Infirmary Health System

Gains meaningful use dollars with improved security and audit reporting

Overview

The need

Infirmary Health System needed to automate and strengthen security and endpoint management to better protect data and meet HIPAA and meaningful use requirements.

The solution

Working with ESM Technology, the organization deployed a comprehensive security solution from IBM that helps staff secure endpoints and better detect and respond to threats across the organization.

The benefit

With a unified security platform, the organization has met data security requirements for meaningful use, qualified for meaningful use funds, and reduced security incidents significantly.

Infirmary Health System is the largest non-government healthcare team in Alabama, treating more than 100,000 patients annually. The organization includes three acute-care hospitals, three rehabilitation hospitals, three outpatient facilities and more than 30 medical clinics.

Meeting "meaningful use" requirements

Under the 2009 U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act, the Department of Health and Human Services set forth "meaningful use" guidelines for electronic health records (EHRs.) These guidelines help to ensure that healthcare organizations achieve specific clinical objectives with the use of EHRs and confirm the privacy and security of all electronic health data.

Healthcare organizations that meet meaningful use requirements can be eligible for millions of dollars in federal incentives. Those that don't comply can be subject to new penalties.

The solution helps Infirmary Health System meet HIPAA and meaningful use requirements for data security, and easily demonstrate compliance for federal incentives. "We can now quickly, easily and accurately produce audit reports for HIPAA and meaningful use compliance," says Eddy Stephens, chief information officer, Infirmary Health System. "This has helped us obtain a considerable amount in meaningful use incentive dollars."

Solution components

Software

- ESM Technology's iT Server Mgmt in-a-box™ Health Care (Security & Compliance) Edition
  - IBM Endpoint Manager, built on BigFix® technology
    - IBM Endpoint Manager for Core Protection
    - IBM Endpoint Manager for Lifecycle Management
    - IBM Endpoint Manager for Mobile Devices
    - IBM Endpoint Manager for Patch Management
    - IBM Endpoint Manager for Security and Compliance
    - IBM Endpoint Manager for Software Use Analysis
  - IBM® QRadar® Security Intelligence Platform
    - IBM Security QRadar Log Manager
    - IBM Security QRadar SIEM

IBM Business Partner

- ESM Technology

"We evaluated several solutions and found that the ESM solution based on IBM security software met all of our requirements and was easy to deploy."

—Eddy Stephens, Chief Information Officer, Infirmary Health System

For Eddy Stephens, chief information officer of Infirmary Health System, IT security has always been a top priority. However, with a growing infrastructure, the increase of security threats worldwide, and new federal regulations, such as meaningful use requirements, Stephens and his team found it difficult to keep pace using point technologies and manual processes.

It often took IT administrators up to two months to apply software patches or deploy new applications across the organization's more than 4,000 workstations. Likewise, consolidating and correlating security events from disparate data sources for investigations and auditing took days or weeks.

"To meet meaningful use requirements, we must ensure all of our workstations and servers have the latest security patches, are properly configured and can be locked down to protect data," Stephens explains. "However, we needed a lot of feet on the ground to manage the sheer volume of work. Our goal was to find a better way to manage this increasingly complex problem."

A comprehensive solution for endpoint and event management

A strong security posture depends on numerous activities—patching systems, stopping malware and other threats before they arrive, controlling endpoint access, understanding exactly who is accessing what applications, servers and data, and much more.

As Stephens and his team evaluated new approaches, they sought a comprehensive and integrated solution that could help them effectively and efficiently address the full range of endpoint and event management requirements. They turned to ESM Technology, a recognized IBM solution provider with a practice in security and service management. ESM is headquartered in New York City with satellite offices in the Southeast United States.

"We've gone from an average of 40 percent patch compliance to 90 percent patch compliance and I am confident that we have stopped malware and other vulnerabilities because these machines are properly patched."

—Eddy Stephens

"We evaluated several solutions and found that the ESM solution based on IBM security software met all of our requirements and was easy to deploy," says Stephens. "ESM also provided the expertise and know-how to help us more quickly achieve our goals."

A "closed loop" system to identify and correct attacks, threats, and non-compliant conditions

ESM Technology's iT Server Mgmt in-a-box™ Health Care (Security & Compliance) Edition solution uses IBM endpoint management and security intelligence solutions to provide healthcare organizations with a unified and turnkey security platform for addressing Health Insurance Portability and Accountability Act (HIPAA) and meaningful use requirements.

For example, IBM Endpoint Manager software, built on BigFix® technology, helps Infirmary Health IT staff keep the organization's 4,000 workstations secure, up-to-date, compliant, and running at peak performance.

IBM® QRadar® Security Intelligence Platform software, including IBM Security QRadar Log Manager and IBM Security QRadar SIEM, collects and analyzes data from network and security devices, services and operating systems, and applications to help staff quickly see developing threats. Because of this, the organization has comprehensive visibility and can detect and identify "real-time" offenses and threats—something which it could not do before. Secondly, Infirmary Health IT personnel also can monitor user activity, allowing them to improve security policies and guidelines. Finally, they can monitor compliance and provide audit reports for auditors.

