Case Study

Medical Associates of the Lehigh Valley Improves Patient Care with Help from AEP Networks

Overview

The Medical Associates of the Lehigh Valley (MATLV) was formed in Pennsylvania in 1993. MATLV provides member physicians the administrative support needed to meet the business and compliance needs of their practices, allowing physicians to focus entirely on the patient experience.

Recognizing that the industry was rapidly changing, MATLV transformed their business from a paper-based system to an automated, electronic environment that streamlined the daily administration of its 30 member offices.

MATLV wanted to implement a robust network infrastructure that would secure electronic patient records according to HIPAA standards.

MATLV also upgraded its communication and network security infrastructure by centralizing network communications for all 30 offices using the AEP Netilla® SSL VPN from AEP Networks. The Netilla SSL VPN has streamlined network management and gives members secure remote access to network applications, including patients' electronic health records, from their offices, clinics or any other location with an Internet connection.

MATLV has also implemented AEP IDpoint, a leading-edge identity-based access control solution, for controlling and auditing access to critical application resources.

The new network and security controls assure MATLV's clients, including hospitals and large healthcare organizations that MATLV has put a best practice solution in place to ensure the security and integrity of patient data that is compliant with HIPAA guidelines.

Automating the Network

Medical Associates of the Lehigh Valley's implementation of an automated network has improved administrative and patient care processes for its members including billing, scheduling and generating electronic patient health records. Prior to the new system, the patient encounter was a paper chart system recorded either entirely by hand or through dictations with a transcription service.

Today, prescriptions and test orders are sent electronically from within the system to pharmacies and labs, scheduling is done online, and insurance company billing is automated, which significantly speeds the payment process.

Securing Network Access

MATLV wanted to implement a robust network infrastructure that would secure its repository of electronic patient records according to HIPAA standards.

With the new infrastructure in place, physician members would be able to access this information from their offices, homes or other locations.

To set up secure access, Medical Associates of the Lehigh Valley installed the AEP Netilla secure socket layer virtual private network (SSL VPN) platform to centrally manage network security and remote access for its 30 doctors' offices.

The Netilla SSL VPN would give MATLV members easy access to its applications and electronic patient records from any standard web browser. It would also allow MATLV to centrally manage security and connectivity for all members, and to remotely manage all the servers within its system.

Bryce Bowman, IT Coordinator, chose the AEP Networks' SSL VPN. Bowman first heard about AEP Networks through a recommendation from a company MATLV works with for data hosting.

The AEP Netilla SSL VPN was chosen because it was "highly recommended," enables easy, yet highly secure access to applications and electronic patient records and offers a variety of remote access connectivity options including thin client, RDP and true tunnel. After choosing the Netilla SSL VPN, Bowman called upon Advanced Micro Computer Specialists in Horsham, PA to assist with the implementation.

The Netilla SSL VPN provides the highest levels of network security by only making applications and patient health records available to authorized users. The Netilla SSL VPN appliance combines three secure application access modes: thin-client access to client-server applications; access to intranet applications via HTTP reverse proxy; and network-layer access which enables PC-based applications to exchange data with central servers through an SSL tunnel. Medical Associates of the Lehigh Valley can be confident that sensitive patient information is completely secure because the Netilla SSL VPN is in full compliance with HIPAA security and privacy laws.

"The Netilla SSL VPN has met and exceeded our expectations for security and centrally managing all communications. The product was easy to install, is straightforward to manage and is very simple for our members to use. We have always received professional, knowledgeable support from AEP Networks, and have been extremely pleased with the service."

Bryce Bowman
Medical Associates of the Lehigh Valley

Medical Associates OF THE LEHIGH VALLEY

"Our greatest challenge," said Bowman, "was how to provide our physicians with real-time access to patient data, while maintaining an extremely high level of security and not compromising ease of use. AEP Networks' Netilla SSL VPN gave us the ability to centralize security and connectivity and provided the flexibility we needed to support our legacy applications while implementing the new electronic health record system. Due to the complexity of rolling out an electronic scheduling, billing and patient record system, we didn't necessarily know upfront what the best method of access for our applications would be. Choosing the Netilla SSL VPN meant we could make those decisions on the fly."

Medical Associates of the Lehigh Valley also uses the SSL VPN in conjunction with other technologies to scan information securely into patient records. Important health information such as x-rays, insurance cards, information on chronic conditions and other non-electronic documents can be scanned into the patient record and stored electronically. By scanning, or abstracting, crucial documents within patient charts and storing them on the network, important medical information can be associated with new digital patient files and accessed via the Netilla SSL VPN.

Scaling the Solution

With more doctors joining the Medical Associates of the Lehigh Valley every year, Bowman installed AEP's load balancing and failover solution—the AEP Netilla Load Balancer.

"From the start, the ability to implement a load balancing and failover solution for our SSL VPN appliances was imperative. With hundreds, potentially thousands of users accessing the network, reliability and availability are critical. The ability to scale our environment was also a key requirement. In less than a year, several new practices have joined the group and that number will continue to grow," said Bowman.

The AEP Netilla Load Balancer is a load balancing and traffic management appliance that provides scalability and high availability to the Netilla SSL VPN. It is designed to integrate easily into an existing network infrastructure, to manage traffic distribution between MATLV's two Netilla SSL VPN appliances, and to continually monitor the health of those appliances.

