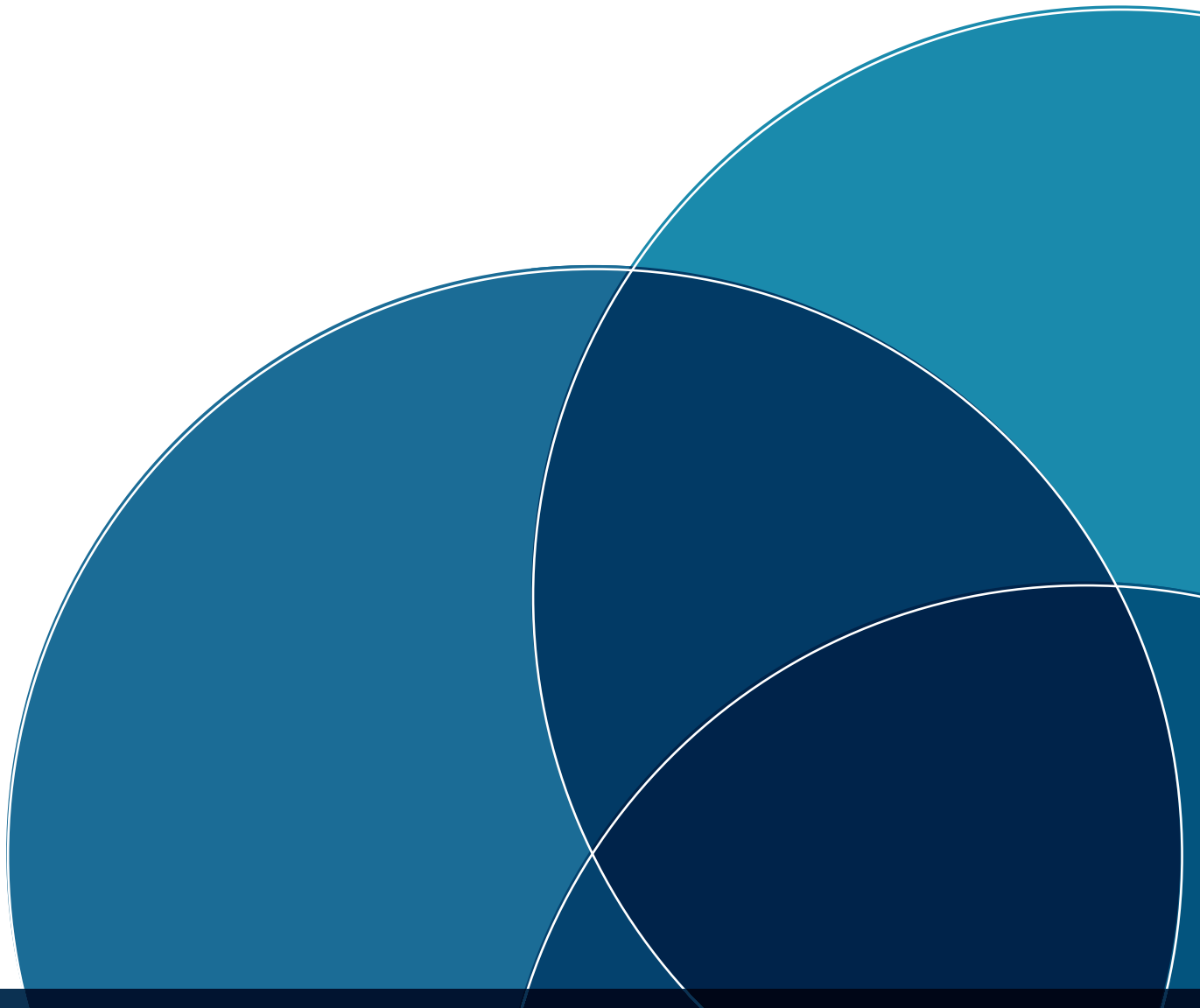
PKWARE®

DESKTOP SECURITY GUIDE

Data-centric Security: Encryption Essentials for Modern, Efficient Protection

JOE STURONAS CHIEF TECHNOLOGY OFFICER, PKWARE



PKWARE®

Contents

Data-centric Security:

Encryption Essentials for Modern, Efficient Protection

In Medieval times, people lived in large stone castles and walled cities to protect themselves from intruders. Protection of citizens and royals inside of these walls focused on strong perimeters: walls were tall and difficult to scale, a drawbridge closed to unwanted outsiders, moats surrounded the walls and hot oil was even poured on those who got too close.

