Entrust® Securing Digital Identities & Information

Securing Your Digital Life

# Protecting Your Most Important Asset:  Information

***How Data Security Mitigates Risk and Enables Compliance***

September 2004

The material provided in this document is for information purposes only. It is not intended to be advice. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

## TABLE OF CONTENTS

# Executive Summary

As organizations open their doors to employees, partners, customers and suppliers to provide deeper access to sensitive information, the risks associated with e-business increase.

Now, more than ever, with increasing threats of cyber terrorism, corporate governance issues, fraud, and identity theft, the need for securing corporate information has become paramount. Information theft is not just about external hackers and unauthorized external users stealing your data—it is also about managing internal employees and even contractors who may be working within your organization for short periods of time.

Adding to the challenge of securing information is the increasing push for corporate governance and adherence to legislative or regulatory requirements. Failure to comply and provide privacy, audit and internal controls could result in penalties ranging from large fines to jail terms. Non-compliance can result in not only potential implications for executives, but also possible threats to the viability of a corporation.

Laws such as California SB 1386, HIPAA, and the European Data Directive include requirements for the privacy and security of your most valuable asset—information. Without the ability to access information or trust in its integrity, organizations cannot do business. If the information is lost or otherwise disclosed, serious consequences may result.

Information is stored all over the network within file folders, on desktops and laptops, stored on PDAs and memory cards or on servers in backend repositories. In order to secure information that is dispersed across a diverse environment, a solution needs to be scalable, yet comprehensive enough to deliver ***authentication***, ***access control***, ***encryption*** and ***digital signatures***—that enable accountability and privacy.

The Entrust Secure Data Solution integrates Entrust's security expertise with a broad range of industry relationships to deliver a comprehensive approach to securing data either in transit or at rest. Entrust solutions promote interoperability and extensibility to help organizations leverage their investments for a greater level of security across their enterprise systems. Depending on the type of data security risks an organization is attempting to mitigate, Entrust products, services and third party product offerings can be deployed individually or in combination to secure data throughout its lifecycle within your organization.

## Primer: Information as it Stands Today

Businesses and governments have become progressively more dependent on the Internet as a foundation for communication, collaboration and commerce. Their employees are becoming increasingly mobile and demanding real-time access to the applications and information that enable them to do their jobs. Their customers want to conduct transactions online to save time and money. Their partners want to leverage the Web to automate business processes and supply chains over the Web for increased productivity and speed.

To respond to the needs of key stakeholders, more and more organizations are extending their enterprises through Web portals, enterprise applications such as e-mail, VPN and Web services. Organizations view the expansion of their online presence as a method for reducing costs and increasing customer loyalty and market share. Some are creating extranets for vendors, suppliers and preferred customers, by setting up virtual private networks to tie offices together, or by providing remote access to networks for employees and business partners. Sales, service and membership organizations are striving to increase customer loyalty by personalizing online service and improving customer relationship management.

With the openness of e-business comes the reality of information exposure and risk. According to a DTI Study conducted in 2004, the most common breach related to Identity Management involved staff gaining unauthorized access to information. On average, companies reported roughly one such incident each month.

To add to the risk, is the pressure of legislative requirements such as Sarbanes-Oxley, HIPAA, FISMA, California SB 1386 and the European Data Directive. Strong information security governance frameworks are necessary to help organizations with their challenge—to balance the need to give stakeholders deeper online access, with the need to protect information assets and comply with regulations for privacy and corporate governance—all while meeting investor expectations for cost control and return on investment.

One important key to the success of a compliance initiative is a broad understanding that information security governance is not just a technical issue that can be addressed by the CIO. It is a corporate governance issue that must be addressed by CEOs and Boards of Directors, and then implemented and enforced at all levels of the organization. And, in today's economic climate, the issue must be addressed in both a timely and cost-effective manner.

For more information on Information Security Governance please visit the Entrust web site: http://www.entrust.com/governance.

> "The need by public enterprises to attest to their internal controls infrastructure in support of regulations such as the GLB Act, HIPAA and Sarbanes-Oxley is putting the spotlight on the security of the IT resource access request process. Strong authentication of the users involved in the process - request, approval and fulfillment, the integrity and non-repudiation of the access request transaction itself and a strong, secure audit trail of the access request process activities - will become important features of the Identity and Access Management solutions within these enterprises."
>
> ***-- Roberta Witty, Research Director, Security and Privacy, Gartner***

# The Need for Secure Data

Business realities are driving the need for identity and access management solutions that secure digital identities and information. Three critical areas that organizations need to consider when addressing their needs for identity and access management include secure identity management, secure messaging and secure data. For the purpose of this paper, we will focus specifically on securing data to help comply with legislation, protect competitive advantage and enable new business processes.

