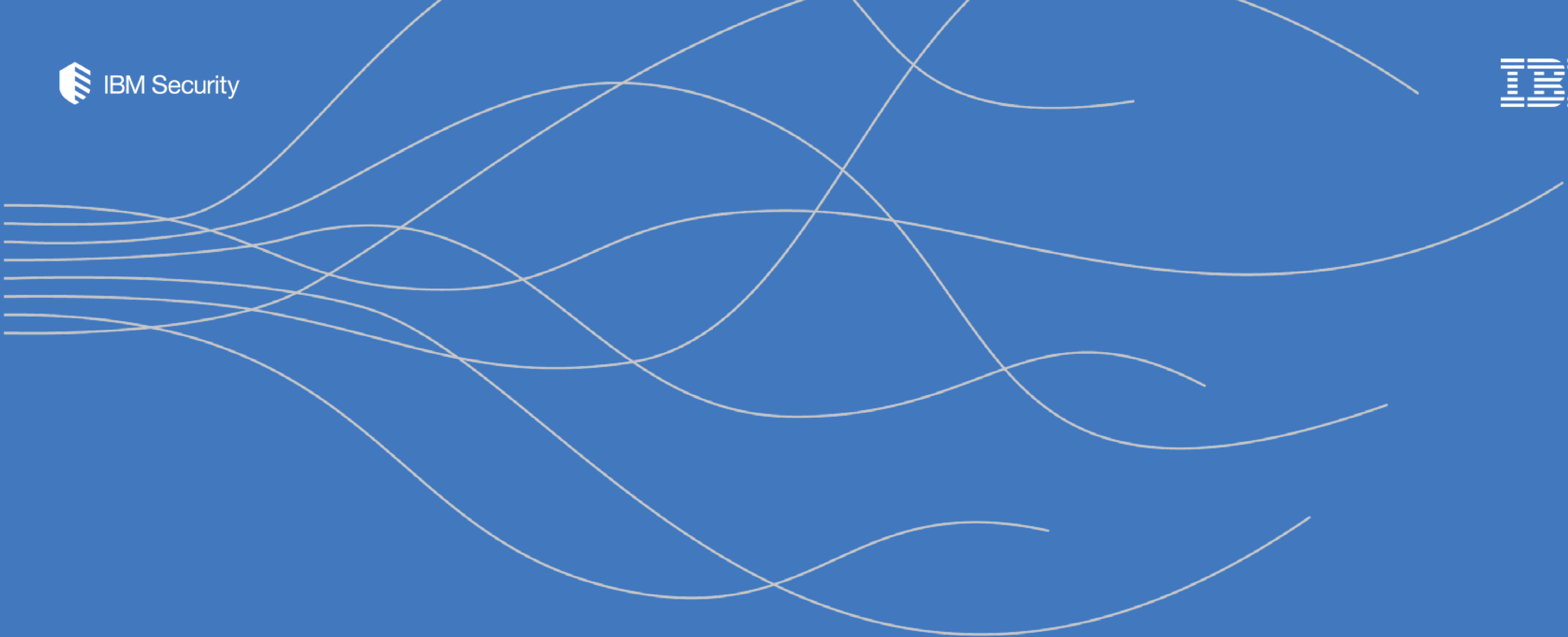
IBM Security



Aggregate, protect, share

New technologies help healthcare systems better protect and manage the imaging deluge

Let’s get started

Contents

Introduction

Medical professionals now store, manage and share far more images than ever before. Thank mobile proliferation in part for the surge. Handheld image-capture devices, smartphones and tablets all allow physicians to snap images at point of care. They also enable patients to take pictures of their bodies to share with their healthcare providers.

New medical applications further contribute to the surge. Once the domain of radiology and cardiology, imaging systems are now used by dermatologists, ophthalmologists, pathologists, plastic surgeons, ER physicians and other specialists. They rely on these images to treat the medical needs of one of the country's largest generation: as 75 million Baby Boomers age, the need for scans will likely increase.

Healthcare CIOs scramble to aggregate, store and share all these images—especially in times of mergers or acquisitions, when they must organize images from multiple medical systems. Traditional healthcare IT infrastructures may hinder this effort: imaging data typically resides in isolated silos, on disparate apps, on individual computers, and even on physicians' mobile devices.

Storing and sharing images, however, is only half the battle. As the number of images being accessed by medical professionals, hospital staff and patients continues to grow, healthcare organizations need a better way to secure images and other sensitive patient data. Unfortunately, the piecemeal nature of many existing healthcare infrastructures can leave data vulnerable to security breaches. This vulnerability can prove disastrous to both patients concerned with their privacy and to the reputation of the affected organization. Healthcare entities must therefore implement more comprehensive, integrated security solutions to help meet compliance reporting mandates.