In response, intruders developed new tactics of attack and used the latest technology to blast away at the presumably strong perimeter walls.

Fast-forward about 1,000 years and it might seem that the scenarios for protecting valuable enterprise data are entrenched in the strategies of the past. Today, organizations are spending their limited security budget on strengthening enterprise walls and fortifying access – without realizing that the changing nature of attacks puts their data and business at risk well beyond the traditional perimeters.

Focusing only on perimeter security is a battle better suited for bygone times. Nowadays, sensitive data regularly moves from platform to platform and from endpoint to endpoint, inside and outside the organization. Some take the approach of securing endpoints and network connections. However, the reality is that these strategies leave data exposed at certain points in the storage and transfer process. In a data-centric security

approach the data itself is protected and is not dependent upon the individual endpoint or network security schemes. Data-centric security involves protecting the data itself through the use of data encryption and authentication that are enforced by policy administration.

To expand upon this notion we have identified three approaches to data-centric security that do not involve huge investments in infrastructure or resources. These approaches, when implemented together, provide a strong and effective data-centric security plan as part of an in-depth enterprise security strategy.

1 Data Protection 2 Policy Administration 3 Contingency Key

In this security guide we will outline the ways in which data-centric security can be an essential part of your overall security architecture. An effective data-centric security plan allows organizations to protect their vital information assets without relying solely on endpoint security.

Data Protection

Encryption Basics

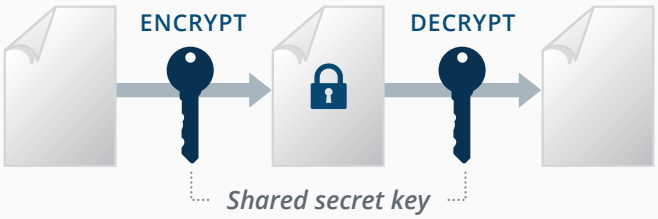
Data protection goes as far back as Julius Caesar. Encryption in Caesar's time of the Roman Empire was used to protect private correspondence. In those days, the encryption was simplistic, though effective for the times. Caesar's cipher was based on a scheme of alphabetic characters that rotated by 13 spots from their origin (known in modern application as ROT13). Figure 1, bottom, gives a basic comparison of the standard alphabet and its cipher.

This basic type of encryption also has an obvious downside. If someone intercepted the information and was able to reverse engineer the encryption process, then they would be able to decrypt every message encoded with ROT13.

While modern day encryption is much stronger and uses highly complex math, a weak key in the encryption process will make for a weak link in your entire data security chain. And, that could cause the data to be easily decrypted.

Data encryption today can be categorized into two groups: symmetric key encryption and asymmetric key encryption (also known as public key encryption).

Symmetric key encryption is most commonly associated with password or passphrase based encryption.



Symmetric Key Encryption

FIGURE 2 — THE FLOW OF A MESSAGE PROTECTED USING SYMMETRIC KEY ENCRYPTION.

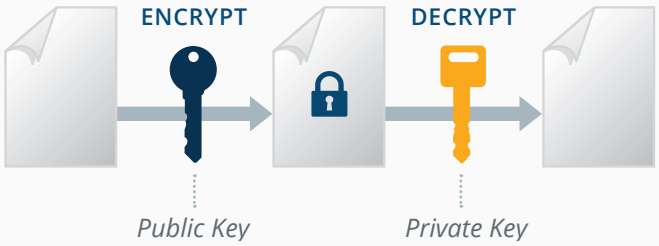
Figure 2, above, shows how the same key is used for encryption and decryption. Symmetric key encryption works best for non-persistent data, or static, non-transactional data.

