Karen Scarfone,
Scarfone Cybersecurity

Meeting Compliance Requirements for Protecting Sensitive Data in the Cloud

With PCI DSS Use Case

About Karen Scarfone

Karen Scarfone is the principal consultant for Scarfone Cybersecurity in Clifton, Virginia. She develops cybersecurity white papers, technical standards, articles, and other publications for a wide variety of organizations. Karen has over 20 years of professional experience in information technology, with over 15 years of that dedicated to information security. Karen was formerly a senior computer scientist for the National Institute of Standards and Technology (NIST), where she oversaw the development of system and network security publications for federal civilian agencies and the public. HIPAA and other regulations cite some of these publications as being mandatory for organizations to comply with. Karen holds a bachelor's degree in computer science from UW-Parkside, a master's degree in computer science from the University of Idaho, and a master's degree in technical writing from Utah State University.
http://scarfonecybersecurity.com

Karen Scarfone,
Scarfone Cybersecurity

Executive Summary

Data security is on the mind of many executives, especially when it comes to moving data or applications to the cloud. However, many cloud providers take the stance that customers are ultimately responsible for securing their own data. Therefore, sensitive data stored in the cloud often lacks sufficient protection from threats, making it more susceptible to being breached. This frequently happens because customers misunderstand the level of protection that their cloud service provider offers for stored information. People may think that because a provider is utilizing or offering self-encrypting drives (SEDs) and full disk encryption (FDE) technologies, which are so strongly recommended for desktops and laptops, that these technologies are also sufficient for protecting data in a cloud environment.

Another source of misunderstanding is that most of the security compliance initiatives that organizations are subject to do not clearly state what type of encryption solution should be used, only that encryption is needed. This can lead an organization to using an encryption solution such as SED or FDE that provides almost no protection at all in a cloud environment. Instead, organizations that want to ensure their data assets are secure in the cloud should rely on filesystem-based encryption (FSE) technologies. FSE solutions work within the guest operating system to safeguard sensitive data at all times except when the data is specifically being used. These technologies may be made available by the cloud service provider, or an organization may need to acquire, deploy, and manage its own FSE technologies to ensure that its sensitive data is properly safeguarded.

The Need to Protect Sensitive Data at Rest

It's obvious that organizations need to protect the sensitive data that they store on their own systems. Organizations do this through a layered approach that encompasses many security controls, including restricting physical access to servers, using identity and access management technologies to limit logical access to sensitive data, and encrypting sensitive data so that it can only be decrypted (behind the scenes) and accessed by authorized personnel using the approved interface for doing so.

Protecting sensitive data in the cloud requires a similar layered approach. Unfortunately, organizations often assume that all cloud service providers take care of some or all of these layers on their behalf. In many cases, cloud service providers offer some degree of protection for stored data, but it is easy for customers to misunderstand how effective this protection will be against real-world threats. This could result in sensitive data being exposed to many more attacks, greatly increasing the likelihood of a major data breach.

The most common misunderstanding is that encrypting stored data fully protects it no matter how that encryption is applied. In reality, some types of encryption only work against particular types of threats. An organization must consider the full range of threats and use one or more forms of encryption to address them.

Examples of potential threats include the following:

- An external attacker who uses sophisticated techniques (e.g., advanced persistent threats) to compromise a virtual server instance and maintain long-term access to that instance and the data it holds
- A cloud customer who, inadvertently or intentionally, circumvents security controls within a cloud server and gains unauthorized access to other customers' sensitive data housed on the same server
- A disgruntled system administrator who abuses privileges to access sensitive data
- A person who steals a cloud server in transit from one cloud data center to another

In addition, an organization must also consider all of its security compliance requirements. Nearly every major security compliance initiative requires the confidentiality of stored sensitive data to be protected through encryption or other means. Encryption at rest technologies used in accordance with secure key management practices have become the standard solution for accomplishing this, in large part because if done well they can be very effective.

Karen Scarfone,
Scarfone Cybersecurity

Technologies for Protecting Data at Rest

Choosing one or more storage encryption technologies to adequately protect an organization's data at rest can be a daunting task, and is even more so when the data is stored in the cloud. The three types of storage encryption most often used for cloud-based data are as follows:

- Self-encrypting drive (SED). In this type of technology, the encryption capabilities are built into the storage hardware itself. Once the user (or device, for unattended systems) has been authenticated before boot, the SED automatically decrypts storage on an as-needed basis.
- Full disk encryption (FDE). FDE technologies prevent the operating system from fully booting until after the user (or device, for unattended systems) has been successfully authenticated by the FDE capability. FDE technologies come in two forms: dedicated FDE products, which are installed just below the operating system level, and FDE features built into operating systems, which effectively work at the very bottom of the operating system level.
- Filesystem-based encryption (FSE). FSE works on designated portions of a filesystem within an operating system. For example, FSE might protect a single file, a group of files, or an entire volume.

