Symantec in Healthcare: *Achieve a New Level of Security*

The headlines keep coming, as one healthcare organization after another falls prey to cyber crime. Since 2009, *a full third* of the US population's health data has been compromised in more than 1100 breaches[1]. Mind you, these are just the ones that have been discovered—and reported. And cyber security experts warn that things will only get worse.

On the black market, healthcare data is ten times more valuable than credit card data[2]. In addition to financial data, it includes names, birth dates, policy numbers, diagnosis codes, billing information, and often physical descriptors or even next of kin—all of which can be used for identity theft, drug abuse, or to file false insurance claims.

Medical centers are trying to keep up with the uncertainties of HIPAA requirements and other conflicting regulations to make medical records both readily available and secure. Since sharing data is often the very thing that puts it at risk, the industry needs a sophisticated approach that allows data to be portable yet protected. However, with intense budgetary pressures and a severe shortage of cyber security professionals, healthcare is "woefully behind" when it comes to cyber security[3]. This heady combination of factors creates an irresistible target for cyber criminals.

Although the challenges are daunting, there is a path forward: a sound strategy and an architecture of layered security solutions that work in tandem with one another can be just what the doctor ordered.

PROTECT HEALTHCARE SYSTEMS AND DATA FROM ADVANCED ATTACKS

For any security organization, the first order of business is protecting patient information and intellectual property from stealthy hackers attempting to use methods like advanced persistent threats to steal data. Symantec Endpoint Protection defends endpoints from known and unknown threats, but goes further, protecting virtual desktops (VDI) as well. Complimentary security services for email and the web are also important. Symantec Email Security.cloud shields you from email-based attacks such as spam, spear phishing, and advanced malware, while Symantec Web Security.cloud thwarts complex web-based attacks. Solutions such as Symantec Advanced Threat Protection go beyond prevention by monitoring endpoints, networks, and email gateways to identify attacks that tend to evade detection. With a single console, you can scan for attack artifacts across the infrastructure, "drill into" the details of an attack, prioritize compromised systems, and quickly remediate. Advanced attacks can be contained in minutes, rather than weeks or months.

SECURE ACCESS TO DATA AND APPLICATIONS

In addition to blocking threats attempting to enter your network, you must safeguard data and applications on-premise and in the cloud by controlling who has access to your network. A data loss prevention solution such as Symantec Data Loss Prevention (DLP) tracks and protects confidential information from malicious or negligent insiders. Further, strong multi-factor and risk-based, token-less authentication such as Symantec Validation and ID Protection Service (VIP) ensures that only authorized people can log in to clinical and business systems. Whether on-premise or in the cloud, these solutions enable you to securely adopt SaaS applications such as Office 365 or Box through a single set of controls.

---

1 2015 is already the year of the health-care hack — and it's only going to get worse. By Andrea Peterson, March 20, 2015
https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/

2 Your medical record is worth more to hackers than your credit card, By Caroline Humer and Jim Finkle, September 24, 2014, Reuters.com
http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

3 This US industry is 'woefully behind' on cyber security, by Caitlin Bronson, Nov 16, 2015
http://www.ibamag.com/news/this-us-industry-is-woefully-behind-on-cyber-security-26719.aspx

MANAGE RISK AND ACHIEVE REGULATORY COMPLIANCE

The first step to achieving HIPAA and HITECH compliance is assessing risk so you have an idea of where you stand and where you want to go. A proper risk assessment includes any devices that generate, store, maintain, or transmit protected health information, including those not on the network.

A software solution that measures risk and tracks the performance of security and compliance programs can be instrumental to meeting these regulations. Symantec's Control Compliance Suite (CCS) assesses risk in IT environments, as well as enables mitigation management for risks posed by business associates. The solution also automates security and compliance assessments across endpoints and physical and virtual data centers, allowing you to evolve from ad-hoc risk assessment to a continuous risk management program.

CONSIDER MANAGED SECURITY SERVICES

Many, if not most, healthcare organizations have limited IT resources and/or talent, and are pressured to implement a solid program that can withstand today's sophisticated attacks. In a situation such as this, extending your team with trusted cyber security experts makes a great deal of sense. The best of these services have the technology and expertise they need to manage security across your network and systems around the clock. Choose one that also has experience protecting healthcare organizations in particular. Symantec offers Managed Security Services, an Incident Response team, and sophisticated threat analytics programs that monitor portal, data feed, and service-based data to better anticipate and mitigate risk.

DON'T FORGET MEDICAL DEVICE SECURITY

Safeguarding patient data goes beyond protecting traditional IT endpoints. Network-connected medical devices, in particular, may create vectors for attacks on networks, or even the devices themselves, potentially putting patient safety, hospital operations and care delivery, or patient data at risk. Symantec is taking a leading role by working with healthcare providers and medical device manufacturers to develop device-appropriate protection strategies. Our signature-less security solutions can be designed into the device at the manufacturer level. Further, we help providers set up a standards-based medical device asset and risk management program, enabling mitigation of risks and the implementation of administrative and technical security controls. In addition, Symantec is working with regulators as well as industry and standards organizations to help develop appropriate frameworks and security best practices, enabling us to move forward collectively to address medical device risks.

To learn more about Symantec's cybersecurity solutions for healthcare, visit our website at *www.symantec.com/healthcare*.