

**Microsoft**  
Your potential. Our passion.™

Focused on **Security**.  
Committed to Success.

# U.S. National Security Team White Paper

## Information Protection Strategies for Financial Services

*Produced by the Microsoft U.S. National Security Team*

*Co-authored by Thomas W. Shinder, MD, MCSE, MVP and Norm Barber, Strategic Security Advisor*

---

### Abstract

The modern financial services firm is seeing profound changes in the workplace. In the past, employees came to the office to obtain access to corporate data. Today, firms require anywhere, anytime access to information in order to gain the competitive advantage. This has caused the lines to blur between the trusted corporate network and all other networks, which may or may not be trusted.

Significant risks come, however, with the increased competitiveness provided by anywhere, anytime access from any device. In contrast to well structured, managed and secured data on corporate databases and file servers, the information stored on more mobile devices, including home PCs, smart phones, PDAs, PDA-based phones and laptops, is often unstructured, unmanaged and poorly secured. This can lead to either unintentional or intentional loss of private and proprietary information, which can put the company at risk of direct financial loss, brand equity, and/or major fines and imprisonment from violation of government information practices regulations.

Microsoft understands the location- and device-dependent scenarios, and the unique security and data protection issues associated with each of them. To meet data security requirements for today's financial services organization, Microsoft provides its customers a wide array of products

and technologies that meet head-on the security challenges posed by each scenario, and help reduce or mitigate the risks that each one exposes.

### **About the U.S. National Security Team (NST)**

The U.S. National Security Team is composed of strategic security advisors who work with Microsoft customers, partners, MS internal constituencies and the information security industry to promote the adoption of security processes and technologies. Its goal is to assist customers and partners to increase their security awareness and implementation to create more secure businesses, mitigate risks and make security costs more effective. Its activities are informed by three simple tenets: protect the consumer, secure the enterprise and enable developers to write secure code.

As part of its mandate, in addition to producing white papers such as this one, the NST is responsible for developing and executing security-focused events and Security Round Tables across Microsoft's U.S. geographies. These events include the annual CSO Summit, which provides formal feedback to business groups, security industry updates from leading analysts, peer perspectives on security management from MSIT, and updates on the latest initiatives and industry trends in enterprise security.

The NST also focuses on driving vertical security solutions for a wide range of industries. To this end, the NST has produced a number of white papers that address the specific security needs of particular industries, such as the professional services and financial services industries.

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.*

*© 2007 Microsoft Corporation. All rights reserved.*

*Microsoft, Forefront, Antigen, Excel, SharePoint, Windows, Windows Server System, and the Windows Server System logo are either registered trademarks or trademarks of Microsoft Corporation or Sybari Software, Inc. in the United States and/or other countries. Sybari Software, Inc. is a subsidiary of Microsoft Corporation.*

*All other trademarks are property of their respective owners.*

---

## Contents

<b>Introduction</b> .....	<b>1</b>
<b>Data Access Scenarios in the Financial Services Sector</b> .....	<b>4</b>
The Road Warrior .....	4
The Handheld-Device User.....	5
The Home Worker.....	5
The Customer .....	6
The Partner .....	7
The Corporate User .....	7
<b>A Technology Framework for Data Governance and Access Control</b> .....	<b>9</b>
Secure Infrastructure .....	9
Identity and Access Control .....	12
Data Encryption.....	13
Document Protection .....	14
Auditing and Reporting .....	14
<b>Summary</b> .....	<b>16</b>
<b>For More Information</b> .....	<b>17</b>