All of these technologies have something in common: they must decrypt stored information before that information can be used. This may sound simple, but its implications are profound. Both SED and FDE technologies only protect stored information before initial user or device authentication occurs. After that, the technologies decrypt storage as needed for the duration of the device usage – that is, until the device is powered off. (There are special circumstances where encryption may be re-applied during device usage, such as a laptop being placed in hibernation, but these circumstances are not applicable to cloud environments.)

In other words, SED and FDE technologies only protect data stored in the cloud when those cloud-based servers or storage devices are not booted. Servers and storage devices in the cloud are normally booted and running at all times, and when they are not booted, they are not remotely accessible over the Internet. As a result, SED and FDE technologies offered by a cloud service provider only protect sensitive customer data from physical threats, such as a person intercepting a used, unsanitized hard drive being transferred from one cloud data center to another, or a malicious insider stealing a server from a data center.

In contrast, FSE technologies protect data whenever that data is not in use. It does not matter if the devices are booted or not. So, in addition to protecting sensitive data against the physical theft of storage media, FSE technologies also provide substantial protection for sensitive data held within a booted operating system's filesystem. Assuming that an organization follows sound secure key management practices, the risk from insider attacks performed by cloud service provider personnel drops sharply because they cannot perform the decryption themselves. An example of these practices is using a key management system that provides complete separation of duties and gives an organization full control over its keys.

FSE should be an integral part of an overall defense-in-depth security approach for protecting sensitive data in the cloud. Because no single security control provides absolute protection against every threat, FSE needs to be implemented in conjunction with other security controls and tools offered or provided by the cloud service provider. Today's advanced threats can often penetrate network-based defenses such as firewalls, intrusion prevention systems (IPS), anti-malware services, and security information and event management (SIEM) solutions, so using encryption technologies as a final line of defense is an absolute necessity.

How Encryption Controls Help Meet Data-at-Rest Security Compliance Requirements

Table 1 compares the relative effectiveness of the three common approaches for encrypting data at rest within the cloud. The left side of Table 1 lists the most relevant security requirements from the Framework for Improving Critical Infrastructure Cybersecurity, better known as the NIST Cybersecurity Framework, and maps these requirements to requirements from several major security compliance initiatives, which are listed in the box. Finally, the right side of Table 1 explains how effectively each of the three approaches for encrypting cloud data at rest meets each of the identified requirements. It also shows how a particular FSE solution, Vormetric Transparent Encryption, compares to other FSE products, as well as to SED and FDE technologies, for meeting the same requirements.

In addition to the NIST Cybersecurity Framework, the other compliance initiatives reflected in Table 1 are as follows:

- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0 [1]
- Control Objectives for Information and Related Technology (COBIT) 5 [2]
- Council on Cybersecurity (CCS) Top 20 Critical Security Controls (CSC) v 6.0 [3]
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)/ Health Information Technology for Economic and Clinical Health Act (HITECH) [4]
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 – Information security management [5]
- National Institute of Standards and Technology (NIST) Special/ Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [6]
- Payment Card Industry (PCI) Data Security Standard (DSS) v3.1 [7]

Table 1 indicates the extent to which the technology supports the security requirement in the context of protecting the confidentiality of sensitive data stored in the cloud.

- Green: completely supports requirement
- Yellow: partially supports requirement
- Red: does not support requirement at all

Table 1: Mapping Encryption Technologies for Cloud-Based Sensitive Data to Security Compliance Requirements

