FORTRA™

CASE STUDY (Digital Guardian)

How A Renowned Healthcare Institution Protects Patient Data In The Cloud

Executive Summary

A world renowned healthcare institution wanted to use the cloud to dramatically improve the ease and speed of sharing information — across their multiple campuses and with their associates around the world — to deliver better patient care. This could not be done without also insuring the protection of Protected Health Information (PHI).

Fortra™'s Digital Guardian® for Cloud Data Protection with Box provided the solution that has been in production since August, 2014.

This paper describes the cloud data protection challenges of a leading healthcare organization, the methodology employed in implementing this solution and the benefits that have been gained. It is addressed to healthcare systems that may be evaluating an investment in cloud technology for scalability, cost reduction or improved collaboration.

Hospital Mandate: Share Information Anywhere

Top executives at a leading edge healthcare institution foresaw how patient care and solutions would be delivered in the future. In this world, connectivity needs to be provided to share information "across settings, sites and devices," as one top hospital executive put it.

The cloud provides cost economies from shared resources and can facilitate easier access to information when and where it is needed. If security requirements could be met, the cloud would present an excellent opportunity to enable collaboration between the healthcare organization's multiple internal centers and business associates as well as with external care providers, research personnel, and patients.

First, it was necessary to make sure that the cloud solution would be secure and meet regulatory requirements. "We want to share Protected Health Information (PHI) within the organization but make sure we aren't sharing it outside," a hospital executive stated.

HIPAA / HITECH Regulations

As both a healthcare provider and a medical school, this institution maintains PHI on patients in its care as well as research materials from other sources that may contain additional PHI. This information is required to be contained and managed according to the dictates of the US Health and Human Services regulatory agencies.

Health Insurance Portability and Accountability of Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) regulations require that, whether data is encrypted or not, the organization must know where patient Personally Identifiable Information (PII) is stored or sent. Encryption, alone, is not enough to meet the necessary standards or to provide the visibility required to govern this type of sensitive data.

Enterprise DLP

Enterprise Data Loss Prevention (DLP) solutions play a key role in addressing sensitive data protection requirements to help healthcare organizations comply with the various HIPAA and HITECH requirements.

Enterprise DLP is defined by Gartner as "providing tools enabling the dynamic application of policy based on the content and context at the time of an operation. These tools are used to address the risk of inadvertent or accidental leaks, or exposure of sensitive enterprise information outside authorized channels, using monitoring, filtering, blocking and remediation features."

Enterprise Data Loss Prevention (DLP) technology has been deployed successfully in the healthcare industry for more than a decade to provide necessary discovery and management tools for PHI and other private or sensitive data inside an enterprise. During this time a high degree of familiarity and a body of best practices has been established that maximize the effectiveness of these solutions.

However, many DLP vendors have been slow or lacking altogether in modifying their offerings to work effectively in the cloud.

Casb Solutions

Recently developed cloud-centric solutions from Cloud Access Security Brokers (CASB) typically provide gateways that inspect information entering or leaving the cloud (in email or web transactions for example), but do not offer either the level of accuracy or the ease of use required by this healthcare institution. Nor are these offerings designed to support broader Data Loss Prevention coverage across an entire enterprise network.

Box And Digital Guardian – A Unique Solution

Box provides a single facility with which individual users can easily store, retrieve and share their information. Digital Guardian operates transparently and without disruption to the Box user experience.

Digital Guardian provides a proven healthcare DLP solution that extends to the cloud. This solution provides the means to move, encrypt, or execute other remediation before PHI can be shared outside the organization or in any manner contrary to institution policies.

Cloud Data Protection - Transparent Operation

Box provides a user interface that is demonstrably simple to understand and easy to use. Users can share and collaborate with-out a Virtual Private Network (VPN); there are no new user names or passwords to remember; and the user can determine with whom they want to share their files and what level of access they want to provide no matter what device they are using.

Digital Guardian Cloud Data Protection operates seamlessly within the easy to use Box environment and doesn't impact end user productivity. No end user training on the tool is required.

Once the institution's information sharing policies are entered into the system, users who follow the prescribed security policies will not be aware of Digital Guardian's presence. However, when PHI policies are not followed the user will be notified of the violation and the resulting automatic remediation action that was taken.

Cloud Data Protection - Extends A Proven Capability

DG's Cloud Data Protection extends its proven Enterprise DLP control over the entire network to now include the cloud. This capability was developed by Digital Guardian in consultation with Healthcare organizations, Electronic Health Record (EHR) providers, cloud storage developers and has been in production since August, 2014.

