



# Extending Enterprise Security Beyond The Perimeter





## Table of Contents

<b>WHY YOU SHOULD READ THIS WHITE PAPER .....</b>	<b>3</b>
<b>DEPERIMETERIZATION: BUSINESS NECESSITY AND BUSINESS RISKS .....</b>	<b>4</b>
<b>SECURITY IS ONLY AS STRONG AS ITS WEAKEST LINK.....</b>	<b>5</b>
CHALLENGES TO SECURING DATA IN A DEPERIMETERIZED NETWORK.....	5
<b>THE SECUWARE SOLUTION .....</b>	<b>6</b>
C2K .....	6
DEVICE MANAGEMENT .....	7
<b>SECUWARE BENEFITS .....</b>	<b>7</b>
COMPLETE 360° PROTECTION FOR DATA .....	7
EASY DEPLOYMENT AND MANAGEMENT .....	8
END USER TRANSPARENCY .....	8
LOW IMPACT ON SYSTEM PERFORMANCE .....	8
HIGH RETURN ON INVESTMENT (ROI) DRIVEN BY LOW MANAGEMENT COSTS .....	8
<b>SUMMARY.....</b>	<b>9</b>
<b>ABOUT SECUWARE .....</b>	<b>9</b>



## Why you should read this white paper

Deperimeterization is one of the latest security buzzwords. What is deperimeterization? Basically, it refers to the erosion of the corporate network's perimeter, the historical point of strategic defense, through the introduction of laptop computers, mobile storage devices, etc. into the enterprise mainstream. The perimeter has not disappeared, but it has become a much more chaotic and dynamic entity, and defining its boundaries has become considerably more difficult.

Some years ago, Sun Microsystems coined the slogan, "The network is the computer." Today, it may be more accurate to say, "The network is everything." Laptops, USB drives, CDs and DVDs, iPods and an array of other devices can all act as gateways to the corporate network and the data which it holds. In today's increasingly fast-paced and peripatetic business environment, it is necessary to allow such access to the network – but doing so also creates a major headache, as the majority of security appliances and applications provide IT with no control over which devices can connect – and what data can be transferred to and from those devices.

This white paper will examine the risks associated with deperimeterization and explain how Secuware's solutions can be used to mitigate such risks without impacting user productivity.



## Deperimeterization: business necessity and business risks

Deperimeterization is a business necessity. To remain competitive and to meet the needs of an increasingly geographically dispersed and mobile workforce, enterprises need to empower staff with anywhere-access to corporate data. As a result, data is no longer exclusively held on stationary desktops or servers that are shielded by the company firewall; instead, it is distributed across a wide range of mobile computing and storage devices over which many IT departments have extremely limited control. This introduces serious business risks, as illustrated by a number of recent cases:

- A hard drive belonging to the UK's Driving Standards Agency containing information relating to 3 million people was lost by a contractor.<sup>1</sup>
- CDs containing unencrypted personal information relating to approximately 25 million UK state benefit recipients were lost in the mail. The disks were reported as having a black market value of more than \$3 billion.<sup>2</sup>
- A research chemist attempted to steal proprietary information worth more than \$400 million from his employer, DuPont, by transferring data to a laptop owned by a competitor.<sup>3</sup>
- A laptop containing the personal information of 800,000 individuals was stolen from the offices of a vendor that managed job applications on behalf of Gap Inc.. Following the incident, Gap Inc. offered to cover the cost of credit monitoring services for each affected person for 12 months.<sup>4</sup>

Such security breaches are not uncommon; according to a 2007 study by the Computer Security Institute (CSI), approximately 50% of organizations have faced a potential data loss as a result of lost or stolen laptops, mobile storage devices or other media.<sup>5</sup> The statistics collected by the consumer advocacy group Privacy Rights Clearinghouse further highlight the extent of the problem: since January 1995, more than 200 billion records containing personal information have been compromised due to data breaches in the US.<sup>6</sup>

Insider threat also presents a real and serious risk. The CSI study indicates that more than 50% of US organizations experienced at least one instance of financial loss as a result of the activities of insiders and, in the 2007 E-Crime Watch Survey conducted by US Secret Service, CERT and Microsoft, 34% of organizations reported that criminal actions by insiders had resulted in greater damage than criminal actions by outsiders.<sup>7</sup> The E-Crime survey also found that 36% of crimes had involved USB drives and other mobile storage media being used to copy customer records, intellectual property and other proprietary or sensitive information.

