



PERIMETER eSECURITY EFFINGHAM HOSPITAL CASE STUDY



A Regional, Rural Hospital Stays HIPAA Compliant through On-Demand Vulnerability Assessments from Perimeter eSecurity

OVERVIEW

Location: Springfield, Georgia
Industry: Health Care

Customer Profile

Effingham Hospital is a 130-bed critical access hospital and nursing home located in Springfield, Georgia.

Business Situation

Effingham Hospital needed to stay HIPAA compliant and protect patient data despite limited IT resources.

Solution

The hospital now benefits from Perimeter's Monthly Network Vulnerability Scanning, an affordable, advanced monitoring, analysis and remediation service.

Benefits

Effingham Hospital is able to meet HIPAA network security standards while ensuring that their network is constantly secure.

“Having Perimeter eSecurity is like having a virtual security expert on staff. I’m able to focus my time on managing our overall IT infrastructure and we were able to avoid hiring additional staff to cover these types of vulnerabilities for us.”

-Bart Hunter, IT Manager

Effingham Hospital, a critical access hospital and nursing home in Springfield, GA, may not be located in a congested, bustling city but the private health information contained within their network is just as valuable to a potential hacker. Not only did they have to remain compliant with HIPAA regulations, they knew it was their responsibility to patients, residents, employees, vendors and many other stakeholders to ensure that their network was properly secured and continuously tested. They turned to Perimeter eSecurity, subscribing to their Network Scanning services to test their network both internally and externally, as well as providing a host assessment for critical servers. Their decision freed up their IT manager to focus on other critical business, as well as saving them money by avoiding the need to hire more full-time staff members.



Hiring a full-time, highly skilled IT security specialist at an affordable rate to monitor the network constantly for vulnerabilities would have been extremely challenging for this rural hospital.

THE IT SECURITY & COMPLIANCE PROBLEM

Effingham Hospital, a 25-bed critical access hospital and 105-bed nursing home facility located in Springfield, Georgia, needed to demonstrate compliance with federal security regulations. As a covered entity under HIPAA, the small, rural hospital had to prove that it assessed the threats to and vulnerabilities of its computer network that could jeopardize the safety of patient data.

Network vulnerabilities in a health care organization can create holes that could lead to the exposure of electronic protected health information (ePHI), defined as any information about health status, provision of or payment for health care that is linked to an individual. Under HIPAA regulations, covered entities such as hospitals are required to implement procedures to identify if they are vulnerable to malicious activity and to develop measures to secure their networks before damage is done. Like any corporate entity, Effingham Hospital's vulnerabilities existed at both the operating system and application level of a network. A vulnerability assessment to expose weaknesses and a solution to protect ePHI was needed. The rural hospital sought a solution that was comprehensive, reliable and affordable.

Hiring a full-time, highly skilled IT security specialist at an affordable rate to monitor the network constantly for vulnerabilities would have been extremely challenging for this rural hospital. Effingham Hospital has one full-time IT manager who is very busy

maintaining the existing IT infrastructure and working on other mission-critical IT projects.

THE PERIMETER eSECURITY SOLUTION

Effingham Hospital decided to subscribe to Perimeter's Network Scanning Services on the recommendation of the CFO. The IT manager simply installed a server, which plugged easily into the hospital's rack of hardware devices. Now, Perimeter performs a Monthly Remote Network Assessment to test the effectiveness of the network security controls at the hospital and to identify associated weakness before malicious activity can take place. The service analyzes the external network (Internet perimeter) along with the internal network (key servers within the organization). In addition, a Host Assessment is conducted on critical servers comparing the server configuration with industry best practices.

In addition to the monitoring, analysis and remediation services, Effingham Hospital knows that Perimeter's vulnerability assessment services are continuously updated to combat the latest threats in the marketplace. Further, the hospital is assured that Perimeter's assessment services have been validated by multiple independent third parties.

Each month a certified Perimeter information security expert reviews the vulnerability scan results, applies a risk level to each

This combination of quality reports and detailed consultation provides a comprehensive, ongoing methodology for addressing network vulnerabilities.

vulnerability and recommends corrective action. This risk level and the corresponding corrective action provide Effingham Hospital with the steps to proactively correct network weaknesses. The Host Assessment provides a server compliance score and lists the details of each policy which is out of compliance.

Each quarter the Perimeter security expert and the hospital's IT manager hold a conference call to review the results of the assessments. When necessary, the consultant provides guidance on network architecture changes. Comprehensive vulnerability assessment reports are made available 24/7 to Effingham Hospital's IT staff on Perimeter ViewPoint portal site online. This combination of quality reports and detailed consultation provides a comprehensive, ongoing methodology for addressing network vulnerabilities.