Cloud Data Protection - Proven Accuracy & Performance

Digital Guardian for Cloud Data Protection harnesses the unique technologies to meet the high accuracy and performance requirements for controlling PHI in Healthcare environments:

- Database Record Matching™ (DBRM™),
- Event Based Scanning

Both are essential to the success of this solution.

The Superiority Of Database Record Matching

Digital Guardian's DBRM™ technology is an advanced detection method using the actual data records themselves to develop the fingerprints used in discovering and inspecting of emails, file shares, the cloud, web postings or anywhere that information would be problematic (and the organization would be out of compliance) if this PHI data was found there. Digital Guardian DBRM™ technology is applied in this case by utilizing the institution's actual Electronic Health Records (EHR) to fingerprint their PHI data. This capability provides the highest degree of accuracy in identifying PHI. Using this method of finger printing while the actual EHR remains safely behind the firewall is a crucial component for both compliance and to provide the accuracy and speed required by this institution.

Pattern matching methods, employed by many new cloud centric, CASB offerings, were judged not sufficient in this health care environment. Medical Record Numbers (MRN) or Medical Insurance policy numbers, for instance, often don't follow the same format across institutions, leading to an array of different possible formats. Some of these MRN's are numeric, some are alphanumeric and they can differ in length and context. Therefore, pre-built pattern matching solutions can require significant tailoring to produce somewhat reliable results and still not be as accurate. In contrast, DBRM, by its nature, easily provides an extremely accurate means to detect an actual MRN in all inspected alphanumeric forms.

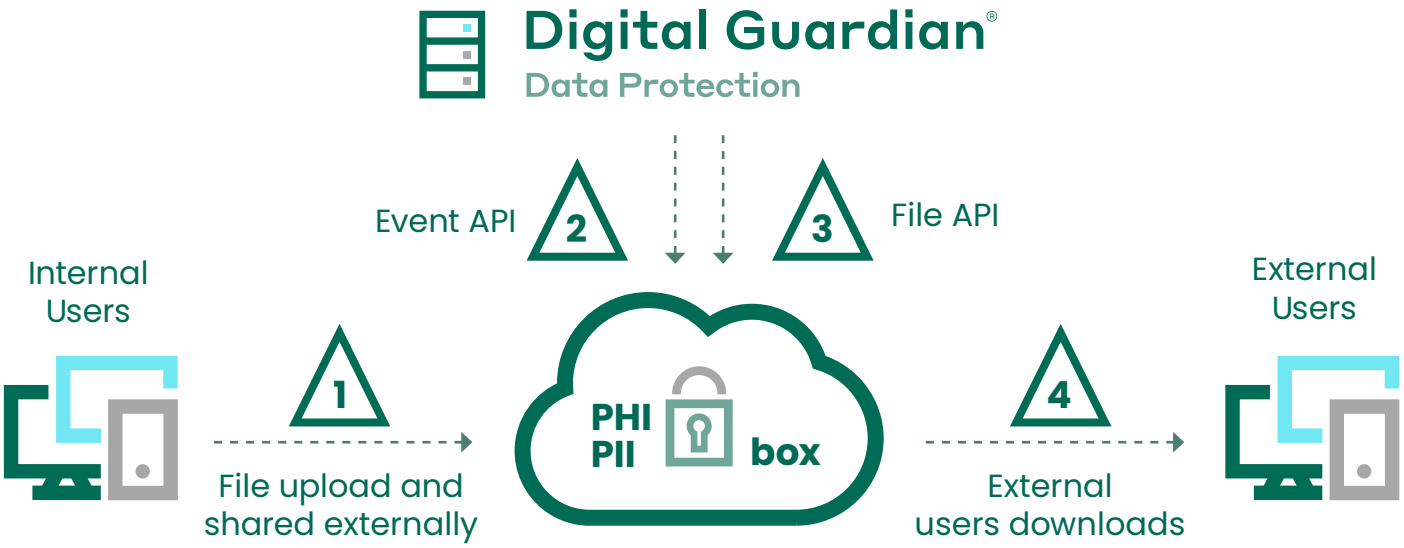
Other methods evaluated by this healthcare institution that were used to find sensitive information were found to have a high rate of false positives and false negatives leading to higher staffing costs, and often resulted in drawn-out implementations that don't lead to accurate, actionable detection. The methods most commonly employed are usually combinations of pattern matching (e.g., looking for 9 digits in the usual SSN xxx-xx-xxxx format) or dictionary matching (e.g., looking for specific words such as medical diagnosis names). Unfortunately, these methods will present a trade off to users forced to choose between: a) wading through a sea of false positives, or, b) allowing more false negatives in order to avoid getting overwhelmed with manual inspections. Organizations will commonly opt to not spend time manually weeding out false positives and, instead, simply accept failing to identify significant instances of regulated information.