Non-persistent data is typically encrypted with a symmetric key (passphrase) and sent to another entity for use. In this way the data is protected at rest before the data is sent, while it is in motion and when it reaches the data consumer. There is no need for the data to persist.

However, symmetric based encryption does not scale well particularly when the data needs to persist or it needs to be shared with multiple recipients.

P	K	W	A	R	E	**PLAIN TEXT**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕		↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
C	X	J	N	E	R	**CIPHER TEXT**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

FIGURE 1 — A CIPHER FROM THE TIME OF CAESAR, KNOWN IN MODERN APPLICATIONS AS ROT13.



Asymmetric Key Encryption

FIGURE 3 — THE FLOW OF A MESSAGE PROTECTED USING ASYMMETRIC, OR PUBLIC KEY ENCRYPTION.

Alternately, when data needs to be protected for longer periods of time for compliance or regulatory purposes and when it is going to be shared with multiple sets of recipients then the best option is asymmetric keys, otherwise known as public key encryption. Public key encryption uses both a public key and a private key. The public key is used for encryption and authentication while the private key is used for decryption and digital signing. The two keys are mathematically related through the use of cool math including prime integer factorization, discrete logarithm and elliptic curve relationships. The strength of the encryption is based on the computational intensity that it would take to exhaustively determine the private key. The public key should be easily accessible to any authorized user, and the private key should be kept private and protected. For more detail, see Figure 3, above.

One or more public keys can be used to encrypt data and any of the corresponding private keys are able to decrypt the data. (Public key encryption is also a critical component of contingency key and policy administration, which we address later on).

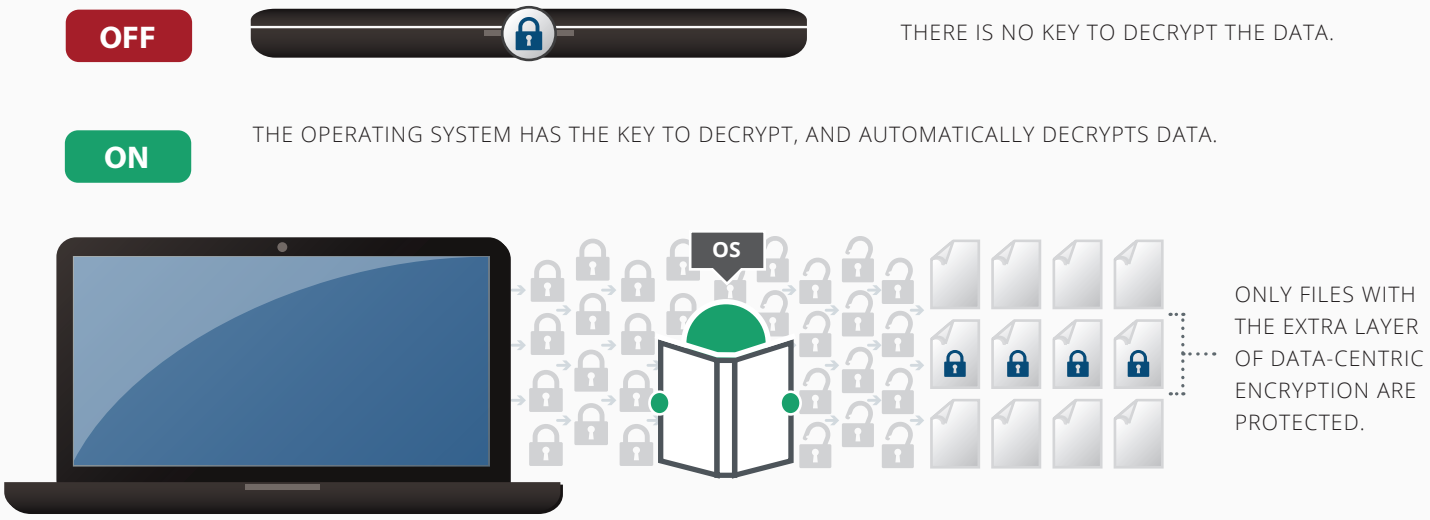
An issue with symmetric key encryption is that companies often end up dealing with so many different passphrases that they are left with uncontrolled encryption. The origins of these uncontrolled passphrases range from employees that have left the organization, to partner exchanges that have gone stale, to rogue employee behavior.