---

## Introduction

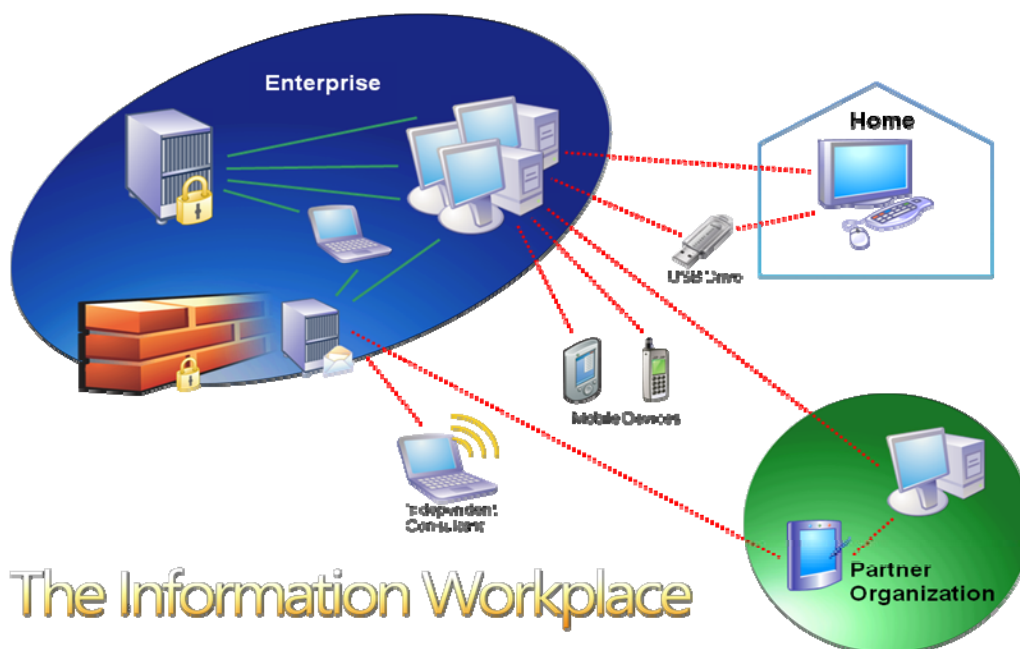
The enterprise-information workplace has changed significantly in the last decade. Previously, a clear demarcation existed between trusted devices on well-managed corporate networks and non-trusted devices on unmanaged and possibly dangerous networks. This line is now blurred because of an increase in the types of devices that must communicate with private information resources on the company's network, the new communications modes used to access that information, and business models that demand a blurring between trusted and non-trusted machines.

These changes have occurred because companies require competitive differentiation, which has driven firms to outsource core business processes to consultants and outsourcing firms. Additionally, a mobile and distributed workforce enables organizations to get closer to the customer and increase overall profitability. Organizations must provide employees with anywhere, anytime access to private corporate data. The workplace is extended to include hotel rooms, convention centers, and even private homes of full-time or part-time employees.

IDC reports that organizations managing patient health information, social security numbers or credit card numbers are being forced by government and industry regulations to implement security controls to address leakage of personal information [Source: Worldwide Secure Content Management 2005-2009 Forecast: The Emergence of Outbound Content Compliance, March 2005].

Connecting to corporate data while away from the office is no longer just a luxury of the top brass in the company and select members of the IT group. To gain the competitive advantage, employees, partners, customers and consultants all need real-time access to corporate data regardless of their location. The stakes are high – superior access to information can deliver better business results and significantly increase the bottom line for any company that remains competitive in this area. Beyond these benefits, however, there is increased risk of information leakage and compromise of proprietary data. In addition to the monetary costs of a security breach, the company also faces the time and effort required to repair damaged systems, potential legal repercussions and a negative impact on brand equity.

Recent changes in administrative and criminal law can lead to potentially devastating losses. Organizations are now exposed to a wide array of industry and government regulatory requirements, which can cost them millions of dollars in the case of a security breach.



Accompanying the risks due to a distributed workforce are those related to the increased variety of devices used by this workforce. Historically, companies usually dealt with only two types of computing devices: client PCs and servers. Tools that were readily available on the market or included in the operating systems that ran the clients and servers made it relatively easy to manage this client/server computing ecosystem.

As depicted in the Information Workplace graphic, the simple PC and server paradigm of yesterday is gone. Now information workers get access and store information using a variety of popular devices, including smart phones, pocket PCs, laptop computers, ultra-mobile PCs, virtual machines, and more. Due to the proliferation of such devices, organizations of all sizes face the challenge of finding effective methods to protect and control information.

