



How Lumension Security's Sanctuary Suite assures governance with the NHS directive for securing data in transit.

v1.0

Monday, February 11, 2008

www.lumension.com



Table of Contents

Introduction	2
Specific Requirements for Securing Data in Transit	2
Protect Data in Transit with Lumension’s Sanctuary Suite	4
Positive Approach to Security	5
Simple, Fast, Flexible Administration and Management	5
Automated Discovery of Applications and Devices	5
Granular Device Control Permission Settings	5
Enforced Encryption.....	6
Flexible Authorisation Rules	6
Comprehensive Security and Detailed Audit Capabilities	6
USB Security Built to Scale.....	6
Award-Winning, Certified and Proven.....	6
Extending Sanctuary’s Data Protection Capabilities with Whole Disk Encryption	6
About Lumension Security	6
For More Information	7



Introduction

In December 2007, the office of David Nicholson CBE, the Chief Executive of the NHS in England, wrote to all Chief Executives of all Strategic Health Authorities, Special Health Authorities, NHS Trusts and Primary Care Trusts, restating the key responsibilities and accountabilities for securing effective information governance and to clarify required actions. Within the content of the letter (Gateway reference number 9185) are specific requirements for securing data in transit.

This document examines how Lumension's Sanctuary Suite, which includes Application and Device Control, assures NHS Trusts of governance with all of the stated requirements for securing data in transit and maps the solution's capabilities to these specific requirements.

Specific Requirements for Securing Data in Transit

NHS Directive	How Sanctuary Suite Addresses the NHS Directive
Check your systems and procedures and deal with any short falls immediately.	Sanctuary Device Control has a unique audit-only capability that identifies any users who are transferring person identifiable data onto removable media. Patented forensics audit the full content of this data to quantify short falls – whether it is written to or from removable media.
Check that your control of the movement of person identifiable data is good enough.	Sanctuary Device Control has a unique audit-only capability that identifies any users who are transferring person identifiable data onto removable media. Patented forensics audit the full content of this data to quantify short falls – whether it is written to or from removable media. Enforcement of acceptable usage is achieved via a centralised policy engine that can distribute reports as needed to demonstrate that your controls are “good enough”.
Buy in some information security expertise if you do not have it in house.	Lumension's and our partners' professional services teams are ready to conduct a complementary risk assessment if needed. South London and Maudsley NHS Trust is a case study site, copies of which are available upon request.
Do not hold person identifiable data on portable media unless it is encrypted.	Sanctuary Device Control has flexible encryption options to guarantee that only authorised personnel can transfer data onto portable media only if using 256 bit AES encryption (an applicable NHS IG data



	<p>encryption algorithm).</p> <p>Advanced encryption management features include:</p> <ol style="list-style-type: none">1. Centralised Password complexity enforcement.2. Failed Login lockout in case removable media is lost.3. Centralised Password recovery.4. Forced Encryption of existing data on removable media. <p>Sanctuary Device Control also ensures that:</p> <ul style="list-style-type: none">☑ Policy is enforced centrally with minimum disruption to the Trust or user.☑ Only authorised personnel are able to write data onto removable media – all other users are denied by default.☑ Temporary, scheduled and offline/online permissions give flexibility where needed whilst ensuring that controls remain good over time.
<p>Do not bulk transfer person identifiable data, unless it is absolutely needed for direct patient care, before you have sorted out your secure processes and do this quickly.</p>	<p>Sanctuary Device Control can:</p> <ul style="list-style-type: none">☑ Prevent bulk transfer via daily Copy Limits, which are centrally controlled. Permissions can be assigned per person, group of users or computer.☑ Whitelist file types to control what specific files are authorized to be transferred onto removable media☑ Prevent unauthorised personnel transferring data to removable media by a unique whitelisting capability (typically activated after the audit-only phase). <p>Sanctuary Device Control is deployed easily, without disruption via most third party software deployment tools or via our own</p>



	complimentary deployment utility. If bulk data transfer is needed for direct patient care, centralised temporary permissions and patented auditing ensure this process is managed and that good governance is maintained.
Check your security policies for laptops, CDs, pen drives, etc.	<p>Sanctuary Device Control enforces written policies for peripheral devices, CD/DVD, pen drives, etc. Policy compliance reports can be automated, scheduled and delivered to the appropriate personnel (Example: any change from written policy for operational reasons delivered via e-mail to the data protection officer).</p> <p>Temporary permission changes enable important direct patient care information to be transported by someone who usually does not have permission to transfer data to portable media.</p> <p>Attempted policy violations can also be automated, scheduled and delivered to the appropriate personnel (Example: security violations delivered e-mail daily to security officer).</p>
Make sure you have a data protection incident reporting and risk assessment process.	Sanctuary Device Control can produce data protection incident reports ensuring the risk assessment process is effective (Examples include: access to removable media denied, copy limit exceeded, temporary policy change, data transfer reporting, etc.). These reports can be easily customised depending on the Trust's specific requirements.

Protect Data in Transit with Lumension's Sanctuary Suite

Protecting against known and unknown threats targeting your enterprise, Sanctuary combines the proven capabilities of its Application Control and Device Control modules, providing organisations with the only endpoint security solution to centrally manage, monitor and control applications and devices on the corporate network.

