Effective Internal Wireless Security for Healthcare Networks in the Age of BYOD

Wi-Fi security challenges and a comprehensive, easy-to-use, out-of-band, agent-less, internal network security solution from PFU Systems, a Fujitsu Company.
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Overview</td>
<td>3</td>
</tr>
<tr>
<td>Device Proliferation, BYOD and BYOA</td>
<td>4</td>
</tr>
<tr>
<td>Attack Trends and Healthcare</td>
<td>5</td>
</tr>
<tr>
<td>Wi-Fi Security Requirements in Healthcare</td>
<td>7</td>
</tr>
<tr>
<td>iNetSec Smart Finder in Healthcare Overview</td>
<td>8</td>
</tr>
<tr>
<td>Healthcare Network Monitoring: Smart Finder Sensor</td>
<td>9</td>
</tr>
<tr>
<td>Healthcare Network Security Reporting: Chart Software</td>
<td>14</td>
</tr>
<tr>
<td>Key Smart Finder Benefits</td>
<td>15</td>
</tr>
<tr>
<td>Smart Finder Awards and Market Focus</td>
<td>16</td>
</tr>
<tr>
<td>About PFU Systems, a Fujitsu company</td>
<td>17</td>
</tr>
<tr>
<td>For More Information</td>
<td>17</td>
</tr>
</tbody>
</table>
EXECUTIVE OVERVIEW

Over the past several decades, the definition of data security has gone from a locked file drawer and a safe to encryption, authentication processes, and software and hardware technologies. During this time, applications and services have evolved from closed mainframe environments to hyper-connected local area networks (LANs), wide area networks (WANs), and wireless networks. Ubiquitous access to networks by billions offers many benefits. But organizations of all sizes are increasingly coming under attack from cyber criminals. Information is being stolen for economic gain, competitive espionage, political harassment, and other purposes. Data tampering is another byproduct of network intrusions.

In healthcare, risks to cyber security have grown as medical employees, patients, and visitors gain access to networks on their personal unsecured devices, rendering network perimeter defenses ineffective. The 2014 “Fourth Annual Benchmark Study on Patient Privacy and Data Security” from the Ponemon Institute found that cyber attacks, resulting in stolen patient data within healthcare networks in the U.S., have increased 100 percent between 2010 and 2014.

An array of technologies exists to prevent against and mitigate cyber attacks. Most solutions are complex to install, manage, and maintain. Integration of the different tools from different vendors is another challenge. And then there are inherent weaknesses of passwords that can be deduced or are shared, lax enforcement of strict security policies among employees, and the ability of solutions to stay ahead of the latest mobile technologies and vulnerabilities.

For healthcare environments with Wi-Fi networks used by medical staff, patients, and visitors, a security solution is needed that:

- Incorporates the best existing security tools
- Continually monitors the network
- Enables easy policy enforcement
- Is simple to deploy and manage through automation and self-provisioning
- Works out-of-band and without the overhead of agent software installation on devices
- Is affordable and efficient

This paper provides an overview of the evolving internal threat landscape that imperils patient privacy, data security, and regulatory compliance in healthcare Wi-Fi networks. It also describes an award-winning product from PFU Systems, a Fujitsu company, that has become the fastest growing unauthorized device prevention solution in Japan since its introduction — iNetSec Smart Finder. This easy-to-use appliance enables wired and wireless device discovery, classification and management, and application control, all designed to monitor and prevent
cyber threats from inside of networks. Released in the U.S. in October 2013, the product’s features and benefits for U.S. healthcare organizations are presented.

DEVEICE PROLIFERATION, BYOD AND BYOA

Unless you live in a secluded place off the electrical grid, it’s impossible to ignore the proliferation of network-connected devices of all kinds all around us. Research conducted in 2013 by Frost & Sullivan estimated that there were one billion devices shipped that year and another three billion expected to be purchased through 2016. The company estimates that by 2020 there will be nearly 80 billion connected devices around the world.

Regularly we hear about the amount of traffic traversing networks, the bandwidth being consumed, and the yottabytes (one trillion terabytes) of information being stored. Ubiquitous access in our homes, at the office, and on the go has raised our expectations and requirements in communications, leisure activities, and work. Those expectations and requirements are behind the push by employees for Bring Your Own Device (BYOD) and Bring Your Own Application (BYOA) initiatives in companies.