Securing mobile devices

In addition to protecting databases and files, healthcare organizations often need help protecting the devices used to take or view images. IBM can help protect desktops and laptops with IBM® BigFix® endpoint protection. To protect mobile devices, learn more about IBM MaaS360® with Watson™.

Using technology to help share images, improve accessibility

New technologies can help healthcare systems meet the twin challenges of sharing and securing medical images.

To help facilitate image sharing, IT professionals often turn to centralized data repositories. Web-based access to these repositories can help accommodate physician demand for anytime-anywhere-any device image access. Since these repositories are typically cloud-based, they can also dramatically reduce storage footprints and associated expenses.

The process starts with the deployment of a vendor-neutral archive—or one that can store images created by a variety of applications. Specialized migration software helps find images housed on disparate picture archiving and communications systems (PACS), sites and devices. The software normalizes and consolidates these images, then securely migrates them to a vendor-neutral archive (VNA).

In the VNA, images can be stored in a cross-enterprise document sharing format. Web-based interfaces can facilitate image viewing and sharing. They allow physicians and other medical professionals to access patient images from virtually any web-connected device, at essentially any time or place, including at point of care. This accessibility can facilitate communications and collaboration among healthcare professionals.

As the number of medical images continues to grow, healthcare organizations need a better way to store them.

Robust security for imaging

IBM Security Guardium solutions can be delivered as either software or as hardware appliances with pre-configured physical servers provided by IBM.

The **IBM Security Guardium®** software solution can help protect imaging data and files while automating workflows to help with compliance reporting. The Guardium security platform offers a broad range of capabilities—from discovery and classification of sensitive data to vulnerability assessment and file-activity monitoring. The solution can be integrated with existing systems, databases and applications stored on traditional or cloud servers throughout the healthcare environment

IBM Security Guardium Data Protection for Databases is a software solution that helps organizations protect against internal and external threats by using cognitive analytics to continuously monitor databases. Guardium detects threats, alerts to suspicious activity, works to prevent unauthorized access, and automates internal compliance workflows to get the right reports to the right people at the right time. Policy-based monitoring—covering data access, change control and other user activities—is designed to block access from unauthorized parties in near real-time, with minimal impact on the performance of data sources. Furthermore, the solution audits user activity and generates audit and compliance reports. At-a-glance operational dashboards simplify security management with quick-search capabilities, heat maps, and a drag-and-drop interface.

A companion product, **IBM Security Guardium Data Protection for Files**, provides activity monitoring for confidential images and health files, both structured and unstructured. This capability is particularly important in the imaging arena, which is rife with unstructured data. The solution helps organizations better understand their sensitive data exposure, critical file locations and user groups. IBM Security Guardium Data Protection for Files accomplishes this by providing insight into file system contents and usage patterns, allowing organizations to discover, track and control access to sensitive files and systems. The solution continually scans and analyzes files to proactively detect unusual read-and-write activity—including anomalous behavior such as mass file and directory copy or deletion. Guardium also detects spikes in file access by user, and alerts when monitored files are improperly accessed.

Benefits of protecting imaging data with Guardium

Guardium offers significant benefits to imaging centers, providers and other healthcare professionals and systems using PACS and VNAs to store and share medical images (see Figure 1). Organizations can use Guardium to help identify security risks that might otherwise contribute to a potential or actual breach. For example, the solution is designed to detect security breaches associated with multiple failed attempts to log in to an imaging organization's databases and files. Guardium then has the capability to deactivate associated accounts to help prevent hackers from gaining access.

In addition, the Guardium solution is designed to prevent database access from outside applications and alert administrators of potential intrusions. The Guardium product set can help organizations prevent PHI from being shared with or accessed by unauthorized parties, and support the creation of policies that the customer can map to HIPAA standards. With the Guardium capabilities, healthcare organizations can work towards improving their data protection and regulatory compliance efforts.

