DATA THEFT PREVENTION FOR HEALTHCARE
HEALTHCARE DATA IS THE TARGET
HERE’S HOW TO PROTECT IT

When critical data is needed, immediate access is key – but it can put confidential data at risk. This paper outlines a data-centric approach to protect data, stay in compliance and – most importantly – enable continuous innovation in patient care.

In the past three years alone, the healthcare sector – including hospitals, labs, pharmacies, drug companies, outpatient clinics and other affiliated medical products and services providers – has experienced the highest number of data breaches in any industry. In fact, in 2014, more than 42% of all publically reported attacks were in the American healthcare industry.¹

Healthcare IT teams face difficult, unique challenges in meeting compliance regulations and defending their data and that of their patients. Data Theft Prevention for Healthcare identifies these challenges and provides a data-centric approach proven effective in helping IT teams efficiently meet these challenges.

1. Healthcare Data Theft: A Global Problem
2. Why Healthcare Data Is a Top Theft Target
3. Top Data Risks: Malicious Breaches and Insider Threats
4. Top Data Security Challenges in Healthcare Organizations
5. How Data Theft Prevention Helps Optimize Patient Outcomes
6. How Healthcare Organizations Benefit from TRITON® APX Solutions
7. Data Theft Prevention Is Our Mission

1. HEALTHCARE DATA THEFT: A GLOBAL PROBLEM

Healthcare data theft is rising rapidly in the U.S., caused by malicious insider threats, user negligence and external attacks. Though both domestic and foreign-based criminals are culprits, user negligence also plays a major role in causing data loss. Vulnerable healthcare organizations need a comprehensive data security solution that addresses these challenges and prevents critical data loss.

But it’s not just healthcare organizations in the U.S. that are ultra-vulnerable to attacks and data leakage. The U.K.’s National Health System (NHS) has also been shown to be extremely vulnerable to data loss and theft. Many of the weaknesses are a function of deferred maintenance and delayed technology upgrades.

For instance, in a 2015 study, more than 2,000 vulnerabilities were identified in over 5,000 NHS websites.² Though the weaknesses were discovered recently, they were likely in place for months or years. Most of the vulnerabilities were due to out-of-date NHS WordPress sites, creating unmonitored opportunities for attacks.

In Australia, the Pharmacy Board of Australia has issued a warning about a threat that holds encrypted patient medical data hostage until a ransom is paid.³ Furthermore, a recent eCrime Study determined that about 25% of Australian IT security professionals feel unprepared to handle a major data theft event.⁴ Healthcare organizations around the globe face a formidable task in defending their critical data against attacks and data theft.
2. WHY HEALTHCARE DATA IS A TOP THEFT TARGET

Healthcare data, which includes electronic personal health information (PHI), personal identifiable information (PII) and critical data that’s proprietary to the organization, is attackers’ top data theft target. Why? It yields the highest profit on the black market. For comparison, a credit card number will yield an average $2,000 profit; a single PHI file can yield up to $20,000 profit.5

Why such a difference? In general, credit card breaches are detected much more quickly than PHI breaches. Stolen credit card data can become worthless in a matter of days or even hours. However, it often takes weeks and even months for a healthcare data breach to be discovered, which allows much more value to be extracted from it. Also, personal health information is difficult or even impossible to change, enabling thieves to take advantage of it for a very long time.

But just as important as its street value is the fact that healthcare data is exceptionally easy to steal.6 Ironically, the data so critical to millions’ wellbeing and valued so highly by thieves remains virtually unprotected and so easily abused on an ongoing, global scale.

Why is healthcare data so vulnerable?

1. Open healthcare environments make data leakage and theft too easy. As often as not, users on healthcare networks aren’t employees. They’re doctors who operate across several data ecosystems at any time, require unfiltered access to websites and use their own unprotected devices to send and receive data. Healthcare IT departments lack control over user training or guidelines. Also, they don’t dare filter or block websites and connected devices because lives may depend on healthcare professionals having unlimited access to the Internet and patients’ PHI.

2. Government mandates have made medical databases “target rich environments.”7 Due to the American Recovery and Reinvestment Act of 2009, all medical records were required to be stored digitally by January 2015. Hundreds of millions of electronic health records (EHRs) have been added to under-defended healthcare organizations’ networks, but the effects of this program are mixed. Because security delays could cost lives, healthcare IT teams hesitate to “lock down” this data.

3. More than 60% of hospitals lack a plan to respond to a data breach.8 Many lack even basic preventable measures, such as intrusion detection systems, visibility into Shadow IT and storage of data in the Cloud, or sufficient controls over their guest networks. Many InfoSec teams also have difficulty blocking – or enforcing encryption for – sensitive data leaving the network via email or USB mass storage devices.

4. Saving lives trumps data security. Healthcare professionals’ primary objective is to achieve the best outcomes for their patients. As noted above, that often requires the sharing of PHI across multiple ecosystems and rapid, unfettered access to the Internet in life-or-death situations. Data security is, understandably, a secondary priority.

