Introducing the **Protegrity Cloud Gateway**: a highly configurable solution that secures your most sensitive data no matter where it resides.

**What is the purpose of a cloud gateway solution?**

Security concerns are often a barrier to greater adoption of cloud services and applications. Protegrity Cloud Gateway removes these barriers by protecting your data before it gets to the cloud, giving you the freedom to use cloud services without the risk of data leaving your organization in any recognizable form. You’re in control of your data, no matter what happens in the cloud—without impacting business processes or sacrificing SaaS functionality.

**How does the Protegrity Cloud Gateway work?**

Protegrity Cloud Gateway sits between users and cloud applications, replacing sensitive data with tokens or encrypted values before it is sent to the cloud. A gateway server cluster handles the traffic to and from the cloud, while a management server allows your security team to configure policies and protection methods. After the data has been processed and returned by the cloud service (i.e. Salesforce, Box, Gmail, Office365, Xactly, etc), Protegrity Cloud Gateway “unlocks” the data, making it viewable by approved business users. No one outside your organization can access your data on its journey to and from the cloud.

**Why is Protegrity Cloud Gateway better than cloud data protection gateways from other vendors?**

Our clients have told us that other cloud data protection gateways cannot be configured easily by their internal teams, don’t always recognize the sensitive data that needs to be protected, negatively impacts the speed or functionality of the SaaS solutions, or have limited scalability. The Protegrity Cloud Gateway addresses these concerns and responds to our clients’ demand to have us apply the same trusted technology Protegrity uses to protect their core on premise systems to their ever-growing adoption of cloud applications and services.

**How is the Protegrity Cloud Gateway deployed?**

The Protegrity Cloud Gateway is deployed as software that can be run on virtual servers or on physical servers in a proven appliance framework using “stateless architecture,” meaning that the individual server nodes are independent from each other and do not share any transient state information at run-time. With a stateless architecture, server nodes can be geographically distributed like most enterprises, you are adopting cloud solutions to better serve your customers and reduce costs. But the cloud can be a perilous place for you and your customers’ private and sensitive data. You need to secure the data before it reaches the cloud.
without sacrificing speed or reliability to deliver the highest level of performance, no matter where the cloud gateway nodes are located.

**What is the typical scope of implementation?**

The Protegrity Cloud Gateway was designed for easy deployment. At the core is a Management Console that configures rules and functionality so minimal coding is required. In most instances the solution is installed, configured and in production in just a few short weeks. However, Protegrity security experts are available to help meet the unique needs of each deployment and help configure specific protection profiles.

**What skills are needed to implement and maintain the Protegrity Cloud Gateway?**

The Protegrity Cloud Gateway is designed for ease of use. The critical knowledge set for implementation and maintenance is an understanding of the data flows and configuration of the third party cloud solution. Typically our customers rely upon the system administrators or sales & marketing operations teams to install and manage the Protegrity Cloud Gateway.

**How does the Protegrity Cloud Gateway work with cloud applications?**

The Protegrity Cloud Gateway runs independently from the cloud application, typically at the perimeter of a customer’s network. It was developed using a “Configuration-over-Programming” (CoP) paradigm, allowing security administrators to “own” the cloud gateway security configuration without depending on internal IT staff or Protegrity for custom coding. Being that there is no link to a particular version of the cloud application, the need for in-depth revisions to the gateway every time the cloud service is updated is eliminated. This development approach also allows clients to use new SaaS features right away as they are rolled out while maintaining the same level of data security.

**Will the cloud applications run slower?**

No. The Protegrity Cloud Gateway is designed to create maximum protection without impeding performance.

**What type of data can the Protegrity Cloud Gateway protect?**

Most customers protect data selectively, allowing public data to be visible to outsiders while protecting specific fields such as credit card numbers, social security numbers, or other personal information. The Protegrity Cloud Gateway can also be used to protect unformatted data such as notes, as well as text in most types of attachments including Word, Excel, PowerPoint and PDF.

**What types of data protection does the Protegrity Cloud Gateway provide?**

The Protegrity Cloud Gateway provides a variety of data security methods including monitoring with no encryption, hashing, format-controlling encryption, strong encryption and Protegrity Vaultless Tokenization. This solution harnesses all of the data protection technology found with Protegrity’s industry leading [Data Security Platform](https://www.protegrity.com/data-security-platform/).
Has Protegrity’s encryption been certified or validated by third parties?

AES (Advanced Encryption Standard) has been certified by NIST under FIPS 197 and Protegrity is in the final certification process for FIPS 140-2. The AES standard has been publicly published and extensively reviewed and tested by many independent organizations. In addition, Protegrity’s implementation has gone through rigorous testing, code review and validation by dozens of major enterprise customers.

Is tokenization more secure than encryption?

Based on key space, Protegrity Vaultless Tokenization is orders of magnitude stronger than encryption. Tokenization may also help meet regulations, compliance concerns, or corporate policies that require specific types of data to not leave the organization, even if it is encrypted.

What are the advantages of Protegrity Vaultless Tokenization over standard tokenization?

Protegrity Vaultless Tokenization (PVT) is a reversible security method that replaces sensitive data with fake data that looks and feels just like the real thing. PVT provides equal or better security than encryption, while retaining the vital usability of data for business processes. When you compare standard tokenization to Protegrity Vaultless Tokenization, you quickly see that the Protegrity solution offers higher performance, simplified management, and unlimited scalability, allowing the gateway to operate as a lightweight, self-contained network appliance without relying on a third-party database (or “vault”) to store the token relationships.

Why is the Protegrity Cloud Gateway security better than native SaaS application solutions?

According to Gartner, “Your security policy depends on how many pieces you control, the more you own, the more you control.” So while many of the SaaS applications you may be relying upon for your enterprise may offer reasonable security, unless you take steps toward securing your own data, you are completely reliant upon a third party vendor’s security policy. The Protegrity Cloud Gateway solution enables you to control your security strategy and lets you decide how your sensitive data is managed.

Can encrypted or tokenized data be searched and sorted?

Yes, Protegrity provides granular control over the level of protection and search-ability for specific pieces of information. Data can be protected on a per-field or per-word basis with industry standard AES 256-bit encryption. In addition, Protegrity provides options for local indexing of selected data to optimize search functions. All of these options can be fine-tuned to meet the searching and maximum security requirements for each customer.

Does the Protegrity Cloud Gateway provide SaaS-specific security profiles?

The Protegrity Cloud Gateway offers a variety of security profiles enabling the user to fully adopt common SaaS applications such as Salesforce.com, Box, Gmail, Xactly, and Office 365. However, Protegrity will work with you to deploy the Protegrity Cloud Gateway with whatever SaaS application you are using.
How is the Protegrity Cloud Gateway licensed?

The Protegrity Cloud Gateway and Protegrity Enterprise Security Administrator (ESA) require an annual term license per unit and includes standard maintenance and support. An annual subscription service based on the number of users is also required for each SaaS application that needs to be protected. On-site product training, installation services, advisory configuration services and testing services can be purchased separately.

For more information about Protegrity Cloud Gateway and pricing options based on specific configurations, licensing options and SaaS subscriptions, please visit www.protegrity.com, call +1-203-326-7200, or e-mail info@protegrity.com.