

FORTRΔ™

The Definitive Guide To Data Loss Prevention

Healthcare Edition





Table Of Contents

- 03** Why Read This Guide
- 04** Part One: What is Data Loss Prevention
- 07** Part Two: How DLP Has Evolved
- 10** Part Three: The Resurgence of DLP in Healthcare
- 25** Part Four: The Shift to Data-Centric Security
- 29** Part Five: Deploying DLP in Healthcare
- 35** Part Six: Business Case for DLP
- 38** Part Seven: Buying DLP
- 41** Part Eight: Digital Guardian Purpose Built for Healthcare
48 Resources at a Glance



Why Read This Guide?

What's Old Is New Again

As healthcare security professionals struggle to keep up with non-stop threats coming from every angle, a 10+ year old technology, data loss prevention (DLP) is hot again. A number of trends are driving the wider adoption of DLP to protect personal health information (PHI). But as we looked at the resources out there, we couldn't find one source that could provide all the essential information in one place. So we created this guide to provide answers to the most common questions about DLP, all in an easy to-digest format.

How To Use This Guide

If You Are...	Go To...
New to DLP	Part One: What is Data Loss Prevention
Familiar with DLP, but want to learn what's new	Part Two: How DLP has Evolved
Not sure where to start?	Part Four: A Data Centric Security
Looking for DLP deployment best practices	Part Five: Deploying DLP in Healthcare
Making the case for DLP to your board	Part Six: Making the Case for DLP to Hospital Boards
Looking to buy DLP	Part Seven: Evaluating DLP for Healthcare
Interested in Digital Guardian's healthcare experience	Part Eight: Digital Guardian Purpose Built for Healthcare



Part One

What Is Data Loss Prevention?



DLP Defined

DLP Basics

What: In short, DLP is a set of technology tools and processes that ensure sensitive data is not stolen or lost.

Why: Accidental (i.e. employee error) or malicious actions (i.e. cyber criminal breach) put your organization's data at risk.

How: DLP detects and protects your organization's sensitive data by:

- Scanning data in motion, in use and at rest
- Identifying sensitive data that requires protection
- Taking remedial action—alert, prompt, quarantine, block, encrypt
- Providing reporting for compliance, auditing, forensics and incident response purposes



DLP [Data Loss Prevention] is a system that performs real-time scanning of data at rest and in motion, evaluates that data against existing policy definitions, identifies policy violations and automatically enforces some type of pre-defined remediation actions such as alerting users and administrators, quarantining suspicious files, encrypting data or blocking traffic outright.



-451 Research,
*"The Data Loss Prevention Market
by the Numbers," July 2015*

50%
OF ORGANIZATIONS




have some form of DLP in place, but Gartner predicts that will rise to 90% by 2018. (source: Gartner *"Magic Quadrant for Enterprise Data Loss Prevention"*, 1 February, 2016 , Brian Reed and Neil Wynne)



Do You Need DLP?

Take a look at these common situations. If any of them apply to your organization, DLP will almost always make sense.

Corporate Objectives Checklist

Objective	Situation	Check if this applies to you
 Ensure Personal Health Personal Information Protection / Compliance	Your organization can't confidently identify all the places where PHI resides within your healthcare system, consequently you're not sure of your data protection and privacy protection risks.	<input type="checkbox"/>
 Enable Care Provider Collaboration with Secure Sharing of PHI in the Cloud	Your organization wants to enable care providers to share PHI across settings, sites and devices – while still protecting the PHI from breaches.	<input type="checkbox"/>
 Improve Effectiveness of Employee Security Awareness Training	Your organization spends a lot of money on security and compliance training, but it's not resulting in measurable improvements in employee awareness and improved security posture.	<input type="checkbox"/>



