DATA SECURITY GATEWAY FOR AMAZON S3

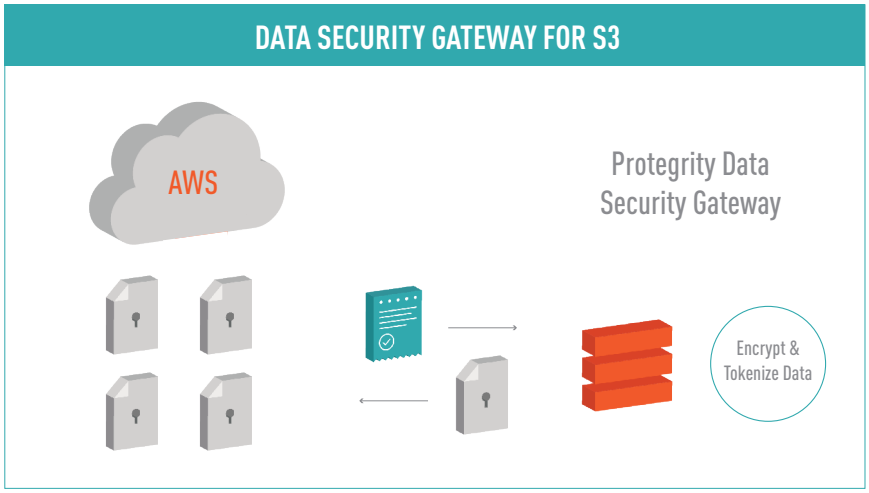
Protect sensitive information transparently without altering applications or services

PROTEGRITY

Data Sheet

Files passed outside the enterprise in Amazon S3 often contain sensitive data, which will likely be subject to compliance, privacy, and business security requirements. Native Amazon course-grained protection secures entire files but provides only an inflexible, all-or-nothing approach to data protection. Precision protection through Protegrity provides far more flexibility and secures specific sensitive data while allowing access to other data within the file.

Protegrity Data Security for Amazon S3 is a high-performance gateway solution that protects sensitive data within files. Delivered as a software appliance and as a containerized solution, the Data Security Gateway protects data within files being created or updated within the S3 environment without disruption to users.



Key Benefits

- Secure sensitive files in Amazon S3 transparently without interruption to users or applications
- Protect specific sensitive data while providing protection at rest, in use, or in transit
- Utilize a variety of security methods, including GPG, Protegrity Vaultless Tokenization, or AES 256 encryption
- Enhance security with enterprise-grade key management and flexible policy controls
- Leverage better visibility with comprehensive activity monitoring and reporting
- Full support for all text formats with custom extensibility
- Configuration over Programming (CoP) for quick deployments and extensibility without programming

Beyond Native S3 File Security

Data Security Gateway for Amazon S3 provides advanced security for specific content within files. As a file enters or leaves Amazon S3, sensitive data is parsed and protected/unprotected using built-in encryption, tokenization, hashing, or masking routines. This process renders specific fields unreadable to users depending on their role defined in the data security policy. Secured files can then be moved to any other instance or platform with the security in-tact.

The Protegrity Data Security Gateway from Amazon S3 secures sensitive information and protects it as it moves over the network and among applications, business processes, and users. The sensitive data adheres to strict, centrally-managed policies to address security, privacy, data residency, and compliance requirements without affecting the data transparency or usability. The gateway polls for file activity to integrate seamlessly with any S3 application without modification.

Multiple Protection Methods for Sensitive Data

Protect sensitive files while utilizing data-centric protection for specific file contents with GPG. Sensitive data is encrypted or tokenized using industry-leading AES encryption and the most advanced and secure tokenization technology on the market – Protegrity Vaultless Tokenization (PVT).

The standards-based AES 256-bit encryption is FIPS-compliant and is trusted by many government and civilian applications worldwide.

PVT is Protegrity's patented tokenization solution, which substitutes sensitive data with randomly-generated values while preserving the original data type and length. PVT is ideal for organizations with strict data residency requirements and those that want to go a step beyond encryption in protecting their data.

Extensible Support for File Formats		
Adobe Action Message Format (AMF)	Extensible Markup Language (XML)	HTTP Message
Binary	Extensible Markup Language (XML) with Tree-of-Tress (ToT)	JavaScript Object Notation (JSON)
Character Seperated Values (CSV)	Fixed Width	JavaScript Object Notation (JSON) with Tree-of-Tress (ToT)
Common Event Format (CEF)	HTML Form Media Type (X-WWW-FORM-URLENCODED)	Multipart Mime

Comprehensive Cloud and Enterprise Protection

Protegrity Data Security Gateway for Amazon S3 can be installed on a physical server or virtual machine behind your corporate firewall. It can also be deployed in a virtual private cloud as well as in AWS environments as an appliance or a containerized solution.

As part of the Protegrity Data Protection Platform, Protegrity Data Security Gateway is interoperable with all other components to provide seamless, centralized enterprise data protection. This level of data protection extends through policy management, monitoring, and reporting. Data is transparently tokenized/encrypted or detokenized/decrypted across any of Protegrity's gateway and protector-spanning databases, Big Data, and the cloud. This ensures that authorized users can always view protected data as it moves across environments while maintaining security.

LOOKING TO LEARN MORE? CONTACT YOUR PROTEGRITY REPRESENTATIVE TODAY!

PROTEGRITY

For over 15 years, Protegrity has set the standard in precision data protection, helping enterprises secure and use a perpetually growing store of sensitive data. Through granular protection and intelligent role-based empowerment, Protegrity helps companies focus on growth, development, and optimization. By securing their internal and customer data, companies can embrace new ways to share while remaining compliant.

Protegrity USA, Inc.
(Global Headquarters)
1165 E Wilmington Avenue
Suite 200
Salt Lake City, Utah 84106
1.203.326.7200
1.650.431.7000

Protegrity (Europe)
1 St Katherine's Way
London, E1W 1UN
+44 1494 857762

Protegrity (Asia Pacific)
1 Nanson Road
Level 3
Singapore 238909
+65 6904 6063

Protegrity (Navi Mumbai)
WeWork, 11th Floor, Tower 1
Seawoods, Grand Central, Sector 40
Navi Mumbai
Maharashtra 400706, India