## The Threat to Corporate Data

The very openness and accessibility that has stimulated the adoption and growth of private networks, the Internet and the Web, also threatens the privacy of individuals, the confidentiality of business information, and the accountability and integrity of transactions. Key concerns include risk of theft, alteration, interception and dissemination of confidential data, as well as fraud, damage to reputation and economic loss. Threats to information security arise from external sources such as competitors and computer hackers, as well as internal sources, such as curious or disgruntled employees and contractors. A further challenge for organizations is sufficiently protecting digital information for both regulatory compliance and prevention and countering threats of cyber-terrorism.

To quantify the risk of data theft, confidentiality breaches tend to cause major disruption to organizations over a long period of time (longer than a month in 15% of cases). Remediation and investigation involved significant staff time (10-20 man days, on average). These breaches also resulted in the largest direct cash expenditure of any security incidents[1].

## The Challenge of Securing Data

The challenge of securing data is daunting, as data is stored in many locations such as within files and folders on desktops, laptops, enterprise servers or other electronic devices. Additionally, data is regularly replicated and moved from point to point both within an organization as well as with customers, partners and regulatory agencies. To truly understand data vulnerabilities, an organization needs to understand the overall lifecycle of its important data assets; from the time the data is created to the time it is destroyed, including all points in between.

As data is stored for longer periods of time, organizations need to figure out how to store the

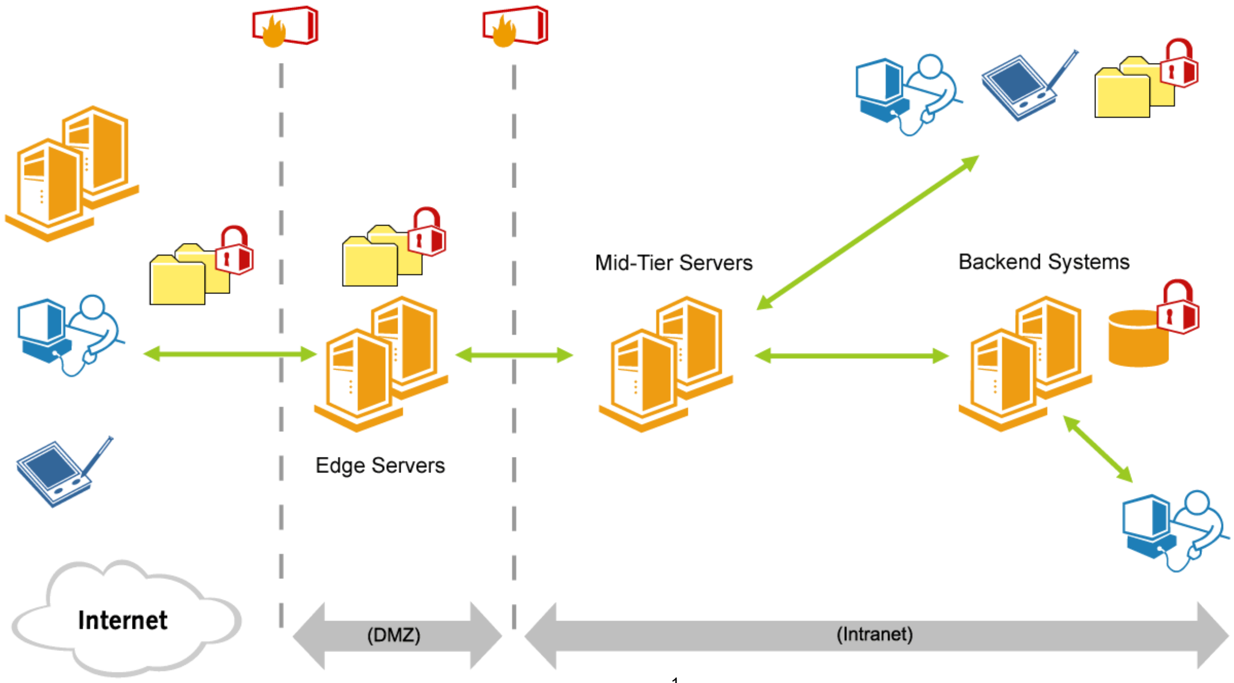


**Figure 1:** The Lifecycle of Data

[1] DTI Information Security Breaches Survey 2004

data securely, but also ensure that the data can be easily accessed 10 to 20 years later, when systems have been changed and applications have evolved or people have left the company. This results in the challenge of providing sound key management and recovery.