CASE STUDY

Compliance:
St. Charles Health System



CASE STUDY

Secure Collaboration:
Renowned HC System



CASE STUDY

Dramatically
Increased Compliance:
Large Managed
Healthcare Provider



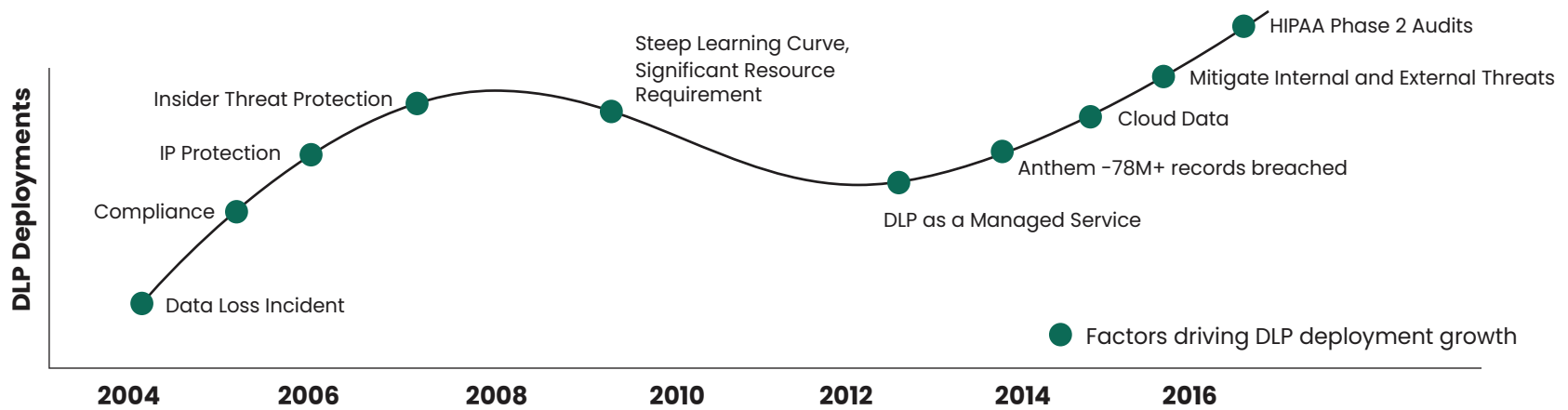
Part Two

How DLP Has Evolved



DLP Back In The Limelight

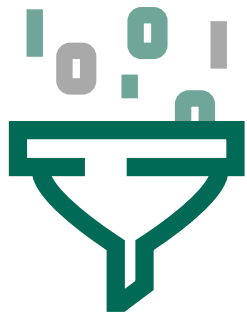
DLP came to market with big interest and bigger expectations. Demand softened as organizations struggled with the cost and complexity of deploying first generation DLP software. The dramatic increase in big breaches, coupled with factors such as DLP as a managed service, DLP functionality





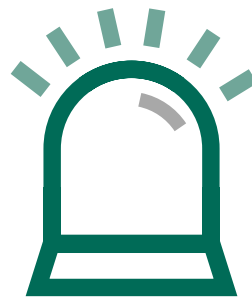
3 Myths Of Data Loss Prevention

Today's DLP is sophisticated, automated and within the reach of more healthcare systems than ever. DLP's history has been one of hype and disappointment, resulting in a few myths that we need to dispell.



MYTH 1: DLP Is Expensive To Deploy, Resource Intensive To Maintain.

Today's DLP options do not require dedicated internal resources to manage and maintain. The introductions of automation and managed security services have eased what was perceived as the "heavy lift" of DLP: hosting, setup, ongoing monitoring, tuning and maintenance. Many implementations can be completed in a single day.



MYTH 2: DLP Is Ineffective, Prone To High False Positives.

Today's DLP uses fingerprinting technology to accurately identify and control PHI. Policies can be set up to trigger only when the SSN of a specific patient is detected in combination with Patient Name or Patient ID. Using actual patient data rather than generic pattern or keyword matching substantially improves accuracy and reduces false positives.



MYTH 3: DLP Doesn't Protect PHI In The Cloud.

Today's DLP enables hospitals to effectively discover, monitor and control PHI, whether on the network, in use on desktops or laptops, at rest on end-user devices and network servers, or stored in the cloud. This means you can now safely adopt cloud storage while maintaining the visibility and control needed to comply with privacy and data protection regulations.



Part Three

The Resurgence Of DLP In Healthcare

A number of trends are driving the healthcare industry's wider adoption of DLP. Let's examine them...



TREND #1

The Healthcare Industry Is A Top Target

The healthcare industry (hospitals in particular) is one of the top industries targeted for cybercrime. Given the high value of a stolen healthcare record, motivated adversaries will continue to go where the money is.

5400%

Growth in number of health records compromised each year from 2011 to 2015.

91%

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

112M

Number of healthcare records lost or compromised in the US in 2015.

253

Number of healthcare breaches in the US affecting 500 individuals or more in 2015.

1 OF 3

 health care recipients will be the victim of a data breach in 2016.

5 OF 8

 of the largest healthcare security breaches over the last five years happened during the first six months of 2015.

