

**Entrust**<sup>®</sup> Securing Digital Identities & Information



## Securing Your Digital Life

***Did security go out the door with your mobile workforce?***

Help protect your data and brand, and maintain compliance from the outside

September 2006

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. 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 AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2006 Entrust. All rights reserved.

## Table of Contents

1. Out of the office, inside the network .....	3
2. Regulatory compliance requires increased security for mobile workers ...	4
3. Picking a solution to help protect data, brand and maintain compliance from the outside .....	5
4. The Entrust Solution .....	7
5. Conclusion.....	9
6. About Entrust .....	10

## 1. Out of the office, inside the network

More and more organizations are arming employees with the tools to work from anywhere, any time. Employees are accessing the corporate network from hotels, coffee shops and their homes. There are fundamental changes in our collective work habits as activities such as evening email checking and on-the-go report writing are now a part of how we work on a daily basis. Laptops and other mobile computing devices such as PDA's give employees the flexibility and freedom they need to be more productive.

As more mobile workers with laptops hit the streets or use smart phones and PDA's to work from anywhere at any time the corporate security architecture starts to lose the power to protect and prevent incidents. A mobile worker's lost laptop, the PDA they left in a taxi cab and even their home DSL connection may be outside of IT's control and ability to protect. The security implications are obvious: mobile workers are a weak link in network defenses.

The mounting costs associated with not adequately protecting mobile workers are staggering. While the hardware is replaceable, a \$1500 notebook could potentially contain millions of dollars in data. In addition, the costs associated with notifying customers, restoring customer confidence and minimizing brand damage must also be included should the data be compromised.

While not all laptops or PDA's contain sensitive customer data, there are other real threats lurking. Online attackers have discovered that devices used by mobile workers are often the path of least resistance into a corporate network. It is estimated that half of all network intrusions are made with network credentials from lost and stolen equipment.<sup>6</sup> Without adequate security checks in place to both authenticate and encrypt data, corporate networks can be compromised by a mobile worker's lost laptop or home network.

New security practices and policies are being rolled out for regulatory compliance, and they all highlight the need for encryption and strong authentication. In addition to the operational costs associated with a breach, a lack of mobile data and device security can potentially lead to increased liability, potential brand damage and loss of customer confidence. You need to extend the corporate security architecture to mobile laptops and PDA's by both protecting the data on the device and stepping up security to access the corporate network.

### The threat is real

- 37% of organizations have had a data breach due to loss or theft of mobile devices<sup>1</sup>
- 68% think a data breach is likely in the future<sup>2</sup>
- 250 companies or public institutions have reported data breaches since February 2005<sup>3</sup> impacting over 91 million individuals
- More than half of breaches are the direct result of equipment such as laptop computers being lost or stolen<sup>4</sup>
- It has been estimated that an ordinary laptop can hold content valued at \$972,000 with some storing as much as \$8.8 Million in commercially sensitive data and intellectual property<sup>5</sup>

---

<sup>1</sup> Source: Osterman Research Survey "Mobile Workforce Security", Sept 2006

<sup>2</sup> Source: Osterman Research Survey "Mobile Workforce Security", Sept 2006

<sup>3</sup> Source: Privacy Rights Clearinghouse <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>4</sup> Source: Kensington Group

<sup>5</sup> Source: Symantec Internet Security Threat Report, March 2006

<sup>6</sup> Source: Kensington Group

## 2. Regulatory compliance requires increased security for mobile workers

The increasing pressure to make more access and information available to employees anywhere any time must be balanced with increasing pressure for corporate and regulatory compliance. From California Senate bill 1386 to GLBA (Gramm Leach Bliley Act) nearly every organization is rolling out new practices in their compliance with regulatory guidelines. Simple security measures such as using passwords are no longer enough to prevent breaches, protect privacy and achieve compliance. Enhanced security including strong authentication and complete encryption must be deployed to a wider audience, efficiently and cost-effectively.

### **California Senate Bill SB 1386**

Passed July 1, 2003, California Civil Code Section 1798.8 is the law formerly known as SB 1386. It applies to any entity doing business in California or that handles the personal information of California citizens. It provides for mandatory notification of affected parties in the event of unauthorized acquisition of Californians' personal information that is stored in electronic form.

An organization is required to disclose a breach in data security to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The legislation is explicit in noting that notification is not required if the information is encrypted, known as the "safe harbor" clause.

