



Protect your critical business information with information security solutions from IBM

Organizations have always struggled to manage the exponential growth of information they create and store, and recently, they have turned their attention to the increased exposure and vulnerability to attacks of all of this information. What's more, new laws demanding stronger accountability from organizations that lose sensitive personal data have intensified the need to adequately protect sensitive corporate information.

As business opportunities expand in the global economy, organizations are becoming more distributed and business models are becoming more collaborative. It is no longer enough to secure information internally; it also must be protected in the context of a business environment with a growing number of collaborators and a constantly changing universe of users. Collaboration also means that it's not enough for an organization to protect its own information—it also has to work to ensure that its partners' information is secure, too.

Information assets are growing in complexity as well as in volume. They must be secured at multiple levels: from stored information, to information in applications, to physical devices in the information infrastructure. For information security to be effective, all areas of risk in the infrastructure must be addressed.

Where thrill-seeking amateurs were once the main threats to an organization's security, security experts acknowledge that professional criminals and organized crime syndicates have

become the principal threats today. These criminal organizations are so well-funded that they can afford the latest in sophisticated technology and can recruit computer scientists to undermine what many consider to be highly secure systems. Today, many of these organizations successfully breach corporate IT security systems to gain access to high-value personal information such as Social Security numbers and credit card information, which can then be used to steal the identities of individuals and drain their bank accounts. With their vast resources, criminal organizations often circumvent security mechanisms that are in place by recruiting company insiders to steal sensitive information or provide access to secure systems. It is a problem that will continue to frustrate businesses as they continue to spend IT resources on securing their infrastructures.

The costs of not securing information in this high-stakes environment can be tremendous, especially when both the direct financial costs and the costs in areas such as loss of customer confidence and risk of regulatory exposure are taken into account. On the other hand, the benefits of successfully securing information can be inestimable. Information security enables business success by building the foundation for trust that's essential to collaboration and innovation. When information is secured and safe, the enterprise is free to pursue new business opportunities in emerging markets or with innovative business models without fear of undue risk.

IBM framework for comprehensive information security

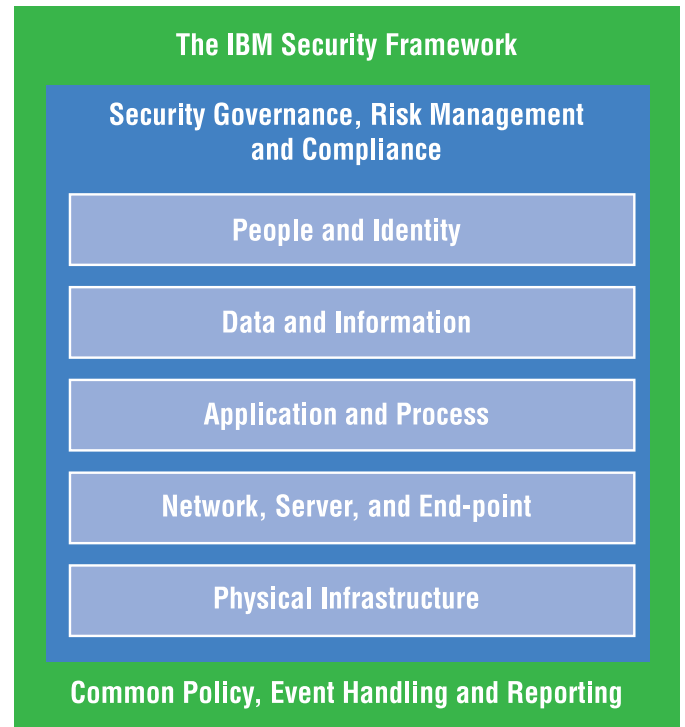
The IBM approach to securing information for today's enterprise is to strategically manage information security across the entire organization—as a Dynamic Infrastructure®—rather than just at the systems or data level. This approach means instituting controls that can manage risk across all IT security domains:

- *Identity: Ensuring that the right people have access to the right assets at the right time*
- *Information: Protecting critical data wherever it is stored in the enterprise, and as it travels across private and public networks*
- *Applications: Securing applications and business services*
- *Systems infrastructure: Staying ahead of emerging threats across the entire IT environment*
- *Physical security: Using the increasing capabilities of digital controls and video monitoring to secure physical spaces*

Rather than focusing on only one domain, or managing only a portion of the total risk, IBM can apply the right technologies and expertise to provide leading-edge security across virtually every domain. IBM is unique in its ability to address practically every dimension of a secure infrastructure and provide the

technology and services to help organizations develop a strategic approach to their security challenges. To that end, IBM offers information security solutions in five strategic areas:

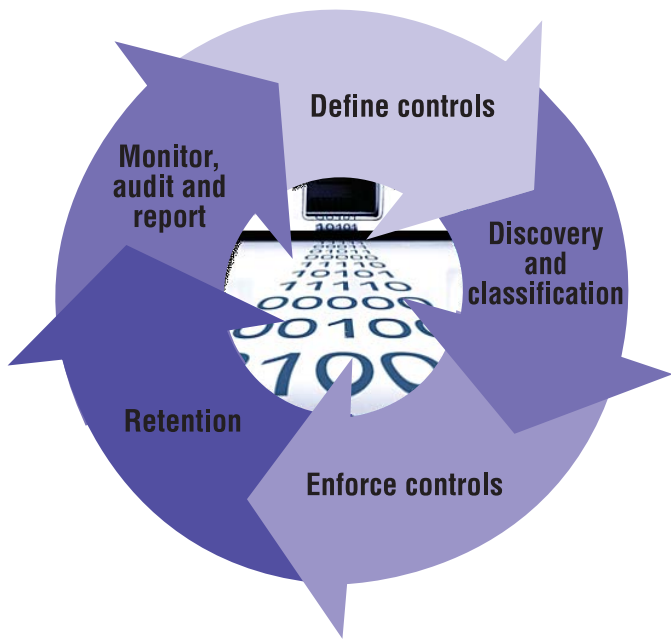
- *Security compliance*
- *Identity and access*
- *Information security*
- *Application security*
- *Infrastructure security*



Information storage solutions from IBM System Storage™ play an important role in IBM's information security strategy, helping organizations better protect and secure information assets that reside across the enterprise.

Enforcing security controls with IBM System Storage information security solutions

IBM System Storage solutions for securing information are part of a larger, lifecycle-driven approach that helps provide comprehensive network protection to secure all points of access to information on the network, at all stages of the information security lifecycle.



Storage solutions are specifically relevant to the point in the lifecycle where security controls are enforced, enabling information to be shared securely within and beyond the enterprise.

Protecting information with IBM self-encrypting storage solutions

IBM System Storage solutions can help organizations enforce security controls by encrypting stored data. Encryption is critical because data center storage is inherently mobile: Tapes get archived, disk drives routinely get replaced, and enterprises become understandably concerned about the sensitive data that resides in their storage systems. The idea of storage encryption is to protect the data stored in these systems so that if a tape cartridge or disk is lost or stolen, the information stored there is useless to anyone who accesses it—unreadable due to encryption.

IBM offers a portfolio of information security solutions based on its innovative self-encrypting disk and tape drives. These drives are designed to encrypt data automatically as it enters the drive to be stored, and then automatically decrypt it as it moves out of the drive. The embedded encryption engine helps to ensure that there is virtually no performance degradation compared to non-encrypting drives. This drive-level encryption approach reduces the risk that information could be compromised when storage media are physically removed from the storage systems for archiving.

IBM introduced the industry's first self-encrypting enterprise tape drive, the IBM System Storage TS1120, in 2006, followed by the next-generation IBM System Storage TS1130 and Linear Tape Open (LTO) self-encrypting drives, which can address a wide range of enterprise and entry-level tape environments. In February of 2009, IBM introduced full disk encrypting drives in its flagship IBM System Storage DS8000® and soon followed that with the announcement of full disk encrypting drives in its mid-range disk platform, the IBM System Storage DS5000. Adding self-encrypting disk solutions to the highly successful self-encrypting tape solutions offers customers a consistent approach to securing data at rest, enabling organizations to adequately address their data security concerns.

Using these IBM self-encrypting drives to encrypt data at the storage end point provides the ability to store data in an encrypted form with minimal operational complexity and minimal impact on performance. Encrypting at the storage end point can help organizations:

- *Minimize the need for host-based encryption, which can drain host performance.*
- *Minimize the need to use specialized encryption appliances that can add to infrastructure complexity.*
- *Accommodate data compression of tape storage, so that fewer tape cartridges are needed.*
- *Reduce the risk that batch processing windows will be affected by placing no significant impact on the tape drive's native performance.*

Self-encrypting drives are rapidly becoming the preferred model for securing data stored on tape cartridges and disk drives. For example, the National Security Agency recently qualified self-encrypting disk drives for protecting information on computers deployed by U.S. government agencies and contractors for national security purposes.

When you talk about securing your information infrastructure, it's difficult to not mention the mainframe. For years, the IBM mainframe has been satisfying the most demanding customers with the highest levels of performance, availability and security. Originally designed to be shared by thousands of users, the mainframe has security built into nearly every level of the system—from the processor level to the operating system to the application level. This design helps protect it from malware, viruses and threats from both within and outside the organization.