According to the **2003 Computer Security Institute and Federal Bureau of Investigation Computer Crime and Security Survey**, the theft of proprietary information caused the greatest financial loss amongst respondents at $70.1 million, with the average reported loss being approximately $2.7 million. Carnegie Mellon noted that there were 137,529 security incident reports in 2003, a 168% increase over the 82,094 reported in 2002.

## Mitigating Data Security Risks

Ultimately, companies need to grapple with balancing the risks associated with the loss, corruption and disclosure of sensitive data with the value gained by storing, analyzing and sharing that information. If the potential gains don't outweigh the risks for a given set of data, the organization should not be handling it.

Unfortunately, striking this balance is not a one-time effort as many factors are continually at play, affecting the balance of risk versus the openness of information, including:

- Increasing value of data in a knowledge economy
- Increasing number and sophistication of threats and vulnerabilities
- Increasing expectations from customers, partners and regulators
- Increasing potential value of damage

Fortunately, there is a common set of capabilities that can be used to mitigate risk and these capabilities are often deployed in combination to address specific data vulnerabilities.

### Authentication

For most organizations, the rules that govern who can see, access or otherwise modify information, is strongly tied to the identity of the requestor. Therefore, the ability to verify the identity of users, devices and applications through an appropriate authentication method becomes a critical component of securing data within an enterprise.

### Authorization / Access Control

Sensitive data and applications need to be protected so that only authorized individuals can access them. Policy-based controls enrich the traditional identity and roles-based access control model, enabling more complex rules based on other criteria such as time-specific restrictions or location of the requestor.

### Encryption

Encryption is a process of transforming data into a format that only the intended recipient understands. This is particularly useful when unauthorized access to the data cannot be prevented absolutely, for instance while it is in transit across a public network, or in an access control system. When deploying encryption as a security control it is important to choose a standards-based encryption product with 3rd party validation (such as FIPS or Common Criteria), which is recognized by Government and Industry security professionals to meet their requirements for protecting sensitive information.

### Digital Signatures

Verifiable digital signatures can also play an important role in securing data. They can be used for accountability and verification of participation features—an important mechanism in providing data controls and audit. Additionally, they provide the ability to detect data tampering, allowing organizations to maintain data integrity.

### Content Analysis

The ability to identify sensitive data through the use of content analysis is a very powerful tool to help organizations understand and mitigate their data protection risks. Answering the challenging questions about what sensitive data is residing on the network and where it is located is crucial before organizations can properly address and prioritize how data ought to be protected.

## The Entrust® Secure Data Solution—Comprehensive

The Entrust® Secure Data Solution integrates Entrust's security expertise with a broad range of industry relationships to provide a comprehensive approach to securing data either in transit or at rest. Depending on what data security risks an organization is trying to mitigate, Entrust products, services and partner products can be deployed individually or in combination to secure data throughout its lifecycle within your organization. Some common risk areas that organizations have used Entrust Security Solutions to address include those shown in the table that follows:

| **Organizational Challenge** | **Entrust Products and Services** |
|---|---|
| Protecting data stored on corporate laptops, desktops, removable media and PDAs | **Entrust Entelligence™ Desktop Manager** delivers a single security layer to enterprise desktop applications that provides strong authentication, authorization, digital signatures and encryption, for greater accountability and privacy.<br>**Entrust Entelligence™ File Plug-in** encrypts files and folders stored on desktop and laptop computers via a plug-in to Entrust Entelligence.<br>**Entrust Entelligence™ Security Provider** is a thin-client application that provides enhanced security for the Microsoft® Encrypted File System.<br>**Entrust Entelligence™ Disk Security**, based on Pointsec® Mobile Technologies award-winning Pointsec® for PC security product provides comprehensive laptop and desktop security capabilities - including strong user authentication, authorization and full disk encryption - that automatically protect the entire contents of a hard disk from unauthorized access without impacting user productivity.<br>**Entrust Entelligence™ Media Security** is a PC based file/folder and media protection application, based on Pointsec® Mobile Technologies' Pointsec® Media Encryption security product, that provides file and folder security capabilities - including strong user authentication, authorization and data encryption - that can be used to protect individual files selected by the user and/or automatically protect data saved to specified folder(s) or removable media.<br>**Entrust Entelligence™ Mobile Security** is a family of PDA/smartphone data protection applications, provided in collaboration with Pointsec® Mobile Technologies, that provide device data security capabilities - including strong user authentication, authorization and data encryption - that can be used to protect applications and confidential data stored on these devices. |
| Protecting data received over the Internet and within the corporate DMZ | **Entrust TruePass™** software provides end-to-end Web security, including strong authentication, digital signatures and encryption with unmatched ease of deployment and user transparency. |
| Protecting data entered and stored in electronic forms | **Entrust Entelligence™ Verification Plug-in** enables organizations to publish secure, digitally signed documents that can be verified by external users without the need for Entrust desktop security software.<br>**Entrust TruePass™** software provides end-to-end Web security, including strong authentication, digital signatures and encryption that can be integrated to protect content in web forms. |

