White Paper

Pervasive Encryption: Achieving Security and Business Gains

Sponsored by: IBM

Sean Pike
Peter Rutten
October 2017

BOLSTER THREAT DEFENSES, EASE COMPLIANCE PAIN

Encryption, if properly deployed and managed, is one of the most powerful tools that organizations can use to avoid costly and embarrassing data breaches. Yet organizations struggle with the complexity associated with the technology that often stems from a history of siloed investments of point solutions designed to largely address pools of regulated data associated with a compliance mandate.

Cybercriminal attacks have become increasingly targeted, and their continued success is evident in the data breach headlines over the past year, with millions of consumers having been impacted because the organizations they placed their trust in failed to maintain consistent encryption and key management policies. In fact, countless breach investigations identify the same staggering statistic: Of the billions of exposed records since 2013, only 4% were encrypted. The breaches frequently stem from simple human errors, employees susceptible to targeted social engineering attacks, and system glitches that lead to data loss. When digital forensics investigators are asked about the challenges that lead to costly data breaches, their answers are also eerily similar. Breached organizations often fail to gain a complete accounting of the whereabouts of sensitive data and invest in security products without ensuring that policy enforcement is being applied to protect the most precious corporate assets and regulated data from external attackers and insiders.

This IDC study found that if the tools were available to deploy encryption ubiquitously, without disrupting existing third-party and enterprise-developed applications or employee workflow, the data breach risk could be significantly reduced while decreasing IT administrative costs. The mandatory requirements for this approach are centralized policy and key management and the establishment of a comprehensive corporate encryption strategy.

Buying multiple products can be costly, but more importantly, it can result in silos of protection and create complexity that attackers seize on. Organizations generally don't go out and shop for multiple products. Separate business units, mergers and acquisitions, and other activities can lead to the creation of these protection silos, thereby resulting in multiple individuals and groups within organizations being responsible for managing encryption keys and a lack of awareness over where encryption should occur and whether intellectual property and other sensitive data are protected. Sadly, for many organizations, encryption ultimately becomes a necessary evil designed to assuage an auditor's scrutiny.

A growing number of organizations, prompted by the robust security components within their mainframe systems, are revisiting their encryption strategies to gain situational awareness and in turn bolster their security postures. This document explores how security professionals can leverage the integrated IBM Z security components to support the adoption of a pervasive encryption strategy — a strategy that encrypts all data at rest and in flight and that provides greater security over the increasing data and transaction volumes driving the rate of application changes made by enterprises.

IDC's interviews with chief information security officers (CISOs) found strong interest in the adoption of pervasive encryption and that many organizations have already started implementing pervasive encryption as part of their corporate encryption strategy. The CISOs told IDC that the approach supports ongoing business requirements by limiting application changes, centralizing key management, and ensuring proactive maintenance and monitoring of the information life cycle.

These organizations share some similarities, including the use of IBM Z for a substantial number of business-critical applications. In fact, according to an IDC survey of U.S. IT security decision makers on the topic of mainframe security, 87% of organizations told IDC that some or all of the data within their IBM Z environments is business critical. The IDC study of 100 IT security decision makers found evolving customer requirements requiring a greater emphasis on support for data protection with minimal impact on performance and a need for a substantial reduction in encryption management complexities. IDC's interviews with security professionals who manage mainframe environments frequently found the desire for policy-controlled encryption that leverages integrated cryptohardware on every core. Sixty-five percent of those surveyed said that if pervasive encryption were to be fully implemented, it would alleviate the silos, complexity, and expense associated with the adoption and support of multiple solutions across the IT architecture.

This IDC study found that pervasive, policy-based encryption can be implemented and be transparent to applications and databases. It requires tight platform integration and the ability to support heterogeneous data sets and file systems and can be implemented without requiring costly application program changes. Today's servers need modern policy controls to support pervasive encryption and simplify the task of compliance.