"Just like the SSL VPNs, the load balancing solution works extremely well. Installing and configuring the load balancer was straightforward and we have had no issues to date. AEP has again delivered as promised," Bowman adds.

Adding an Additional Security Layer

Bowman has also implemented the Netilla SSL VPN's built-in network access control feature to make the Medical Associates network even more secure. Client machine identification (CMID) restricts and manages which remote computers can log on to the network. By implementing this extra layer of authentication, Bowman ensures that only approved computers are able to gain access to the network. This security feature is especially important in healthcare for meeting HIPAA requirements surrounding securing patient data.

"The implementation of CMID is an important step in further assuring the overall security of our system. The Netilla SSL VPN has allowed us to take a layered approach to access security while providing the flexibility and portability of an Internet-based system," said Bowman.

Taking Security to the Next Level—Identity-Based Access Control

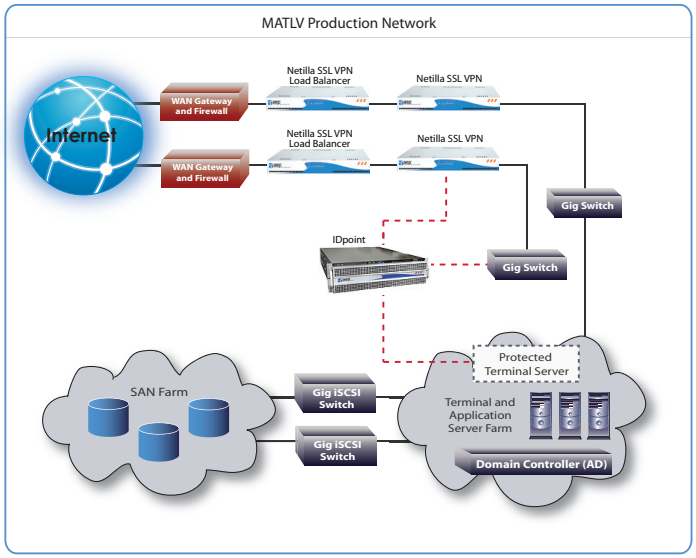
Bowman is taking network security to the next level by implementing AEP IDPoint, an appliance that sits in front of critical network resources. It inserts a secure, unique cryptographic representation of user identity, called AEP PacketTag™, into every IP packet destined for a protected resource as proof of who accessed the resource. MATLV wants to use 'identity' as an authentication factor for controlling and auditing access to critical application resources inside the network perimeter.

The Medical Associates of the Lehigh Valley are rolling out IDpoint in phases. In the first phase, IDpoint was installed in MATLV's hosting facility where it protects a limited number of back-end servers. It provides identity-based access to the terminal server farm from the management LAN at the central office and from the hosting facility.

"AEP Networks implements the concept of identity-based access control extremely well. They have worked very hard to design IDpoint to seamlessly integrate into an existing network security strategy," said Bowman.

In the next phase, currently underway, MATLV will use IDpoint to control and audit access to all of its back-end servers. IDpoint will work in tandem with the Netilla SSL VPN, allowing MATLV to use the identity of its 450 users to define and limit their access once they've been authenticated onto the network.

IDpoint will also be used to generate audit trails for monitoring access to restricted resources. This reporting capability is critical for simplifying the audit process and for keeping tabs on appropriate access levels. Generating user-based access reports for a given resource is fast and easy. With IDpoint, IT managers no longer have to correlate logs from various other network-level components.



AEP Netilla SSL VPNs works in tandem with AEP IDpoint to enable secure network access, while generating audit trails based on user identity.

Because MATLV is familiar with the Netilla SSL VPN interface, adding IDpoint into the mix is easy. “The concept is different,” said Bowman, “but IDpoint is similar in look and feel to the Netilla SSL VPN. The integration of this functionality into our existing infrastructure is extremely simple and AEP Networks has done a great job of keeping the learning curve to a minimum.”

The Result

By offering secure, reliable, real-time access to centralized health information resources, MATLV helps members streamline administration and guarantees HIPAA-compliant security standards. Giving physicians anytime, anywhere remote access to patient health records and administrative applications means doctors can spend less time filling out forms and searching through paper files and more time providing patients with a higher level of care.

By taking advantage of AEP’s load balancing solution and CMID security feature, MATLV ensures its network is both highly reliable and secure.

Bowman adds, “Additional layers of authentication and security can often be a hindrance to functionality. IDpoint, along with the Netilla SSL VPN, gives us the ability to go to the next level in ensuring the security of our patients’ medical records without diminishing the usability of the system. Adding IDPoint to our infrastructure provides additional tools that make it easier to address HIPAA compliance and the confidentiality of patient information.”

About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP’s integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, CAPS approved high assurance IPSec-based VPN encryptors, and FIPS certified hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company has design and development offices in its headquarters in Somerset, New Jersey, USA and Hemel Hempstead, UK.

Contact Us:

United States
Tel: +1 (732) 652-5200
Toll-Free: 1-877-638-4552

Europe
Tel: +44 1442 458 600

Email: sales@aepnetworks.com
Web: www.aepnetworks.com