Americans are leading proponents of using their personal smartphones, tablets, and PCs for both personal and work activities. Small and medium-sized businesses have led the BYOD trend, with 62 percent of them allowing access to their networks by personal devices according to the Frost & Sullivan study. Others ban personal devices, have loose security guidelines, or no formal wireless policies. And among healthcare and educational organizations of all sizes in the U.S., BYOD adoption has steadily increased since 2011 (Figure 1).

Figure 1. U.S. Healthcare and Educational Organizations with BYOD Activity – 2011-2018
Source: Frost & Sullivan

BYOA is another trend that actually predates BYOD. It is the downloading of non-business related applications by employees on either company-issued or personal devices. These
applications (e.g., BitTorrent, Facebook, Twitter, YouTube, and many other news and entertainment sites) have the potential to create serious security issues. Some also make extensive use of company bandwidth.

Among U.S. healthcare organizations of all sizes specifically, the Ponemon Institute study found that: “Despite the concerns about employee negligence and the use of insecure mobile devices, 88 percent of organizations permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to their organization’s networks or enterprise systems such as email.” Only 21 percent of these healthcare networks scan BYOD devices prior to connecting and half of all healthcare organizations have little confidence in their current network security solutions.

ATTACK TRENDS AND HEALTHCARE

Today hundreds of millions of people enjoy anytime access to information, news, entertainment, and communications. And we want it anywhere a wired connection or network signal are available—from devices at our desks, at home, in the car, in our pockets, on the water, and in flight.

But the negative side of ubiquitous access and the warehousing of huge amounts of personal and business data are now becoming clear. Network breaches leading to the theft of credit card data from millions of customers at the large U.S. retailers Target and Neiman-Marcus in 2013 showed the insecurity of major networks. Malware attacks (including computer viruses, worms, Trojan Horses, and botnets) have surged. Security vendor McAfee Labs reported in 2013 that they analyzed 100,000 new malware samples every day in 2012. That included 44 times the number of mobile malware samples than in 2011 (Figure 2).

Figure 2. Increasing Volume of Mobile Malware
Source: McAfee Labs “State of Malware 2013”
Within organizations, unauthorized access to Wi-Fi and other networks have been attributed to lax security and a lack of adherence to security policies by employees. This has resulted in everything from theft and data tampering to overuse of bandwidth, all costing organizations in lost business, intellectual property, competitive advantage, customer trust, and criminal negligence.

Healthcare organizations in the U.S. face the added mandate of protecting the privacy of patient data and the threat of severe penalties based on the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other such laws. Yet medical identity theft is growing. It accounted for 43 percent of all identity theft reported in the U.S. in 2013, according to a report by the U.S. Department of Health and Human Services. The agency estimates that since 2009 between 27.8 million and 67.7 million individual medical records have been breached. A 2012 survey by the Healthcare Information and Management Systems Society (HIMSS) adds to the evidence of the insecurity of healthcare networks. Based on responses from 303 IT and security professionals employed by hospitals and ambulatory care providers, the HIMSS study found that 22% reported a security breach in the previous year.

While there are many reports of hacker networks in remote parts of the world where law enforcement is weak, a majority of network security incidents originate within network firewalls. A 2009 study by the Computer Security Institute found that 60 to 80 percent of network attacks and misuse occur from within and that internal breaches are much more costly than external ones.

“What companies do is look for attacks at the perimeter, but the adversaries are inside the perimeter,” said Chris Ingliss, former deputy director of the U.S. National Security Agency at a conference in April 2014.

The flood of smartphones, tablets, and network-enabled medical devices in healthcare environments introduce new vulnerable entry points that can exacerbate the incidence of internal breaches. Security experts also cite anecdotal evidence of employees routinely sharing wireless passwords with non-employees and even the posting of passwords on white boards in conference rooms.

It is therefore not surprising that a 2013 study by Forrester Research reported that 78 percent of enterprises in North America and Europe said that updating their security to support mobile access was a critical or high priority while these same organizations were simultaneously aggressively expanding BYOD and other mobile initiatives (Figure 3).
The most severe data breaches are caused by targeted attacks such as Advanced Persistent Threats (APTs). The most common type of malware used for these attacks today is the Remote Access Trojan (RAT), which infiltrates the network by disguising routine business communications such as email and is very difficult to discover using conventional antivirus software or intrusion-detection systems. To protect against such sophisticated malware activity, in addition to the conventional perimeter security protections, it is necessary to employ protection methods inside of networks.