(sources: HHS, IBM, IDC, Identity Theft Resource Center)



Healthcare Data Breaches Are Frequent & Large











2015 was a bad year for healthcare data. The size and frequency of breach incidents is growing – a troubling trend. Here’s a roundup of the biggest data breaches last year, by total records lost.



SEE HHS REPORT

Search and sort the full list of breaches of health information, as reported to the U.S. Department of Health & Human Services.

Top 10 Healthcare Data Breaches 2015

Organization	Records Breached	Type of Breach
 Anthem	78,800,000	Hacking / IT Incident
 PREMERA	11,000,000	Hacking / IT Incident
 Excellus	10,000,000	Hacking / IT Incident
 UCLA Health	4,600,000	Hacking / IT Incident
 mie	3,900,000	Hacking / IT Incident
 CareFirst	1,100,000	Hacking / IT Incident
 DMAS	697,586	Hacking / IT Incident
 GEORGIA DEPARTMENT OF COMMUNITY HEALTH	557,779	Hacking / IT Incident
 BEACON HEALTH SYSTEM	306,789	Hacking / IT Incident
 DJO GLOBAL	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)



TREND #2

Stolen Patient Data Is Worth More Than Any Other Data

Medical records are worth up to 10 times more than credit card numbers in resale value on the black market. This has led to an explosion in medical identity fraud. According to a recent Ponemon study, 2.32 million US adults indicated that they or family members have been victims of medical identity theft.

What's in an electronic health record that makes it so appealing to scammers, spear phishers and other cyber criminals? It's the depth and breadth of information they contain – from card data to date of birth, email addresses, social security numbers, employment information and medical history.

What's more, healthcare data has a longer shelf life than personal financial data. Healthcare fraud may go undiscovered by a patient or their provider for months or years, giving criminals longer to monetize patient information.

Medical identity fraud takes the form of either fraudulent billing by unethical providers or misuse of another person's medical records to obtain care – such as prescription drugs.

(sources: Verizon Data Breach Investigations (VBDIR) Report 2015; Ponemon Institute's "2015 Annual Study: U.S. Cost of a Data Breach"; PWC "The Global State of Information Security® Survey 2016")

\$363

Average cost of a lost/stolen data record for healthcare companies

\$154

Average cost of a lost/stolen data record for other organizations

136% HIGHER

than the global average cost of a non-healthcare related data breach per lost or stolen record

What's The Value Of A Stolen X-Ray?

MORE THAN YOU'D THINK

Did You Know?

Cyber criminals are interested in all kinds of health data. A recent data breach incident at Beth Israel Deaconess Hospital in Boston revealed how varied and complex the market for stolen PHI is.

Beth Israel's CISO revealed that even stolen medical records like chest x-rays have incredible monetary value to sellers with access to the right black market forums. A malware attack on an unpatched medical records server nabbed 2,000 patient x-ray images and downloaded them to a system in China.

Why x-rays? An image of a clean lung can be resold to Chinese nationals with infectious lung diseases such as tuberculosis so that they can obtain visas to travel outside the country – making x-rays a valuable commodity.

**A chest x-ray can
be resold to Chinese
nationals with TB
so that they can
obtain a visa**



**SEE OUR
BLOG**

To learn more, read What's The Value of a Stolen Chest X-Ray? More Than You'd Think on our blog



TREND #3

Insider Threats Are Growing

Employees May Be Your Biggest Risk

Because of the high value of medical records, the threat of insiders stealing and selling health information has gone up dramatically.

An “insider” is anyone who has physical, logical or remote access to a company’s EHR systems and PHI databases. In 2015, IBM’s CyberSecurity Intelligence Index revealed that 55 percent of attacks across all industries were carried out by someone who had insider access to an organization’s systems. That includes threats by malicious insiders as well as by inadvertent actors.

Profiles of malicious insiders include the disgruntled employee, a user seeking financial gain, or trusted third-party providers who have been granted insider access. Inadvertent actors include employees who fall prey to social engineering schemes, letting in an outside attacker.



55%

of all breaches in 2015 were carried out by someone with insider access



Messing With Texas

TWO DISGRUNTLED EMPLOYEES VIOLATE HIPAA PRIVACY RULES.



