Customer Stories:

NHS Management, LLC

AT&T Business

NHS Management uses AT&T Managed Threat Detection & Response in 50 nursing homes to help protect networks and confidential patient data

- **Business needs** - The lean NHS IT staff wanted to create a highly secure and consistent network environment and prevent unwanted access to confidential patient data.
- **Networking solution** - AT&T Managed Threat Detection & Response provides coordinated threat detection, incident response, and threat management to help protect NHS against pervasive, potentially destructive cyberattacks.
- **Business value** - NHS enhanced security and reduced risk thanks to round-the-clock access to cybersecurity experts who prioritize and manage threats.
- **Industry focus** - Nursing home management
- **Size** - $500 million in annual revenues

About NHS Management, LLC

NHS Management, LLC, provides administrative and consulting services for individual health care facilities and companies across the southeast. Quality of care remains the number one priority among the 50 facilities NHS serves. Each is committed to providing patients and residents with an enriching environment to keep them involved in the community and to assist with the activities of daily living. Facilities served by NHS provide skilled nursing and rehabilitative services including physical, speech, and occupational therapy, along with dietary, recreational, pharmacy, and environmental services.

The situation

Malicious attacks on corporate networks occur thousands of times daily. NHS recognized a need to layer its protection by adding security information and event management (SIEM), which provides near-real-time alerts and correlates network event logs. However, the company lacked the IT staff to comb through the logs and security alerts. NHS needed threat intelligence, collaborative defense, and effective security to protect its networks.

Solution

AT&T Managed Threat Detection & Response gives NHS coordinated threat detection, incident response, and threat management. It has built-in security capabilities, integrated threat intelligence, and virtually seamless workflow for rapid remediation. The solution vastly increases network security at a fraction of the cost it would have taken for the company IT team to provide the service.

People come first

NHS was started by the grandmother of its current owner to provide compassionate, quality care for older adults. As a nurse in the 1950s, she saw people who needed care but had no family to help them. She welcomed folks into her own home until she ran out of room and then decided to build a care facility.

Her legacy lives on today. NHS operates 50 long-term and skilled care facilities in 4 southern states, continuing the family tradition of providing the best possible care. Every day, staff try to live the motto: "Our family caring for your family." They work to meet their residents' needs by developing and delivering quality, cost-effective services. The organization strives to attract and motivate employees who perform their responsibilities with care and professionalism.

NHS CIO Stephen Locke said the company considers it a privilege to serve the people in its care. "Norman Estes, our President and CEO, places a high value on tenured employees," he said. "He believes tenured workers get to know their residents as family and are better able to care for them and carry on the company ethic of taking care of our residents and fellow employees."

Estes's "people first" philosophy is one reason that NHS has been so successful, Locke said. "We're in this business to care for people and to do so profitably, but people come first."

Protecting networks and containing costs

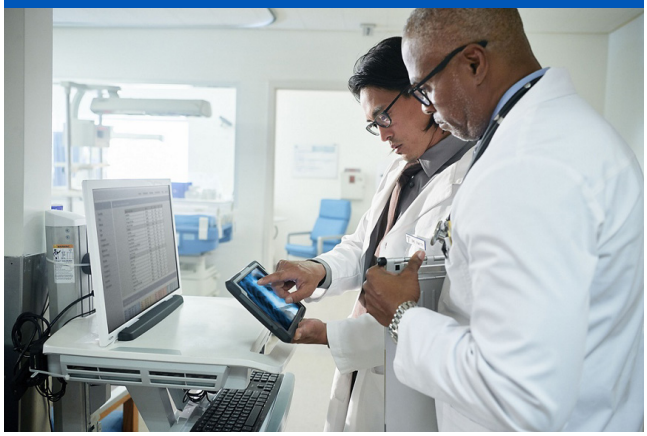
The company's commitment to excellence extends across all departments, from nursing to housekeeping, therapy, and IT. It employs about 7,400 staff, which includes nearly 200 in payroll, accounting, and other management services. Locke's IT staff, which serves all 50 facilities, includes just 13 people.

"One of our challenges is managing and providing high-quality services with a small staff," he said. He's proud of the work this small team produces.

"I'd put our IT experience, support of the customers, and quality of the data and services above anybody else's out there," he said. "I'm continually told by other folks that our team is the strongest at the level of services we provide. People come to work at NHS from all sorts of other companies, and they're always surprised by the level of IT services and support that we provide."