IN THIS WHITE PAPER

This document explores the benefits of adopting a pervasive encryption strategy through powerful, integrated security components. Modern tools must enable IT administrators to support ongoing business requirements while addressing complexity issues and reducing the compliance burden. Security professionals should be able to achieve true end-to-end encryption transparently and gain proactive maintenance and monitoring of the information life cycle. Pervasive encryption must be supported through an overarching corporate encryption strategy designed to protect and control access to the network and to the data itself.

METHODOLOGY

IDC produced this study using direct primary research, which included a quantitative customer survey, interviews with senior security professionals, and a review of existing research in this area. To understand the most important issues challenging implementers of mainframe encryption policies, tools, and practices, we conducted in-depth, qualitative discussions with chief information security officers and other mainframe security experts, exploring the issues and challenges they found most pressing. In addition, designers and implementers of IT infrastructures shared perspectives on the practical issues involved in designing and maintaining the establishment and management of efficiency within the IT infrastructure. This study reflects these research perspectives.

DATA IS THE NEW PERIMETER

The mainframe is often called the backbone of the global economy because the world's most critical applications and data rely on mainframe systems to function. Eighty-seven percent of organizations surveyed by IDC indicated that some or all of the data in their IBM Z environments is business critical. In fact, an estimated 30 million transactions per day run through a single mainframe system and as many as 60% of those surveyed indicated that IBM Z usage will likely increase over the next 12–24 months.

The increase in the velocity and volume of data being processed by organizations intensifies the need for a policy-based data protection strategy that is consistent throughout the organization. Customer expectations of security and privacy due diligence are also prompting organizations to assess and sharpen their approach. This makes data protection a key component in creating business value, supporting business growth, and enabling consistent worker productivity.

Pervasive encryption addresses the internal process and technology challenges associated with traditional data discovery and classification exercises because all structured and unstructured data is encrypted regardless of whether the data is in motion, at rest, or in use. At its core, pervasive encryption puts a layer of data protection over all corporate assets. It is managed centrally so administrators gain full situational awareness of and unified access to encryption keys and certificates. With modern tools, pervasive encryption can be achieved to ease key management pain associated with any architecture, regardless of whether data is located in a public or private cloud, on a physical server, or on a laptop or workstation.

IDC's survey and interviews with security professionals who manage mainframe environments found the following significant challenges and how pervasive encryption addresses them:

- **Encryption complexity.** Organizations have selectively applied encryption, fueling the resulting complexity in place in today's environments. Mainframe users have already done a significant amount of encryption, having gone through the process of data discovery, classification, and encryption based on the sensitivity of the information contained within the mainframe database management system. The IDC survey found encryption is frequently used in data transfers. In addition, nearly half of those surveyed indicated they use field-level encryption and more than 40% said they encrypt VSAM files. Pervasive encryption eases the challenges in the data classification process, reducing the risk associated with misclassified sensitive data by wrapping all data within a layer of encryption. It also provides the foundation from which additional layers of protection can be applied or maintained. For example, existing database encryption can be wrapped with another encryption layer, providing added protection.

- **Application changes.** Interviews with security professionals found that application changes are the bane of their existence, with these professionals seeking ways to make encryption transparent to their applications, databases, and middleware. The complexity often stems from encryption requiring changes to application logic so the application can understand and implement encryption. This puts pressure on application developers and operations teams concerned with performance and optimization because, in some cases, hundreds of applications must be modified. The fact that the data may be accessed by legacy applications, with no developer available to implement the required changes, compounds the problem. A pervasive encryption strategy supports policy-controlled encryption and eliminates the need for complex application changes. Encryption remains transparent to authenticated database users. Modern tools can tie encryption to fine-grained access controls to Linux file systems and mainframe data sets.
- **Evolving threats.** Mainframes often contain the organization's data crown jewels, making stolen encryption keys a coveted resource and favorite target of attackers. Pervasive encryption makes it difficult for an attacker to identify sensitive data because it is all encrypted. Keys are also stored securely via an embedded hardware security module (HSM), a hardened environment where the master keys are maintained. Because of on-chip acceleration, keys never reside in memory, greatly reducing the ability of an attacker to successfully carry out memory-scraping attacks. In addition, IT maintains ownership of the keys with this approach, enabling organizations to take advantage of backup and data replication services with confidence.
- **Compliance audits.** IDC found that organizations spend a significant amount of time and effort on compliance audits, often days or even weeks. Revolving-door audits conducted by a variety of regulators can be costly and impact routine maintenance. These mainframe users require a new set of capabilities that leverage the increased visibility and documentation provided by pervasive encryption. In addition, large unstructured objects that are stored within the database management system can be encrypted. Log files can also be encrypted as they are being written to disk.