Because of ineffective controls, there is no guarantee that information can be contained within the corporate network on managed devices that are carefully monitored to prevent theft or loss of information. In a study conducted by Jupiter Research [source: Digital Rights Management

The annual Information Security Study (Source: 2006 Information Security Study, Wave 6) polled key decision makers at 850 large enterprises such as Citicorp, Pfizer, Sears, Merrill Lynch, Reuters, etc, reports the following key facts:

- Data protection is in the top 10 IT security projects that an organization undertakes.
- 80% believe that effective data protection is important in securing internal networks.
- Over 85% believe effective data protection is critical to satisfying regulatory compliance mandates.
- Enterprises spend an average of \$350,000 on data protection software alone annually. Overall expenditure approaches \$2 million per customer.
- Over 50% of customers surveyed expect to increase their investment in data protection and security software over the next year. An additional 30% expects to spend at least same amount.

in the Enterprise, May 2004), decision-makers reported that loss of information through e-mail leakage is among their top three security concerns.

In its Worldwide Outbound Content Compliance 2005-2009 Forecast and Analysis (published November 2005), IDC said that unstructured content represents the biggest challenge for protecting private corporate information and intellectual property. Unlike structured content stored in well-managed databases on IT managed database servers, unstructured content is not well organized, centrally managed or easily found. And most importantly, it isn't subject to stringent corporate security policy for information retention, access and control.

In regard to regulatory compliance or discovery, this unmanaged, unstructured and unsecured content in most organizations represents a time bomb waiting to explode.

It's clear that information protection is a top concern among IT decision makers, but to protect the information, you need to know not only the physical location of the information, but also the type of device on which it is stored. In this next section we'll explore some common scenarios that IT decision-makers in the financial services sector encounter in heterogeneous computer and computing environments.

---

## Data Access Scenarios in the Financial Services Sector

Of all the vertical markets, the financial services sector requires the most interfaces with many end points. This is due to the nature of the sector itself – all businesses and individuals who wish to participate in the economic system must interact with financial services. To reach all these customers and partners most efficiently and effectively, financial services companies must distribute their employees all over the globe.

Because of an almost ubiquitous interaction of financial services firms, this industry sector is the most exposed industry worldwide. To solve the problem of information protection in this highly exposed environment, IT decision-makers need to understand the physical location and types of devices on which proprietary data is accessed and stored, and the risks involved in a number of scenarios. Through this understanding they can take proactive measures to ensure that data is protected and managed.

Among the most common data protection scenarios are:

- The road warrior with a personal or corporate issued laptop
- The handheld device user
- The home worker with corporate VPN access
- The customer who requires access to private data
- The partner who requires access to shared private data
- The corporate user on the internal network accessing server data

The following section describes each scenario in detail along with the unique risks each one brings to a financial services firm. Microsoft offers customers an array of products and technologies for information protection, many of which will be discussed later in this paper.

### The Road Warrior

The road warrior might be an analyst or an executive who needs to leave the corporate network to conduct business. Road warriors most often use a laptop computer while out of the office and connect to networks at customer sites, hotels, conferences and airports. The laptop might be a company-issued and managed computer, or more often than not, it is the employee's personal laptop.

Road warriors can compromise corporate data in a variety ways. Consider the following scenarios:

- The road warrior often connects to unsecured networks that contain viruses and other exploits, often infecting the road warrior's laptop. The road warrior subsequently connects to the corporate network and spreads the exploits to the company's workstations and servers.

- Road warriors often connect to wireless access points that allow them Internet access. Attackers can easily set up rogue wireless access points that trick users into sharing credit card information. In addition, these connections are not encrypted and the owner of the rogue access point can read any user name and password information moving through the access point.

Hundreds of thousands of laptops are lost or stolen every year. Many are stolen in a deliberate attempt to gain access to data stored on the device. Simple “offline” attacks are readily available that allow bypassing many of the operating system’s access controls.

Road warriors often use their computers in public environments. This increases the risk of “shoulder surfers” stealing user name and password information by watching the user enter this information.

## **The Handheld-Device User**

Handheld devices such as PDAs, smart phones, and PDA-based phones represent the fastest growing category of computing devices used to connect to the corporate network today. Handheld-device users span the ranks in any financial services organization, including anyone from the front-desk manager to the president and CEO of the company. All of these devices store information in built-in memory, and many of them enable users to store files on attached memory cards.