NIST Cybersecurity Framework Mapping	Self-Encrypting Drive (SED) and Full Disk Encryption (FDE) Technologies	Typical Filesystem-Based Encryption (FSE) Technologies	Vormetric Transparent Encryption (VTE)
ID.RA-3: Threats, both internal and external, are identified and documented. [1, 2, 3, 4, 6, 7]	SED and FDE technologies cannot detect any threats against sensitive data.	All access attempts involving encrypted data are logged, but the technologies do not evaluate the nature of these attempts.	All access attempts involving encrypted data are logged, and policies can be configured to generate alerts when certain events happen.
PR.AC-1: Identities and credentials are managed for authorized devices and users. [1, 2, 3, 4, 5, 6, 7]	These technologies offer no identity management features for access to sensitive data on a booted system.	FSE identifies and authenticates users and devices, but it only provides rudimentary key management capabilities.	VTE identifies and authenticates users and devices. Also, VTE provides robust key management for all encryption keys.
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. [1, 3, 4, 5, 6, 7]	SED and FDE do not offer any access control features for protecting sensitive data on booted systems.	Typical FSE technologies offer rudimentary access control features but do not support the principles of least privilege and separation of duties because of their limited key management capabilities and their lack of support for roles.	Policy-based encryption is implemented, adding an access control layer that allows only authorized users and services to decrypt designated files. VTE implements separation of duties through its flexible key management options (such as storing keys off-premise) and its support for multiple data security management (DSM) roles (e.g., different roles for keys, policies, domains).
PR.DS-1: Data-at-rest is protected. [1, 2, 3, 4, 5, 6, 7]	Data-at-rest is only protected when the system is not booted; it offers no protection at all when the system is up and running, which is almost all the time.	Data-at-rest is protected at all times except when the data is actually being used.	Data-at-rest is protected at all times except when the data is actually being used.
PR.DS-2: Data-in-transit is protected. [1, 2, 3, 5, 6, 7]	The encryption is local to the storage medium, so data transmitted to another system is unprotected.	The encryption can move with the data, so data transmitted to another system stays protected.	The encryption can move with the data, so data transmitted to another system stays protected.
PR.DS-5: Protections against data leaks are implemented. [1, 2, 3, 4, 5, 6, 7]	There is no protection against data leaks when the system is up and running.	Because individual files containing sensitive data are encrypted and as long asusers have no direct access to keys, no one will be able to extract the contents of an accidentally or intentionally leaked file.	Because individual files containing sensitive data are encrypted and users have no direct access to keys, no one will be able to extract the contents of an accidentally or intentionally leaked file.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. [1, 2, 3, 4, 5, 6, 7]	SED and FDE technologies do not control access to sensitive data on booted systems.	Access attempts involving encrypted data are logged. The technology generates log reports for log review/audit purposes.	Access attempts involving encrypted data are logged according to policy so that each action can be tracked back to its source. The technology generates log reports for log review/audit purposes. It also integrates with SIEMs for investigating unauthorized access attempts and other reporting.
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. [1, 2, 3, 4, 5, 6, 7]	SED and FDE technologies do not control access to sensitive data on booted systems.	Typical FSE technologies restrict basic access to files, but they do not restrict administrator access	Authorized users can decrypt files; privileged users can back up encrypted files and perform other administrative duties but cannot access the contents of encrypted files.

As Table 1 demonstrates, FSE technologies provide superior capabilities for protecting sensitive data stored in the cloud as compared to SED or FDE technologies. SED and FDE technologies only protect stored data when cloud servers are not booted, so they are only able to stop attackers who gain physical access to cloud server storage devices, a rare circumstance. Nearly all threats against sensitive data in the cloud come not from physical attacks, but from logical attacks. FSE technologies can stop both physical and logical attacks, so the attack surface for data stored in the cloud using FSE technologies is greatly reduced.

Another major advantage of FSE technologies is that the encryption moves with the file. If a sensitive file protected by FSE technologies is copied from a cloud system to another system, that copy will also be encrypted. Many data breaches are caused by user errors, such as accidentally emailing the wrong file attachment; FSE greatly reduces the chance of this happening for cloud-based files.

Put simply, SED and FDE technologies don't make the grade when it comes to meeting compliance requirements for protecting sensitive data in the cloud.

Differences Among FSE Technologies

The two rightmost columns of Table 1 not only show that FSE technologies are much more effective than SED and FDE technologies, but also that all FSE technologies are not created equal.

Many FSE technologies have limited key management capabilities that necessitate manual maintenance. They may store the encryption key in the same place as the encrypted data, which puts the encrypted data at much greater risk of compromise and violates requirements from several security compliance frameworks and regulations. Instead of relying on manual key management processes, some leading FSE technologies have highly automated solutions for key management. These policy-driven key management capabilities take care of key generation, distribution, rotation, and termination behind the scenes.