One such open source provider, 7-Zip, has a symmetric key approach. Here's how their symmetric key approach operates. Company A agrees to use symmetric key encryption with a password to encrypt/decrypt data for an exchange with Company B. Then Company A needs to exchange data with Company C. To make sure Company B can't decrypt Company C's data in this exchange (and vice versa), Company A will need to use different passwords for both. The problem of different passwords becomes intractable when Company A then needs to exchange data securely with 100 different companies.

On the other hand, customers using asymmetric encryption keys, as offered in SecureZIP for Windows Desktop, are able to take advantage of public key encryption to simplify the above scenario.

With asymmetric encryption, Company A encrypts with a public key Company B obtains from a public LDAP directory. A public key created from this directory is unique and easily accessible to Company B. This would then be the case for any other number of companies with which Company A would like to share secure data.

FIGURE 4 — WHOLE DISK ENCRYPTION **SECURITY WHEN OPERATING SYSTEM IS POWERED ON VS. OFF.**



Data-centric Encryption vs. Whole Disk Encryption

Whole disk encryption (or WDE) provides a semblance of encryption at the device level. What is sometimes confusing is that WDE is not data-centric security and provides limited protection. Whole disk encryption (as well as folder encryption, such as that provided by Microsoft® BitLocker®) is useful when the endpoint is powered down and falls into the wrong hands. An "endpoint" is any extended enterprise network device where there is physical storage and the network device contains enterprise data (examples include server, desktop, laptop, tablet, mobile phone). Because the data cannot be accessed without the proper credentials it is presumed that the data is "safe".

However, when the endpoint is powered on and the operating system is up and running, whole disk and folder encryption provide no protection. Files are automatically decrypted as they are accessed and moved off the endpoint. So, the data is in motion and unencrypted – and thus is subjected to the same risks as if it were not encrypted at all.

Data-centric security protects the data when the endpoint is powered off as well as when the operating system is running. Data in an encrypted ZIP or OpenPGP file remains encrypted as it is copied off the endpoint. Whole disk encryption and folder encryption are useful as another layer in the defense in depth security approach which, provides layers of security that protect data at rest, data in motion and data in use. However, when WDE or folder encryption are used on their own, they don't provide true data-centric security.

Use Case: Swiss Manufacturer Protects Data at the Source

A manufacturing company in Switzerland is probably one of the best examples of implementing very effective defense in depth endpoint protection globally throughout the organization. The company was not satisfied until they had data-centric security implemented on their endpoints. They had implemented whole disk encryption, as well as a suite of firewall, VPN, anti-virus, malware and spyware. The CISO's point was very simple. He was doing everything he could to protect the 30,000 endpoints. But what he could not protect were the 1,400 administrators that had access to all the content from those endpoints. He wanted those 1,400 administrators to have the ability to back up the files but not see the contents, which is what data-centric security does. He wanted the administrators to back up the mergers and acquisition documents on the laptops of the CEO and General Counsel, but not see the contents. By locking down the data at its source and authorizing access, this CISO secured data regardless of the endpoint and enabled employees at all levels to keep their data protected.

What's Your Data Security Philosophy?

A variety of factors such as risk appetite, resources and regulatory demands pit companies in a race where they sometimes overlook the greater security threats. Are you trying to be very secure or are you focused merely on a lower threshold, like compliance? Security is very gray and complicated. Balancing your security philosophy should, at its core, mean you can out pace the auditor as well as the hackers.

If organizations fear the auditor more than they fear the bad guys, then the organization's data is likely not secure. Worse yet, the bad guys know the regulations and the vulnerable areas not covered by regulation and that's where you might lack necessary attention. Companies that fear the auditor simply work to pass the audit. Companies that fear the bad guy look for all the areas of vulnerability by hiring third-party penetration testing (Pen-Testing) to do both black box testing (where the pen tester can't see the underlying code) and white box testing (where the pen tester can see the underlying code).