Many compliance solution vendors have simply chosen to err on the side of accepting false negatives in order to reduce the burden on the user to have to check false positives. Their logic being that many organizations handling PHI will not be aware of, won't see, and, therefore won't complain, about, false negatives – until such time as a loss of data becomes public.

The Superiority Of Event Based Scanning

Digital Guardian DLP solution is not dependent on scheduled scans at a specific point of time, although that is an option. Scheduling a scan for PHI content every evening may be a common approach for managing files within the enterprise network. However, for their cloud storage, this healthcare organization determined that scanning for the removal of PHI from shared files was required to occur within specified time intervals measured in seconds in order to mitigate the risk as determined by the organization's compliance team assessment. As a result, every change to the files triggers an event to be inspected. Data will be inspected and remediation will take place at the frequency specified, in this case, currently 60 seconds.

Implementation Details - How The Solution Works



1. When a file is uploaded for external sharing, an event is generated.
2. DG Cloud Data Protection scans the files for event activity at the specified time interval.
3. DG Cloud Data Protection reviews the new content against policy instructions for external access, takes appropriate action (ignore | audit | report | alert | move | remove) and remediates the information accordingly.
4. External users access information, business as usual, as permitted by policy.

Event Based Scanning is implemented using the Box API set. Digital Guardian Cloud Data Protection monitors and protects PHI without impact to end user interaction. This provides the highest degree of performance in discovering and dealing with PHI when it should not be shared.

In this case, the institution created one folder for each user that can be shared with the other centers as well as identified partners (e.g. insurance providers, pharmacies, other universities-that meet the required security requirements)—these folders are not allowed to contain PHI. Digital Guardian Cloud Data Protection scans these folder/files for PHI whenever an event dictates. If PHI is discovered the file is immediately moved back to a folder that does not have the capability to be shared.

In audits of system performance to date, over 99% of the notifications that a file was moved do not generate a user objection or request for explanation. This is confirmation that the solution meets the extremely high discovery accuracy required to adequately protect PHI.

Benefits Of Secure Collaboration

The Box and Digital Guardian solution provides a means to facilitate collaboration, data exchange, and improved workflow within and outside the institution from research to the delivery of patient care. These benefits are possible only because the organization is confident that PHI is being protected and not inappropriately shared. Among the use cases this world class organization is seeing for this cloud based solution are:

- Sharing current studies or intellectual property among faculty, staff and researchers.
- Exchanging information while caring for patients or billing and accepting payment for care.
- Coordinating care between teams in a variety of locations. Easily handing off files from one medical professional to another.
- Providing access to journal archives, articles currently in development and the status of grant projects.
- Delivering personalized content directly to patients allowing patients to consume, interact with and assemble follow up questions for care teams.
- Sharing research, organizing, adding comments, assigning tasks.
- Delivering continuing medical education.
- Accessing learning materials, videos, publications, and case discussion using tablets, mobile phones, or laptops.
- Providing quick, secure access to critical information on any device—perhaps in an exam room, an office or even at home.
- Enabling collaboration seamlessly on any device while files containing sensitive data stay secure.
- Scanning all files before they are uploaded to cloud storage for confidential or regulated data will ensure HIPAA compliance.
- Performing remediation based on potential risk provides the organization with maximum flexibility. Alerting an administrator, alerting a user, moving the potentially sensitive file to a more protected folder, changing file properties like disabling external file sharing, or removing the file from cloud storage are some of the options available.

Mandate Archieved: Secure, Compliant Cloud Sharing

This healthcare organization's goal was to deliver optimal patient care by utilizing the latest cloud technology and still remain in compliance with all HIPAA regulations. They wanted and got a solution that would allow them to share, manage and use information on any device, anywhere and do it securely.

Digital Guardian Cloud Data Protection allows this organization to adopt cloud storage without giving up visibility and control required by today's regulatory environment. All files uploaded to cloud storage are scanned for confidential or sensitive information and remediation is automatically applied. This combination of Box and Digital Guardian Cloud Data Protection has allowed this world class medical facility to meet its goal of secure, compliant cloud sharing.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.