In addition, as of September 2006 more than 20 other states have enacted their own version of the California legislation including New York and Texas.<sup>7</sup> Several bills are also under review at the federal level.

### **Sarbanes Oxley Act**

The Public Company Accounting Reform and Investor Protection Act, known as the Sarbanes-Oxley Act (SOX), is legislation intended to reform accounting practices, financial disclosures and corporate governance of public companies. SOX requires that organizations ensure the accuracy of financial information and the reliability of systems that generate it.

Section 404 requires an annual assessment of internal controls over financial reporting, certified by an external auditor. Unlike many other legislative guidelines, SOX does not specifically dictate IT security measures be incorporated in to internal controls but companies must demonstrate system and application integrity for tools used to generate financial reports. These internal controls cannot be adequate unless they include strong IT security, including encryption and authentication.

### **Gramm Leach Bliley Act**

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLBA, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Pretexting Provisions and the Safeguards Rule.

The Safeguards Rule requires all financial institutions and related companies that receive customer information such as credit reporting agencies to design, implement and maintain safeguards to protect customer information. Laptops and mobile devices should be considered an important aspect of compliance and companies should ensure that all information on the devices is protected by stored data encryption.

---

<sup>7</sup> Source: Summary of State Security Freeze and Security Breach Notification Laws  
<http://www.pirg.org/consumer/credit/statelaws.htm>

While the specific requirements and language for each of these regulations may differ, their message is clear and unanimous. Organizations must take precautions to secure data whether it is consumer information or financial reporting systems, no matter where it may reside or be used. As mobile workers walk out the door with this data, organizations can help to prevent the fall out resulting from a public disclosure by simply encrypting the data that resides on laptops and requiring the use of strong authentication to access corporate resources.

### 3. Picking a solution to help protect data, brand and maintain compliance from the outside

Two critical components of security can extend the corporate security architecture to include the mobile worker and provide protection for data and the corporate brand while addressing compliance with regulatory guidelines.

#### Strong Authentication

Adding factors of authentication can add security and limit vulnerability to attacks for mobile workers. From VPN's to windows sign on, properly designed and implemented multifactor authentication methods can offer stronger breach prevention with minimal impact on the mobile worker. With strong authentication, a lost laptop is no longer a master key into the corporate network for an intruder.

#### Full Disk Security

Full-disk encryption for laptops and desktops can provide transparent security on-the-fly to mobile workers. With full disk security, the confidential information and customer data contained on a lost laptop will be strongly protected.

With such a broad range of security tools available, selecting the appropriate solution can be daunting. A single vendor with a total solution for your mobile workforce can often maximize security coverage and provide one of the most cost effective solutions. Three key criteria must be examined when comparing solutions: security, usability and cost. Use the following framework to help evaluate solutions and vendors:

	<b>Strong Authentication</b>	<b>Full Disk Encryption</b>	<b>Vendor</b>
<b>Security</b>	<b>Certified</b> – by industry certifications such as FIPS	<b>Certified</b> – by industry certifications such as FIPS and Common Criteria EAL-4	<b>Trusted</b> -reputation and focused security expertise.  <b>Proven</b> - Customer references, especially in government and financial services where regulatory pressure has been the most intense.
<b>Usability</b>	<b>Minimal user impact</b> - Choose a system that can follow existing user interaction models and that does not require increased technology knowledge for employees.	<b>Minimal user impact</b> - automatically encrypt data stored on laptops with little impact to normal behavior performance.	<b>Experienced</b> – Proven customer deployments

	<p><b>Flexible</b> – look for a platform that can address your needs now and has scaling capabilities as the organization grows and changes over time.</p> <p><b>Integration</b> – Make sure it supports leading applications like VPN remote access from range of vendors, Microsoft Outlook Web Access and includes native Microsoft desktop application integration</p>	<p><b>Extend</b> - to other devices, mobile storage. Can the same solution provide complete encryption for other vulnerable devices.</p>	
<b>Cost</b>	<p><b>Purchase cost</b> - examine up-front costs to acquire and deploy the solutions</p> <p><b>Operating cost</b> – analyze the cost of a lifetime of renewals, device replacement, management and deployment costs. There can be significant differences between expensive time-synchronous tokens and security grids which can offer a lower total cost of ownership.</p>	<p><b>Total cost of ownership</b> – can be lowered with centralized administration for creating, deploying, managing and updating corporate laptop and desktop security policies</p>	<p><b>Maximize coverage</b> – Be sure to look for opportunities to lower costs by using a single vendor with bundled solution to stretch budget dollars while extending overall security coverage.</p>

One key to assessing and selecting appropriate solutions is to examine the security needs of mobile workers holistically, looking at both the need for strong authentication and complete disk encryption as a single system. Select a solution and a vendor that can deliver both today and that can respond and adapt to future needs.

