SONICWALL

HEALTHCARE NETWORK SOLUTIONS

Application intelligence and control in healthcare information systems

Background: Healthcare becomes a system

Healthcare IT systems are increasingly being integrated across enterprises, between different care providers, and opened up to outside information service providers, patients, and communities. The number and complexity of applications and systems being interfaced creates a daunting task for IT staff to implement and manage.

As this dynamic has gained momentum, a matrix of concerned entities across government and the healthcare community has provided guidance as well as impetus for the change. These include:

- Integrating the Healthcare Enterprise (IHE), a global initiative that creates technical frameworks for passing vital health information from application to application, system to system, and setting to setting—across multiple healthcare settings
- Health Level Seven (HL7), another global initiative addressing standards for electronic interchange of clinical, financial, and administrative information among healthcare computer systems
- Public Health Data Standards Consortium (PHDSC), a national membership-based public and private sector organization with the goal of empowering the healthcare and public health communities with health information technology standards
- The Healthcare Information Technology Standards Panel (HITSP), formed for the purpose of integrating standards for sharing information among healthcare organizations and systems (HITSP's contract with the U.S. Department of Health and Human Services concluded on April 30, 2010)
- Digital Imaging and Communications in Medicine (DICOM) is a global Information Technology standard that is used in virtually all hospitals worldwide to ensure the interoperability

of systems that manage medical images derived structured documents, and related workflow

All this standardization has greatly increased the portability and interoperability of healthcare data and applications. This enables healthcare providers to accomplish key initiatives that can improve patient care, and increase the efficiencies and cost-effectiveness of their operations, such as improved application-to-application integration, better transactional performance, which in turn yields better workflow. As a result, the IT networks of the healthcare community are beginning to carry increasingly significant amounts of data, much of it in the form of distinct file types or content.

But these same organizations are still bound by their obligations to address three imperatives of healthcare information management.

1. Confidentiality: electronic health information cannot be made available or disclosed to unauthorized persons or processes
2. Integrity: electronic health information cannot be altered or destroyed in an unauthorized manner
3. Availability: electronic health information must be accessible and useable upon demand by a authorized person

Threats to the health of healthcare systems

All these networked systems and myriad forms of information are particularly susceptible to electronic threats—both directed and random. Often the weakest link is the people who access the systems. In fact, one of the earliest recorded incidents of "show-off" hacking (in 1983) disrupted the monitoring systems of cancer patients in a New York City hospital.

In other, more recent episodes:

- Spyware infected computers at Akron (Ohio) Children's Hospital after a disgruntled boyfriend installed a virus on his ex-girlfriend's computer[1]
- IT networks in hospitals across England were shut down by a computer worm after a worker logged into the network with an infected laptop[2]
- A hospital in Atlanta, Georgia, was hit by a Trojan that began recording personal information from thousands of patient records, then transmitted the stolen data back to the attacker via email[3]

But just as dangerous are the automated threats from Web 2.0 applications. As an increasing number of community and consumer-facing functions are managed through Web portals, the potential for these threats to enter the network grows. Their presence can be easily overlooked in the volume and variety of applications in a healthcare system network. These Web application threats include:

- SQL, OS, and LDAP injection to a data interpreter as part of a command or query (the attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data)
- Cross-site Scripting (XSS) flaws send untrusted data to a Web browser without proper validation (XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions or redirect the user to malicious sites)
- Broken Authentication and Session Management allow attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities
- Insecure Direct Object References can expose a file, directory, or database key (without adequate protection, attackers can manipulate these references to access unauthorized data)
- Cross-site Request Forgery (CSRF) forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable Web application (this allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim)
- Insufficient Transport Layer Protection can cause applications to fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic (the applications will then use expired or invalid certificates, or not use them correctly)
- Unvalidated Redirects and Forwards allow attackers to redirect victims to phishing or malware sites, or use forwards to access unauthorized pages

Vulnerabilities in Web applications made up 80 percent of all Web-related flaws in the second half of 2008, and rose in prevalence by about eight percent from the first half of 2009. Such Web application vulnerabilities were found in Adobe®, SAP®, Microsoft®, Mozilla, Sun®, Apache, and Oracle® products.[4]

In addition to the threat to an organization's information assets and personally identifiable information (PII), there is the issue of network availability and capacity. Certainly, a network shutdown for disinfection can be catastrophic in a hospital or clinic. More dangerous is the unsanctioned or illegal appropriation of bandwidth for personal or recreational use. When real-time data feeds are supposed to be prioritized or large image files need to be moved across the network, having the network clogged with malicious traffic or streaming entertainment media can literally become a matter of life and death.