The Monthly Network Vulnerability Assessment includes the following services:

EXTERNAL NETWORK VULNERABILITY ASSESSMENT:

The external assessment is conducted from Perimeter's BorderShield Security Operations Center to give a true picture of the organization's external exposure. BorderShield's vulnerability assessment methodology utilizes multiple industry-tested and -approved scanning tools. The findings from these tools are correlated against each other to eliminate false positives and to allow the customer to focus on the true risks to the environment. Results from the assessment are reported to

management and IT administrators to provide a clear snapshot of their network's current vulnerability status.

INTERNAL NETWORK VULNERABILITY ASSESSMENT:

The internal assessment provides details on the corporate network components (servers, workstations, etc.). A resource server preloaded with scanning tools is placed in promiscuous mode inside the network. On a preset date and time the server queries all of the windows servers within the network for known vulnerabilities. No interruption in network traffic flow occurs during these internal scans. The results are compiled into a report that is reviewed by Perimeter's dedicated information security expert.

HOST ASSESSMENT:

As part of the Monthly Network Vulnerability Assessment service, a server audit is performed on critical servers on the internal network. Utilizing the resource server deployed for the Internal Assessment portion of the service, this assessment queries servers inside the network. The tool provides a detailed report of the state of policy compliance for each server. A numeric score shows the overall state of compliance (0 to 100, with 100 being full compliance) for each server. If a server configuration is out of compliance with best practices, the report details the corrective action to be taken on that policy.

The review by the Perimeter security expert sorts through all of the detailed findings to determine the accuracy and relevance to the hospital's network.

**“Our network is secure.
The monthly reports make
the CFO happy and we are
ready for any auditor who
should come our way.”**

- Bart Hunter, IT Manager

The final report contains relevant information -- a risk level, the technical description, the recommended correction and the device(s) affected -- on all vulnerabilities.

THE NET RESULT

The final report contains relevant information -- a risk level, the technical description, the recommended correction and the device(s) affected -- on all vulnerabilities.

As a result of deploying Perimeter’s Monthly Vulnerability Assessment Service, Effingham Hospital benefits from best-of-breed security technology and expertise. It receives:

- Comprehensive reports to identify relevant and accurate network vulnerabilities
- A dedicated Perimeter information security consultant to review the hospital’s network each month and, via a telephone conference each quarter, to proactively correct network weaknesses in an acceptable time window. Risk is reduced by providing information a comprehensive audit trail for improving the state of network security over time.
- A secure, online portal providing 24/7 access to reports
- Extensive high level and highly detailed reports to demonstrate the hospital’s level of compliance to auditors. Reports also show senior managers the number of threats that were averted while using this service.

- An affordable subscription-based service with no integration project, additional staff or capital expenditure requirements
- The flexibility to add more services on demand from Perimeter’s integrated ViewPoint portal
- Vulnerability assessment services that are continuously updated to combat the latest threats in the marketplace and an infrastructure that has been validated by multiple independent third parties

Effingham Hospital is now compliant with the HIPAA regulations. Reports are available at any time to demonstrate to federal auditors that the hospital performs continuous vulnerability assessments.

“Our network is secure. The monthly reports make the CFO happy and we are ready for any auditor who should come our way,” said Bart Hunter, manager, Information Technology at Effingham Hospital. “Having Perimeter eSecurity is like having a virtual security expert on staff. I am able to focus my time on managing our overall IT infrastructure and we were able to avoid hiring an additional employee to cover these types of vulnerabilities for us.”

Perimeter eSecurity - The only provider of complete security On Demand and the leading provider of network security for Health Care Institutions. We guarantee HIPPA compliance and ensure the safety of electronic Protected Health Information.

ABOUT PERIMETER ESECURITY

As the leading and only provider of complete ePHI security on demand, Perimeter makes security easily available and affordable for all Healthcare Institutions. Perimeter's on demand ePHI security services protect thousands of computer networks nationwide, offering more than 50 different technologies on a subscription basis. Perimeter's services are continuously expanded, enhanced and upgraded for current and future regulatory compliance. With seven geographically distributed technical offices and three redundant data centers, Perimeter's complete, on-demand and affordable ePHI security services are always available and have been validated by multiple independent third parties.

FOR MORE INFORMATION

If you would like to speak with us or view a product demo, please give us a call at 800.234.2175 Option #2 or visit our website at www.PerimeterUSA.com.



Complete. On Demand. Affordable.