Users of these devices present a unique security risk to the financial services organization. Consider the following scenarios that highlight these risks:

A managing director purchases his own smart phone and connects it to the corporate mail server. He later misplaces the device and finds that all of his e-mail messages have been deleted.

An analyst for a brokerage house uses a PDA-enabled phone to access e-mail and sensitive e-mail attachments. The analyst saves all of the attachments to a memory card inserted into the phone. One night after dinner, the analyst notices that the phone isn’t in his pocket and returns to the restaurant. He finds the phone, but the memory card was missing.

A large asset-management company has implemented rights management technologies to protect sensitive e-mail messages. The company CEO depends on her smart phone for e-mail access while on the road. She received several critical documents regarding a merger prior to the meeting, but cannot read them because her device does not support rights management.

A federal intelligence agent accesses highly sensitive national security information over an SSL encrypted session using a handheld device. It is discovered later that a foreign government breached the communications stream because the SSL session, limited to 128-bit encryption, was cracked by an array of supercomputers run by the foreign intelligence agency.

An administrator for a national bank uses her handheld device extensively for network support while on the road, using built-in remote desktop and VPN connections. The administrator configures the RDP and VPN client software to remember her user name and password. Someone steals the device and accesses these saved to breach security.

## **The Home Worker**

Many financial institutions are finding significant cost savings when they move employees away from office buildings and allow them to work from home. This is especially true for employees working as part of the company’s contact center. But in addition to call center agents, many other types of employees have the option to work from home one or more days a week. Home workers with VPN access to the corporate network present their own cluster of security challenges to the financial services institution. The following scenarios provide examples of these issues:

A call center worker for a large bank works from home and connects to the company network through a VPN connection through her home computer, which she shares with other family members. Her children inadvertently download worms, viruses and trojans to the machine. The exploits are subsequently sent over the VPN connection to the bank's network.

A CEO for a large savings and loans company has a home network that includes an unsecured wireless access point. A corporate spy parks in front of her house, connects to the unsecured wireless access point and establishes a connection to the S&L network through the CEO's VPN connection.

An investment banker is supplied with a corporate-managed computer to ensure that the machine complies with the company's security specifications, including Internet access controls. Someone breaks into the banker's home, steals the computer and extracts private company information from the hard disk.

An accountant for a company that works on large reorganization projects stores many proprietary documents on his home computer's hard disk. An intruder breaks into the home and silently copies the contents of the hard disk to a high-capacity USB key.

## **The Customer**

Customers present quite a different threat model. They typically access resources through a multi-tier architecture rather than having direct access to the corporate network. While a well-designed multi-tier architecture can go a long way toward protecting private data from exposure to customers, the other side of the coin is that customer-facing data is also accessible to malicious non-customers.

The following scenarios can help provide some insight into security issues that should be considered when dealing with customer-facing data:

A customer receives an e-mail message purportedly from his bank stating that he must click the link in the message to visit the bank's Web site to provide confirmation of private account data. This is in fact a phishing link that takes the user to a malicious Web site that harvests his private account information.

A customer receives an e-mail message informing her that a contract will be taken out on her life if she does not divulge private account information to the sender of the email.

A large insurance company has invested heavily in a revamp of its customer Web site. Soon after completion of the site, a high profile case of mass identity theft due to a highly effective phishing scheme is released to the news media. Customer use of the bank's new Web site is only 40 percent of anticipated use due to fears of using the Internet.

A customer is tricked into visiting a malicious Web site where a key logger is downloaded and installed. The key logger records the user's brokerage account's user name and password and sends this information to the malicious Web site owner.

An Internet attacker has been informed of a security issue in the public-facing Web site that exposes payroll information to human resource managers. The attacker can steal this information because the exploit can be run in an anonymous context and does not require user authentication.

## The Partner

Partner- and consultant-related security issues are similar to those encountered with remote employees, although generally a lower level of trust exists, and the access to information provided to partners is more restricted. In many cases, however, partners obtain relatively high levels of access to proprietary information that might be stored on collaboration servers, e-mail servers, and file and database servers.

The following scenarios highlight the more common security issues encountered with partner access:

A consultant performing a regulatory compliance review of a custody services firm requires access to security-section data contained on a SharePoint server run by the security and compliance teams. The consultant copies several key security infrastructure documents and sells them to a competitor who leverages the information to conduct corporate espionage.