There is a common myth that regulation and compliance, such as Payment Card Industry Data Security Standard (PCI DSS), benefits data security. In other words, thanks to these mandates audited by Qualified Security Assessors (QSAs), data is more secure where it otherwise would not be. That leads some organizations in compliance to believe that they are also secure. This is not necessarily true. It only means that they are following the regulation. Compliance and security are not synonymous.

So, how could a regulation aimed at data security actually make companies who comply with it less secure? It happens when the compliance benchmark is seen as the main goal of data protection. Here, regulation sets a basement for security, which lowers the bar for security rather than raising it. Since the regulation only focuses on the minimum amount of security required to enforce the regulation across all companies, it in fact promotes the lowest common denominator.

Compliance with any standard does not equate to an assessment whereby a company's security is automatically appropriate. Standards are not necessarily commensurate with the size and complexity of the business environment or the type and amount of data involved. We highly recommended that security measures go well beyond the well-intended parameters of required mandates.

There are numerous examples of organizations that were in compliance with a regulation but still suffered a security breach. The most notable example is Heartland Payment Systems. They were found to be in PCI compliance yet lost millions of credit card data records because they were not secure enough. Deemed the largest credit card crime of all time, for months hackers had broken into Heartland computers used to process 100 million transactions from more than 175,000 merchants. Card issuers flagged suspicious transactions which revealed a masterminded scheme to steal more than 130 million credit and debit card numbers as well as personally identifying information

(PII). The hacker had breached Heartland a year before it was discovered, initially through an SQL injection attack. That then allowed the hacker access to all internal systems whereby the hacker was now acting as an insider with access to the underbelly of the sensitive systems.

Heartland has paid out millions to settle claims over the breach. As far as the data security ramifications, a post-mortem of the breach resulted in changes to PCI-DSS policies, as well as a move by Heartland toward a holistic data-centric security approach.

Encryption as a Standard: FIPS 140-2

Most U.S. government agencies and the private sector companies that work with them, such as banks and healthcare insurers, are required to encrypt data with software that meets Federal Information Processing Standards (FIPS) 140-2 compliance.

Data encryption software is FIPS 140-2 compliant when it uses cryptographic algorithms that have been validated through the U.S. National Institute of Standards and Technology's (NIST) Cryptographic Module Validation Program (CMVP). Cryptographic modules that have been validated are issued a certificate number. Only software that is able to identify the NIST certificate number for the cryptographic algorithm's FIPS 140-2 validation can be FIPS 140-2 compliant.

SecureZIP for Windows Desktop is FIPS 140-2 compliant and it lists corresponding FIPS 140-2 validated cryptographic algorithm certificate numbers. Not all FIPS levels are the same. For instance, WinZip® is only FIPS 197 compliant, which is not the same crypto depth and standard as FIPS 140-2. FIPS 197 addresses just the AES algorithm and does not address other more comprehensive requirements found with FIPS 140-2. For data encryption software to be FIPS 140-2 compliant, while in FIPS mode it must list the FIPS 140-2 validated cryptographic libraries that it uses along with the certificate numbers.

Policy Administration

Policy administration, or policy management, is the means by which the organization can exercise oversight, control and proper use of strong encryption in the enterprise. This includes ensuring that encrypted data can be recovered should a given encryption key (public and private) be forgotten, deleted or corrupted. Only with oversight of the encryption process of what data is encrypted by users will organizations be able to use encryption as broadly and effectively as the current threat and regulatory environments require.

Auditors, regulators and customers all confirm that strong encryption is the "safe harbor" for sensitive data – even if the data is lost or stolen. Inevitably, security professionals have to grapple with the practical management of encryption in the context of the existing best practices. Certainly, sensitive data should be encrypted, but how is data oversight, recovery and audit or compliance inspection addressed?

The first layer of control is determining who in the organization has a legitimate need to use encryption. For example, senior executives, salespeople, human resources or the finance group may require access to sensitive data while the typical call center operator or fulfillment agent does not. The organizational risk of encryption use can be greatly reduced by ensuring that the encryption application available to these latter groups restricts their use. Unfortunately, several of the popular compression and file management utilities fail to provide this capability, leaving the powerful tool of encryption in the hands of many who are unprepared for its appropriate use. Policy management enables the organization to provide encryption to those knowledge workers to use it with the appropriate control and oversight to satisfy auditors and regulators.