**Children's
Medical Clinics**

A staff member at Children's Medical Clinics of East Texas engaged in widespread theft of patient data, including taking screenshots of some patient records while taking others home. The information was provided to a former co-worker who was engaged in a dispute with the clinic, intending to aid the disgruntled employee's retaliatory agenda. The clinic notified the police. A subsequent search of clinic log files revealed that the employee in question had been improperly accessing patient health information. Potential exposure reached 16,000 patients of Texas pediatric clinics. It is not clear what – if anything – was done with the data.

The incident underscores the difficult challenge faced by care providers, who must provide access to patient information to a wide range of staff, but are also bound by the federal HIPAA regulations to protect that data from inadvertent exposure. According to the resulting lawsuit, the malicious insider who stole the data was authorized to access it and had received HIPAA training. Nevertheless, forwarding that information outside the clinic was a violation of HIPAA privacy rules.



**SEE OUR
BLOG**

To learn more, see Pediatric Clinic Breach affects 16,000 in Texas, Underscores Insider Threat on our blog



TREND #4

Health Data In The Cloud

There Are 3 Factors Contributing To EHR And PHI Data Migrating To The Cloud

1. Software as a service (SaaS) solutions allow a growing number of healthcare organizations to lower costs and improve efficiency by hosting applications and data in the cloud.
2. Health information exchange (HIE) systems, which allow for the mobility of healthcare information electronically across distinct systems, are increasingly cloud-based. A variety of US federal and state incentive programs strongly encourage their adoption and use.
3. Healthcare providers are migrating EHR/PHI data to personal cloud storage. Many cloud service providers now offer specific agreements and commitments covering HIPAA compliance.



HEALTHCARE CASE STUDY

Enabling Secure Cloud Collaboration

SITUATION: A world-renowned hospital system wanted to use the cloud to quickly and easily – but securely – share PHI across its worldwide network.

SOLUTION: They selected Fortra™'s Digital Guardian® for Cloud Data Protection and Box. Because Digital Guardian integrates directly with the Box API, the hospital could extend their DLP policies to the cloud in a way that was completely transparent to their care providers. No end-user training was required. No need for the care providers to log into a Cloud Access Security Broker.

The healthcare institution's multiple campuses, external care providers, research personnel and patients can now securely collaborate for patient care. Meanwhile, Cloud DLP ensures that PHI can't be shared in any manner contrary to institutional policies.

RESULTS: The hospital's mandate for secure, compliant cloud sharing has been achieved. PHI is protected and not inappropriately shared. The solution improves collaborative workflow within the institution and beyond – from research to patient care delivery. The institution has adopted cloud storage without giving up visibility and regulatory control.



PHI in the cloud is accurately discovered and protected with automatic remediation according to hospital policy.



**MORE
INFO**

Read the in-depth case study



TREND #5

Providers Pay For 3rd Party Insecurity

The security of third-party firms that manage health data is a growing issue for healthcare firms of all sizes. There have been multiple incidents of leaks of patient data that were the result of third-party compromises by trusted third parties such as partners, clients and maintenance contractors.



The compromise of Indiana-based EHR vendor Medical Informatics Engineering affected some 4 million patients of 230 hospitals, doctors' offices and clinics.



When insurers denied its claim Cottage Health was held responsible for a \$4 million loss caused by its vendor INSYNC Computer Solution's lack of data protection.