"With IBM QRadar software, we can now better defend against internal and external threats. We can see exactly who is doing what. … And with the new intelligence we've gained, we've applied new settings that strengthen our security posture and reduce the number of potential security incidents significantly."

—Eddy Stephens

Through the tight integration of IBM security solutions, the organization gains a "closed loop" system that can identify threats and alert security administrators to take the necessary corrective action based on observed conditions. For example, using the information collected by IBM Endpoint Manager, IBM QRadar software can see immediately if someone is trying to exploit an operating system vulnerability, and then alert the security team to use IBM Endpoint Manager to remediate the condition, such as applying a software update.

Proactively defending against internal and external threats

According to Stephens, IBM security software offers critical capabilities to meet meaningful use requirements including:

- Continuous patching of endpoints for zero-day protection. "We've gone from an average of 40 percent patch compliance to 90 percent patch compliance and I am confident that we have stopped malware and other vulnerabilities because these machines are properly patched," says Stephens.
- Near-real-time protection from malware and other malicious threats through cloud-based virus definitions instead of traditional signature files. "When we used Symantec antivirus products, we had issues with new-to-the-market viruses," says Stephens. "The move to IBM Endpoint Manager for Core Protection has been a positive one and helped us stop this type of problem."
- Secure transmission of patient information. "Workstations that are used to access and transmit patient information are secured and locked down using IBM security software," says Stephens.
- 360-degree visibility of enterprise security to help IT staff detect threats that might otherwise be missed. "With IBM QRadar software, we can now better defend against internal and external threats," Stephens says. "We can see exactly who is doing what. We know if there are external attacks or unauthorized people trying to get into our networks. We can monitor for compliance policy violations and provide the reports auditors require. And with the new intelligence we've gained, we've applied new settings that strengthen our security posture and reduce the number of potential security incidents significantly."

"When we used Symantec antivirus products, we had issues with new-to-the-market viruses. The move to IBM Endpoint Manager for Core Protection has been a positive one and helped us stop this type of problem."

—Eddy Stephens

Qualifying for meaningful use dollar incentives from the federal government

The solution helps Infirmary Health System not only meet HIPAA and meaningful use requirements for data security, but also easily demonstrate compliance for federal incentives. Audit reports that once took Stephens' team weeks to create can now be generated in minutes.

"We can now quickly, easily and accurately produce audit reports for HIPAA and meaningful use compliance," says Stephens. "This has helped us obtain a considerable amount in meaningful use incentive dollars."

Managing physicians' mobile devices

For Stephens, the solution also enables his team to secure physicians' mobile devices, and clear a device of sensitive data if it is lost or stolen.

"The Bring-Your-Own-Device trend is becoming more of an issue for healthcare as physicians look to access applications and data using their own mobile devices," says Stephens. "With IBM mobile device management capabilities, we have a unified platform that enables us to give our physicians the access they need, while confirming that access is secure."

Reducing operational costs with improved endpoint management

While compliance mandates drove the organization's investment in a new solution, the IT team has also used the solution to reduce operating costs and improve the end-user experience.

"With IBM mobile device management capabilities, we have a unified platform that enables us to give our physicians the access they need, while confirming that access is secure."

—Eddy Stephens

Here are just a few improvements that Stephens says the organization has realized with near-real-time visibility and control of its endpoints:

- Reduced licensing costs and enhanced licensing compliance with greater visibility into software usage. "Microsoft did not do an audit this year because we could provide comprehensive usage analysis reports," says Stephens. "And, with a better view of how software is being used, we have saved countless hours tabulating license inventory and avoided compliance fines from various vendors."
- Improved end-user experience and extended the useful life of workstations. "Other antivirus solutions tend to use up CPU performance," he says. "With IBM Endpoint Manager software, our workstations run without user slowdown times as with other antivirus software."
- Reduced the time to deploy software by 95 percent. "We deployed our EPIC EMR applications to all our desktops in just a few days," says Stephens. "Before, this would have taken us nearly eight weeks."
- Improved IT planning by delivering accurate asset inventory in minutes. "In the past, we had to physically go out to each site to take inventory, which could take weeks," says Stephens. "Now, I can get the same information within a few minutes, which expedites planning and support tremendously."
- Decreased the time to resolve help desk requests by 50 percent with remote control capabilities.

"We can handle the rapid change and address evolving requirements without having to increase our staffing requirements," says Stephens. "Without this solution, we would have never been able to keep up."

For more information

To learn more about IBM security solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

For more information about ESM Technology, visit:
www.esm-technology.com

For more information about Infirmary Health System, visit:
www.infirmaryhealth.org

© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
January 2014

IBM, the IBM logo, ibm.com, BigFix, and QRadar are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

iT Server Mgmt in-a-box™ Health Care (Security & Compliance) Edition is not an IBM product or offering. iT Server Mgmt in-a-box™ Health Care (Security & Compliance) Edition is sold or licensed, as the case may be, to users under ESM Technology's terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for iT Server Mgmt in-a-box™ Health Care (Security & Compliance) Edition is the direct responsibility of, and is provided directly to users by, ESM Technology.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Please Recycle

ESM Technology
Managing People & Technology

WGC12356-USEN-00