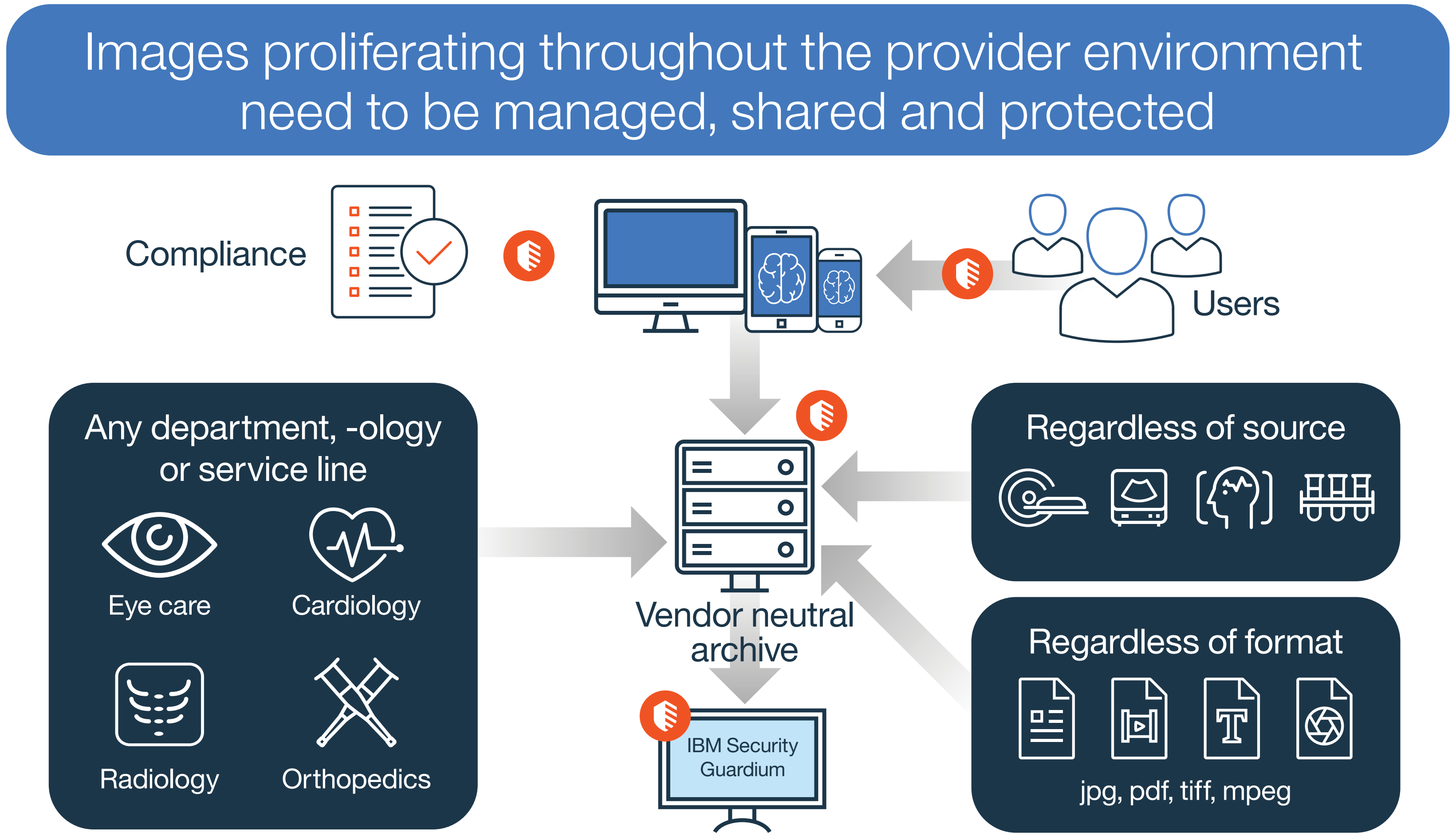


Figure 1. *Guardium solutions help healthcare images to be managed, shared and protected.*

Why IBM?

With more than 8,000 professionals serving 17,500 customers in 133 countries, IBM Security is available to help healthcare organizations protect medical images to facilitate more secure viewing and sharing of those images.

For more information

For more information on how IBM Security can deliver integrated systems of analytics and near real-time defense capabilities to better secure your organization's data, visit our web site: ibm.com/security

Guardium at work in the eye care field

With about 1.8 million patients, MyEyeDr. is one of the fastest growing optometry companies in the United States. The chain offers its patients full-service vision care, plus a wide selection of prescription glasses, contact lenses and sunglasses.

MyEyeDr. needed a better way to protect data across the organization. It also wanted greater visibility into who was accessing what data, and the ability to more quickly correlate and analyze log data. To accomplish this, MyEyeDr. deployed an IBM Security Guardium solution including IBM Security Guardium Data Activity Monitor and IBM MaaS360 endpoint device protection. The solution delivers security insight, intelligence and control across the environment. These capabilities provide MyEyeDr. IT staff with analytical insight needed to help govern data access and to uncover anomalies that may signal a security threat. The company also deployed IBM MaaS360 software to secure mobile devices, so that qualified personnel can access patient data from whatever device they choose.

As a result of implementing this solution, the company reports it is able to more quickly uncover threats to patient data. In addition, automated reporting capabilities help the company accelerate compliance reporting for HIPAA.

Produced in the United States of America
November 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.