**WI-FI SECURITY REQUIREMENTS IN HEALTHCARE**

IT has little choice but to embrace mobility and BYOD and BYOA initiatives within healthcare networks as they complement work and lifestyle trends supported by millions of healthcare professionals, patients, medical device designers, administrators, and others. Wi-Fi is used to support infusion pumps, oxygen monitoring devices, smart beds, and applications such as electronic medical records (EMRs) and X-ray and MRI scans. Remote areas now connect with medical specialists through telepresence and other types of video delivered over Wi-Fi.
Providing security for Wi-Fi networks requires different strategies and solutions as compared to traditional network security that sits at the network perimeter. With Wi-Fi networks there is no longer a network perimeter, so a reliable security solution must be able to continually monitor the Wi-Fi network to see who is on it, when they are connecting, what devices and applications they’re using, how much bandwidth they’re consuming, and other metrics. It must also be able to enforce security policies easily and non-intrusively so that enforcement does not become a burden on end users or IT. Having to install agent software on every single wireless device and update the software is cumbersome and intrusive solution. Contrast this with an automated, self-provisioning Wi-Fi security solution that resides on an out-of-band instead of inline appliance. It doesn’t utilize bandwidth or impact network performance. There is no agent software to install on devices or software updates to manage.

Such a solution should be easy to deploy in under two hours and easy to manage, which is a big plus for small or informal IT departments in healthcare organizations. And it should be affordable.

These features are all found in the leading solution for unauthorized device prevention in Japan and that country’s fastest-growing unauthorized device prevention solution—iNetSec Smart Finder. Newly introduced to North America, an overview of Smart Finder’s features and benefits follow.

**INETSEC SMART FINDER IN HEALTHCARE OVERVIEW**

SmartFinder is a comprehensive internal network security appliance that incorporates the leading wired and wireless network security solutions and other useful features all in one easy-to-deploy and manage product. It provides wired and wireless endpoint visibility, Layer 7 application control, and intrusion prevention systems (IPSs). These empower IT administrators to monitor and prevent network threats from the inside.

Unlike other types of traditional security products—such as firewalls and Unified Threat Management (UTM) solutions that are designed to protect the network perimeter—iNetSec Smart Finder provides security for the interior of network environments. Thus Smart Finder provides an additional layer of security that has become necessary in the age of mobility and BYOD. Perimeter solutions are also deployed in-line, with longer operational processes, utilizing network bandwidth and often requiring network down-time for full deployment. Many healthcare environments, particularly small to medium-sized clinics and hospitals, have only one or a handful of IT staff. Complex enterprise solutions that are expensive and time-intensive do not meet their needs. Instead, Smart Finder can be deployed quickly. It is an out-of-band appliance that does not utilize network resources and users can learn how to operate the solution in minutes.
Called a hybrid solution because it integrates capabilities of various products into one, Smart Finder includes the essential and most beneficial features of leading internal security solutions that have been among the most effective in preventing and mitigating internal cyber attacks and controlling network access and usage.

They include:

**Network Access Control (NAC)** controls access by any device to the Wi-Fi or wired network. NAC ensures that any device that is allowed to connect complies with defined security policies. NAC is extremely useful in providing BYOD security. Typically, NAC products are complex to manage and require the installation of a software agent on each device. This entails ongoing administration by IT administrators. But Smart Finder is agent-less and enabled when the solution is first deployed in the network. Smart Finder provides full endpoint visibility and is very easy to use.

**Behavioral IPSs** monitor the entire network to look for suspicious traffic from application usage and for malware including APTs. Unlike traditional IPS technologies that are deployed in-line to protect the network perimeter, iNetSec Smart Finder is deployed out-of-band so it does not cause any bottlenecks or bandwidth degradation. Additionally, Smart Finder can inspect packets up to Layer 7 for a higher analysis of the network activities.

Healthcare environments are also being attacked by different types of malware including APTs that cannot always be detected by ordinary antivirus software or by traditional IPS technologies. Often malware infections are launched through remotely controlled operations that are disguised in the flow of ordinary communications from outside of the network. RATs, among the most common types of malware, can bypass signature detection and other standard forms of security. These infections can easily spread and last for long periods before they are discovered because discovery is difficult at the exit points of networks. iNetSec Smart Finder features a technology to discover and neutralize these threats. Smart Finder can analyze, detect and stop malware and activities caused by APTs by uncovering the relationships between multiple communications from outside and within the network to discover activity that is characteristic of APTs and stop it at choke point gateways within the network.

