Security solutions
To support your IT objectives

Adopt a unified, holistic approach to a broad range of data security challenges with IBM Data Security Services.

Protecting the valuable data throughout your enterprise is critical. You want to retain the confidence of organizations and individuals that trust you to protect their sensitive data. You want to make sure that your intellectual property doesn't fall into the hands of someone who isn't authorized to have it. Plus, you need to be able to demonstrate the effectiveness of your controls to meet diverse compliance requirements related to your industry, country and region, as well as your company policies.

It is tempting to lock away the organization's critical data to keep it safe. But that stifles the ability of employees to collaborate and innovate. Your employees need to be able to collaborate and access data more, not less. Using information you already own in different ways helps drive innovations that can differentiate your business and generate new revenues. Today's business climate requires a data security solution that encourages collaboration while mitigating the risks associated with data access.

Highlights

- Balance effective security with optimized data access to increase collaboration and ensure appropriate use
- Deploy and manage a comprehensive data security solution by leveraging IBM information security expertise and proven services methodologies
- Enforce data access controls and encryption requirements at endpoints, where data is accessed and used
- Take a holistic approach to preventing data loss with both network-level and endpoint-level controls
- Monitor and report on security events throughout the enterprise to facilitate compliance efforts and protect against database and application vulnerabilities
IBM Data Security Services enable organizations to protect data throughout its life cycle — while in use, in motion and at rest. IBM offers a full range of data security services to help an organization design effective data protection solutions and support compliance efforts, including access to IBM information security expertise and proven services methodologies. IBM Data Security Services is one of the many entry points into IBM security solutions, which help customers establish effective risk management strategies to manage and secure business information and technology assets, anticipate vulnerabilities and risk, and maintain timely access to information. IBM security solutions help organizations align technology with business priorities — redirecting resources that might otherwise be dedicated to resolving security problems toward innovative initiatives that deliver substantial value to the business.

Move beyond perimeter-centric, inbound threat protection to point-of-use and outbound data loss prevention
The traditional view of security thinks of threats as flowing inward — from the perimeter toward your valuable data in all the places where it resides throughout your organization. Control the perimeter, the thinking goes, and you control security.

In today's business environments, this should not be the only approach. First, effective collaboration includes data-driven interaction with people and organizations outside your own perimeter, which exposes your organization to necessary but increased risk. Lock down the perimeter, and you make it difficult or impossible to collaborate with business partners or interact with customers in all the ways that drive your business forward.

Beyond the need to readdress the perimeter, insider threats represent a major vulnerability that perimeter-focused protection does not fully address. Although malicious attacks by insiders are important to prevent, even unintentional harm — caused by careless employees or by privileged users overeager about job responsibilities — can be substantial.

Plus, valuable data is not always locked away in centralized repositories that...
can only be accessed by controlled remote clients. With the portability of laptops and other mobile devices, data can quickly and easily travel all over the enterprise and beyond.

These risks require a different way of thinking. When you concentrate on protecting against the outward leakage of sensitive data as it flows throughout and away from your organization, you can:

- Prevent data leakage at its origins — the places where data is accessed and used.
- Enable collaboration by allowing for appropriate use of data.
- Facilitate compliance efforts by understanding data flows and data use.

Rather than attacking each problem separately, you can turn to IBM service professionals to help you establish a data security framework and deploy the solutions your environment requires.

IBM Data Security Services address the challenges associated with deploying a comprehensive solution by managing cost and scope, accelerating speed of implementation, leveraging IBM information security expertise and eliminating the need for additional headcount.

Use endpoint data protection to control information where it is most commonly accessed

Because valuable data is increasingly hosted and used on endpoint devices, organizations often concentrate their initial data security investments on endpoint protection. IBM data security solutions leverage encryption technology and data loss prevention controls to help protect sensitive data stored on endpoints, when devices are powered down or in use. These solutions also help you secure data stored on external attached storage media (such as USB storage devices) and data that are transmitted by e-mail.

IBM offers multiple flavors of encryption that individually and in conjunction with each other support a holistic data security approach. Full-disk encryption allows you to protect data even when the device it is stored on has been lost or stolen. Encryption of files, folders, virtual disks, removable media and shared media helps you protect data while it is being accessed or used on an endpoint. E-mail and instant message encryption, which extend to attachments, help you prevent against data leakage in case of message interception.

To enforce endpoint data loss prevention controls, IBM helps you automatically discover and classify data on the endpoint using the criteria you choose. Based on this classification, the solutions enforce the data protection policy you establish, whether it is to:

- Permit the action.
- Block access.
- Encrypt the data.
- Mask sensitive data on view at an application's end-user interface.
- Require users to validate the business reasons for their data requests.
- Notify users of potential risks or policy violations.

Because data is analyzed as it is accessed — by applications or users — your policies account for the context in which data is accessed. For instance, you could allow a user to view a file but not copy or alter it, based on the file’s content, classification, metadata, disposition and other contextual factors.