Lumension Security's Sanctuary Application Control provides policy-based enforcement of application use to secure endpoints from malware, spyware, zero-day threats and unwanted or unlicensed software. When integrated with Sanctuary Device Control, you can secure endpoints from becoming a doorway for sensitive data to escape and for security threats such as malware to enter. Sanctuary:

- ☐ Removes the risk of data theft, data loss or data leakage as a result of



unauthorised applications

- ☒ Prevents the execution of unknown/malicious code including malware, spyware, zero-day threats and all other destructive viruses, which target systems and data
- ☒ Controls and manages any devices through any ports including USB, Firewire, WIFI, Bluetooth, etc. and blocks USB keyloggers
- ☒ Encrypts removable media
- ☒ Audits device and application usage
- ☒ Enables compliance with evolving directives or regulations governing privacy and internal controls
- ☒ Maintains IT system integrity and improves IT system performance and network bandwidth
- ☒ Improves end user productivity

Positive Approach to Security

Sanctuary validates applications and removable devices as they are used within an enterprise. By employing a whitelisting approach, Sanctuary enables only authorised applications to run and only authorised devices to connect to laptops, PCs, servers, terminal services servers and thin clients. By default, unauthorised applications cannot execute and unauthorised device access is prohibited. Sanctuary policies are managed per user or user group as well as per computer.

Simple, Fast, Flexible Administration and Management

Through a central console, application and device control policies are quickly established and enforced through two simple steps. Sanctuary enables the administrator to rapidly identify devices and applications and then assign permissions at a high level or all the way down to device class, specific device or application to users, user groups or a particular computer. Sanctuary links application and device policies to user and user-group information stored in Microsoft® Windows® Active Directory™ or Novell® eDirectory™, dramatically simplifying the management of endpoint application and device resources.

Automated Discovery of Applications and Devices

Sanctuary enables discovery of applications and devices in use through a non-blocking audit option, as well as through a variety of scanning tools to assess the current state and simplify policy definition and management.

Granular Device Control Permission Settings

To eliminate the risk of unauthorised devices from connecting to the network, device policies are enforced by time constraints, encryption, volume of data, data transfer and more. Sanctuary also controls the types of files moved to and from removable devices to reduce the risk of unwanted files from entering and sensitive files from leaving the network. Separate policies can be defined and enforced when the user is online or offline.



Enforced Encryption

Portable devices can be encrypted for safe use and transported without the fear of exposing your confidential data to unauthorised users. Users can access their encrypted data even on computers that do not have Sanctuary installed. Centralised and decentralised encryption schemas provide the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and enforce the use of that encrypted media.

Flexible Authorisation Rules

Administrators can allow trusted users to authorise their own applications. This option provides ultimate flexibility, while alerts keep the administrator informed.

Comprehensive Security and Detailed Audit Capabilities

Sanctuary's patented bi-directional Shadowing records filename or file content as it is read from or written to floppy, CD/DVD and removable devices and provides a comprehensive audit log of every event whether allowed or attempted. All application execution and device access attempts can be logged and reviewed with flexible filter, sort and display options and stored custom query templates. Administrator actions, including changes in policy settings, are logged ensuring a full audit trail of policy enforcement.

USB Security Built to Scale

With a three-tier architecture and load balancing capability, Sanctuary is designed to provide USB security to organisations ranging in size from 50 to 100,000 endpoints and integrates easily within your existing technical infrastructure and logical organisation.

Award-Winning, Certified and Proven

Lumension's Sanctuary Device Control was recently named Security Product of the Year at the 2007 CNET Networks UK Business Technology Awards and is Common Criteria EAL2 Certified, CSIA Claims Tested and DIPCOG Approved.

Extending Sanctuary's Data Protection Capabilities with Whole Disk Encryption

Lumension Security has partnered with PGP to provide customers with an integrated data protection solution that includes whole disk encryption along with device and application control that can be managed from one user interface. Based on a unified key management and policy infrastructure, the PGP Encryption Platform offers the broadest set of integrated applications for enterprise data security. The platform enables organisations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, file transfers, automated processes, backups, and shared files on network storage. This integrated solution enables organisations to effectively protect data at rest and data in transit, and also provides FIPS140-2 encryption on USB devices.

About Lumension Security

Lumension Security is a leading global security management company, providing unified



protection and control of all enterprise endpoints, applications and devices to more than 5,100 customers and 14 million nodes worldwide. Lumension enables organisations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions, including vulnerability management, endpoint policy enforcement and extensive policy compliance reporting.

For More Information

See how you can effectively protect data in transit and ensure that your endpoints are properly secured with the leading endpoint policy-enforcement solution on the market today. For more information, to obtain a demonstration of Sanctuary Suite or to enjoy a 30-day free trial, contact us by any of the following means:

Phone: 01908-357897

Email: info@Lumension.com

Web: www.lumension.com



Lumension Security

Unit C1 Windsor Place
Faraday Road, Crawley
West Sussex, London RH10 9TF
United Kingdom

www.lumension.com