To be safe, we recommend that organizations choose a security solution that encrypts the data at the file-level before it leaves a trusted zone. A quality data-centric solution protects data, enables secured data to across all computing platforms and operating systems, and works within any computing environment. This gives you end-to-end control over your data. Used properly through policy administration, data-centric encryption prevents unauthorized access and tampering regardless of the state of your data and regardless of where the data travels.

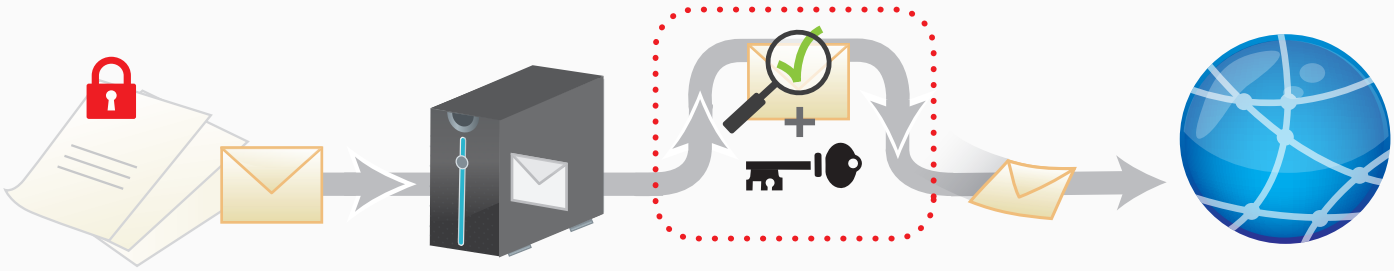
Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. The data remains protected regardless of whether it is in motion or at rest. The owner of the decryption keys maintains complete control over the security of that data and determines access to that data. Encryption procedures can easily be integrated into the existing workflow.

For data-centric protection to be effective, it needs to be enforced by a security policy such as the PKWARE Policy Manager, which is a Microsoft Management Console (MMC) snap-in to enforce data security encryption policies. For example, certain departments might need to only encrypt with FIPS 140-2 compliant crypto. Those users could be enforced to use FIPS 140-2 compliant data encryption, while other users might be required to use an AES-256 bit encryption algorithm. Different policies can be deployed for different categories of users depending on the business and regulatory requirements.

Another element of policy management, data loss prevention (DLP), defines the type and strength of encryption used as well as the assignment of contingency keys to insure viable recovery of the encrypted information. Gone are the days where DLP merely inspects unencrypted information as it egresses the organization. Just because data is encrypted, does not mean that it should still leave or enter the organization. DLP inspects encrypted information as it travels through and from the organization (for detail, see Figure-5, below). A policy based contingency key ensures the DLP inspection. DLP can then make the determination to allow the information to egress, or block it based on organizational policy.

Based on independent research by the Ponemon Institute, a 2013 multi-national survey concludes that "provisioning and access policy management" is the most important endpoint management feature. In addition, Osterman Research, an independent analyst specializing in workforce security and processes, reported in a survey that adoption of policy-based, automatic encryption increased from 27% in 2012 to 35% in 2013. Adoption of policy management that is tightly aligned with security strategies is definitely on the rise as security minded organizations look to increase protection of their critical data assets.

FIGURE 5 — THE POLICY ADMINISTRATION PROCESS, INCLUDING DATA LOSS PREVENTION (DLP).



EMPLOYEE SECURES DATA AT THE FILE LEVEL & SENDS.

POLICY MANAGER ADDS CONTINGENCY KEY & VERIFIES APPROPRIATE ENCRYPTION IS USED. DLP INSPECTS THE ENCRYPTED FILE TO ENSURE POLICY AS WELL AS SECURITY.

FILE IS SENT WITH CONTINGENCY KEY. DLP & ORGANIZATION HAVE ACCESS.