Data leakage is not the only risk associated with mobile computing and storage devices; such devices also have the potential to act as vectors for malware. This is nothing new, of course. From the Elk Cloner virus<sup>8</sup> to Sony's much publicized rootkit<sup>9</sup>, mobile storage media have long been used to spread malicious code. Until recently, it was reasonably easy for IT departments to combat the problem: the majority of employees had no need to use mobile media and so CD drives and other plug-and-play devices could simply be disabled. However, in many enterprises this is no longer an option; mobile workers need equally mobile data.

Additionally, mobile computing and storage devices increase the challenges of achieving compliance with the Sarbanes-Oxley Act (SarbOx), the Health Insurance Portability and Accountability Act (HIPAA),



the Gramm-Leach-Bliley Act and other mandates that specify standards for data protection. But criminal or civil sanctions are not the only adverse consequences of a data breach. Remedial action can be expensive and the resultant negative press can be extraordinarily damaging to an enterprise's reputation and ultimately even threaten its very survival.

## **Security is only as strong as its weakest link**

In the past, the perimeter was considered to be the most important point of defense: lock it down and the corporate network and its data would be secure. While protecting the perimeter - even in its less distinct form - continues to be an important and integral component of any security strategy, intrusion detection systems and firewalls alone simply do not provide adequate protection in today's mobile world.

Security is only as strong as its weakest link, and the value of a hardened perimeter is substantially eroded if other uncontrolled gateways to the network exist. The risk associated with the use of mobile devices is now widely recognized; attendees of the 2007 InfoSecurity Europe conference listed mobile devices as their main security concern.<sup>10</sup> However, while awareness may be increasing, finding a manageable solution to the problem can be elusive.

## ***Challenges to securing data in a deperimeterized network***

Security becomes a much more complex and challenging subject in a deperimeterized environment.

- How can security policies be enforced on intermittently-connected mobile devices, be that device a laptop or a mobile storage medium?
- How can data held on those devices – or on devices to which the data may be subsequently transferred – be secured?
- How can intentional or unintentional data leakage via mobile devices be prevented?
- How can all this be achieved without impacting either the usability of devices or end user productivity?

Traditional security solutions simply do not deliver in a deperimeterized infrastructure. Firewalls and intrusion detection systems can protect data held on a Storage Area Network (SAN) or on Network Attached Storage (NAS), but neither can protect unstructured data that is distributed across a multitude of mobile devices. Encryption products, while providing an additional tier of security, do not cut it either. Even when an encryption product is in place, users can still choose to disregard policy and copy data to a laptop or USB drive in an unencrypted form and, as a result, enterprises continue to be exposed to the risk of both the intentional theft of data and the careless loss of data.

To ensure complete and cost efficient protection for critical data, enterprises need a solution that integrates seamlessly with the existing security and policy framework to restrict access to data, that automatically enforces policy on any device connecting to the network and that continues to protect data even after it has been moved beyond the confines of the corporate network.



## The Secuware solution

Secuware's integrated approach to security has been designed from the ground up to provide comprehensive protection for enterprise data without degrading system performance or impacting end user productivity. Built around the concept of closed circuits for information, meaning that predetermined users or groups of users will share the same encryption keys and be able to access the exactly same data, the solution currently consists of a centralized management console implemented as a directory snap-in that acts as a front-end to two easily distributable client modules:

### C2K

C2K is used to create and enforce security policies in relation to pre-boot authentication and physical and logical encryption using a combination of Computer Profiles and User Profiles. C2K Computer Profiles enforce full disk encryption and pre-boot authentication, and set the permitted authentication mechanisms (USB tokens, smartcards, etc.). User Profiles prevent internal data leakage and unauthorized access to information and can be applied to individual users, groups of users, an entire domain or any combination of these. These profiles can also be used in conjunction with **Device Management** (see below) to restrict access to data, applications and devices. Any group of users to whom a given User Profile is assigned will be within the same closed circuit for information,

Administrators can create as many or as few Security Profiles as are considered necessary. Some enterprises may need to create only a relatively small number of User Profiles, with each Profile being assigned to a large organizational unit, while other enterprises may wish to drill down further and assign small functional groups or even individual users with a unique User Profile. One Secuware customer has created only three profiles to cover its entire 10,000-strong workforce - one for senior management, one for middle management and one for non-management – while others have created many profiles in order to achieve much more granular control.