VALUE OF APPLYING ENCRYPTION TRANSPARENTLY

Transparent encryption, which is at the core of a pervasive encryption strategy, provides the ability to encrypt sensitive application data on storage media completely transparent to the application itself.

Enterprises are using a combination of third-party and built-in tools for encryption. Cost is an important factor for companies investing in encryption, but IDC found the top barrier to the adoption of pervasive encryption is the need for integrated tools that ease administration and any impact on mainframe performance. Those interviewed by IDC said they need to be confident in their ability to recover any encrypted data. They added that encryption keys must be in the control of the organization.

MIPS consumption growth, fueled by increased transactions and data volume, is already taxing applications. According to a recent IDC interview with the chief information security officer at a financial services firm, the ability to apply encryption without application changes would be a significant improvement. The company's team of 12 administrators manages four mainframes containing 8PB of data associated with 500 business applications. The CISO said any changes to critical business applications can impact as many as 200 software developers. The stress is only increasing. The total number of MIPS at the financial services firm has grown 10% and is expected to increase by an additional 10% over the next two years.

The CISO said pervasive encryption, if implemented properly, could address the challenge of policy enforcement, which is a significant issue for applications that have been running for decades. He added that management and consistent enforcement of security policies and best practices are the most significant challenges.

"One of the big challenges we have really has to do with maintenance of those rules. It's not for the fainthearted," he said. "If I were to print out the rules, it's hundreds of thousands of lines … If you have to adjust something, that would be a challenge. I would say, from a security perspective, that's probably the most challenging."

According to a security architect who oversees a team of administrators and software developers, applying encryption transparently, with minimal or no impact on performance, is extremely important. Most of the activity supported by the organization's mainframes is transactional and associated with core banking, trading, and inventory management activities. Throughput is paramount, he said, followed by speed and sequential processing. One of the company's largest and most critical systems was written about 50 years ago and optimized for the mainframe environment, so required changes would likely be arduous.

PERVASIVE ENCRYPTION — KEY ELEMENT OF A COMPREHENSIVE SECURITY PROGRAM

Focusing on data security in combination with other security controls results in productivity gains and less regulatory compliance pain and is increasingly being seen as a competitive advantage as organizations shift from providing customers with pure product offerings to services delivery.

A senior security executive at an investment bank said encryption is perhaps the most important tool to protect sensitive data, but it must be implemented properly and integrated into a comprehensive security program. Policies must be updated, communicated effectively, and supported with a reliable enforcement mechanism. Nevertheless, maintaining compliance has always been a challenge, he said, adding that security administrators must not only maintain adequate data protection but also ensure that the latest software updates are applied and protection is available for ongoing threats.

"A lot of what we maintain is transaction data, but there is also obviously personal information. We definitely want to have that secured and encrypted," he said. "We've analyzed to essentially have data encrypted and decrypted and stored in an encrypted way. This was a costly initiative."

The use of encryption on the mainframe as part of a broad, pervasive encryption strategy could cut the time spent remediating software vulnerabilities and configuration issues and, in turn, result in a cost savings of an estimated $300,000 annually, he said. The savings could free up software developers to work on value-add projects such as enriching the features of the platform.