Even with a top-notch team, NHS and every other organization today face difficult challenges. Because its networks store confidential patient data, the company must comply with stringent government regulations, including the Health Information Portability and Accountability Act (HIPAA). "We have to provide a highly secure and consistent work environment and prevent unwanted access to our data and our networks," he said. "IT is not a revenue-generating area, so we need to contain costs, and at the same time keep the quality high and keep everything protected."

> **"We have to provide a secure and consistent work environment and prevent unwanted access to our data and our networks."**
>
> **Stephen Locke**
> CIO, NHS Management, LLC



Vigilant defenses across touchpoints

Network attacks, including ransomware, are a major concern for corporations. The FBI estimates that more than 4,000 ransomware attacks have occurred in the U.S. daily since the start of 2016. Locke and his team recognized a need to layer defenses by adding security information and event management (SIEM), which provides near-real-time alerts and correlates network logs.

"It's a common security control that you need to have in place, but we have no ability to do that with our small staff. To do this in house is expensive; there's a $100,000 application that has to be set up, and you also have to dedicate somebody to review the alerts and the logs to determine if something needs to be addressed," Locke said.

While Locke and his staff have the ability to implement the Center for Internet Security's 20 top critical controls for protecting networks and protected data, he said, "We can't cover it all and keep up with the pace of the mutation of how attacks occur." NHS needed a cost-effective way to correlate the network logs across all the company's platforms,

firewalls, routers, switches, services, and applications while simultaneously keeping up with the ever-changing threat landscape.

Expertise and intelligence to manage cyberthreats

Locke began looking at available SIEMs and very quickly determined the best choice was AlienVault. As he was considering the solution, AlienVault was purchased by AT&T. Since NHS already used AT&T for networking, mobility, and phone services, Locke called his AT&T account team to discuss adding the solution.

Now known as AT&T Managed Threat Detection & Response, the solution provides 24/7 access to Tier 1 – 3 cybersecurity analysts who handle and prioritize large volumes of threats.

"We couldn't do the things that AT&T brings to us for even four times what we're paying now," he said. "Even if we did, we wouldn't have the same level of expertise and intelligence of what's happening in the cybersecurity world. The security teams at AT&T are much more up on that, so it was a no-brainer to outsource the service."

"It was so easy to implement, and we've just ratcheted up the level of security that we provide for the company at a fraction of the cost," he said.

Reduced risk and liability

The experts in the AT&T Security Operations Center review all intrusion detection and prevention system logs and notify NHS of any alerts. "I now have somebody who's highly qualified in security looking at our logs and helping us address them. This makes a huge difference for us in terms of managing our security environment," he said.

> **"We couldn't do the things that AT&T brings to us for four times what we're paying now."**
>
> **Stephen Locke**
> CIO, NHS Management, LLC

Mitigating the risk of attacks is valuable from a corporate and management perspective. "Adding AT&T Managed Threat Detection & Response reduced my risk and liability tremendously, and that's a huge deal for an organization," he said.

"The quality of security program from AT&T affects a lot of things. I'm able to accomplish what the organization needs at a very high level with very little cost and very little trouble, compared to what my solution would be otherwise," Locke said.

The solution also removes some of the worries that comes with being a CIO. "To say that I am relieved is a very minor word. As a security and IT professional, you know this risk is out there. You know you can be compromised, but you don't always know where the next attack might come," he said. "You have to be alerted as soon as possible if something is potentially wrong and be able to act quickly. With AT&T cybersecurity solutions in place, I am confident that we will know sooner than just about anybody else if something is suspicious in our systems."

Locke concluded: "I do feel much more confident that when something happens, I can put my name on it and say, 'I'm providing a superior level of service because I have this in place.' And that does help me sleep at night."

Quality, responsiveness, trust

Locke said he has often recommended AT&T services, particularly its cybersecurity offerings. "There's no question in my mind, from a security perspective, that AT&T has tremendous services. I like the ability to have all that in one place and be able to work with one organization."

He also appreciates the responsiveness of his account team. "I've worked with other companies that provide circuits, but when something goes wrong, or a network is down, the service level is not the same," he said. "If I send an email to AT&T, I'm going to get a response back within 30 minutes, and that's pretty much the way it's been with AT&T all along. We appreciate our relationship with AT&T. It's a straightforward process to work with them, and we get the quality we need."

He plans to work with AT&T on several future projects, including a wireless backup network for the company WAN, some broadband consolidation and possibly some third-party penetration tests. "I can't say enough good things about AT&T. I'm very excited to have them on my team. I know I can trust them, and that's a huge deal for me. That's what partnerships are about, after all," he said. "AT&T is my first stop for security and technology."