Contingency Key

A contingency key is a private key held by the organization using their current key management/access methodology, whereby designated individuals have the corresponding private keys that allow decryption of data for contingency access. The contingency key holders could be the InfoSec team from an organization-wide perspective, or departmental owners at a more granular level.

Policy settings do not have to be the same throughout the organization. Policy management can be as granular as desired even to the point where each business unit or department has their own policy settings, and thus their own contingency keys. Policy management enforces that contingency keys are used effectively throughout the organization.

Protecting data through encryption without policy management and contingency keys can be dangerous and reckless. Encryption without proper policy management puts the organization at risk of quickly losing control of their data. Employees will be able to encrypt, but if someone leaves or is a "bad actor," the organization may lose access to that encrypted data. Focusing on data protection really means implementing controlled encryption, with policies in place that include contingency keys with every encryption operation so that the organization never loses control of the data, even if someone leaves.

Strong encryption with no policy based contingency key creates a high risk for lost data. For instance: A government entity we spoke with thought they were acting in good conscious by allowing knowledge workers to encrypt data with a product incapable of providing policy based contingency keys or private key escrow. As it turned out, this encryption product was also not the level of FIPS compliance they needed, FIPS 140-2. By allowing the use of this product, they were left with gigabytes of encrypted, inaccessible, useless data. If they had only implemented a FIPS 140-2 compliant, policy based encryption solution, all of that data would have been protected and accessible.

Security minded companies should be cautious when evaluating encryption solutions. Providers like WinZip and 7-Zip enable organizations to secure data with password-based encryption however they do not have policy management or contingency key capabilities. An enterprise security product like SecureZIP for Windows Desktop provides the ability to centrally manage encryption through policy, so that one or more contingency keys can be applied to every encryption operation throughout the enterprise. This gives the organization peace of mind in how encryption is being used and the ability to access encrypted data for audit or recovery purposes.

Use Case: The Importance of Passwords and Policy at One German Manufacturer

In another example, a manufacturing company in Germany asked if we could crack an encrypted ZIP file they provided us. A product manager had encrypted the designs for a new product and sent them to a competitor. We could tell that it was encrypted with AES-256 encryption which employees had access to on their desktops/laptops. We explained to the company that this file was encrypted using strong security, without any contingency key administered by policy. Without the password, there was no way to decrypt the encrypted file. They could tell from the file name this was probably rogue behavior, but without the ability to prove what was in the file, they were not able to pursue criminal charges. Worse yet, having this information in the hands of their competitor was very damaging.

DATA PROTECTION

ASYMMETRIC ENCRYPTION

SECURITY FOR DATA AT REST, IN MOTION AND IN USE

POLICY ADMINISTRATION

CONTROLLED SECURITY

MEET COMPLIANCE LIKE FIPS 140-2

CONTINGENCY KEY

MASTER ACCESS

PROTECTION FROM LOSS OR ROGUE USE

Summary

Enterprise security is really about defense in depth. The various layers of security protect data at rest and as it moves outside of the enterprise perimeter. Today's security reality is that data is moving from many different endpoints and across many different platforms, making it impossible to protect every data endpoint in a consistent, comprehensive manner. By focusing on protection of the data itself, the dependency on endpoint protection is less critical and risks are reduced.

Protecting the data takes a three-pronged approach:

1 Data Protection 2 Policy Administration 3 Contingency Key

With this combined, data-centric approach your organization can make efficient steps toward protecting your data while maintaining control and access in the face of today's evolving threats.

CORPORATE HEADQUARTERS
648 N. Plankinton Ave.
Suite 220
Milwaukee, WI 53203
1.800.219.7290

UK / EMEA
Building 3 Chiswick Park Chiswick High Road,
London W4 5YA
United Kingdom
+44 (0) 208 899 6060

Copyright © 2014 PKWARE, Inc. and its licensors. All rights reserved. PKWARE, PKZIP, SecureZIP and vZip are registered trademarks of PKWARE, Inc.
Trademarks of other companies mentioned in this documentation appear for identification purposes only and are property of their respective companies.