With C2K, enterprises can create highly granular security policies that protect data through a number of mechanisms:-

- Pre-boot authentication to ensure that only authorized users can boot a system and access the data that it holds.
- Full encryption of local hard disks to ensure that data is unreadable to anyone other than the authorized user.
- Logical encryption of network-based files and folders to ensure that they can be accessed only by authorized users or groups of users.
- Full encryption of CDs, USB storage devices and other mobile media to ensure that data is only readable by authorized users using computers on which the Secuware solution is installed.

C2K enables enterprises to secure data regardless of its location and storage media. Data that is encrypted remains encrypted if copied to a mobile device and can only be accessed once it has been copied back to a computer on which C2K is installed – and, even then, only by a user who has been authorized to access the data. By restricting access to data to authorized users, C2K enables enterprises to minimize the possibility of both intentional and unintentional data leakages.



## **Device Management**

Device Management enables security administrators to create a whitelist of allowed USB and FireWire devices based on the manufacturer and/or serial number of each individual device and to assign each to device to one or more User or Computer. Users or computers with Security Profiles that have no device assigned will be unable to access any device while users or computers under a Security Profile with a device or devices assigned will be able to access only those assigned device or devices.

This enables enterprises to specify which users can access mobile devices and which devices those users can access. By limiting usage to approved users and approved devices, enterprises can minimize the possibility of data leakage and also minimize the number of channels through which malware could be introduced to the network.

Secuware ensures that best practice is followed by enforcing a division of responsibilities between the security administrator and the system administrator: only the security administrator can create and modify policies and only the system administrator can assign policies to users and computers. This reduces the risk of error and improves security by ensuring that an administrator can perform only the tasks that are within his or her area of expertise.

These two modules, together with the management console, combine to ensure that only *authorized users* using *authorized devices* can access *authorized data* and provide truly mobile protection for today's mobile data. Additional modules are planned for introduction during 2008.

## **Secuware Benefits**

### **Complete 360° protection for data**

C2K enables an enterprise to choose what data is to be encrypted and which users or groups of users are to be permitted access to that data. Data that a user has decrypted will be automatically re-encrypted if copied to a mobile device and will be accessible only by authorized users on authorized computers with Secuware software installed. By restricting access to data and ensuring that it cannot be moved outside of the network in an unencrypted form, C2K eliminates the risks associated with lost or stolen devices, minimizes the opportunity for data leakage or intellectual property theft and militates against both insider and outsider threats.

C2K takes compliance out of the hands of end users through the automatic enforcement of policy. Data that an enterprise determines should always be encrypted *will* always be encrypted regardless of its location and storage media.

**Device Management** guards against data leakage by enabling an enterprise to specify which USB or FireWire devices can be used and which users or groups of users can access those devices. Enterprises may decide to block certain groups of users from accessing mobile devices or may decide to whitelist only devices with relatively small storage capacity in order to limit the amount of data that can be



removed. Additionally, restricting device usage to approved users and devices can also help reduce the chance of malware being introduced to the network.

### ***Easy deployment and management***

Secuware's solutions integrate tightly with Microsoft Active Directory (AD) and other LDAP-based directory services to make deployment and management a snap. User Profiles and Computer Profiles are stored in the Active Directory as schema and, once created, can be easily and speedily applied to all existing users and computers. Similarly, changes to Profiles are automatically implemented when users next login or at the next Group Policy Object push. When a new user is assigned to a Group, the User Profile and/or Computer Profile associated with that Group will be automatically applied to that user.

Interoperability with AD and other directory services also results in Secuware being highly scalable. No matter how large an enterprise may become and no matter how granular its security policies need to become, the solution will continue to be easy to manage.

