eclypses™

Cybersecurity Brief

Securing Data with a Private Digital Vault

How to Protect the Most Sensitive Information in Your Organization

The digital information stored on your computers and in the cloud is the lifeblood of your organization. You know it, your customers know it, and would-be hackers know it too.

It's inevitable; cyber criminals are constantly using new techniques to "get in" and try to grab your crown jewels – because the barriers to most companies put in place simply are not adequate to stop cybertheft.

This is particularly true for the data you warehouse, known as data at rest. It's where the "money" is. From financial information to medical records and intellectual property, adversaries work very hard to bypass conventional and outdated methods of data protection.

Yet, there is a way to prevent companies from becoming the next victim of a catastrophic data loss – even if the bad guys manage to breach your defenses, which they eventually will. MicroEncryption® is becoming the preferred approach for business and government alike to stop cyber criminals cold in their tracks and render attacks useless.

"Eclypses is a leader in protecting the information we need to be safe"

Richard Purcell, Former Microsoft Corporate Privacy Officer

Standard Encryption Techniques for Data at Rest in the Cloud = Data at Risk

Files located in the cloud on servers connected to the Internet are susceptible to threats. Cloud storage services commonly protect data-at-rest using standards such as the Advanced Encryption Standard (AES-256) technique, one of the most widely used and analyzed ciphers in the world, combined with firewall deployment.

Developed in 2001, AES originally used 128-bit key encryption and has since migrated to 256-bits along with a few other improvements over time. Unfortunately, AES does not offer enough security in today's world of cyber criminals and terrorists who have high-powered quantum computers. Data breaches, system vulnerabilities, and shared technology weaknesses continue to be an issue with AES and firewall solutions.

Although transmitting the data over the Internet using the Secure Sockets Layer (SSL) protocol or its successor, Transport Layer Security (TLS), help protect files while in transit, the big problem is when files are stored on the servers. One reason is because AES and other encryption methods are "bulk" type encryption schemes, encoding the entire data structure as a block. This includes the framing bits and embedded addressing bits, exposing the entire data stream to hacking. In fact, attacks are common that extract thousands, if not millions of customer records at the same time, referred to as mass data breaches.

Data encryption creates other challenges for user. For instance, the computational overhead introduces latencies. Because of this, data availability can be sluggish, reducing application speeds that in turn impact the user experience.

A Private Digital Using MicroEncryption® Vault Will Stop Successful Cyber Attacks

MicroEncryption is a smarter, ultra-secure solution that replaces sensitive customer data at the byte level with MicroTokens™ that are useless to hackers. Based on the Eclypses™ MicroToken Exchange™(MTE) technology, an extremely high level of end-to-end privacy is provided by creating a secure on or off premise Private Digital Vault.

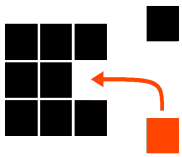
The MTE security framework is a proven method of "hiding" your company's valuable digital assets while at rest. MicroEncryption can be applied to structured and unstructured data. MTE has an extremely low latency allowing users to store and share files nearly instantaneously, having negligible impact on the user's experience.

The first step in the MTE process is creating a MicroToken™ to replace individual data elements down to the field level of a record within a database or a file. MTE's proprietary tokenization process can be applied to file types of any kind, including PDF, video, and audio to name just a few.

Tokenization is the process of transforming a meaningful piece of data into a random string of characters called a token that has no meaningful value if acquired by an unauthorized action. MTE MicroTokens serve as reference to the original data yet cannot be used to guess or expose those values to hackers and adversaries.

The real data is held in the Digital Vault, securing each piece as MicroEncrypted information. Then instead of being held all in one place, the data is atomized. Finally, MicroTokens representing each data element is warehoused throughout servers within a data center and at widely dispersed locations across the network.

Figure 1 gives a simplified overview of how the MicroEncryption and tokenization process "hides" and protects data:

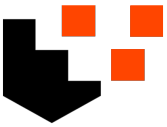


1. Replace

Data is replaced with MicroTokens™, which contain NO original data.

