Key Security Considerations for Your Healthcare Organization's Move to the Cloud

Healthcare organizations have as much to gain from the use of cloud apps and services as any other industry. Unfortunately, given the nature and sensitivity of healthcare data and its inherently high value to hackers, they're at a much higher risk of data loss.

WHITE PAPER

Symantec™

Introduction

Physicians and healthcare providers use hosted or collaboration services such as Microsoft Office 365, Gmail, and Evernote, as well as commercial file sharing services like Dropbox, Box, and Google Drive to share diagnosis and results, collaborate with colleagues, and participate in research projects. Sharing protected health information (PHI) can reduce the need for duplicate medical testing and streamline communication. It can also help your healthcare organization lower costs and deliver better and faster patient care.

However, without proper controls in place your healthcare organization has a higher risk of security incidents and data loss when medical records and processes are moved to the cloud. Failing to comply with strict regulatory requirements, such as HIPAA, can result in financial penalties. Your customers' goodwill and trust can also be negatively impacted if their personal information is compromised in a breach.

"Over 70% of healthcare organizations have multiple security concerns about the cloud, most commonly with data ownership and control."

- IT Security and Risk Management Study, HIMSS Analytics, March 2018

In this paper, we'll discuss how IT Security Leaders like yourself can keep your healthcare organization's sensitive data safe in the cloud while monitoring and controlling access in real time – wherever it lives. You'll also learn why a new, integrated approach to information protection that includes monitoring, protecting, and controlling information throughout its lifecycle is essential.

Healthcare Security Breaches Continue to Rise

Lawmakers and healthcare organizations have good reason to be concerned about safeguarding patient data, especially in the cloud where it is at risk of exposure. According to the Ponemon Institute, 89% of healthcare organizations have experienced a data breach, which involved patient data being stolen or lost, over the past two years.[1] Hacking/IT incidents accounted for 17 of the 20 largest healthcare data breaches in 2017, and all but three of the 10 largest hacking incidents were due to ransomware. Unauthorized access and disclosures also continue to be a leading cause of healthcare breaches, as well as loss or theft of devices and records.[2]

"69% of healthcare organizations say employee negligence and carelessness is their greatest security concern."

- "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data", Ponemon Institute.

The more quickly a breach is identified and contained, the less damage is done. On average, it takes 191 days for organizations to identify breaches and 66 days to contain them.[3] It's no longer enough to rely on the older, traditional approach of just securing your network and data center. You need visibility into all activities that are going on in your infrastructure – especially data that is being shared via the cloud.

Maintaining Control of Your Data in the Cloud

It's critical that as healthcare organizations move more data to the cloud, they have visibility and control over it, including who is accessing it and how it's being used. There are two types of user scenarios IT Security Leaders must address when it comes to protecting their data: controlled and uncontrolled cloud adoption.

Three key questions to consider when moving to the cloud:

1. Where is my healthcare organization's sensitive data and how much is stored on-premises and in the cloud?
2. How do I protect my data should it fall into the wrong hands?
3. Who is accessing my data, and what is the risk of account takeover?

In a controlled cloud adoption scenario, such as a hospital's electronic health record (EHR) system moving to the cloud, security leaders are engaged in the process and the necessary security protocols are typically designed in from the start to protect the data. In this example, you have visibility into where your sensitive data lives, and you're in a better position to protect it, which also makes it easier to maintain control and protect against internal and external threats.

1. "2017 Cost of Data Breach Study", Ponemon Institute, June 2017.
2. "Largest Healthcare Data Breaches of 2017," HIPAA Journal, Jan. 4, 2018.
3. "2017 Cost of Data Breach Study", Ponemon Institute, June 2017.

By contrast, an uncontrolled cloud adoption scenario can be more complex and presents greater risk, because of the lack of visibility and control. This type of scenario can apply to malicious insiders who intentionally exfiltrate data, perhaps with the intention to profit from it. Or it could be well-intentioned employees who are uploading PHI and other sensitive data to cloud applications, such as clinicians uploading a patient's lab results through unsanctioned file-share sites. Both examples can result in exposed data unless you have the right security protocols and technologies in place to detect them before real damage is done.

Restricting cloud use to IT-sanctioned apps doesn't eliminate the risk of data disclosure either. Your organization's lack of visibility regarding the type of data and how it's being shared within sanctioned apps can result in unauthorized disclosure of regulated data. For example, if a physician uploads files using a sanctioned app and inadvertently configures them to be broadly shared, privileges may be granted to those who shouldn't have access. This lack of visibility and control drives healthcare organizations to look for solutions that will secure their sensitive data while satisfying security and privacy requirements.

Help Keep Data Safe with Symantec Information Centric Security

One of the essential cornerstones of successful data protection is this: as your sensitive data moves, your security must move with it. Symantec addresses these specific threat risks with integrated security controls that work together to help secure your sensitive data regardless of where it lives. Symantec Information Centric Security (ICS) is a new approach to integrated security that unifies five technologies essential to help in monitoring, protecting, and controlling your sensitive information throughout its lifecycle:

- Data Loss Prevention (DLP)
- Cloud Access Security Broker (CASB)
- Encryption
- Multi-Factor Authentication
- User and Entity Behavior Analytics (UEBA)

Information Centric Security in Action

Even if your staff has full data protection knowledge, is it realistic to rely on them to consistently apply policies and never make a mistake? Let's examine how Symantec Information Centric Security addresses a common uncontrolled cloud adoption scenario: A doctor uploads patient test results to Dropbox to get a second opinion from an outside specialist (see the call-out box below for more detail).