| | |
|---|---|
| Protecting data exchanged in web service applications | **Entrust Authority™ Toolkits** provide a set of XML standards-based, security capabilities that can make it possible for developers to rapidly integrate security services into web service applications.<br>**Entrust® Secure Transaction Platform** delivers a comprehensive set of Web Services security capabilities for integrating authentication, authorization, and digital signatures into Web Services applications. |
| Protecting secure file transfer between organizations | **Entrust Authority™ Toolkits** provide a set of standards-based, application programming interfaces (APIs) that can make it possible for developers to rapidly integrate security services into file transfer environments across multiple applications and platforms.<br>**Entrust TruePass™** software provides end-to-end Web security, including bi-directional data encryption that can be used to protect data transferred over the web. |
| Controlling access to web based applications and information | **Entrust GetAccess™** software provides high performance, scalable Web access control and single sign-on to Web applications. It centrally manages access to single or federated portals and can be easily extended to support Web Services environments. |
| Building security into corporate applications and protecting data in backend data repositories and archives | **Entrust Authority™ Toolkits** provide a set of standards-based, application programming interfaces (APIs) that can make it possible for developers to rapidly integrate data security services into their applications so that data can be stored encrypted in backend repositories. |
| Adding security to existing ERP/CRM systems | **Entrust Authority™ Toolkits** provide a set of standards-based, application programming interfaces (APIs) that can make it possible for developers to rapidly integrate security services into their environment across multiple applications and platforms. **Entrust TruePass** provides end-to-end Web security, including strong authentication to web apps. |

## Partners in Data Protection

Entrust also has a broad range of integrated third party partner product solutions that help organizations extend Entrust capabilities to solve more specific security challenges. For more information on third party partner products and services, please refer to the Entrusts web site: http://www.entrust.com/partners.

# Choosing a Trusted Advisor

Organizations realize that protecting their business data through technology alone is not enough. Many other elements need to be considered when evaluating a potential security vendor.

For many years, Entrust has sponsored a blind study conducted by an external research firm. The aim of this study is to measure the vendor criteria deemed most important by Information Security Customers and the performance perception of Entrust relative to its direct competitors across all major functional areas including Product Capability, Customer Support, Professional Services, Sales and Marketing. The study not only provides insight, clarity and direction regarding areas where Entrust should focus its efforts in order to continue to offer best-in-class products, but also serves as a point of reference for the key criteria that customers should consider when choosing a vendor.

| Vendor Criteria | What To Look For in a Vendor |
|---|---|
| **Product Capability** | |
| Breadth of offerings | □ Integrated across a wide range of solutions including:<br>– Secure Data<br>– Secure Identity Management<br>– Secure Messaging |
| Product security | □ Vendor with a strong reputation in security:<br>– Solutions requiring frequent patches is a sign that security is not an integral part of their product philosophy<br>□ Vendor with third party security validations such as FIPS-140 |
| Product reliability | □ Products based on open standards |
| Rapid and cost-effective deployment to large numbers of users | □ Deploys quickly and easily via user self-service registration which eliminates need for expensive administrator involvement<br>□ Key backup and recovery<br>□ Low cost, highly secure processes<br>□ Ease of use and transparency |
| **Customer Support** | |
| World class support | □ Support should include:<br>– Range of options to meet your requirements and budget<br>– Software Maintenance - including software upgrades<br>– Online Support - 24 x 7 access to information including FAQs, documentation, technical bulletins, newsletters, and service request submissions and updates<br>– Customer Satisfaction Program – letting customers offer feedback regarding each experience they have with support so that the vendor can perform regular performance-to-objectives and satisfaction reviews<br>– Service Reviews - regular collaboration of R&D, product management, professional services and customer support to enable an integrated approach to customer service<br>– Internal Help Desk Training - annual help desk training profiling<br>– End-User Training – in-class training and computer-based training<br>□ Knowledgeable, professional customer support personnel |
| **Professional Services** | |
| Comprehensive service offerings | □ Vendors with comprehensive offerings should provide:<br>– Security consulting<br>– Deployment and application integration services<br>– Managed security services and partner solutions<br>– Training<br>□ Knowledgeable, professional personnel |
| **Sales and Marketing** | |
| Understands what we are trying to do | □ Proactive account teams focused on helping you succeed:<br>– Listen and understand end user, application and business requirements<br>– Experience helping other customers meet their security goals |