By providing the ability to enforce, monitor and manage security, IBM System z® is the logical central management point for enterprise-wide security. For user identification and authentication, access control and auditing, distributed directory services, networking security and security administration, the mainframe is designed to provide integrity, process isolation and cryptographic capabilities to help keep information secure. On top of this solid hardware foundation, System z operating systems offer a variety of customizable security elements within the Security Server and Communication Server components.

And of course along with the inherent security built into the mainframe, there are additional security management offerings from IBM Tivoli® software, such as identity and access management solutions and the IBM Tivoli zSecure suite, which can provide advanced security to help protect the information infrastructure.

Successful key management strategies

Just as each tape drive has an embedded encryption engine, each disk drive also has an embedded encryption engine, and it, too, uses IBM's encryption key management software to manage the keys associated with the solution. This simplified and proven key management system is being used in some of the largest banks in the world. As with the encrypting tape solution, the encrypting disk solution is designed to be transparent to the operating system, applications, databases, system administrators and users, making deployment much simpler than with specialized encryption appliances.

IBM currently addresses key management in its self-encrypting tape storage solutions with the standards-based IBM Tivoli Key Lifecycle Manager (TKLM) and its predecessor, Encryption Key Manager (EKM). TKLM is designed to help manage the growing volume of encryption keys across the enterprise with simplified deployment, configuration and administration over their lifecycles.

Part of IBM's holistic approach to storage and security challenges

Successfully implementing an end-to-end approach to information security requires more than technology; it requires expert planning, design, implementation and support services.

IBM offers an extensive services portfolio that can help clients address their short-term security concerns, as well as design and deploy a holistic information security environment. This, combined with our integrated and unrivaled portfolio of security offerings and capabilities, makes IBM your partner of choice for end-to-end information security. Consider what IBM offers:

- *Skilled professionals: IBM's security and privacy business includes 3,500 professionals in regions around the world, including 1,700 who have completed IBM's rigorous security and privacy methodology training.*
- *A worldwide presence: IBM maintains security and privacy practices in the U.S., Canada, EMEA (Europe, Middle East, Africa), Asia, Australia, and Latin and South America.*
- *R&D leadership: IBM holds more security and privacy copyrights and patents than any other company in the world.*
- *Ability to deliver: IBM demonstrates security leadership daily through successful service delivery within IBM and to IBM customers worldwide.*
- *Industry recognition: IBM has been recognized repeatedly by industry analysts for our leadership in managed security services and related security areas.*

Case in point: deploying drive-based encryption technology across the enterprise

The IT organization of a large U.S.-based healthcare firm needed to encrypt all data across the enterprise to help fulfill the company's commitment to compliance with data privacy regulations.

Challenge

Data would have to be encrypted across multiple technology environments: IBM System z mainframe computing, distributed computing, and Microsoft® Windows®-based desktop computing. The solution could not add significant time to the company's current data backup processes.

Solution

The company turned to IBM System Storage for a tape encryption solution that would help ensure both the security and availability of their data in all IT environments. They deployed the IBM System Storage TS1120 tape drive, enabling full-fledged encryption across the company's mainframe, distributed and desktop computing environments.

Solution benefits

- *Delivers full-fledged encryption and simplified key management across the enterprise*
- *Simplifies and streamlines IT by enabling a common encryption solution across all computing platforms*
- *Helps ensure protection of sensitive data and facilitates compliance with regulations, including the privacy components of the Health Insurance Portability and Accountability Act (HIPAA)*



For more information

To learn more about how IBM's comprehensive information security solutions can help protect critical business information throughout its lifecycle, contact your IBM representative or IBM Business Partner or visit ibm.com/security.

For more information about how IBM System Storage solutions can secure stored data on your network, visit ibm.com/storage.

Information concerning non-IBM products was obtained from the suppliers of their products their published announcements or other publicly available sources. Questions on the capabilities of the non-IBM products should be addressed with the suppliers. IBM does not warrant that the information offered herein will meet your requirements or those of your distributors or customers. IBM provides this information "AS IS" without warranty. IBM disclaims all warranties, express or implied, including the implied warranties of non infringement, merchantability and fitness for a particular purpose or non infringement. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

© Copyright IBM Corporation 2009

IBM Systems and Technology Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2009
All Rights Reserved

IBM, the IBM logo, ibm.com, DS8000, Dynamic Infrastructure, System Storage, System z and Tivoli are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (@ or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

This document could include technical inaccuracies or typographical errors. IBM may not offer the products, services or features discussed in this document in other countries, and the product information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. The information contained in this document is current as of the initial date of publication only and is subject to change without notice. All performance information was determined in a controlled environment. Actual results may vary. Performance information is provided "AS IS" and no warranties or guarantees are expressed or implied by IBM.



Recyclable, please recycle