**READ
THE BLOG**

A Hospital and Its
Technology Partner
Share \$90k HIPAA Fine



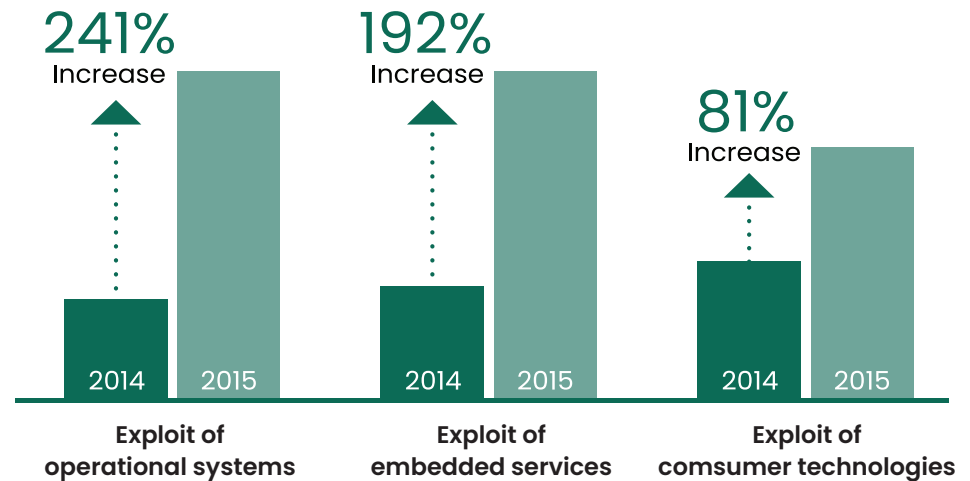
TREND #6

Connected Medical Devices Are Under Attack

The healthcare segment of the Internet of Things (IoT) revolution is forecast to reach \$117 billion by 2020. The sheer number of IP connected devices in hospitals or patients' homes – ventilators, drug infusion pumps, external defibrillators, insulin pumps, patient monitors – continues to grow exponentially.

IoT proliferation is a security challenge for healthcare. Researchers have been uncovering vulnerabilities in these devices, many of which play a vital role in supporting or sustaining life. Remote attackers could modify critical settings or device firmware with disturbing real-world consequences: drug pumps reprogrammed to deliver incorrect dosages, such as injury or even death.

Manufacturers have built medical devices to do specific jobs and be resilient, but not resistant to attack. Most have no built-in defensive measures, leaving them wide open to compromise. Attacks on IoT components skyrocketed from 2014 to 2015. When these devices are connected to the internal network of a medical facility, attackers can gain a nice foothold for other, more financially motivated exploits.



Time to Stop the Bleeding on Medical Device Security



Unsecured Medical Devices Could Really Cost You



Lahey Hospital & Medical Center

Lahey Hospital and Medical Center agreed to pay \$850,000 for losing data on just 600 patients. That works out to more than \$1,400 per record. The cause? Weak security controls over medical devices.

It is believed to be the first case of HIPAA violation concerning the security of a medical device in a hospital setting. Most suits to date have been linked to either stolen/lost employee laptops or patient data stored in electronic health record (EHR) systems.

Lahey is a Boston area medical facility that first reported a laptop stolen from an unlocked treatment room. The laptop operated a portable CT scanner and produced images for viewing. It contained the PHI of 599 patients.

The investigation noted a wide range of violations including failure by the hospital to conduct a thorough risk analysis, an absence of both physical and logical safeguards for the workstation, no ability to track user identity, and poor policies and procedures to safeguard PHI on laptops used with diagnostic and laboratory equipment.

HHS is sending a loud message to other hospitals to secure their medical devices and related clinical or diagnostic systems.

\$850,000

for losing data on just 600 patients



SEE OUR BLOG

To learn more, see Latest HIPAA Settlement Underscores Medical Device Risk on our blog



TREND #7

The Security Talent Shortage Is Here To Stay

Cybersecurity has become a big business. As a result, it's become an IT specialty in which organizations can't find qualified practitioners fast enough to address the growing threats. Maybe you've already felt this pinch in your IT group. As an organization, you should be betting that this trend continues, because the security talent shortage is not going away anytime soon.

209,000

Number of cybersecurity jobs in the U.S. that remained unfilled at the start of 2016.

74%

Rise in the number of job postings over the past 5 years.

ONE MILLION

Number of cybersecurity job openings worldwide, a backlog that could take up to 20 years to fill.

53%

Growth in demand for information security professionals expected over the next 2 years.

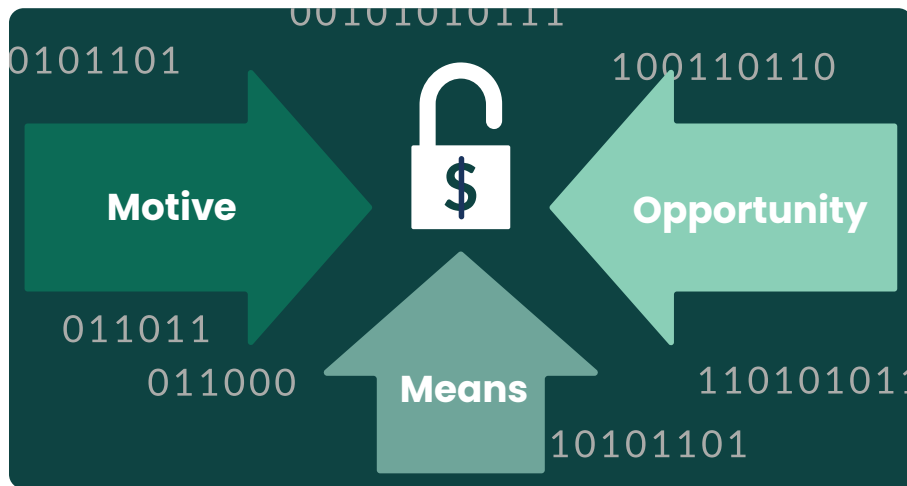
6 MILLION

Number of information security professionals needed globally by 2019, with a projected shortfall of 1.5 million.