A federal tax collection and enforcement agency outsources some aspects of tax collections to private firms. The partners need access to taxpayer data contained on network file shares on the agency's network. A disgruntled employee accesses 100,000 taxpayer records and sells that information on the black market.

A large hedge-fund group has partnered with an accounting firm to help streamline operations. As part of the partnership, the hedge-fund group has provided the accountancy e-mail accounts in their organization. One accountant decides to make some extra money by sending spam e-mail messages through the hedge fund's mail server with subsequent blacklisting and negative media attention.

A brokerage firm uses instant messaging to facilitate communications. One analyst informs a trader of some inside information. The trader takes immediate action on this tip and makes a large profit. The contents of the instant messaging session are later read in court after being produced in discovery.

## The Corporate User

The security challenges from the internal corporate user are perhaps the most complex and prevalent of all the security scenarios discussed so far. While not historically considered to be a major threat vector, security risks from insiders are real. The 2005 E-Crime Watch Survey conducted by the U.S. Secret Service, CERT and CSO magazine found that when the identity of the person perpetrating a computer crime was discovered, 20 percent of the incidents were due to insider attacks. Other estimates have claimed that more than 50 percent of information-security breaches are due to insider influence. One attack perpetrated by an insider was a case of fraud committed against a financial institution and resulted in a loss of more than \$700 million.

Insiders have a significant advantage over anonymous or external attackers. They have much greater access to corporate servers, including mail servers, database servers and collaboration servers. They have legitimate user credentials that they can use to start an attack on information resources, and they can extend their influence by leveraging physical access to clients and servers. Firewalls, intrusion detection systems and other components of the security infrastructure typically are designed to detect outsider intervention; all of which enable the insiders' attacks to fly "under the radar."

The following scenarios illustrate some security risks that can come from insider attacks:

A network administrator was released from his job at an Insurance underwriting institution due to a recent felony arrest. Before being escorted from the building, the employee introduced a logic bomb into the company's main database servers, causing the deletion of more than 100,000 customer records. It took the company more than a year to recover the data loss, plus a cost of tens of millions of dollars in lost opportunities.

An employee of a credit-rating agency was approached by a large car dealership for assistance in altering credit ratings on the dealership's customers so that they could obtain loan approvals more easily. The employee agreed to do so for a set fee. He made changes to the database without alerting the database administrator because he had permissions to access the database, and the credit card ratings database had not been configured to limit write-access to specific users.

An executive at a large investment management firm was interested in starting his own company that would compete with his present employer. He knew that key players in his current company shared valuable proprietary information that would give him a competitive advantage in his planned startup. This executive enlisted the help of a network analyst, who "sniffed" user names and passwords as they traveled over the network. With these user credentials, he could access the e-mail accounts containing valuable data that would give him an immediate advantage over his employer.

## A Technology Framework for Data Governance and Access Control

Each of the scenarios discussed briefly above needs to be addressed through a solution that includes organization (e.g., roles/responsibilities, training), policy, process and technology elements. However, attempting to address each scenario with its own unique solution can be expensive and time consuming. A more effective approach is to adopt a governance approach to managing and protecting sensitive data.

Microsoft has developed a framework for managing and protecting data that consists of five key elements that provides a flexible and comprehensive approach. All five elements of an effective technology-based framework are necessary to protect and manage information responsibly in a distributed device and computing infrastructure. These are described in Table 1.

**Table 1: A framework for managing and protecting distributed data**

A Framework for Managing and Protecting Distributed Data	
Need	Description
Secure infrastructure	Safeguards that protect against malware, intrusions and unauthorized access to personal information, and protect systems from evolving threats
Identity and access control	Systems that help protect personal information from unauthorized access or use, and provide management controls for identity access and provisioning
Data encryption	Safeguards that protect sensitive personal information by converting data into incomprehensible code that requires a “key” for decoding that is held by an authorized recipient
Document protection	Protection of personal information stored in a document throughout its entire life cycle
Auditing and reporting	Monitoring to verify the integrity of systems and data in compliance with business policies

The following sections describe some of products and technologies Microsoft provides relative to each of the five elements of the technology framework listed above.