How to Protect Sensitive Data When Employees Share Files via Cloud Apps

Situation: A doctor in your organization needs an outside specialist's second opinion on a patient's test results. To do this, he/she uploads the data to Dropbox in order to share it with the specialist.

Symantec Information Centric Security solutions work together to help protect your data:

1. **CloudSOC CASB:** Uncovers users uploading, storing, and sharing content and passes suspicious content to DLP for deeper inspection.
2. **Data Loss Prevention (DLP):** Helps assess the content against your DLP policies to determine how sensitive it is (e.g. – is it PHI?) and what protective action to take. If it can be shared, the file is encrypted and uploaded to Dropbox. Otherwise, it can be blocked altogether.
3. **Information Centric Encryption:** Persistent encryption and rights management are automatically applied to the test results as they're uploaded to comply with data protection regulations.
4. **Multi-Factor Authentication:** The receiving doctor must verify his or her identity to verify only the intended recipient is being given access to the data.
5. **User and Entity Behavior Analytics:** Helps identify abnormal and risky user behaviors based on alert information from DLP.

In this example, the content monitoring controls in Symantec Information Centric Security help detect the sensitive data as it's uploaded to Dropbox and assess it against your DLP policies to determine if the data is allowed to be posted. If the data is deemed to be benign, it can be uploaded without restrictions. If it's determined to be sensitive, it's encrypted, or the upload is aborted if data should not be posted. Finally, to be sure only the intended recipient is accessing the information, the receiving

doctor must verify his or her identity before being granted access to the file. Once the consult is completed, that access can be revoked to prevent future breaches.

In this scenario, the data was uploaded to a cloud app, but the integrated Symantec security controls would operate similarly if the data was located on-premises. The policies and controls you set follow your data everywhere it goes for comprehensive protection.

Unified Security Eliminates Gaps

Symantec Information Centric Security drives data protection policies across every channel – cloud, email, web, storage, and endpoints – from a single, integrated platform that helps eliminate the security gaps created by siloed point products. ICS works to inspect these channels for sensitive content, detect data exposures, encrypt files automatically, control file access and usage, and analyze events so you can quickly act on risks such as in our file sharing scenario. Together these solutions help eliminate blind spots, assist you in staying compliant, and safeguard your sensitive data.

Symantec Information Centric Security:

- Integrates data loss prevention, cloud access security, encryption and rights management, multi-factor authentication, and user and entity behavior analytics to help ensure information is monitored, protected, and controlled throughout its lifecycle.
- Follows sensitive data wherever it goes with persistent protection that automatically encrypts and applies rights management before it leaves your organization.
- Restricts data access to trusted and intended users with simple-to-use, identity-based decryption.
- Monitors who is accessing data and how it's being used to provide insight into abnormal and risky user behaviors.

Components of Information Centric Security

Data Loss Prevention (DLP)
Monitors sensitive data in use across all channels with central policy controls

CloudSOC
Extends DLP policies to sanctioned and unsanctioned cloud apps

Validation and ID Protection Service
Secures access to critical applications and data with multi-factor authentication

Information Centric Encryption
Protects data with persistent encryption and digital rights management

Information Centric Analytics
Identifies malicious activity patterns with user and entity behavior analytics

Information Centric Tagging
Augments DLP classification with user-driven tagging

What Makes Symantec Unique?

Our tightly integrated Information Centric Security gives you the confidence to do business in an environment of always-on data sharing. To that end, Symantec Information Centric Security builds on these unique differentiators:

- **Integrated cyber defense platform.** To successfully embrace the cloud, integrated security controls help you stay secure without impacting your users' productivity. Symantec's Integrated Cyber Defense Platform unifies both cloud and on-premises security to help govern access, protect your information, and defend against advanced threats.
- **Transparent technologies for both cloud and on-premises infrastructures.** Symantec has extended DLP, multi-factor authentication, and encryption technologies from traditional on-premises environments to the cloud. By using one common solution, you eliminate redundant systems, which works to reduce capital expenditures, training, and maintenance efforts.
- **Best-in-class technologies as determined by industry analyst firms.**
  - Gartner named Symantec a leader in Data Loss Prevention for 10 consecutive times in the Gartner Magic Quadrant.
  - Gartner named Symantec a leader for Cloud Access Security Brokers in the Gartner Magic Quadrant, Q4 2017.
  - Leading healthcare IT market research firm, KLAS, named Symantec DLP "2018 Best in KLAS," an award that is given to companies with the highest ratings according to customers.

Take the Next Step to Protect Your Sensitive Healthcare Data

The use of cloud services doesn't have to mean increased risk of data loss for your healthcare organization. With Symantec Information Centric Security, you'll eliminate the detected risk of users circumventing data protection policies or making innocent mistakes that may result in serious repercussions. You'll also have the confidence to conduct business in a more safe and secure manner while satisfying stringent healthcare regulations.

To learn more about how Symantec can help secure your healthcare organization's journey to the cloud, visit **www.symantec.com/healthcare**, or contact us at (877) 294-5255.

About Symantec

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**