The concern is so great that some organizations have banned access to popular Websites altogether. For example, Visiting Nurse Service of New York has blocked use of social networking sites. Yet other organizations have stepped back from such measures because these same sites can be important tools for staff recruitment and community outreach.

In short, IT networks can no longer operate in secure silos, nor be isolated from the rest of the community or world.

An intelligent solution to application-layer threats

In this interoperable environment, static firewalls and user policies are inadequate to secure personally identifiable information, prevent malware infections, and assure maximum availability of network resources.

At the same time, conventional firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Services (IPS), are not up to the task of totally securing an environment with so much traffic that includes so many different applications and file types. While the technology has developed to serve a range of industries, Application Intelligence (AI) is uniquely well-suited to securing healthcare information environments.

Application intelligence and control is the ability to recognize application behavior and assess its impact on network resources. This goes beyond simply identifying file types, and is crucial in addressing Web-based threats that use common protocols or stolen credentials to access and disrupt information.

In a security context, application intelligence and control is obtained and applied as a considerably more robust form of inspection at key network filter points: firewalls, Next-Generation Firewall appliances, VPN devices and wireless network access points. When properly implemented, this technology is able to distinguish acceptable application activities from dangerous ones.

But network security measures informed by application intelligence and control are not a panacea for eliminating network threats in and of themselves.

First, there is the challenge of obtaining the necessary information. By its nature, the traffic information is being gathered through deep packet inspection of each of the data packets that passes through a filter point. If traffic must be 'paused' (usually side-tracked to a proxy environment) in order to conduct the inspection, network performance can be degraded to unacceptable—and unproductive—levels. In order to be practical, a security solution utilizing Application Intelligence must be able to conduct inspections without adversely impacting overall network performance.

Then there is the issue of how to address a threat once it has been identified. Many network security technologies simply shut down the port or network segment through which the threat is operating. This, of course, is the definition of network disruption. In short, the solution is only slightly better than the problem. The best solution is one that can isolate and remove only the threatening application elements while permitting useful traffic to continue. To be a fully satisfactory solution, this remediation process must also operate with minimal impact on network traffic flows.

How SonicWall applies application intelligence and control

The SonicWall Next-Generation Firewalls running application intelligence and control not only block traditional network-layer threats, but also extend protection, management and control over application-layer traffic, enhancing compliance, content filtering and data leakage prevention, while ensuring performance-under-attack from advanced persistent threats. Application intelligence can dedicate throughput for mission-critical or latency-sensitive applications, and restrict productivity-draining applications like YouTube® and Facebook® based on user group, time of day, or mobile device type.

Leveraging patented (U.S. Patent 7,310,815; 7,600,257; 7,738,380; 7,835,361) high-performance SonicWall Reassembly-Free Deep Packet Inspection® technology, SonicWall Application Intelligence and Control can identify and control unauthorized browsers, Web 2.0 sites, Instant Messaging clients, and EXE, SRC, PIF or VBS files—as well as dynamically evolving anytime, anywhere applications. Continuously and automatically updated with an industry-leading 2,800+ unique application uses, SonicWall's Application Intelligence and Control can identify and control application traffic regardless of port, protocol, platform or even encryption.

SonicWall's Application Intelligence and Control can also block and control unauthorized outbound transmission of sensitive, proprietary or watermarked data via FTP uploads; or via email attachments over corporate SMTP, POP3 or even personal web mail services such as Gmail®. And, unlike other solutions, SonicWall Application Intelligence and Control scales to meet the needs of any size organization through its ability to scan large numbers of concurrent downloads of unlimited file size.

More importantly, SonicWall implements application intelligence and control and performs threat remediation in real-time. Application-level bandwidth management functionality ensures Quality of Service (QoS) by allocating dedicated throughput levels for designated mission-critical applications, or user groups, and can be enabled for various times of the day.

[1] IDG News Service, Robert McMillan, September 18, 2009

[2] Enterprise Security, John Leyden February 9, 2010

[3] http://trojanhorseremovers.com/articles-for-trojan-horse-removers/what-is-a-backdoor-trojan.php

[4] SC Magazine, Angela Moscaritolo, March 18, 2009

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com