### Secure Infrastructure

The growing importance of information technologies to the way we work underscores the need to ensure that the underlying infrastructure is as secure as possible. Fundamentally, safeguarding and managing sensitive information depends on a secure infrastructure that protects against malicious software and hacker intrusions. Table 2 describes a number of Microsoft products and technologies aimed at providing a secure infrastructure.

**Table 2: Secure infrastructure products and technologies**

<b>Product or Technology</b>	<b>Description</b>
<b>Windows Vista Security Technologies</b>	
Windows Firewall	A host-based firewall controls access to inbound and outbound communications.
Automatic Updates	This feature enables Windows computers to automatically update the operating system with the latest security updates.
Windows Vista User Account Control	This technology allows users to run with least-required privilege and prevents malware from installing in the background without the user's knowledge. UAC presents an obstacle to non-UAC aware malware.
Windows Vista Service Hardening	Windows Vista services are designed and configured to run with least-required privilege, reducing the harm that can be done by a compromised service.
Windows Vista Kernel Protection	This technology prevents malware from making alterations to the operating system kernel, which helps prevent installation and execution of root kits.
Windows Defender	An anti-malware application helps to prevent the installation and execution of spyware and other unwanted software.
Network Access Protection	A network-access control solution prevents unapproved client and server systems from connecting to network resources.
USB and Removable Device Control	A hardware control system enables administrators to block access to USB and other removable devices.
<b>Internet Explorer Security Technologies</b>	
Internet Explorer 7 anti-phishing filter	A browser technology warns users against potential phishing Web sites.
Internet Explorer 7 pop-up blocker	A browser technology prevents pop ups that might be used to trick users to visit malicious Web sites or download malware.
Internet Explorer 7 IDN protection	IDN protection helps prevent phishing Web sites from tricking users via use of international characters. (Malicious websites include international characters in the Address Bar for phishing attacks and to hide the true website domain name.)
Internet Explorer 7 Security Status bar	A browser technology makes it easy for the user to determine the trustworthiness of a Web site based on certificates.
Internet Explorer 7 Protected Mode	In Protected Mode, Internet Explorer 7 in Windows Vista cannot modify user or system files and settings without user consent. Protected Mode requires the user to confirm any activity that tries

	to put something on your machine or start another program. Ensuring the user consents to these kinds of actions reduces the likelihood of automated and/or unwanted software installation.
<b>Microsoft Server Security Technologies</b>	
Forefront Client Security	An enterprise grade anti-virus, anti-malware solution enables centralized deployment and management of the anti-malware solution, and provides high-visibility reports on the current security status of the entire organization.
Forefront Security for Exchange	An enterprise grade anti-spam and anti-malware application helps prevent spam and malware from spreading through the e-mail channel.
Forefront Security for SharePoint	An enterprise grade anti-malware and document content control system helps prevent malware and inappropriate content from being posted to SharePoint sites.
Forefront Security for Office Communications Server	An enterprise grade anti-malware and communications control system helps prevent malware and inappropriate information from being sent over the IM channel.
ISA Server 2006	An enterprise grade network firewall and application layer inspection gateway provides for strong inbound and outbound access control, logging and reporting.
IAG 2007	An enterprise grade SSL VPN solution enables high-security remote access to both Web and non-Web based applications on the corporate network.
Exchange Server 2007	The server provides Integrated antispam protection, support for messaging policies and encrypted communications.
Microsoft Data Protection Manager	A continuous backup solution enables organizations to back up information in real time, and quickly and easily restore information from backup.
<b>Windows Mobile Security Technologies</b>	
Windows Mobile Remote Wipe	This technology enables wiping of a Windows Mobile device to prevent data leakage in the event the device is lost or stolen.
Windows Mobile support for User Certificate Authentication	This technology allows Windows Mobile devices to present a user certificate to the Exchange Server, thus preventing unmanaged devices from connecting to corporate mail resources.
Information Rights Management e-mail	This technology enables users to read rights-protected mail from a handheld device.