The goal of an effective security program is to mitigate risk associated with business activities. Security shouldn't restrict productivity or limit innovation. It should result in operational efficiency improvements and greater organizational performance. This study found that when a data-centric security approach is integrated into an organization's security program and the program is properly executed and proactively maintained, the following benefits can be achieved:

- **Productivity.** Modern encryption products have components that address business disruption, making encryption transparent to the end user. In fact, an analysis of organizations that successfully thwarted a ransomware outbreak found that they did so because their core focus was on data protection. Debilitating ransomware infections in the past several years have crippled business operations and caused costly damage in the form of disrupted services. While the attack technique has been around for decades, the threat has grown extremely dangerous with the added use of strong encryption to lock up data and hold the decryption keys for ransom. This widespread attack has served to make the value of operational data for productivity obvious.
- **Competitive advantage.** Customer expectations over the protection of data have risen significantly. Customers favor organizations that demonstrate adequate proficiency in security and are transparent about their internal processes. In addition, it has been found that businesses choose to partner with organizations that have created a culture of security and data protection among employees. These forward-leaning organizations have better controls in place to safeguard research, develop new products, and apply new approaches to solve problems.
- **Regulatory compliance.** Data knows no boundaries, but regulators have stepped in to address data security and privacy in a variety of ways. The EU General Data Protection Regulation (GDPR), which will take effect in May 2018, requires organizations to gain an understanding of the location, ownership, and security of data collected on EU citizens. Similar regulations exist elsewhere, and IDC predicts legislation may be created to address public safety issues as a result of the Internet of Things.

Data encryption should be coupled with a strong key management solution and access control to determine who is authorized to encrypt within the organization. A key tenet in information security revolves around the least privileged to allow access to the data for the minimum necessary number of individuals. Authentication is used to enforce who is authorized and who is unauthorized to decrypt. CISOs seek modern solutions that enable organizations to monitor user access with context-based control. Strong identity and access management solutions are easier to use and are flexible enough to apply user access to a mixture of web, mobile, and cloud technologies.

Data loss prevention (DLP) products, which monitor key ingress/egress points such as email gateways and internet access points, are often a significant component to a data security strategy. Placing sensors to identify when and where sensitive data is transmitted provides key insights into whether the data is being used legitimately or leaked, either purposefully or mistakenly.

Organizations are also sharpening their incident response activities by coupling active investigation tools with a strong analytics backbone. Cognitive analytics is serving to accelerate investigations, shortening the time it takes to determine the scope of a security incident and contain the incident before data is exfiltrated.

LAUNCH OF THE NEW IBM Z14

In the summer of 2017, IBM launched a new-generation mainframe, the IBM z14. While the previous generation launched in 2014 was focused on performance increase combined with cloud, open source, and developer friendliness, the z14 has been developed around three pillars that address the most urgent needs of the z customer base as well as potential new z users:

- **Pervasive encryption.** The focus of this white paper, pervasive encryption removes the complex decision-making process around what data to encrypt and what data to leave unencrypted. IDC believes that IBM is delivering an industry first with a system of this scale that provides built-in encryption of all data at rest and in flight across the platform, including the APIs with which it links to the outside world.
- **Analytics and machine learning.** As a leading transactional and data-serving platform, the IBM z14 provides analytics and machine learning on core enterprise data that resides on the mainframe, opening a virtual goldmine of cognitive insights that too often is not mined because it sits behind corporate firewalls. With machine learning on the z platform, there's no need to move data around, which has typically been a security and governance concern. And by ingesting the most current data as transactions occur, a continuous stream of real-time cognitive insights becomes available to the business. Thanks to a tripling of memory (32TB) as well as z14's greater processor capacity, life-cycle management of the behavioral models that are at the heart of machine learning is greatly accelerated.
- **Open enterprise cloud.** In keeping with IBM's continuing efforts to simplify the platform for a new generation of users, the IBM z14 enables businesses to tap into their z workloads with standard APIs to "cloudify" their infrastructure and deliver services to their customers in a secure cloud consumption model.