Smart Finder has three main components, the Sensor, the Manager Software, and Chart Software.

**HEALTHCARE NETWORK MONITORING: SMART FINDER SENSOR**

Aside from the fixed network devices within healthcare networks, a growing number of mobile devices are accessing network resources and applications as well. Medical staffs use Wi-Fi enabled devices and applications to communicate and to improve and facilitate care. Patients and visitors to hospitals and clinics use applications to monitor and manage their own health.
According to IMS Health, a healthcare services and technology company, there are now over 40,000 such apps to choose from.

In the age of distributed computing, network segmentation and perimeter control alone should not be counted on for the security of modern networks. With the great influx of new devices and applications, IT administrators must continually monitor healthcare networks to determine what devices and applications are allowed and to set limits on bandwidth and access to internal resources and databases.

The Smart Finder Sensor (Figure 4) is a small footprint hardware appliance that can detect and identify connected devices and network applications. It enforces network access policies at endpoints. Policies are created via the Manager Software.

The Sensor can be configured to handle up to 3,000 endpoints, 1,000 concurrently. It can also handle up to 16 IP segments or virtual LANs (VLANs) with a trunk port connection (in tagged VLAN mode).

Figure 4. iNetSec Smart Finder

Smart Finder is licensed based on how many wireless or wired IP segments (LANs or VLANs) customers need to control. In larger hospitals, network topologies may include multiple subnets.

The Sensor discovers all of the wired and wireless devices on the healthcare network along with the applications being used. Policies can be applied based on device type, OS type, and application usage privileges. IT administrators gain the power to allow certain devices access to the network while blocking others. For example, visitors in a waiting room may be restricted from watching streaming videos with high bandwidth. A rogue device that may be set up to try to gather healthcare information can be identified and not allowed to access the network.
HEALTHCARE NETWORK SECURITY MANAGEMENT & POLICIES: THE MANAGER SOFTWARE

Healthcare networks are complex. They include many network devices and legacy applications that have never been tested against security best practices. Patient data exists in many places and on many devices and it can be stolen or targeted by malware. Additionally, portals and social media are now being used more and more by healthcare organizations to spread information on preventative care, to educate patients about upcoming procedures, to facilitate dialogue between patients with common conditions, and many other things.

All of these open up risks to patient data security and privacy along with regulatory compliance. Security solutions for healthcare networks must therefore not only continually monitor networks but also include flexible policies that can evolve in real-time to adjust to changes in the environment.

The Manager Software provides these features. It collects data from the iNetSec Smart Finder Sensors deployed on the network and displays the data on screen. It provides full visualization and classification of all wired and wireless devices on the network such as Windows and Apple Macintosh computers, printers, routers, and mobile devices; their OS type; and other information. In addition it provides visualization of the applications used, such as media-streaming, peer-to-peer (P2P) file sharing, social networking, email, and business applications. It also enables the creation of network admission policies and the creation of device white lists and black lists. Other policies include network access policies and application approvals. Additionally, the Manager Software offers behavioral IPS features to automatically detect and block specific malware attacks. The Manager Software is able to display and monitor of up to 10,000 endpoint devices and up to 250 IP segments.
Figure 5 above shows the range of device-related discovery and mitigation controls available to an IT administrator in a healthcare network environment using the Smart Finder Manager Software. Figure 6 shows the output from the Sensor based on a network scan of applications use and the related access controls, traffic volume, and sessions.

Figure 6. Smart Finder Manager Software: Application Monitoring
Figure 7 shows how the Smart Finder Manager Software can display functions or sub-applications and enable access control functions for each one. In the example below, specific functions of the Facebook application (e.g., chat, post, events) are displayed along with their relative risk level. The IT administrator can choose to allow or block a device from accessing a specific function or sub-application using this feature.

Figure 7. Smart Finder Manager Software: Application Function Monitoring

To classify devices and applications the Smart Finder Manager compares information captured by the Sensor (the equivalent of a packet sniffer) with entries in its device and applications dictionaries (Figure 8). Software updates, including the device dictionary, application dictionary, and firmware updates, can be downloaded and are part of the support service contract. The Manager software runs on Microsoft IIS and functions as a Web-based console with a user-friendly graphical user interface (GUI).