5. Well-funded criminals are sharing advanced attack techniques.9 The dissemination of successful breach techniques has led to an explosion in the number of data thieves and advanced attacks against healthcare networks.10
The consequences of these factors have been predictable. A handful of attacks within the past 18 months have resulted in the theft of tens of millions of patient records from health insurers, hospitals and even government databases.\textsuperscript{11}

The Anthem breach in 2014, for example, yielded 80 million health records to the criminals who stole them. By law, a theft of 500 or more records must be reported, and as of mid-August, 36 such incidents have already been documented in 2015.\textsuperscript{12} And, in a June 2014 Healthcare Information and Management Systems Society (HIMSS) survey, two-thirds of the respondents had experienced a significant security incident, while 42\% said there were too many threats to track. By any measure, the rising data theft trend in healthcare constitutes a true and deepening crisis, both for healthcare organizations and their patients.\textsuperscript{13}

Analysts, predictions and recent events would all seem to indicate that industrial-scale data theft in healthcare is only the beginning of a long-term trend.\textsuperscript{14} Armed with that knowledge, it might be expected that healthcare organizations would respond to these rising risks with greater investments in their data security. For the most part, however, most healthcare organizations spend just 3\% of their IT budget on security. In comparison, the SANS Institute, the largest provider of cyber security training and certification, suggests spending at least 10\%.\textsuperscript{15}

By law, a theft of 500 or more records must be reported. As of mid-August, 36 such incidents have already been documented in 2015.

3. TOP DATA RISKS: MALICIOUS BREACHES AND INSIDER THREATS

Even healthcare organizations that attempt to secure PHI and PII and adopt new technology while adhering to the strict Health Insurance Portability and Accountability Act (HIPAA) privacy standards face an uphill battle. Open environments and the typically weak data security that accompany them will directly lead to massive data loss from both malicious attacks and insider threats. Achieving key technology objectives – while keeping data safe – is more difficult to achieve than ever.

Open data environments with expansive data sharing and unfiltered web access are unique to the healthcare industry. Too often, however, they also create the potential for data loss in the form of the “accidental” data leak by doctors and other healthcare professionals. These open conditions also easily enable malicious insider actions to steal millions of PHI records. These types of insider threats are major sources of data loss and theft in the healthcare industry that must be addressed and remedied.

Another unique aspect of the healthcare industry is the ratio of external and internal causes of data theft. Unlike other industries, where accidental or negligent user behavior remains the primary cause of data theft or loss, external malicious data breaches have recently begun to outnumber accidental causes in the healthcare sector.\textsuperscript{16} These too, however, can be controlled and mitigated with the right data security approach.
4. TOP HEALTHCARE DATA SECURITY CHALLENGES

As caregiving evolves, with duties performed across a variety of ecosystems and devices, IT teams are further challenged to keep PHI, PII and other sensitive data secure yet accessible. Of course, saving lives – not protecting data – is the top priority for doctors, nurses and other healthcare personnel. And, although the migration to EHR has led to improved patient outcomes, it has also created a compliance headache and a security nightmare for IT staffs.

And some existing security solutions severely inhibit caregivers’ efficient access to patients’ medical data, prompting medical personnel to avoid important security protocols. While the Internet makes it much easier for caregivers to quickly, easily share data, it was certainly not designed to protect it.17

Despite these complexities, healthcare organizations must face and meet these top data security challenges:

1. Compliance and regulation
   Reliably track and show progress between audits.

2. Business enablement
   Embrace new technologies that improve quality of care.

3. Protecting the brand and reputation
   Retain and nurture patient trust.

4. Securing research and IP
   Maintain a competitive advantage by keeping such data private.

Staying in compliance is especially difficult for healthcare organizations; however, even achieving and maintaining compliance doesn’t mean that critical data is adequately protected.18 Use of PHI on emerging medical and communication devices is dramatically improving patient care and business efficiency, but it also exposes high-value medical information to data theft in many new ways. And a successful attack can tarnish a reputation built over decades, damage an organization’s business model and lead to stagnation and market share decline.

91% of healthcare organizations reported at least one data breach in the last two years

Recent breach statistics reflect the fact that the risks of a data breach are rising dramatically. In the past two years, 91% of healthcare organizations reported at least one data breach, 39% reported up to five incidents, and 40% reported more than five data breaches. The risks and number of insider threats are rising as well, both from malicious activities and broken business practices, such as using Dropbox™ or Gmail™ without sufficient data protection.
5. HOW DATA THEFT PREVENTION HELPS OPTIMIZE PATIENT OUTCOMES

Raytheon|Websense’s approach to Data Theft Prevention provides medical personnel access to the right data whenever and wherever it’s needed. It also helps organizations remain in compliance, which is now mandatory for organizations’ reputation and financial viability. This allows greater adoption of technological innovations, enabling providers to deliver superior care to their patients. Unlike traditional approaches to security such as focusing only on web or email filtering, a focus on Data Theft Prevention can play a critical role in helping healthcare organizations achieve the best outcomes for their patients.