Windows Mobile OWA based Remote Wipe self-service	This technology enables users to perform remote wipe on lost or stolen devices without requiring a call to the help desk or administrator.
<b>Office 2007</b>	
Integrated support for IRM	Client-side technology enables organization to set limits on what can be done with corporate documents
Outlook 2007 Postmarking	This technology stamps Outlook 2007 with a transaction marker that is processor-intensive, thus helping e-mail systems assess whether a spammer sent the message.
Office 2007 Document Encryption	Document encryption using strong AES 256 encryption to encrypt Microsoft Office documents, requiring a password to view its contents.
Office 2007 Document Signing	An electronic “stamp” of authentication on a document that confirms the document originated from the signer and was not altered.

## Identity and Access Control

All financial services organizations must handle increasingly large amounts of confidential data, which must be secured for competitive reasons, to protect customer privacy and comply with an expanding range of laws, regulations and policies.

To reduce the risk of a deliberate or accidental data breach, and to help organizations comply with regulatory requirements, Microsoft offers identity and access control technologies that help ensure the protection of private information from unauthorized access or use, while seamlessly facilitating its availability to legitimate users.

Table 3 provides a list of Microsoft products and technologies that help meet identity and access control challenges in a distributed computing environment.

**Table 3: Identity and access control products and technologies**

Product or Technology	Description
Active Directory	A centralized database of user and machine accounts enables centralized management of all machines and users within the organization.
Active Directory Federation Services	This technology enables federation of multiple Windows domains, which streamlines management and control of partner access to corporate resources.
Microsoft Identity Lifecycle Manager 2007	An enterprise-ready solution enables federation of disparate identity management systems and centralizes the management of user-identity information based on digital certificates.

Windows Vista Smart Card Support	This technology enables two-factor authentication for user logon and data access.
Windows CardSpace	Windows CardSpace, formerly code-named "InfoCard," is a piece of client software that enables users to provide their digital identity to online services in a simple, secure and trusted way.
Exchange Server support for two-factor authentication	Two-factor authentication requires two methods to gain access to resources. Typically users provide a physical card or token and a PIN to access authorized resources.

## Data Encryption

Supported by strong identity and access controls, data encryption can help safeguard information that is stored in databases, on mobile devices, laptops and desktop computers, or transferred via e-mail, across the Internet or other non-trusted networks. Encryption used to secure storage, transmission and disposal of sensitive information greatly reduces the risk of a harmful data breach by an intruder or hacker break-in, or from a lost or stolen computer or mobile device. Table 4 includes a sampling of Microsoft products and technologies that support data encryption in a distributed computing scenario.

**Table 4: Data encryption products and technologies**

Product or Technology	Description
Encrypting File System (EFS)	EFS encrypts disc data on a per-file or per-folder basis.
Windows Vista BitLocker	This technology helps prevent offline and other attacks against the disk data by encrypting all data on the system disk volume.
IPSec	This encryption and network access control technology can be used to control access to servers and encrypt data over the network.
Virtual Private Networking	This remote access technology enables encrypted communications over the Internet.
Windows Mobile 6 memory card encryption	This technology helps prevent data leakage from lost or stolen Windows Mobile devices, or from the cards inserted into them, by allowing encryption of the contents installed memory cards.
Exchange Server support for encrypted e-mail	Encrypted e-mail prevents unauthorized persons from reading or capturing e-mail in transit.
Exchange Server Hosted Services	Exchange-hosted services provide an off-site solution for e-mail encryption, anti-virus and anti-spam.
SQL 2005 database encryption and client data encryption	SQL 2005 enables a database administrator to encrypt the contents of a database or database information stored on client computers.

## Document Protection

Rights Management tools help assure document protection. These technologies can be applied to desktop productivity, e-mail and line-of-business applications to help safeguard information and control how information is used, through “persistent protection” that extends throughout the life of the document. They also help ensure that sensitive data such as financial reports, merger information, customer data or confidential e-mail messages do not intentionally or accidentally get into the wrong hands.

Table 5 includes a listing of some Microsoft products and services targeted at document protection.

**Table 5: Document protection products and technologies**

Product or Technology	Description
Rights Management Services	A collection of technologies controls which users can access documents and what they can do with those documents.
Support for XrML	This technology enables rights management controls for virtually any type of document.
SharePoint Server 2007	A document management and collaboration server integrates with Windows Right Management to allow for strong document control and auditing.
XPS format support	A document format enables strong access controls based on Rights Management Services.
Exchange Server 2007 Ethical Firewall	This policy-based solution enables organizations to control what content is allowed through the e-mail channel.
Exchange Server 2007 IRM support	This policy-based solution integrates Rights Management Services with the corporate e-mail server, enabling rights-driven access control over who can view mail messages and what they can do with them.

