CRYPTERON

SECURING THE CLOUD

Turn-key Database Encryption for Developers

Build secure and regulatory compliant .NET applications in the cloud or on premises without worrying about your data-at-rest or in-transit.

Testimonials

> "We built CipherStor into our application and it took our developer a grand total of two hours of development time to start encrypting the our users' data" – Leading HR Firm
>
> "We continue to look at the benefits of Crypteron technologies and really see it as the way to go" – Criminal Justice Information Services - FBI client

Key features

- ✓ Military grade encryption: Authenticated AES256-GCM encryption that's so robust that even the National Security Agency (NSA) recommends it for protecting of military classified information.
- ✓ Easy Integration: CipherDB wires into the most popular ORM APIs so you're productive from day 1 with no expensive hardware to maintain or gateway solutions to monitor.
- ✓ Automated Key Management: Use the Crypteron Dashboard to manage your Apps, Security Partitions and Access Control Lists. Each Security Partition has its own encryption key that is itself signed and encrypted using Elliptic Curve cryptography and stored remotely for greater security.
- ✓ Regulatory Compliance: CipherDB enables app-level compliance with standards like HIPAA, PCI, FIPS-140-2, CJIS / Law Enforcement, FISMA, EU Data Protection and more, even when the underlying infrastructure cannot.
- ✓ Self-Scaling Architecture: Our stateless security architecture scales with your application for near native performance at any scale. The overhead is marginal at about 1ms per record containing multiple encrypted fields.
- ✓ Works With All Popular DBs: By integrating directly with Entity Framework or NHibernate, CipherDB is able to support all popular databases including SQL Server, SQL Azure, Oracle, IBM DB2, MySQL, Amazon RDS, PostgreSQL, Sybase, and more.

Overview

All merchants who accept credit cards, online or offline, must comply with the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is a world-wide framework for protecting consumer credit card data requiring companies to properly secure and protect credit card data. Non-compliance companies that suffer from a breach are subject to penalties and fines.

How Do I Comply with PCI-DSS?

Our military grade encryption, key management, auditing, and authentication functionality protects your data in the cloud or on your dedicated systems while satisfying compliance requirements. We ensure that requirements of the PCI-DSS are satisfied using our security solutions.

Product Key *CipherDB* *CipherStor* *TotalAuth*

Requirement 3: Protect stored cardholder data

☑ 3.4) Render primary account number unreadable anywhere it is stored	CipherDB and CipherStor both feature complete data-at-rest security and is fully independent of the underlying security of the storage medium or policy. Even unintentional logging on SQL server doesn't leak any sensitive data.
☑ 3.5) Protect any keys used to secure cardholder data against disclosure and misuse	CipherDB and CipherStor employ a patent pending way of securing and handling encryption keys. This includes physical isolation, cryptographic isolation, automatic rotation of encryption keys as well as policy based usage for older keys.
☑ 3.6) Fully document and implement all key-management processes and procedures	We take care of the key management difficulties so you don't have to.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

☑ 4.1) Use strong cryptography and security protocols	CipherDB/CipherStor uses strong military grade encryption (FIPS-140-2, NSA Suite B) used by the government and DoD. We have the highest standards for protecting your data.

Requirement 6: Develop and maintain secure systems and applications

☑ 6.5) Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities	Our security software maintains data privacy even in the face of SQL injections, insecure underlying data storage, insecure communications, improper error handling and many more. Data privacy is 100% maintained even if your SQL administrator password is compromised!

Requirement 7: Restrict access to cardholder data by business need to know

☑ 7.1) Limit access to system components and cardholder data to only those who require such access	DualAuth brings multi-layer authentication for more secure authentication of end users or software administrators. CipherDB as well as CipherStor employ cryptographic techniques to enforce that only authorized software programs have access to secured data.
☑ 7.2) Establish an access control system for systems components with multiple users that restricts access based on a user's need to know	DualAuth brings multi-layer authentication for more secure authentication of end users or software administrators. CipherDB and CipherStor use cryptographic methods to ensure that only the organization's designated security officer can introduce new master keys or authorize new applications to begin using such keys.