(sources: Forbes; Stanford University analysis of Bureau of Labor Statistics; Cisco 2014 Annual Security Report; Bureau of Labor Statistics; Cisco)



Anatomy Of A Data Breach



MEANS Tools, resources and skills provide adversaries the capability to dominate the Kill Chain, while remaining undetected.

MOTIVE State Sponsored: Acquire intelligence for military, political or economic advantage. Cyber criminals: Make money using any means necessary. Hacktivists: Promote their political agenda.

OPPORTUNITY Timing and knowledge of the target increases the chances of a successful intrusion. Attackers leverage this information to achieve their objectives.

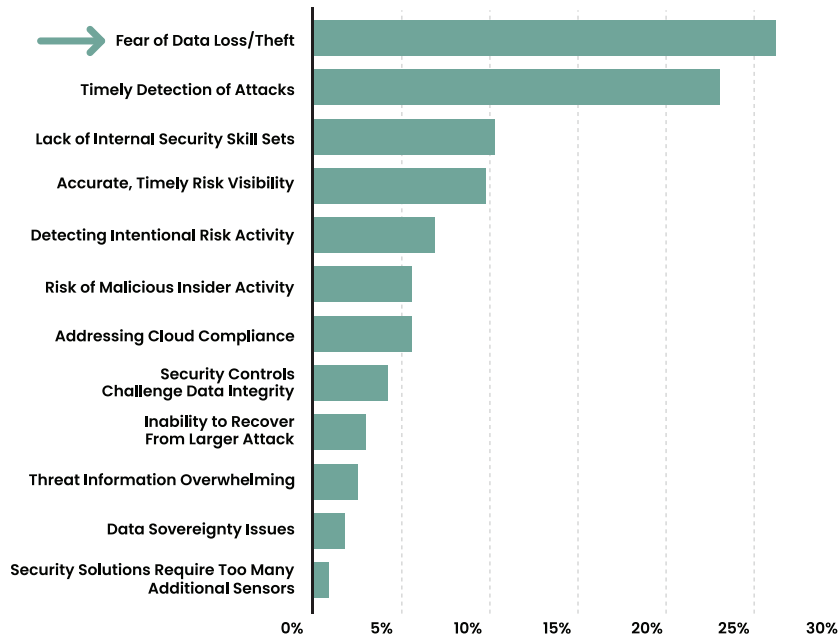


DLP By The Numbers

“Fear Of Data Loss Or Theft” Ranked As The Top Security Challenge Over The Next 12 Months...

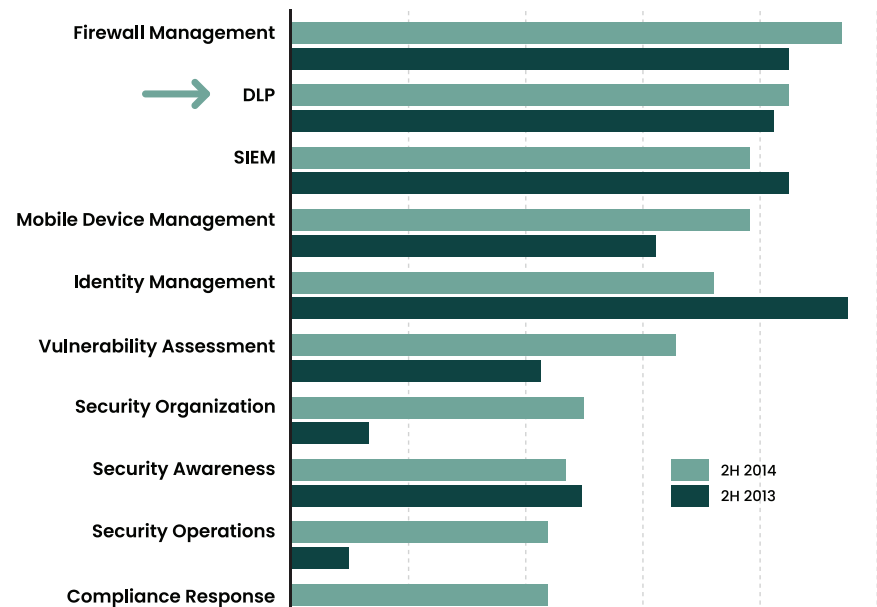
Biggest Security Challenge—Next 12 Months

Q: What is your top information security challenge for the next 12 months?