## 4. The Entrust Solution

The Entrust mobile workforce solution can help to mitigate risk, protect your brand and address compliance with regulatory guidelines. Composed of two industry leading products; Entrust IdentityGuard and Entrust Entelligence™ Disk Security, the Entrust mobile workforce solution can provide enhanced security for mobile workers while minimizing impact on user experience.

### ***Entrust IdentityGuard delivers strong authentication***

*“Simple passwords alone no longer provide sufficient confidence in users’ asserted identities.”*

Gartner IT Security Conference  
“User Authentication Solved!” Ant Allan  
June 5-7, 2006

Organizations need to secure the identities of mobile workers to protect the contents of their laptops and add security to their corporate networks and resources. Entrust IdentityGuard is a multi-factor authentication platform enabling strong authentication for the Windows desktop, remote access deployments, and corporate intranets.

Entrust IdentityGuard provides:

- Two-factor authentication for remote access (secure VPN provided from leading vendors like Check Point, Cisco, Citrix, Nortel, and Juniper)
- Support for leading applications like Microsoft Outlook Web Access
- Native Microsoft desktop application integration

The flexibility of the platform allows organizations to help minimize the risk of fraudulent activity caused by the low security associated with usernames and passwords, without having to deploy a ‘one-size fits all’ solution (such as tokens). Unlike traditional battery-powered time-synchronous token offerings, Entrust IdentityGuard can provide a broad range of authentication capabilities most cost effectively, can be deployed as required to address security requirements, and does not require specialized hardware. Entrust IdentityGuard uses a knowledge-based mechanism and security grid that can be easily understood by users with minimal impact on their experience.

Entrust IdentityGuard helps to:

- **Manage cost and complexity** with a single platform that provides a range of strong authentication methods.
- **Streamline administration** with central policy management that can help decrease the risk of policy inconsistency.
- **Be ready for what comes next** thanks to an open architecture and stable platform committed to adding new and innovative authentication options like those developed by Vasco.

Entrust IdentityGuard is a proven solution used by multiple large financial institutions today including Commercebank, Banco Santander, Bank of New Zealand and Schufa.

***Entrust Entelligence™ Disk Security delivers complete data protection***

*“There is only one tool to protect sensitive information on a lost laptop: encryption — preferably whole-drive encryption”*

Gartner  
“Top Five Steps to Prevent Data Loss and Information Leaks”  
Rich Mogull  
July 12, 2006

Entrust Entelligence Disk Security helps to:

- **Government strength protection** with the highest level of security including pre-boot full disk encryption and proven technology certified by FIPS 140 and Common Criteria EAL-4
- **Streamlined administration** with easy, centralized management and administration tools including recovery, logging and audit capabilities.
- **Minimal impact to mobile workers and performance** with transparent, automatic encryption of data stored on their laptops that has little overall impact on system performance.
- **Extended protection to other devices** including portable media devices and mobile devices such as USB keys, CD/DVD's, PDAs and smart phones using Palm, Symbian and Windows Mobile operating systems.

## 5. Conclusion

The explosion in the use of laptops and other mobile computing devices has given organizations the opportunity to improve productivity and efficiency. As the pressure to comply with regulatory requirements combines with the growing number of users working outside the boundaries of the corporation, the need for security for the mobile worker has never been greater. Employees now have the flexibility and freedom to work when they want and enterprises can rest assured that their productivity will not be impeded by invasive security measures.

Policies remain an essential part of the answer to the issues facing mobile workers and security, but relying on employees to personally comply as some 67% of organizations do, does not offer the level of protection required. Security must enable employees to continue working with the freedom and flexibility provided by mobile technology. Transparent solutions such as the Entrust mobile workforce solution provide security without changing how employees work or impeding mobility and flexibility.

Security must be cost effective and manageable to preserve the efficiency gains made by the mobile workforce. The Entrust mobile workforce solution provides two essential types of protection, from a proven security expert; strong authentication and full disk encryption designed to help organizations protect data, the brand and maintain compliance.

## 6. About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,500 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.