In addition to these capabilities, some leading FSE technologies provide other tools to alleviate the burden of key management. For example, an FSE may support the definition and enforcement of access control policies to provide granular access control to different files, instead of the organization using more encryption keys to accomplish granular access control. Using more keys leads to higher management costs and increased risk of a key being compromised. Using FSE-provided policy-based access controls makes it much easier, cheaper, and safer for an organization to restrict access to encrypted files.

As the rightmost column of Table 1 shows, a particular industry-leading FSE solution, Vormetric Transparent Encryption, provides much more comprehensive protection for sensitive data stored in the cloud than typical FSE solutions. In addition to supporting all the standard FSE features, as well as highly automated key management and policy-based access controls, Vormetric Transparent Encryption also supports the definition and use of multiple data security administrator roles through Vormetric's Data Security Manager (DSM) product.

The roles created and maintained through the DSM are extremely useful because they allow an organization to grant varying levels of access to encrypted files for different administrators (both people and devices). For example, one administrator might only need read access to encrypted files so they can be backed up, without also having the ability to decrypt those files. Another administrator might need the ability to decrypt files in case of emergency. Role-based administration enforces separation of duties and further differentiates Vormetric Transparent Encryption from typical FSE technologies.

By using roles that leverage Vormetric Transparent Encryption's support for Active Directory, LDAP, and other enterprise authentication solutions), an organization can easily enforce the least privilege principle for its encrypted files. The importance of this for cloud-based sensitive data cannot be understated because of the presence of third parties with elevated privileges to systems where the sensitive data resides. Basically, this approach enables an organization to reduce its risks and leverage the cloud for more workloads and applications.

Conclusion

The confidentiality of sensitive data at rest in the cloud must be protected from physical and logical threats to prevent data breaches. Most organizations also need to protect this data because of requirements from one or more security compliance initiatives. In nearly every case, the best solution for this is to use storage encryption technology (i.e., SED, FDE, or FSE).

These technologies vary in terms of the degree of protection they provide. SED and FDE technologies only protect stored cloud data when cloud servers or storage devices are not booted. Simply put, these technologies only protect against physical threats targeting the equipment in a cloud data center. In contrast, FSE technologies provide strong protection for the confidentiality of a sensitive file at all times except when the file is actually being used.

Some FSE technologies go further by offering additional security features, including policy-based access control, DSM administrator role definition, integration with existing enterprise identification and authentication technologies, and highly automated key management. Vormetric Transparent Encryption brings all of these features together in a single product to effectively protect sensitive data stored in the cloud while also making that protection stronger, easier, and lower cost.

Cloud customers and cloud service providers should work closely together to ensure that cloud customers are clearly informed as to the encryption at rest capabilities the cloud service provider offers and what those capabilities can protect and under which circumstances. Cloud service providers should make FSE technologies available to their customers, and in turn customers should use those technologies to prevent data breaches and ensure compliance with regulations and other sets of security requirements.

For more information on Vormetric Transparent Encryption, visit the Vormetric website at http://www.vormetric.com.

Use Case: Securing Stored Cardholder Data

To illustrate how the concepts from this paper affect real-world security, let's walk through a use case involving a US retailer. This retailer performs payment card processing, so it is responsible for safeguarding the confidentiality of cardholder data. The primary set of requirements the retailer must meet is the Payment Card Industry Data Security Standard (PCI DSS) version 3.1. Suppose that this retailer recently conducted an audit of its security controls. The audit indicated that while the retailer was generally providing adequate protection for sensitive data, it was not following sound practices for protecting cardholder data stored in the cloud. This included multiple violations of PCI DSS version 3.1 requirements. To address these issues, the retailer decided to improve its security practices for cloud-based cardholder data.

PCI DSS requirement 3.4 states that organizations must ensure that all primary account numbers (PANs) are not readable wherever they are stored. Although this requirement allows the use of any of four methods for making the numbers unreadable, three of the options rely on the use of strong cryptography. The fourth option is to truncate each PAN, which causes loss of data and is unacceptable to the retailer. The cryptography options protect the stored PAN from external and internal threats that use a wide variety of physical and logical attack techniques, such as infiltrating the guest operating system or virtual machine storing the PAN.

PCI DSS requirement 3.4.1 provides additional details on acceptable cryptographic solutions. Specifically, it mentions the use of disk, file, and column-level database encryption, and it says that if disk encryption is used to protect PANs, "logical access must be managed separately and independently of operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials.)"