DLP Ranked #2 Among Planned Information Security Projects Across More Than 20 Categories...

Information Security Projects—Top Categories



To learn more, download the 451 Research report, "The Data Loss Prevention Market by the Numbers," 2015



Part Four

The Shift To Datacentric Security

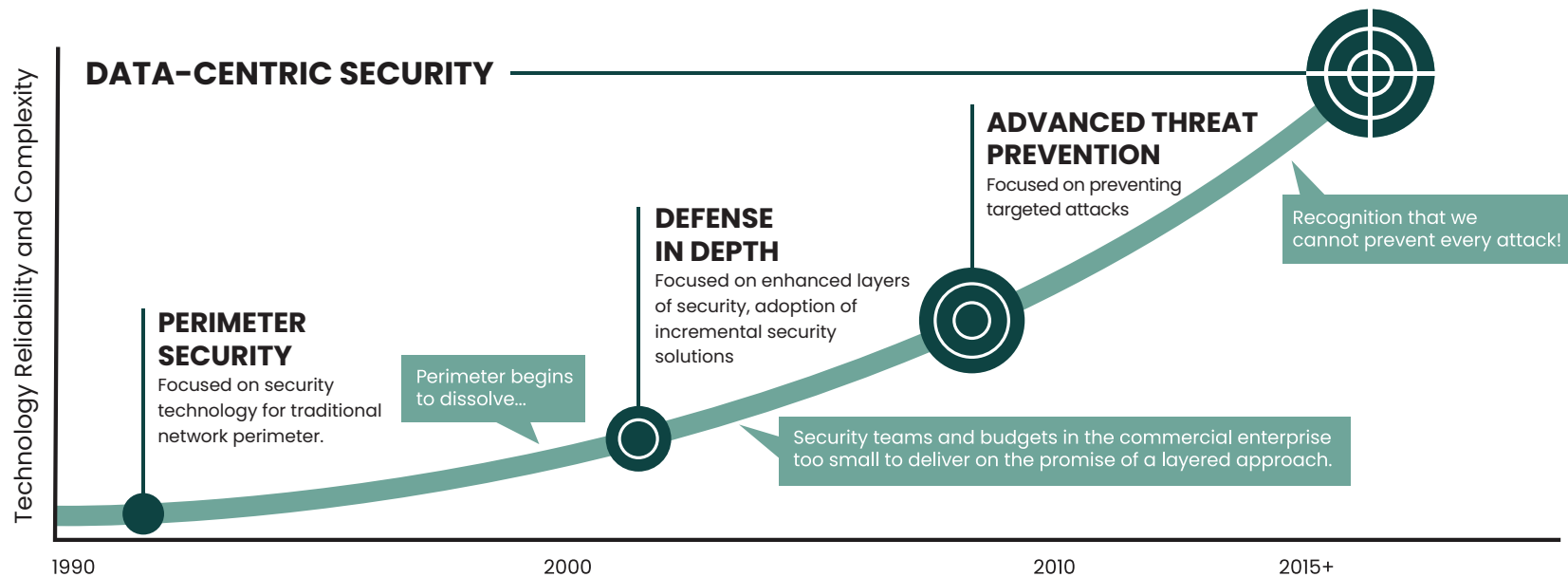
“S&R pros must take a data-centric approach that ensures security travels with data regardless of user population, location or even hosting model.”

–The Future Of Data Security And Privacy. Growth And Competitive Differentiation, Forrester Research, Inc., July 10, 2015



All The Trends Lead To Data-Centric Security

The Security Paradigms That Served In The Past Must Evolve



Simply stated, DLP is the foundation for data-centric security.



“

In this new reality, traditional perimeter-based approaches to security are insufficient. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model.

