 Type II compliant** and holds various AWS Partner competencies and certifications including: **Public Sector, Authority to Operate, the Security Software Competency, and is a trusted AWS Marketplace Seller.**

2 | How we Interact With Your Account

In order for the solution to run effectively, DataDefender requires a small number of policies to be applied to your account via CloudFormation Template. **These policies are the bare minimum required to run the solution.**

3 | How we Use Your Data

Cloud Storage Security does not store customer files or objects for DataDefender to provide its full set of features. DataDefender only ingests and processes log files and metadata to provide Inventory, Security Checks, and Activity Monitoring to customers. **Any metadata not needed to provide DataDefender is redacted or not included.**

4 | How Easy we Are to Use

DataDefender by Cloud Storage Security is a powerful, intuitive tool that is easy to deploy and use. Deploying DataDefender can be **completed in 30mins or less** and be accomplished with a single member of your team.

5 | Regulatory Considerations

DataDefender was built, and Cloud Storage Security is headquartered, in the United States. To meet regulatory requirements, **DataDefender can operate both inside and outside of United States AWS regions**, if necessary. Data residency requirements can be satisfied with DataDefender as only metadata is shared with the platform, not customers' data itself.

Beta onboarding open now for our second class!

Award winner in three 2024 Cybersecurity Excellence Award categories: Cloud Native Data Security, AWS Cloud Security, and Antivirus.

Learn more:

Cloudstoragesecurity.com

Cloudstoragesecurity.com/DataDefender

[1] IBM Cost of a Data Breach Report 2024

This document is provided for informational purposes only. Cloud Storage Security makes no warranties, express or implied, in this summary. Statistics and third-party data are sourced from publicly available industry reports as of the date of publication and may be subject to change.

CLOUD STORAGE SECURITY

DEPLOYMENT GUIDE

DataDefender by Cloud Storage Security

Prevent breaches and resource misuse through control of your storage layer.

Breaches involving cloud storage often cost organizations over $5.17 million/incident[1]. DataDefender, by Cloud Storage Security, offers environment-wide inventory, over 90 security checks on misconfigurations, and activity monitoring that answers the who, what, where and how much of all your data in cloud storage. The information below details the process of deploying DataDefender.

Deploying DataDefender

Getting Started

To successfully deploy DataDefender, you or another member of your team will need to contact a Cloud Storage Security Sales Representative or Support professional to schedule a dedicated onboarding session.

Onboarding and deploying DataDefender is quick and hassle-free. If your environment possesses fewer resources, the deployment process should take **30mins** or less to complete. Larger, complicated environments --particularly for enterprises-- may take up to **1 hour.**

Our support professionals are prepared to guide you through the process and ensure every resource you need is covered by DataDefender.

What You'll Need

To ensure we make the best use of our shared time onboarding to DataDefender, there are few items important to come with prepared into our onboarding session. Be sure to include members of your team with the necessary permissions to link your buckets, volumes and storage resources to DataDefender. With that, a list of the desired resources for DataDefender is always helpful!

Completing Your Deployment

With a scheduled onboarding, and your necessary team members and resources ready, we can complete the onboarding and deployment process. A member of the Cloud Storage Security Support team will begin by sharing a CloudFormation Template. After applying the CFT, your team will be invited to create an account on the DataDefender platform and CSS will grant your team the appropriate entitlements. After these simple steps your storage-layer security has begun!

All that remains is linking your storage resources in the session, and after if preferred for larger environments.

Beta onboarding open now for our second class!

2024 WINNER
CYBER SECURITY
EXCELLENCE AWARDS

Built by the team that won three 2024 Cybersecurity Excellence Awards for cloud data security, AWS security, and antivirus.

Learn more:

Cloudstoragesecurity.com

Cloudstoragesecurity.com/ DataDefender

[1] IBM Cost of a Data Breach Report 2024

This document is provided for informational purposes only. Cloud Storage Security makes no warranties, express or implied, in this summary. Statistics and third-party data are sourced from publicly available industry reports as of the date of publication and may be subject to change.