## Auditing and Reporting

Compliance with internal policies, government regulations and consumer demands for better control over private information require the use of monitoring technologies to assist organizations with audit and reporting related to data, systems and applications. Systems management and monitoring technologies can verify that system and data access controls are operating effectively, and identify suspicious or noncompliant activity.

Table 6 provides some examples of auditing and reporting products available from Microsoft.

**Table 6: Auditing and reporting products and technologies**

<b>Product or Technology</b>	<b>Description</b>
System Center Operations Manager	An enterprise-ready network and server management solution enables centralized reporting and management of all computing devices on the network. Operations Manager also provides strong Audit Collections functionality (through Audit Collections Services) and provides data segregation, thus providing separation of duties and non-repudiation.
SystemCenter Configuration Manager	An enterprise-ready systems management solution enabling centralized software deployment and management throughout the organization.

---

## Summary

The computing environment in the financial services sector is becoming increasingly complex because of the demands for anywhere, anytime information access from many different types of devices. Each type of device and the location in which the device operates brings a unique set of security issues that the financial services sector CSO must address. Security and data protection policies and actions depend upon not only on the user's location, but also the type of device used in that location. Microsoft understands these scenarios and offers a wide range of security products and technologies for the financial services company looking to meet these challenges.

---

## For More Information

For more information on Microsoft products and technologies that help protect data in financial services organizations, please visit the following Web sites:

**Windows Vista Security Guide** <http://www.microsoft.com/technet/windowsvista/security/guide.aspx>

**Internet Explorer 7 Technology Overview**

<http://www.microsoft.com/downloads/details.aspx?FamilyId=2717A8CB-0FAA-4A8E-B5D3-987DC654ACBB&displaylang=en>

**Windows Server Update Services**

<http://www.microsoft.com/windowsserversystem/updateservices/default.aspx>

**Windows Defender** <http://www.microsoft.com/athome/security/spyware/software/default.aspx>

**Windows Firewall** <http://www.microsoft.com/technet/community/columns/cableguy/cg0106.aspx>

**Network Access Protection (NAP)** <http://www.microsoft.com/technet/network/nap/default.aspx>

**Virtual Private Networking (VPN)** <http://www.microsoft.com/technet/network/vpn/default.aspx>

**Forefront Security Products** <http://www.microsoft.com/forefront/default.aspx>

**Exchange Server 2007** <http://www.microsoft.com/exchange/evaluation/overview/default.aspx>

**Windows Mobile 6** <http://www.microsoft.com/windowsmobile/6/default.aspx>

**Microsoft Office 2007** <http://office.microsoft.com>

**Information Rights Management**

<http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.aspx>

**Microsoft Active Directory**

<http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.aspx>

**Active Directory Federation Services**

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/adfs/default.aspx>

**Windows CardSpace** <http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx>

**Microsoft Identity Lifecycle Manager 2007**

<http://www.microsoft.com/windowsserver/ilm2007/overview.aspx>

**Encrypting File System**

<http://www.microsoft.com/technet/security/guidance/cryptographyetc/efs.aspx>

**BitLocker Hard Disk Encryption** <http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx>

**Internet Protocol Security (IPSec)** <http://www.microsoft.com/technet/network/ipsec/default.aspx>

**Microsoft SQL 2005 Security**

[http://www.microsoft.com/sql/technologies/security/securityfeatures\\_1.aspx](http://www.microsoft.com/sql/technologies/security/securityfeatures_1.aspx)

**Microsoft SharePoint 2007** <http://www.microsoft.com/sharepoint/default.aspx>

**Microsoft Data Protection Manager** <http://www.microsoft.com/systemcenter/dpm/default.aspx>

**Microsoft System Center Operations Manager 2007**

<http://www.microsoft.com/systemcenter/opsmgr/default.aspx>

**Microsoft System Center Configuration Manager 2007**

<http://www.microsoft.com/smsserver/default.aspx>