WHITE PAPER

PARADOXBOX

A TOOL TO HELP WITH GDPR COMPLIANCE THROUGH EFFECTIVE ENCRYPTION

TERILYN FLOYD-CARNEY | CISSP, CISA, HCISPP, CCSFP, QSA, PA-QSA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

INTRODUCTION

Secure Channels provides innovative, effective security solutions designed to complement existing investments in security. Their products offer advanced data protection, adaptable encryption, authentication, enterprise confidentiality solutions and proximity-based monitoring and intelligence capabilities.

In this white paper, Coalfire will discuss how the Secure Channels' ParaDoxBox™ Enterprise Data Protection Platform can provide a secure environment for an organizations' data that needs to be protected through advanced encryption, key management, and authentication controls.

AUDIENCE

This assessment white paper has two target audiences:

1. **Senior Leadership and Mid-Level Decision Makers:** This audience may be evaluating ParaDoxBox™ for use within their organization to support GDPR compliance initiatives.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating ParaDoxBox™ for use within their organization for regulatory compliance.

THE GENERAL DATA PROTECTION REGULATION (GDPR)

OVERVIEW

Although the GDPR pertains to the rights of European Union (EU) residents, its impact is global since it applies to any organization collecting or processing that data regardless of where the organization is located. A U.S. based e-commerce firm selling goods to EU residents or a Canadian marketing firm collecting information about EU residents for product development purposes would both be subject to the regulation. It is likely that organizations based outside of the EU will be caught unaware by these new regulatory requirements unless they not only have an understanding of the requirements but also understand their business processes and whether personal data pertaining to EU residents is part of those processes.

The GDPR identifies two types of entities that fall into scope with different but overlapping responsibilities.

Controllers are organizations that own the relationship with the affected EU residents and determine what data is collected and for what purpose. Controllers are responsible for ensuring the rights of the EU residents ('data subjects' under the regulation) are protected and their personal data is secured. Examples of Controllers include, but are not limited to: e-commerce firms, healthcare providers, financial services firms, social media platforms, and other business models that aggregate personal data.

Processors are organizations that process data on behalf of Controllers. While these third-party Processors do not have the same direct responsibilities regarding EU resident rights as Controllers, they are responsible for ensuring that the processing services they perform facilitate the Controllers' compliance with the regulation. Liability for breaches and non-compliance is shared between Controllers and Processors, so Controllers must carefully select and manage vendors acting in this role.

AFFECTED DATA

Personal data that falls into scope for the GDPR can be generally described as information related to a uniquely identifiable "natural" person, excluding corporations or other legal entities. Examples include name, physical address, email address, and credit card or other identifying numbers. The regulation also recognizes sensitive categories of data that cannot be processed without explicit consent from the individual, such as racial or ethnic origin, health, or biometric information.

DATA PROTECTION

More and more organizations have felt the pain of data breach or loss. In some of these cases encryption controls have not been implemented the way they should be within the organization, and data has been lost. There have been many situations over the years in which laptops have gone missing, either lost or stolen, and their sensitive data was not encrypted. A server can also be compromised, resulting in information being stolen or leaked. In any of these cases, there may be regulatory requirements to report the data leaked. Encryption is not a magical solution and cannot solve all problems, but it can mitigate many of the security risks to sensitive data by reducing areas of exposure.

One way to meet regulatory requirements for consumer data protection as is required to comply with GDPR Article 32, is with encryption, both at rest and in transit. In addition, there is the burden of locating and securing data within an organization not to mention every endpoint. ParaDoxBox™ Data Protection Platform from Secure Channels, offers an integrated central management platform with rich enterprise administration features that manages data on endpoint devices with full disk, partition, and/or file level encryption as well as cloud hosted data locations.

The ParaDoxBox™ Data Protection Platform has a cloud based administrator platform that can be used to easily deploy to all of an enterprise's endpoints. Once installed and registered, ParaDoxBox™ can be used to provide any desired combination of full disk, partition, volume, hidden volume, file and file-for-sharing encryption at the administrator's discretion for any operating system supported file system, and has the ability to create hidden (encrypted) volumes on the fly. With the file-for-sharing encryption feature the files can be restricted to specified individuals.

Key management is a critical componenet of encryption, the effective key security and key distribution of any solution ultimately depends on protecting the keys. If the key is exposed, the data being protected with the key is, essentially, exposed. ParaDoxBox's administrative functionality guarantees that the enterprise retains complete, secure control of keys, ensuring data access and security.

For data in transit, the data is traveling across the network, which dictates different encryption solutions for the data in transit. Each organization should identify all data flows to understand where they are vulnerable. ParaDoxBox™ Data Protection Platform incorporates advanced Secure Channels' PKMS2 E3 Protocol encryption for data in transit. The PKMS2 E3 Protocol encryption extends the effective key length of standard 256-bit ciphers by approximately 50% to 387 bits. Data protected using the PKMS2 E3 Protocol remains protected even if one of the eight available encryption suite's ciphers is found to be insecure in the future. Additionally, the effort an attacker must exert to recover an entire message is significantly increased.

Another important tenant of layered security best practices involves the use of multifactor authentication to ensure only for protecting and controlling sensitive data is ensuring only authenticated users have access the data. The ParaDoxBox™ Data Protection Platform uses enhanced multifactor authentication gateway, Secure Channel's SUBROSA® technology; supporting something known, possession, biometric, machine inherence and external location based managed knowledge factors. These authentication credentials that can be tailored or combined based on enterprise requirements to provide the desired level of authentication assurance. SUBROSA's credentials technology, are long (thousands or tens of thousands of bits), non-human readable, binary strings that are unknown to but easily entered by the user. Users can't reveal what they don't know and they can't share what they can't read or write down.

CONCLUSION

ParaDoxBox™ provides an innovative approach to simplifying and enhancing the use of encryption of sensitive data, and when properly implemented following the guidance from Secure Channels, can provide reasonable assurance against data loss, data breach, and regulatory compliance. However, as most computing environments and configurations vary drastically, it is important to note that use of this product does not guarantee security and even the most robust encryption solutions does not prevent attacks from other vectors. A defense-in-depth strategy that provides multiple layers of protection should be followed as a best practice.

ABOUT THE AUTHORS

Terilyn Floyd-Carney | Senior Consultant

Terilyn brings over 20 years of experience in the Information Technology Security field to the Healthcare team leading extensive consulting and assessments engagements against the HIPAA Safeguards, HITRUST Framework, DEA EPCS regulations, and the FDA standards.

As a lead assessor Terilyn supports assessments of all sizes with in the Healthcare sector for both HIPAA Safeguards and the HITURST Framework. Within the payment sector she supported some of the largest payment software providers in the world though the assessment process. Her experience working at a major Healthcare provider and Hospital in the Denver area is invaluable for understanding the unique environment that is Healthcare, where uninterrupted care is the first security concern.

Terilyn also works with a number of software vendors of healthcare, pharmacy and prescriber applications to support their achievement and maintenance of regulatory compliance.

May 2018

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com