## Interoperability of Entrust Solutions

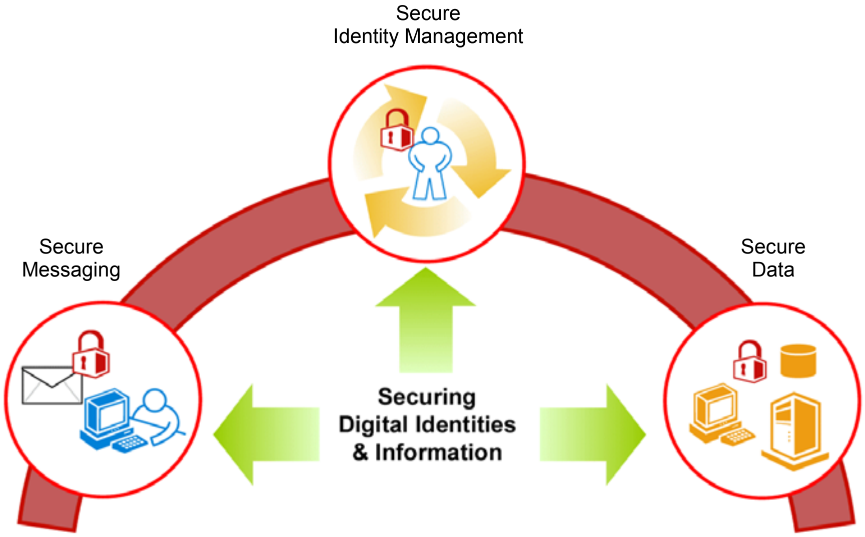
Strong information security governance frameworks are necessary to help organizations with their challenge—to balance the need to give stakeholders deeper online access, with the need to protect information assets and comply with regulations for privacy and corporate governance—all while meeting investor expectations for cost control and return on investment. It is these business realities that are driving the need for identity and access management solutions that secure digital identities and information across all of an enterprise's applications and networks.

The Entrust Identity and Access Management Solutions are designed as part of an extensible security environment that can provide organizations with the ability to secure one application to start and add capabilities as needed, while continuing to leverage their initial investment. Whether the first step toward securing an organization involves protecting e-mail and attachments, safeguarding a Web portal environment, protecting access to laptops and enterprise applications, or authenticating users to a network, Entrust can provide enterprises and governments with solutions that enable them to more easily secure information, and cost effectively extend security across the organization. The Entrust portfolio includes Secure Messaging, Secure Identity Management and Secure Data solutions, all with the ability to seamlessly interoperate and enhance the protection of your organization's digital identities and information, while in transit or at rest.

**Secure Identity Management** allows organizations to securely manage identities and access for users, applications and devices across client-server, Web and Web service architectures;

**Secure Messaging** allows organizations to secure a broad range of e-mail environments to protect the confidentiality of message content and attachments and provide an audit trail for e-mail communications—helping to mitigate the risks associated with communicating sensitive information to employees, customers and partners; and

**Secure Data** allows organizations to protect sensitive information, reducing the risk of loss, disclosure, or corruption, regardless of where it is stored or how it is transmitted and without changing the way users work.



## Protecting Your Data: The Need to Act Now

The very openness of and accessibility to information that has stimulated the adoption and growth of private networks, the Internet and Web services, also threatens the privacy of individuals, the confidentiality of business information, and the accountability and integrity of transactions. Key concerns include risk of theft, alteration, interception and dissemination of confidential data, as well as fraud, loss of reputation and corporate viability.

With so much at stake -- regulatory compliance, good corporate governance, brand equity and customer satisfaction, organizations should consider these issues and evaluate potential solutions to ensure everything is being done to protect data. To help you, the Entrust Secure Data Solution integrates Entrust's decade of experience addressing the data security needs of Global 1000 companies with a broad range of industry relationships to deliver a comprehensive approach to securing data either in transit or at rest.

For more information on the **Entrust Secure Data Solution**, please visit: http://www.entrust.com/data.

## About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities.

For more information on how Entrust can secure your digital life, please visit: **www.entrust.com.**