2. Encrypt

Pieces of data are individually encrypted.



3. Separate

Encrypted pieces are broken apart into multiple segments.

4. Disperse

Segments are distributed through an array of servers, collocated or remote.

MicroEncryption with tokenization is the most effective data obfuscation technology available. The MTE architecture provides an impregnable secure digital vault to store data at rest in the data center; and using for MTE data in motion, "real data" is *never* transferred between endpoint devices. Your digital assets are invisible to cyber threats.

Unlike bulk encryption, each data element is secured and protected as if it were its own database with its own sets of keys. MicroEncryption literally replaces sensitive customer data, at the byte level, with MicroTokens. When a breach occurs, hackers cannot access the sensitive data because it is no longer there – only useless place holders or MicroTokens exist that do not allow access or knowledge of where the "real" data is located.

For example, a database with 100,000 records, in which 10 sensitive fields are protected in each record is treated as if it were 1,000,000 individualized protected databases.

The individual data elements are encrypted with the organization's algorithm of choice and the sensitive data remains fully protected until the very last moment, as its use is called upon by an authorized action.

"Eclypses has cracked the code on how to properly secure data that's both at rest and at motion. This has huge implications for companies of all sizes, in all industries."

Richard Marshall, Former U.S. Department of Homeland Security Director of Global Cyber Security Management

Industry Leading Security – Real Business Results

Sooner or later adversaries will break in to your systems and try to exploit your data. The MicroToken Exchange with MicroEncryption will prevent data theft and differentiate your business from the competition – by making data Invisible.

With patents issued and pending, Eclypses' technology is as unique as it secure.

- Millisecond operational speeds means that user experience is not impacted
- Easy to scale securely and maintain performance as database increases in size
- Easy to exchange and share private data in an ultra-secure environment
- GDPR compliant and certified to standards including PCI-DDS Level 1, HIPAA, and Pii

MicroEncryption is scalable and designed to evolve with future best security practices without sacrificing cybersecurity or accessibility. It is an advanced solution relevant across all industries and exceeds industry security standards and regulations by securing one piece of data at a time in real time.

About Eclypses

Eclypses' industry leading disruptive cybersecurity software replaces user data with MicroTokens™ using MicroEncryption® to provide the highest level of data privacy available with the company's patent pending MicroToken Exchange™ (MTE) technology.

Applications range from secure command and control needs, including Internet of Things (IoT), to secure storage and retrieval of sensitive data, such as credit card information and healthcare records. Eclypses' MicroToken Exchange technology is helping enterprises and government agencies protect their most sensitive and private information from cybercriminals cyber terrorists today.

Eclypses' MicroToken Exchange (MTE) software complies with the European Union's General Data Protection Regulation (GDPR). In addition, Eclypses' technology is certified as Payment Card Industry Data Security Standard Level 1 (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliant.

The Digital Safety Deposit Box of CertainSafe®, a business unit of Eclypses, has been selected as a 2018 Editors' Choice Product by PC Magazine (PCMag) for best encryption software. In addition, the Digital Safety Deposit Box was designated as the most secure solution tested. The Digital Safety Deposit Box is an ultra-secure cloud-based service that makes it easy for businesses to securely store, access, and share valuable and private assets, and is built on Eclypses' cybersecurity software.

In recapping the coveted award, PCMag's Lead Analyst for Security Neil J. Rubenking writes, "When backing up your sensitive files to the cloud, CertainSafe Digital Safety Deposit Box emphasizes security over all else, but it doesn't sacrifice ease of use." Rubenking added that of all the solutions reviewed, "The Digital Safety Deposit Box has the most secure encryption software."

Located in Colorado Springs, Colorado, you can contact Eclypses at 719-323-6680 or via email at info@eclypses.com. Please visit us at www.eclypses.com and www.certainsafe.com.

"Eclypses will change that way data is stored well into the future as there's no other platform today that provides the same level of protection or compares to Eclypses' ability to ensure the security of sensitive data."

Former Chairman of the U.S. House Intelligence Committee