Figure 8. Smart Finder Manager Software: Device and Application Dictionaries
Beginning in 2012, the U.S. Department of Health and Human Services, Office of Civil Rights, has taken a much more aggressive approach to ensuring that healthcare organizations are complying with HIPAA privacy, security, and breach notification guidelines. Instead of merely investigating complaints, the department is now actively choosing healthcare organizations to audit. One of these audits in 2013 resulted in a $1.7 million fine paid by WellPoint, a managed care organization.

The network self-assessment possible with Smart Finder is an extremely useful tool that can be compared and tailored to mirror the Office of Civil Rights’ audit to anticipate requirements and areas of focus. It provides hospital administrators with clear answers to questions about network asset, activities and vulnerabilities.

HEALTHCARE NETWORK SECURITY REPORTING: CHART SOFTWARE

As part of compliance requirements, healthcare organizations must provide documentation of security infrastructure, policies, and adherence. Smart Finder Chart Software (Figure 9) is an Adobe Integrated Runtime (Adobe AIR) application, a cross-platform system that can be run as a desktop or mobile device application for building Rich Internet Applications (RIA). Chart Software provides graphical views of the number of devices and types accessing the network, the number of pages printed on printers, power consumption of devices, and other information. Data can be exported in CSV format to easily populate Microsoft Excel and other spreadsheets.

Figure 9. Smart Finder Chart Software
This information is useful not only to healthcare IT managers who are responsible for network security but also to management that seeks to optimize power, cooling, and other resource utilization.

**KEY SMART FINDER BENEFITS**

- **All in one solution:** Includes device management and application management with IPS to handle both threat detection and threat prevention for the equivalent of an internal UTM solution.

- **Centralized control:** Smart Finder empowers IT network administrators in healthcare environments to gain greater visibility and control of the network to provide effective and ongoing security and resource oversight.

- **Easy to use:** Fast, automated installation in under two hours means that IT is not burdened with a complex, cumbersome solution to deploy and maintain. Users with lower-level IT knowledge and experience can quickly learn how to operate Smart Finder.

- **Agent-less:** the solution does not rely on the disruptive and time-intensive installation of agent software on every device accessing the network. So software updates are unnecessary. Instead, Smart Finder uses a variety of data sources to monitor, analyze, and manage access and activity of every device.

- **Non-disruptive:** Smart Finder’s out-of-band versus inline operation does not impact network resources or bandwidth. Its deployment doesn’t require any network downtime or reconfiguration.

- **Affordable:** With Smart Finder’s unique blend of essential NAC and IPS features, there’s no need to pay for a full-featured NAC, IPS, or UTM solution that are not needed for Wi-Fi networks.
iNetSec Smart Finder was awarded the 2013 Frost & Sullivan Price Performance Value Leadership Award for BYOD Security Management in North America. And in 2014, the Info Security Products Guide, the industry’s leading information security research and advisory source, gave Smart Finder awards in four categories: BYOD Security; Intrusion Detection, Prevention, or Combinations; Security Products and Solutions for Education; and Security Products and Solutions for Enterprises.

Offering endpoint discovery and classification, application visualization, and access control features, Smart Finder is an ideal solution for wired and Wi-Fi network security in healthcare organizations. With a blend of NAC, IPS, and UTM solutions, Smart Finder was specifically designed and priced for small to medium sized businesses (SMBs) and small enterprises.

It fulfills the growing market requirement for a simple, easy-to-use, automated, and resource-efficient solution to monitor, measure, and manage access and resource utilization from inside of private networks. By providing these functions, Smart Finder enables IT administrators in healthcare organizations to effectively protect their networks from cyber attacks, malware, misuse of network resources, and other unwanted network behavior. And these features are fully complimentary with the increased use of external mobile devices in BYOD and BYOA initiatives, customer Wi-Fi, and other evolving network applications that are making healthcare environments more efficient and user friendly.
ABOUT PFU SYSTEMS, A FUJITSU COMPANY

PFU Limited, a Fujitsu company, is a leading technology solutions provider – empowering its clients to achieve greater success through superior quality hardware, innovative software and reliable customer service.

Headquartered in Sunnyvale, California with engineering, manufacturing and sales facilities in Plymouth, Minnesota, PFU Systems Inc. is the U.S. operations of Japan-based PFU Limited, a $1.2 billion global enterprise that designs, develops, manufactures, sells and maintains computer hardware, imaging scanners, peripheral products, enterprise software, systems and network security solutions.

FOR MORE INFORMATION

http://www.inetsecsmartfinder.com