TITAN

TITAN UP YOUR SECURITY INTRUSION PREVENTION SYSTEM

INTRUSION PREVENTION SYSTEM
SECURITY BEFORE THE FIREWALL

Case Study

San Fernando Valley Urological Associates

Healthcare Provider

SAN FERNANDO VALLEY Urological Associates

Executive Summary

No industry has as many different data breach risks as healthcare. Financial, identity, and privacy risks are just the beginning. But insurance payment depends on keeping up with government mandates such as Electronic Health Records (EHRs) and CMS-compliant reports, and more is on the way. In 2017, the Healthcare Information Exchange (HIE) requirements will open practice computer systems in radical new ways. Reduced payments, penalties, and denied claims push providers to take risks they aren't prepared for without comprehensive protection.

Hackers exploit this chaos actively. Traditional antivirus and firewall protections are failing thousands of companies. San Fernando Valley Urological Associates (SFVUA) is a specialty practice that knows they are a target. A recent hospital ransomware attack raised their awareness to the point of action and they found Oasis Titan, a full-scale solution that protects banks and other high value targets. Hackers targeting SFVUA systems will be forced to look elsewhere.

Major concerns include:

- Lack of effective security and integration standards in a chaotic commercial software market
- Vulnerability of healthcare billing, communications, and patient records systems
- Increasingly aggressive attacks on small- and medium-sized healthcare organizations
- Successful attacks on large organizations inside and outside the healthcare industry
- New strategies, such as ransomware
- Timed government mandates, which may put functionality in place before protections are developed

An Overall Solution

Expanding interconnection requirements between practices and EHR vendors, billing contractors, and—soon—HIE connections, is creating more complex Internet exposure for healthcare providers' servers. Current point-to-point connections are expanding to allow providers and organizations to connect to any other permitted entity.

> "Titan gives me another layer of security. I have a lot of layers of security, but this is the first layer of 'rebound'—it's kind of like a hacking attempt hits a wall and bounces back before it starts hitting my inside sentry."
>
> **Patti Barton**
> SFVUA Administrator

Current security solutions, such as firewalls, are designed to cover unnecessary vulnerabilities, but may not provide adequate protection for required port openings due to future interoperability. Oasis Titan provides a complex defense that stands at the mouth of the practice's broadband connection, before the firewall, handling both valid traffic and hacking attempts equally.

SFVUA's results with Titan revealed the degree to which hacking attempts were already occurring and began to handle them before they reached the internal network. Titan also provided an unexpected benefit by drastically reducing unnecessary network traffic to the server and internal network, reducing the burden on their broadband connection, and significantly improving IT system performance for the practice.

The Power of Titan™

Oasis Technology's Titan system is an advanced network security solution to safeguard healthcare companies from the growing specter of international cyber intrusions and terrorism activities.

OASIS TECHNOLOGY
Oasis Technology, Inc. 601 Daily Drive, Suite 226, Camarillo, CA 93010-5839 | (805) 445-4833

Background

The practice administrator at SFVUA, Patti Barton, is highly experienced at medical practice administration. She keeps abreast of evolving government requirements and regulations affecting her organization. She shares what she learns with other practice administrators, but she is seen as well informed. Her opinion about current issues, such as Internet risks, is valued by others. She notes that while she has not been directly affected by issues such as ransomware yet, she personally knows victims of past attacks.

A recent article in the September, 2016 Vanity Fair, mainstreaming what had previously been a tech industry insider topic, raised her awareness of the depth of the Internet hacking problem worldwide. She noted the extent of the unknown risks her organization likely faced. In addition, she had noticed rising activity on the practice's broadband connection that did not seem to correspond to their computer use. Having received emailed information about Oasis Titan and its capabilities, she investigated further to see if it might help her protect against inevitable future risks to her organization's IT systems.

Company Overview

San Fernando Valley Urological Associates is an active practice with six physicians and additional ancillary staff providing urology services including surgery and oncology. The breadth of a practice like theirs generally requires connections to billing services, EHR providers, hospital systems, electronic prescribing systems, oncology ordering systems, and more. The practice administrator, Patti Barton, has 30 years of experience dealing with change in her profession, including the original introduction of computers years ago.

Ms. Barton has been actively self-educating, working with service providers, and initiating proactive security measures as voluntary and mandated interconnections increase the practice's exposure to Internet activity. Recent annual liability insurance updates have included inquiries about the practice's cybersecurity efforts.

High-Value Targets

Small- to medium-sized medical practices are "high-value targets" for hackers on the Internet who can quickly turn information into cash at hidden international marketplaces. Medical billing databases alone contain a wealth of personal information such as insurance policy numbers, addresses, dates of birth, and—until changes take effect—even social security numbers used by government health insurance as patient ID numbers.

Because these healthcare organizations are not under the IT umbrella of a larger organization, their security practices are dependent on the experience and wisdom of in-house administration. As Ms. Barton notes, recent news about attacks on a large hospital and the IRS suggest that they are "just little people" and even more vulnerable. As they move forward in response to rapidly evolving government mandates for greater electronic communication, health care practices are, in effect, on the leading edge of Internet security practices by default.

Titan Brought Both Protection and Awareness

The SFVUA administrator, after researching the Titan product online, contacted Oasis for more information and accepted an offer for an on-site consultation. The Oasis engineer surveyed their systems, providing a wealth of information about their exposure, including some system exposure that she had not previously been aware of. She initiated a trial of Titan and observed that in addition to providing protection and a report of potential problems and hacking attempts, Titan served another important function.

Titan was also keeping the anarchy of the Internet from their internal network and systems beyond what the firewall had been able to do. While blocking and monitoring hacking attempts, Titan significantly reduced the practice's Internet bandwidth use, leading to much faster communication and local system operation.

Patti Barton, expressing her relief at better addressing her Internet concerns, said, "If people in the health field could understand how important something like Titan would be for them...it really should be pushed...when I talk to people because they have concerns, I tell them they really need to look into this."

With her growing understanding of the issues at hand, she also notes that, "[Titan] gives me another layer of security. I have a lot of layers of security, but this is the first layer of 'rebound'—it's kind of like [a hacking attempt] hits a wall and bounces back before it starts hitting my inside sentry."

Since Titan receives frequent updates on a subscription basis, Barton compared the ongoing cost to the amount at risk should something happen as "pennies." It was clear, though, that her overriding concern was for the practice to continue to do right by its patients, understanding the risks of misdirected patient data in this evolving, interconnected world.

Summary

Oasis Titan is a broad-based response to cyberattacks on healthcare organizations that is simple to implement. It sits outside the firewall as a protection in addition to security measures implemented as part of their IT systems. Since many small practices like SFVUA rely on IT consulting services, Titan can save significant amounts by requiring little or no IT specialist involvement during installation or operation.

Providing overall protection, Titan helps to address eventualities—as further interconnection mandates emerge and new attack modalities are developed, Oasis Titan is in place, guarding healthcare information systems and keeping patient data out of the hands of hackers on, as healthcare practice administrator Patti Barton calls it now, the "dark side" of the net.

For more information on Titan, visit:
http://www.oasistechnology.com/titan/