



Data Loss Prevention Protects Patient Privacy

A case study in data privacy and
regulatory compliance

December 2009

"We absolutely wanted an appliance-based product....backed by a proven secure encryption technology [that] met our high-availability requirements. XCS ticked a lot of the boxes on our checklist of what we wanted in terms of a technical design. Then during the proof of concept, it met our functionality requirements, and did exactly what we needed. XCS also provided a very slick interface. It was quite an easy decision in the end." - **Matt Connor, IT Development Manager for St. Helens and Knowsley HIS**

BACKGROUND

In the wake of widely publicized breaches, government organizations throughout the U.K. face new mandates to protect private data. Within the National Health Service (NHS), St. Helens and Knowsley Health Informatics Service (HIS) has taken an especially proactive role in identifying appropriate solutions. The HIS protects not only the acute-care hospitals, which are housed on a split site, but also two primary-care trusts and a mental health trust that serves five boroughs. There are approximately 12,000 users in all. To meet requirements for securing data-in-motion, the HIS chose an Extensible Content Security (XCS) appliance from WatchGuard.

CHALLENGE

Under the new mandates, all NHS Trusts must develop a plan of action for meeting the new requirements, which encompass everything from encrypting data on laptops to securing data flows over the Internet. For email traffic, the NHS has its own secure internal mail service – NHS

mail— but emails going outside of this group even via the NHS internal N3 network needed to be secured as well. That posed a problem.

As Matt Connor, IT Development Manager for St. Helens and Knowsley HIS, explains, “It's challenging. We're inside a secure NHS network, but we need the ability to interface with patients and organizations outside of the NHS network. That means some technology won't work, because it can't connect back into the secure network to retrieve the encryption key for the email. That requirement alone effectively ruled out quite a few products.”

WATCHGUARD® SOLUTION

After an extensive evaluation of other solutions and performing a trial and proof-of concept, the team chose a pair of WatchGuard XCS high performance devices running in high-availability mode. Declares Connor, “We absolutely wanted an appliance-based product. It didn't require any change or any software installation on the mail servers. It was backed by a proven secure encryption technology and met our high-availability requirements. XCS ticked a lot of the boxes on our checklist of what we wanted in terms of a technical design. Then during the proof of concept, it met our functionality requirements, and did exactly what we needed. XCS also provided a very slick interface. It was quite an easy decision in the end.”

BENEFITS

The appliance comprises a complete solution for handling the inbound and outbound data-in-motion piece of the government directive.

Information Now, Enforcement Next

The product supports a phased rollout. “What we didn't want to do was a big-bang approach,” states Connor. “It was important to bring this in gently. We're dealing with quite a large number of groups and departments, with differing electronic data transfer requirements and these requirements need to be analysed and implemented safely. We're in the first phase now, which is getting the word out. The facility is there to use electively – encrypting a message with XCS is a very simple process.”

The next phase is using information logged by the system to develop a set of efficient, automated policies that will minimize the risk to patient data, with a minimal number of false negatives. James Graham, Technical Development Engineer, explains: “We've got the content-filtering on, but just in passive logging mode at the moment, as we work with our Security team and the Information Governance Team, and we start to shape up the policies. But it's the ability to have that information and use it to tweak the policies. That's what's important to us now.”

Full-Featured, Functional and Flexible

Using a variety of tools including digital fingerprinting, the product examines both the content of the message, including attachments, as well as its context. The context includes the identity of the sender and the recipient to determine if the message is in policy violation. Based on the identified data-loss risk, the appliance can block, re-route, quarantine, or transparently encrypt the message through a secure-envelope service.

The policies can be assigned across the company, or by group or even individual. That's a key feature, as Graham relates: "Because we're a service provider, we provide mail services to different organizations that all have different requirements. One of the elements of the product that we're pretty impressed with is the ability to tune the policy engine right down to the user. That is excellent – far beyond the functionality of the fairly basic filtering technology we've seen in other products."

The HIS is also making use of the anti-spam and anti-virus features of the product, as part of a defense-in-depth strategy for protecting the desktops. And while the solution is handling only email at the moment, it is capable of also preventing data leakage via web mediums including wikis and blogs.

Supporting Multiple Elements of the NHS Directive

The new data-handling guidelines are far-reaching, and mandate enacting "core measures" to:

- 1) **Define** sensitive personal data and identify it
- 2) **Encrypt** if it passes outside the internal N3 network
- 3) **Log and control** misuse
- 4) **Protect** against external threats

The WatchGuard appliance supports all of the core measures, but it also plays a supporting role in other elements as well – notably, by helping the HIS build a culture around protecting patient data. As Connor explains, "Those requirements are around policy, procedure, and process. Robust internal mechanisms are important, as are people being responsible for patient data."

Connor continues, "Departments and organizations have internal processes to audit data transfers; however electronic data transfers through the email systems are now secured by XCS through the granular controls and audit information it provides. It allows our Security Team to analyze data transfers through this medium more effectively, work with the departments to review the data transfer processes, and help implement controls and policies to enable secure transfer of relevant NHS information."

Rock-Solid, Zero Impact

With email accounting for such a critical and vast medium of communications, the St. Helens and Knowsley Health Informatics Service appreciates the fact that it can meet the email compliance section of the mandates so well, without burdening their team. As Graham says, "If the email system is affected in any way, it's literally 30 seconds to the first call. Any piece of equipment you can put in and it works, that's good for me. It does what we need to do. It's rock solid. It's excellent. And in terms of management day to day, it's been practically zero impact."

Connor agrees. "It works well, not just from a functionality point of view in terms of encrypting the emails, generating the logs, and all the things we configure it to do, but it's also a critical part of our mail system. And so far, we've had flawless reliability with it. "

ABOUT ST HELENS & KNOWSLEY HEALTH INFORMATION SERVICE

St Helens & Knowsley Hospitals NHS Trust in northwest England provides a full range of acute care in-patient, out-patient, day case, and emergency services to around two million people living in St Helens, Knowsley, and parts of Halton and Liverpool. The organization's Health Informatics Service provides the St Helens and Knowsley Health Community with accurate, reliable and timely information at the point of care through robust technology, to ensure that informed decisions are made by patients, caregivers and other staff to gain most benefit from the resources within both the community and wider NHS.



www.sthk.nhs.uk

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. The newest appliances – the WatchGuard XTM 8 Series and XTM 1050 – provide high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard extensible content security (XCS) solutions deliver comprehensive email and web traffic protection for security, privacy, and compliance. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66673_120709