Additionally, by leveraging the existing infrastructure, Secuware enables enterprises to leverage existing expertise. Administrators already acquainted with LDAP-based directory services will find the learning curve to be extremely low.

Secuware can be rapidly deployed using any standard software distribution mechanism, such as SMS, and does not require a dedicated database or database server.

### ***End user transparency***

Secuware is completely transparent to the end user. Pre-boot authentication is integrated with the Windows log in process - users simply need to provide standard userIDs and passwords, smartcards or USB tokens – and encryption/decryption occurs automatically and entirely in the background. Secuware will not impact end users' ability to work collaboratively, nor will it impact their ability to use mobile computing and storage devices.

The only time that end users will notice that Secuware is running is if they attempt to access a folder or file that they have not been authorized to access or attempt to access an unauthorized device.

### ***Low impact on system performance***

Encrypting and decrypting data can have a high overhead and slow operations. To avoid this, Secuware uses extremely efficient symmetric cipher block algorithms to minimize impact on performance and its encryption and decryption processes impose only a minimal 0.15% overhead.

### ***High return on investment (ROI) driven by low management costs***

Secuware's interoperability and holistic approach to data security, combined with its single-console, centralized administration, result in a solution that is far easier to manage than any collection of platform-specific and/or device-specific products. It is thus able to deliver a far superior ROI than products that provide only a partial solution to the problem of data security.



## Summary

Secuware's solution has been designed from the ground up to provide a cost-efficient solution to the problems associated with securing data in today's deperimeterized environments. The **C2K** and **Device Management** modules enable enterprises to enforce strong, data-centric security policies and to extend those policies beyond the confines of the corporate network, transparently protecting data in real time, regardless of its location and storage medium.

In simple terms, Secuware brings order to the chaos of today's network perimeter.

## About Secuware

Secuware is a leading provider of secure IT infrastructure solutions for the enterprise. The company's flagship products protect sensitive information on desktops, laptops, and other devices while blocking unauthorized access to local and network resources. Founded in 1998 to develop proactive security controls for some of the Ministries of Defense in Europe, the company's operations and customer base now extend to government and commercial entities across several continents, including Wal-Mart, Telefonica, Warner Brothers, and BBVA. For more information on the company and its solutions, visit [www.secuware.com](http://www.secuware.com).

### North American Headquarters

440 North Wolfe Road  
Sunnyvale, CA 94085  
Phone: 408-524-3070  
Fax: 408-524-3072  
Toll Free: 1-800-720-0734

### European Headquarters

Plaza Ruíz Picasso, s/n  
Torre Picasso, Planta 14  
28020 Madrid  
Spain



## References

<sup>1</sup>Millions of L-driver details lost

[http://news.bbc.co.uk/1/hi/uk\\_politics/7147715.stm](http://news.bbc.co.uk/1/hi/uk_politics/7147715.stm)

<sup>2</sup>Discs 'worth £1.5bn' to criminals

[http://news.bbc.co.uk/2/hi/uk\\_news/politics/7117291.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7117291.stm)

<sup>3</sup>Massive Insider Breach At DuPont

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197006474>

<sup>4</sup>Gap Inc. Security Assistance

<http://www.gapsecurityassistance.com>

<sup>5</sup>CSI Computer Crime and Security Survey

<http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>

<sup>6</sup>A Chronology of Data Breaches (Privacy Rights Clearinghouse)

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>7</sup>2007 E-Crime Watch Survey

[www.cert.org/archive/pdf/ecrimesummary07.pdf](http://www.cert.org/archive/pdf/ecrimesummary07.pdf)

<sup>8</sup>Elk Cloner Virus (Wikipedia)

[http://en.wikipedia.org/wiki/Elk\\_Cloner](http://en.wikipedia.org/wiki/Elk_Cloner)

<sup>9</sup>Extended Copy Protection (Wikipedia)

[http://en.wikipedia.org/wiki/Sony\\_rootkit](http://en.wikipedia.org/wiki/Sony_rootkit)

<sup>10</sup>Security's Top Five Priorities

[http://www.darkreading.com/document.asp?doc\\_id=123294](http://www.darkreading.com/document.asp?doc_id=123294)