IBM services for endpoint data protection also assist with your efforts to centralize policy and compliance management. By enforcing data protection policies on endpoints, managing
IT staff can receive timely alerts if any deviations or tampering are detected on any endpoint. They can take appropriate actions to mitigate the risks — without disrupting necessary business activities. Furthermore, IBM services for endpoint data loss prevention monitor and record all user access so that you can build an audit trail.

IBM Data Security Services for endpoint data protection leverage encryption technology from PGP Corporation and data loss prevention technology from Verdasys, Inc.

**Approach enterprise content protection holistically**
For organizations that want to take a more comprehensive approach to data loss prevention, IBM can help establish an enterprise content protection framework. To support the solution, IBM can also deploy the appropriate combination of network and endpoint data leakage solutions for the environment, using a proven implementation methodology.

Before outbound data passes through the network perimeter, the network-focused solutions analyze network traffic “on the wire” (in-band or out-of-band) and through integration with existing network-centric devices. Even protected information that is passing through as an attachment or that has been encrypted can be logged or prevented from going outside your organization, in accordance with your data security policy. As necessary, the technology can identify suspicious activity to your administrators, empowering them — or IBM on your behalf — to take the appropriate actions.

IBM can help you translate and enforce your corporate data management policies. Enterprise content protection technologies include key policies that help track common types of protected information and support efforts to comply with various regulatory requirements. Policy-description language can be used to look for individual “data identifiers,” such as credit card data, that may violate regulations, including PCI and other privacy regulations. IBM enterprise content protection solutions also help you prevent design information, source code and other types of intellectual property from going outside your network.

Certain types of network behavior, such as peer-to-peer networking, expose

---

**Rely on IBM services to support your data security needs**
Every organization has its own security priorities, its own preferences about what kinds of security it will take on itself and which kinds it prefers to outsource, and its own business processes and environments that need to be integrated with security solutions. That is why IBM services are designed not only to address every phase of developing and maintaining data security solutions, but also to meet your particular requirements and priorities.

IBM security services integrate risk assessment, design, planning, deployment, documentation, technology, education and managed services. They assist you in blending market-leading services, technologies and security intelligence into a single solution that can be used when, where and how you need it. You choose how you want the technology managed — outsourced, in house or a combination of both. As a result, you can align security technology to address evolving business requirements more strategically.
organizations to unnecessary security risks. Consequently, IBM services are designed to spot use of these “dangerous” protocols and control them by blocking the traffic, throttling the bandwidth that these technologies consume or alerting administrators about them, so that they can take appropriate actions.

IBM Data Security Services for enterprise content protection leverage technology from Fidelis Security Systems, Inc. for network data loss prevention and Verdasys, Inc. for endpoint data loss prevention. The technologies together deliver integrated network and endpoint data loss prevention.

IBM provides a comprehensive set of services to address key compliance requirements, including managed database scanning, log management and user activity monitoring. Customized solutions use established, regulation-specific policy templates to help customers improve visibility into each area of potential exposure within their enterprises.

Meeting compliance requirements — particularly when you face multiple audit types — can require a significant manual effort to collect and protect information across heterogeneous resources. IBM services help you improve your compliance posture by regularly assessing the security of your databases. As a complement, IBM provides an automated monitoring solution for collection of user activity and events from databases, operating systems, applications, mainframes, security devices and network devices. Using this centralized and normalized information, the solutions offer direct visibility to database security posture and user activity for forensic investigation. Supporting reports are preformatted to meet many major regulations and auditor requests.

Employees who are granted authority to handle business-critical information to perform their core job responsibilities represent a significant threat. To support compliance initiatives, privileged users’ activities must be tracked — so you know if they decide to act maliciously or unintentionally mishandle data.

IBM solutions help your organization properly balance the need to let privileged users perform their jobs and the need to have visibility into their actions, including alerts when those actions violate your data security policies. IBM services enable you to set up policies to identify when potential violations occur and alert administrators about noncompliant activities, which allows them to perform further investigation.

To get started with database vulnerability management, leading security experts from IBM can help you assess which databases need to be covered, how often they should be checked and under what circumstances you should ask users to remediate their own activities — or when administrators should be alerted to take appropriate action.
IBM Data Security Services for activity compliance monitoring and reporting leverage IBM Tivoli® Compliance Insight Manager to provide visibility into your organization’s security compliance posture through automated, enterprise-wide user activity monitoring. Additionally, these services use database vulnerability management technology from Application Security, Inc.

For more information
IBM provides a full range of solutions to help you address your data security requirements. Whether you need to implement endpoint data protection, enterprise content protection, or activity compliance and monitoring, IBM can help. When you want to adopt a strategic model for data security that not only protects information but also helps you extend its value through collaboration, turn to IBM.

To learn more about how your organization can use IBM security solutions for data security — or to find the IBM security solutions entry point that is right for your organization — contact your IBM representative or IBM Business Partner, or visit ibm.com/itsolutions/security

About IBM solutions for enabling IT governance and risk management
IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards—based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit ibm.com/itsolutions/governance

© Copyright IBM Corporation 2007
IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2007
All Rights Reserved

IBM, the IBM logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

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

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer’s sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.