In other words, requirement 3.4.1 makes it clear that SED and FDE technologies are not sufficient to protect PANs stored in the cloud. SED and FDE are disk encryption technologies that rely on a person being authenticated by the operating system or the underlying hardware or software, which then triggers the decryption of the disk. The intent of requirement 3.4.1 is to have a separate authentication mechanism just for decrypting PANs. Using the same authentication credentials for multiple purposes is not a recommended practice because a single compromise of a credential will be much more damaging. SED and FDE technologies cannot protect data in the runtime cloud environment, but FSE technologies do. Retailers and other organizations storing PANs in the cloud must use an FSE solution such as Vormetric Transparent Encryption to achieve compliance with PCI DSS requirements.

As demonstrated in Table 1, there are several other PCI DSS requirements related to protecting the confidentiality of cardholder data, and the Vormetric Transparent Encryption solution fully supports all of them. Vormetric Transparent Encryption is particularly helpful for automating and managing cryptographic key management processes. PCI DSS requirement 3.5 directs organizations to "document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse." This is much broader than simply protecting PANs; the scope of this is all keys used to protect any portions of stored cardholder data.

Documenting and implementing these procedures sounds simple enough, but in practice it can be incredibly complicated. For every operating system, service, and application that has to perform cryptographic operations, the organization needs to make decisions about the cryptographic algorithms, the algorithm mode or modes, the minimum key length for each type of key, the cryptoperiod for each key, and the values of many other parameters. Information about these cryptographic attributes is generally very hard to understand and is quickly outdated. An organization then has to implement and configure the necessary cryptographic technologies, and manage and maintain them on a daily basis.

Additional PCI DSS requirements related to keys for protecting stored cardholder data include the following:

- Minimizing access to secret and private keys
- Storing each secret or private key so its own confidentiality is protected (most often through additional encryption mechanisms and separate secure storage of their keys)
- Minimizing the number of locations used to store each secret or private key
- Documenting and implementing secure key management processes and procedures that include key generation, distribution, storage, replacement, retirement, archival, and destruction

Vormetric Transparent Encryption supports all of these requirements through its flexible and robust key management capabilities and its policy-based encryption implementation.

Cryptographic implementations are only one part of securing stored cardholder data. Organizations are also responsible for implementing user and device authentication, access control, and other means for ensuring that only authorized users can access the cardholder data when necessary. This includes restricting access by system and database administrators, as well as other privileged users who pose a significant insider threat to cardholder data. All attempts to access cardholder data must be monitored continuously and alerts generated when unexpected activities occur.

Most IT decision makers are not aware how difficult meeting PCI DSS requirements can be without outside expertise. Fortunately, there's a solution that can help retailers and other organizations with stored cardholder data to more easily meet PCI DSS requirements: Vormetric Transparent Encryption. Unlike SED, FDE, and typical FSE technologies, Vormetric Transparent Encryption meets all of the PCI DSS technology requirements. This includes protecting stored data at all times except when the data is actually being used, providing robust key management services, logging all attempts to access encrypted data, and generating alerts when unusual access attempts are observed. By taking advantage of Vormetric's expertise in securing sensitive data stored in cloud-based environments, an organization can save itself a great deal of time and effort in achieving PCI DSS compliance and preventing data breaches.

In addition to supporting all the PCI DSS requirements already mentioned in this paper for safeguarding stored PANs and cryptographic keys, Vormetric Transparent Encryption also supports several other PCI DSS requirements, including the following:

- Requirement 7: Ensures that only authorized users may access cardholder data when needed in the course of their jobs. An important component of this is preventing administrators from decrypting cardholder data.
- Requirement 8: Supports integration with existing enterprise authentication systems. Prevents anyone other than authorized administrators and processes from directly accessing encrypted data stored in databases.
- Requirement 10: Monitors and audits all attempts by both users and processes to access encrypted cardholder data.

FDE and SED products do not support these requirements, just small parts of Requirement 3. In comparison, Vormetric Transparent Encryption helps organizations address several PCI DSS requirements with a single solution. For additional information, please visit the Vormetric PCI DSS compliance page at: http://www.vormetric.com/compliance/pci-dss.

For more information on how Vormetric can help secure cardholder data for your organization, see http://www.vormetric.com/data-security-solutions/industries/data-security-compliance-solutions-for-the-retail-industry.

About Vormetric

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual, big data, and cloud environments. With data at risk as never before, Vormetric helps over 1500 customers, including 17 of the Fortune 30 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database, and any application—anywhere it resides—with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation, and security intelligence.

www.vormetric.com