Customer Success Story

University Health Care System

University Health Care System Partners with Lumension to Keep Its Endpoints Healthy and Secure

March 2010

CS-EN-03-03-10

Background

As one of the largest healthcare providers in Georgia, University Health Care System (UHCS) has a deep commitment to the health of the community it serves, encouraging individuals to achieve healthy lifestyles. Through its long tradition of caring, UHCS has set the highest standards for quality among comprehensive healthcare networks. That's because UHCS provides a continuum of care — from promoting preventive care to treating illnesses all the way to offering after-care services. This dedication to high-quality healthcare has resulted in the improved health of the community and exceptional clinical outcomes.

Information Security and Computer Operations Manager George Ward is responsible for the security of the large amount of personal data housed at UHCS. In his role, he leads a team that works to proactively discover weaknesses in the network and determine the necessary steps to keep endpoints healthy and data secure and to meet industry requirements. Over the past five years, the company has witnessed the threat landscape change as hackers' strategies have evolved and the industry has embraced a mobile workforce. This combination has made information security — especially within the healthcare industry — harder to track and manage, opening the door to a wide range of potential attacks.

The Challenge

Protecting patient data has become incredibly difficult over the past year, especially as economic and competitive pressures continue to increase.

> "With the combination of an influx in HIPAA and PCI regulations along with the four other regulations we work to meet as well as an increase in personal healthcare records, we needed to find a better way to fully understand our security parameters while at the same time get our hands around all the personal data that exists within our organization."
>
> **Manager George Ward**
> **Information Security and Computer Operations**
> **University Health Care System**

Another factor signalling the need for change included data-sharing outside the organization. "As accessibility to medical and billing records increases, so does the risk," Ward explained. "Luckily UHCS hasn't been impacted by malicious insiders accessing sensitive data, but we had seen a few examples of others in the industry who were devastated by these types of attacks and we knew we needed to find a better way to protect our data from those even inside the company."

Ward and his staff knew it was crucial to implement the right endpoint security solution in a timely and efficient manner.

"Fines for non-compliance with HIPAA are now as large as $250,000 per incident."

"Being in the healthcare industry, our organization is widely exposed to insider threats and outside vulnerabilities – to combat this, we reviewed multiple solutions from Trend Micro, McAfee, Symantec, Safend and Smartline for our endpoint needs. Once we agreed on our key requirements for a solution, we eventually decided to go with Lumension® Device Control since it met all of our endpoint security requirements and did so much better than the others we tested."

Manager George Ward
Information Security and Computer Operations
University Health Care System

The Solution

UHCS deployed *Lumension*® Device Control for comprehensive data protection to help safeguard patient and employee medical, financial and intellectual data as well as to ensure compliance.

With Lumension Device Control, UHCS is able to automatically and more efficiently protect its 3,000 employees and more than 2,500 workstations. Ward had a positive first impression of the Lumension solution at work, noting that it has delivered on its promise of enabling business productivity without disrupting workflow.

"Fines for non-compliance with HIPAA are now as large as $250,000 per incident, we knew that without a device control solution like Lumension Device Control, the potential impact of data loss was a very real concern," he said. "In order to protect information such as patient data, personal identification identifiers, authentication credentials, corporate financial data, intellectual property and classified files, we needed to deploy a solution that would eliminate the risk of data being lost or stolen from within or outside of the organization."

With Lumension, UHCS is able to survey its entire network for an inventory of all assets connected to the network and implement a trust-based environment using a "whitelisting" approach to define what devices are allowed onto the network. In addition, UHCS is able to implement and enforce a company-wide usage policy based on a user's role or identity to continuously monitor and report on

the health of its network environment. UHCS generates detailed forensic reports and an audit trail about how company devices and data are being accessed, transferred and/or stored. Led by Ward, UHCS administrators can now centrally manage these devices, protecting private healthcare records and limiting the potential for a data loss or theft.

> "Lumension Device Control allows us to improve communication and conduct intensive testing. With Lumension's assistance, our management team is very happy with our ability to better control our removable USB devices and force encryption to ensure devices are fully protected."
>
> **Manager George Ward**
> **Information Security and Computer Operations**
> **University Health Care System**

As a result, Ward and his team are now able to enforce policy by role as well as ensure that audit findings are remediated without worry about a loss of personal data.

Benefits of Lumension® Device Control

"In 2010, device management will be key as more and more workers use mobile devices to access enterprise data," Ward said. "We have hundreds of workstations that are subject to an infinite amount of devices being transferred both inside and outside our organization. Without having a device control solution in place to protect our organization, we leave the door wide open to a large amount of risk. With Lumension in place, we are very confident that our customers' personal data will remain secure."

As a result of UHCS's deployment of Lumension Device Control, Ward's IT staff has the ability to enforce encryption and add devices by type or serial number.

"We set a policy that requires all devices that would be considered portable memory to be encrypted or device control will not allow attachment," Ward explained. "Therefore, all files that are copied to such devices are encrypted. We have some locations that we do not allow USBs to be attached, but we can grant an exception using the device ID."

Since implementing Lumension Device Control in early 2009, 354 unauthorized users have been blocked, more than 20,000 unauthorized access attempts have been prevented and a weekly log monitoring protocol has been successfully put into place.

More than 20,000 unauthorized access attempts have been prevented.

> "As a result of working with Lumension, we have been able to decrease administrative costs, reducing the database footprint and increasing database query and maintenance speed. We are able to now continuously monitor the effectiveness of device and data usage policies in real time as well as identify potential security threats. The customized reports on all device and data activity have enabled us to better organize and maintain our security goals while remaining business-focused."
>
> **Manager George Ward**
> **Information Security and Computer Operations**
> **University Health Care System**

Conclusion

According to Ward, Lumension plays an integral role in its ever-changing security strategy, which has greatly evolved as the bad guys continue to stay one step ahead of the market and organizational needs continue to evolve to better suit employees.

"With Lumension Device Control, we are benefitting by receiving the assurance that if a USB device was lost or stolen, enforced encryption will provide us with a level of security to prevent unauthorized access to the device," Ward said. "I sleep better knowing that we have reduced the risk that we will have to report loss of Protected Health Information to the Secretary of Health and Human Resources because someone lost a USB Drive."

Global Headquarters

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.888.725.7828

fax: +1.480.970.6323