New IBM z14 Characteristics That Power Pervasive Encryption

To achieve pervasive encryption in a way that does not affect transactional or analytical performance, IBM has brought forth a range of hardware and other improvements:

- The new system is built around uniprocessors with 1,800 MIPS capacity each and with a maximum of 140,000 MIPS in a single system image that is divisible into 85 partitions or fewer.
- According to IBM, processors are delivered with up to 10 cores on a die, running at 5.2GHz, with Level 1 and Level 2 cache on the core and Level 3 off the core.
- The platform's memory was tripled to up to 32TB of main memory (among the highest in the industry), while a new virtual flash memory capability was added to the memory subsystem.
- The I/O side of the system matches the greater processor performance with a larger microprocessor cache subsystem and a memory subsystem with new PCIe 3 hyperlink technology that, according to IBM, cuts application response time in half compared with the IBM z13, with no application changes.
- The platform is available with 3PB of all-flash storage on IBM's own DS8000-8800 storage platform.
- For coupling, IBM is migrating from InfiniBand to PCIe links to achieve faster throughput on the z14.

- With the strong popularity of running Java on the platform, IBM is providing new instructions to further support Java capabilities.
- New instructions are available in the single instruction, multiple data (SIMD) capability, which provides parallelism and can enhance processing tasks such as machine learning.
- Compression enhancements have been made with new Huffman coding, an efficient method of compressing data without losing information.

Pervasive Encryption on the IBM z14

On the IBM z14, bulk encryption is enabled in the z/OS operating system, which simplifies the process of encrypting, makes encryption more efficient, and eases monitoring. At the same time, the system runs hardware-accelerated encryption on every core, using a set of cryptographic instructions (CP Assist for Cryptographic Functions) that provides improved performance — up to 7 times faster than the z13, per IBM. Also, the platform is equipped with a PCIe HSM, which provides secure storage for RSA keys and accelerates RSA operations, as well as with cryptographic coprocessors.

Furthermore, IBM's secure service containers provide tamper-resistant installation and runtime, restricted administrator access, and encryption of data and code. A secure service container partition is a specialized container that acts as a virtual representation of the system's hardware resources, including processors, memory, and I/O adapters. It is used for installing and running firmware or software appliances, which consist of integrated operating systems, middleware, and software.

Pervasive encryption protects all the network traffic on the z14 platform; the platform's Linux file systems and z/OS data; the z/OS Coupling Facility, which is a critical piece of hardware that allows multiple processors to access the same data; the DS8000 storage units; and the transaction processing facility (z/TPF), which is the platform's combined operating system, transaction processor, and database for very high-volume transaction processing.

The pervasive encryption solution further protects all application and database data, including DB2, IMS, and VSAM, without impacting business applications running on the system and without interrupting ongoing operations. This includes CICS/VSAM applications, which routinely process thousands of transactions per second and which are typically subject to stringent compliance. Data that is covered by the encryption solution also includes large unstructured data objects in databases that contain sensitive data — for example, medical records that are stored in PDF or image format.

Pervasive encryption extends beyond on-premise and into the cloud where it protects transactional logs that often reside there. z/OS data set encryption, z/OS storage automation, and Transparent Cloud Tiering automatically transfer and encrypt data end to end in the cloud, while encryption is centrally managed by the z host.

The host not only protects itself and the cloud data but also covers all the in-flight network data and APIs. The solution encrypts all incoming and outgoing network connections as well as all APIs to the cloud at high speed. This, for example, allows it to integrate z/OS subsystems with transactions on the blockchain, a fast-growing SaaS solution on LinuxONE systems in the IBM Cloud, through encrypted APIs.

The z14 security also protects the encryption keys, using tamper-responding cryptographic hardware at FIPS 140-2 Level 4, which is the highest level for this security standard as defined by the U.S. government. At Level 4, a system detects all unauthorized attempts at access to the keys and responds with immediate and automatic deletion.

CHALLENGES

Encryption is no panacea. It must be implemented properly and be a component of a comprehensive security program. Encryption should be closely aligned with access control, vulnerability, and configuration management; real-time monitoring; and strong incident response procedures. IBM's new-generation mainframe provides tools to support pervasive encryption on IBM Z, but it requires organizations to integrate the strategy across non-mainframe environments in order to achieve the full benefits.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice