



Global healthcare company is first to deploy Lanxoma to tighten up access to privileged systems by IT workers.

Highlights

- Roll out to 2000 users in three months
- Access to privileged systems protected from anywhere in the world
- A transparent process to protect against the insider threat has been achieved

Privileged access to IT systems is out of control. The increasing number of surveys and news reports of IT workers abusing their password privileges reveals a worryingly rising trend. These insider threats range from IT workers simply snooping on employee records at one end of the spectrum through to far more serious malicious activity and fraud. The growth in incidences is intensifying a security problem that auditors have long been aware of, but have had no easy way to guard against: namely controlling access to privileged information and data.

A solution to the problem was borne out of the needs and deeds of the world's largest and most diversified healthcare company, which operates in 54 countries, employing over 116,000 people.

In mid-2006, within the devices and diagnostics division, IT systems were undergoing considerable change. The number of contractors and remote third party outsourcers with access to protected information - often involving patient medical records for items like surgical implants - was rising.

Set against the general climate of corporate governance and regulatory controls such as Basle II and Sarbanes Oxley, which are designed to reduce risk and demonstrate compliance to the rules, the company's internal auditors raised concerns, not for the first time, over the widespread, cross-border access to privileged information.

The auditing concern was being aggravated by the increase in outsourcers with many of the day-to-day maintenance tasks outsourced to countries including South Africa, Argentina and India. The controls that did exist tended to be paper-based or involve before and after screen shots and were deemed rudimentary, open to abuse, and clearly those with malicious intent could ignore them. Those that did not, found the procedures slowed down their systems work.

At this time of rising concern and apathy that nothing could be done to improve the status quo, Unity Enterprise Solutions (UES), a third party contractor on site to implement a large Oracle ERP system, was approached by the company's infrastructure and security management to explore and evaluate possible solutions. Unity was a typical illustration of the problem itself in having around 20 IT technicians with deep access to the operating system, databases and systems onsite. The question to Unity was, could there be a way to record and monitor all IT access, which was then viewable by auditors and secure?

Over the following months, Unity scoured the world for a solution to control and record privileged access, but eventually drew a

blank. Their report concluded that while there were some elements such as single sign-on and simple recording of screens which could help, there simply was not a comprehensive solution available which could provide the watertight audit trail that would satisfy the auditors.

Several months later, the problem was still a fascination at Unity, so much so, that the decision was made to investigate what it would take to invent a new product to do the job. A technical specification was sketched out that would meet a number of criteria. These included protection of any asset; seamless integration with back end systems through a straightforward to use interface and permission granting system that would precede existing password protection; automated starting and stopping of recording to avoid user control over this; playback and recording in real time that would be valid in a court of law; and user-controlled triggers for management to set which create automatic alerts to suspicious activity.

Gradually a check list of key design criteria emerged. Several elements existed but the added value of Unity was to bring these elements together into a single solution.

Unity went back to their healthcare customer to present the 'paper' solution. The response was a resounding yes, this is what we absolutely want. Unity cost the project and was given the go ahead in April 2007. The first prototype was live by December 2007 and the commercial product which was completed in summer 2008, was launched at DemoFall in San Diego that same year. Unity undertook the development of what was to become Lanxoma and retained their intellectual property in the product.

The key features of Lanxoma are demonstrated in the following scenario. An IT technician requires access to an Oracle database to fix some corrupted data. Typically he would simply log into the database and carry out his fixes and then log out. He may make some notes and keep a record of what he did (just in case) and of course there are database logs as well.

With Lanxoma in place, he won't be able to just log into the database; access would have been revoked and he needs to complete a short web-based form qualifying what he intends to do and how long he needs to do it. Lanxoma seeks authorisation from a designated manager, such as by desktop alert, text message or email, and notifies the IT technician once the approval is in place. It will then start recording the user's screen, mouse moves, keyboard strokes and audio and, at the same time, enables the appropriate Oracle privileges and notifies the technician. Now as the user logs into the database to carry out the updates, Lanxoma recording begins and the user can see the allotted time ticking down on screen. At the end of the session the privileges will be revoked, the recording stopped and the user logged off automatically and a notification may be sent to management. A wide range of automated alerts can be defined by the user such as sending a message if only a small amount of the anticipated access time was used. The manager could then immediately playback the technician's every action, in real time, to see just what did happen. The beauty of Lanxoma and its special appeal to auditors is that the audit trail is immediately intelligible

and doesn't require wading through hard-to-decipher computer logs. The classic questions of who? what? when? where? and how? are all answered.

One of the issues that this first Lanxoma customer needed to address as their plans to roll out the product to 2000 users across Europe unfolded, was expected push back from employees and some unions on privacy/surveillance. There was some initial resistance and even a legal challenge in Germany, but these were all resolved satisfactorily by all parties. Unity has also determined that Lanxoma complies with US privacy and employment law. Contracts with outsourcers and contractors were simply updated to include a monitored access condition.

As well as protecting against the insider threat and malicious activity, Lanxoma is also a tool which protects and defends honest employees and also has a key role to play in training on compliance and internal security procedures.

By early Spring 2009, Lanxoma went live on 2000 desktops, allowing IT technicians and power users controlled access to privileged systems from anywhere within their organisation, across the healthcare company's operations in France, Germany, Ireland and the UK as well as to external support staff in Argentina, India and South Africa.

The roll-out to this first user was achieved within three months including a phased roll-out of the supported back-end systems with the most critical being addressed first. Lanxoma has been developed so that users can bring on new servers and environments themselves which increases the cost-effectiveness of the solution.

The healthcare customer has already benefited from the deterrent factor and the internal auditors are also delighted with the improvements made possible. They now have a transparent process to control the activities of IT technicians and systems administrators; they have an intelligible audit trail which is based on real-time recordings of live action; an easy way for people to understand their responsibilities and achieve policy adherence, all backed up by a secure audit log that cannot be changed. In addition should an incident arise they are now equipped to resolve it extremely rapidly. Privileged access to IT systems is no longer out of control for this major international organisation.

About Unity Solutions and Lanxoma

www.lanxoma.com

Lanxoma was developed by the in-house software research and development team of Unity Solutions in the UK in response to the auditors' requirement of a global pharmaceutical manufacturing company, a long-term client of Unity Solutions.

Unity Solutions (UES Limited) was established in the U.K. in 1999 and rapidly established a global client base for its utilities and tools for ERP users.

UES Limited, Unit 3, Beswick House, Greenfold Way, LEIGH, WN7 3XJ, UK.

T: +44 1942 267 488 info-uk@unitysolutions.com

Unity Solutions LLC, 13575 58th Street North, Suite 136, Clearwater, FL 33760-3746 USA

T: +1 727 538 4143 info-usa@unitysolutions.com www.unitysolutions.com

Copyright © 2009 Unity Solutions LLC

