# Securing Networks and Protecting Facilities in the Healthcare Industry

In recent years, the healthcare industry has been under persistent attack by cybercriminals. Technology may have dramatically improved performance and effectiveness in the healthcare industry, yet these recent attacks have highlighted critical vulnerabilities in the healthcare sector's networks.
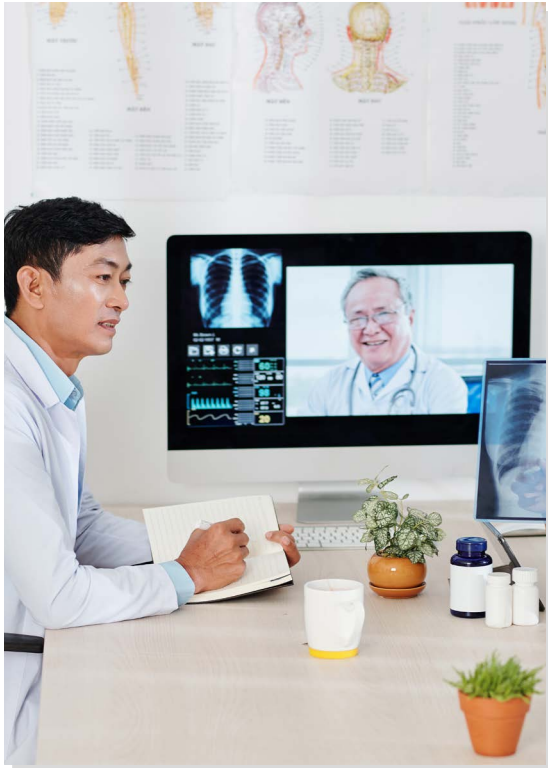
To protect their organizations and patients, Healthcare leaders need a comprehensive approach to network security. Arista's Edge Threat Management solutions provide IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

> *"NG Firewall is simple and secure, but it's also really flexible."*
>
> **– Jason Zeinstra | Network Manager, Orthopaedic Associates**

Network Security Checklist

Take these simple steps to stay ahead of evolving threats and hackers.

Control Access to Protected Health Information
Ensure employees are only given access to the systems that they need. Patient information should be available based on pre-established, role-based privileges, ensuring that different roles within an organization don't have access to all the same information.

Update Software
Maintaining software updates for all devices is crucial to ensure any vulnerabilities found are swiftly mitigated.

Define Administrative Control
By preventing staff from downloading applications that could house malware, you can minimize exposure and protect the network.

Keep Separate Backups
Always have backups of critical data in a separate location that are updated regularly, so in the event of a malware or ransomware attack, you can quickly get your data and configurations restored without paying the ransom.

Separate Network for Visitor and Staff Devices
By separating the main network from all visitor and staff devices that you don't control, you can quickly mitigate any issues that may happen on the guest network without impacting overall network performance.

Use Threat Intelligence
Using solutions that have built-in threat intelligence engines that proactively protect against unknown and emerging threats is critical to staing protected against hackers and malware.

Deploy a Next-generation Firewall
Next-gen firewall solutions provide protection at the gateway in an all-in-one solution that encompasses advanced security features like virus blocking and threat prevention, and network optimization and controls like web content and application filtering, bandwidth shaping, and WAN balancing.

Healthcare Case Study

Genesis Physicians Group

Location: Texas
Industry: Healthcare
Size: 27 users
Challenges:

The Genesis Physicians Group serves 1,700 doctors in the North Texas area, acting as an intermediary between its clients and the insurance companies, and offering a range of other services – including the compilation of patient outcome data, credential management and secure email. As such, Genesis must maintain a tight, secure network that ensures privacy and confidentiality. Physician email accounts need to be kept free of spam and sensitive patient data needs to be protected from corruption by viruses and exploitation by spyware.

Results:

Dan Nickason, the IT manager, wanted to add an additional layer of protection to their network. "We started using NG Firewall to address our security issues and to handle network monitoring," he says, "and straight away found that productivity went up. We used to have some small problems with staff visiting game sites during office time. That doesn't happen anymore. The best part is that NG Firewall's content control is very flexible: like most filters, it blocks access to sites with drug references, which can sometimes be a problem in a medical environment, but if a site needs unblocking, I can do it in an instant."

> *"When I open up my browser, I have my NG Firewall settings as the default page. I can see everything that's going on. Everything's in one place."*
>
> **– Dan Nickason | IT Manager, Genesis Physicians Group**

About Arista Edge Threat Management

Arista's Edge Threat Management solutions help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Edge Threat Management provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. The award-winning products are trusted by thousands of customers and protect millions of people and their devices. We are committed to bringing open, innovative and interoperable solutions to customers through a rapidly growing ecosystem of technology, managed services, and distribution partners worldwide.
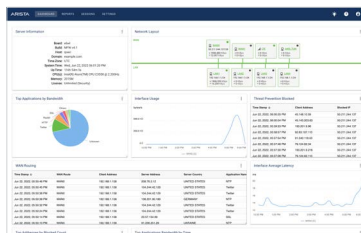
Advanced Security

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud
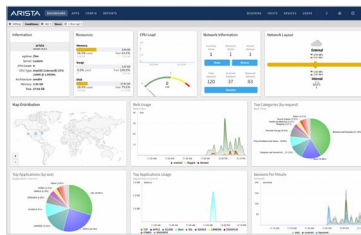
Intelligent Edge Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Optimal predictive routing technology for first packet, dynamic path selection
- Centrally manage one or many appliances

Cloud Management at Scale

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints
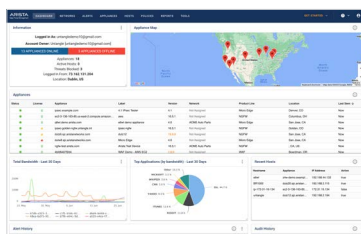
Network Security for Healthcare

- Stop viruses and other malware before they can enter the network
- Integrate with existing Active Directory/LDAP to bring preconfigured user context into your organization
- Set up different policies to control Internet access tailored specifically for doctors, administrators and other medical staff
- Identify every user on the network with Captive Portal to allow access to network resources only to those that require it
- Filter web content based on different types of users from medical staff to visiting patients with user policy based web filtering
- Prioritize mission-critical applications that directly affect the level of care provided to patients
- Prevent network slowdowns caused by any individual or group of users and applications

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com