The symbiotic relationship between all of these healthcare factors can be understood as a pyramid of objectives and outcomes:

- Data Theft Prevention provides a foundation for focusing security and compliance efforts.
- Data security, which is necessary for regulatory compliance, protects brand reputation and the financial viability of the organization.
- Financial viability enables organizations to innovate with technology, helping maintain market competitiveness.

These objectives combine to free healthcare organizations to focus on their core mission of delivering optimal patient care.
6. HOW HEALTHCARE ORGANIZATIONS BENEFIT FROM TRITON® APX SOLUTIONS

The best security solution protects data everywhere it lives – from the Cloud to any endpoint – addresses internal and external threats, and yet is quickly and easily deployed and managed. It should work with the caregivers’ core objectives, not against them. To do so, the approach also needs to be adaptive, contextually aware, apply behavioral analytics and deliver actionable data in real time. Raytheon|Websense Data Theft Prevention works with organizations’ current security staff to stop data theft, not data access.

TRITON APX security solutions protect and enable healthcare organizations to deliver better patient outcomes by addressing key security challenges:

1. **Stay in line with compliance and regulations.** Reliably track and show progress between audits. Healthcare organizations must stay in compliance and pass semi-annual compliance reviews that demonstrate improvement between audits. With ever-increasing compliance standards, it’s more difficult than ever. TRITON APX comes with standard security policies, the ability to customize policies, and ongoing monitoring and reporting.

2. **Protect patient records on endpoint devices on and off the corporate networks.** Data doesn’t have to be at risk, even as caregivers are mobile throughout their day, delivering diagnoses and care in multiple locations, working with data on and off the healthcare network.

3. **Secure PHI workflows throughout the healthcare ecosystem.** Hospitals, physicians offices, clinics, surgery centers, labs, pharmacies, insurance providers and patients can safely access and share data.

4. **Achieve just as high levels of security on guest networks as on employee or staff networks.** A guest network can serve as a potential backdoor, but TRITON APX helps you avoid this by delivering seamless data protection, providing the same controls and security as you have for the employee and staff network.

7. DATA THEFT PREVENTION IS OUR MISSION

Defending organizations from data theft is our mission. We are continually adapting our security solutions to both the needs of care providers and to the evolving threat landscape. In our quest to stay ahead of the threat curve, Raytheon|Websense Security Labs ensures that our TRITON APX suite remains the industry-leading security solution in all major categories.

We are particularly successful in helping healthcare organizations protect their networks, deliver great care and remain in compliance. But don’t just take our word for it. Read case studies that illustrate how Raytheon|Websense TRITON APX provides Data Theft Prevention for healthcare industry leaders including:

- The US Department of Health and Human Services
- Adventist Health
- Visiting Nurse Services of New York
- Hutt Valley District Health Board

To schedule a TRITON APX demonstration or to simply find out how Data Theft Prevention for Healthcare can protect and enable your organization, visit [www.websense.com](http://www.websense.com).
REFERENCES

1 Identity Theft Resource Center, January 15, 2015
2 “Hundreds of NHS sites vulnerable to hackers,” Alphr, March 5, 2014
4 “Developing Your Rightsized Security Strategy”, Raytheon|Websense (Australia, New Zealand) eCrime study, August 2015
5 “Criminal Attacks Now Outnumber Accidental Breaches In Healthcare” CSO Online, May 7, 2015
6 “Hackers Are Homing In On Hospitals”, MIT Technology Review, September 2, 2014
7 “Healthcare organizations under siege from cyberattacks, study says”, Los Angeles Times, February 18, 2014 (SANS-Norse Healthcare Cyberthreat Report)
8 2015 Business Travelers Risk Index
9 “Group that hacked Anthem shared weaponized 0-days with rival attackers,” Ars Technica, July 28, 2015
10 Websense 2015 Threat Report
11 The Health & Human Services’ Office of Civil Rights (OCR) estimates that the personal health data of up to 30 million Americans has been compromised since 2009
12 The Health & Human Services’ Office of Civil Rights (OCR). OCR estimates that the personal health data of up to 30 million Americans has been compromised since 2009
13 “Hackers Are Homing In On Hospitals”, MIT Technology Review, September 2, 2014
14 “Hackers Are Homing In On Hospitals”, MIT Technology Review, September 2, 2014
15 “Analyst: Threats Drive Improved Practices States Cybersecurity Organizations”, www.sans.org Reading-Room
16 “Criminal Attacks Now Outnumber Accidental Breaches In Healthcare” CSO Online, May 7, 2015
17 “Cyber Risk Management In Healthcare”, CSO Online, Mar 6, 2015
18 “Companies Are Not Spending Enough On Cybersecurity”, CRN.com, June 9, 2015
Work smarter

At Insight, we’ll help you solve challenges and improve performance with intelligent technology solutions.

Learn more