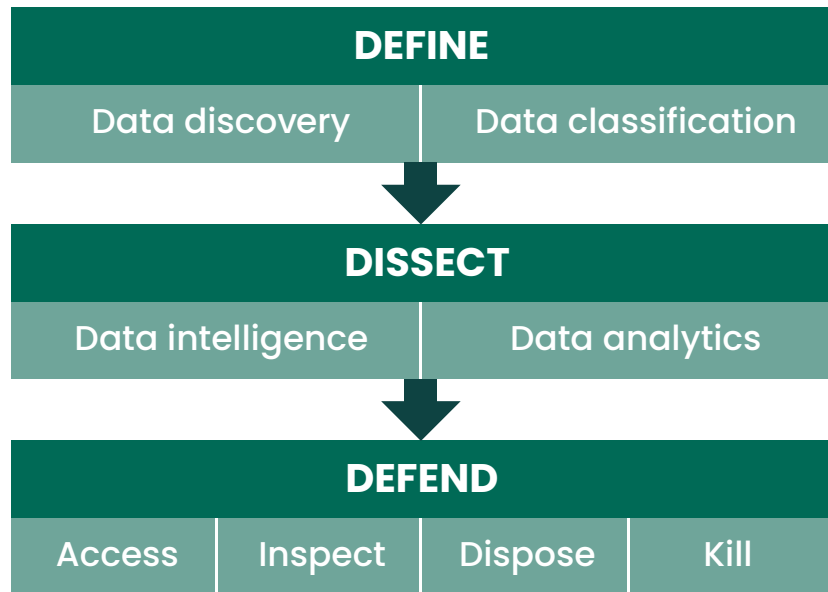
”

(source: The Future Of Data Security And Privacy. Growth And Competitive Differentiation, Forrester Research, Inc., July 10, 2015)



A Data-Centric Security Framework

Many organizations need help getting started. Forrester has created a framework to guide you on this journey. Their “Data Security & Control Framework” (figure below) breaks the problem of controlling and securing data into three steps: Define, Dissect, Defend. With these steps completed, organizations better understand their data and can allocate resources to more efficiently protect critical assets.



DEFINE: This involves data discovery and data classification.

DISSECT: This involves data intelligence (extracting information about the data from the data, and using that information to protect the data) and data analytics (analyzing data in near real-time to protect proactively toxic data).

DEFEND: To defend your data, there are only four levers you can pull – controlling access, inspecting data usage patterns for abuse, disposing of data when the organization no longer needs it or “kill-ing” data via encryption to devalue it in the event that it is stolen.



To learn more about data-centric security, get Dan Geer's "5 Myths Holding Your Security Program Back" eBook



Part Five

Deploying DLP In Healthcare



How DLP Can Help Meet More Stringent HIPAA

With HHS dramatically stepping up HIPAA enforcement, including the broader Phase 2 audits, it's more important than ever to make sure you have the right people, processes and technology in place.

	HIPPA Statute	How DLP Helps
1	164-306, Security Standards, Confidentiality	Detects and prevents PHI from being transmitted via email, networks, USB devices or DVD/CD media. Secures unencrypted PHI found on workstations, laptops or file shares
2	164-308, Administrative Safeguards, Risk Analysis	Continuously scans all network traffic destined for the internet to identify and block external transmission of unencrypted PHI. Determines if storage locations have proper controls. Prevents copying.
3	164.312, Technical Safeguards, Access Policies and Procedures	Discovers and safeguards unencrypted PHI on systems such as file shares, workstations, laptops, servers and databases.
4	164-312 (e)(1), Technical Safeguards, Transmission Security	DLP audits and detects unencrypted PHI leaving an organizations network via email, HTTP/HTTPS or any other protocol.



4 Ways DLP Can Help You Meet More Stringent HIPAA Compliance



Ransomware Infections Are Reportable Under HIPAA

New Guidance From The Office Of HHS Health And Human Services Says That Ransomware Infections Affecting Health Information Are Breaches That Must Be Reported Under HIPAA.

“When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired,” HHS said in its guidance. Looked at simply: “individuals have taken possession or control of the information,” HHS wrote. That constitutes a ‘disclosure’ not permitted under the HIPAA Privacy Rule.”

Healthcare organizations are asked to do in-depth incident response and use the data collected in that process to help answer questions about whether covered patient data may have been misused. Among the factors to consider: the exact type and variant of malware discovered, the “algorithmic steps undertaken by the malware,” and communications made by the malware including “exfiltration attempts” between malware and the command and control servers that stand behind most malware. Organizations should consider whether the malware propagated to other systems, potentially affecting additional sources of electronic PHI (ePHI).

“Correctly identifying the malware involved can assist an entity to determine what algorithmic steps the malware is programmed to perform. Understanding what a particular strain of malware is programmed to do can help determine how or if a particular malware variant may laterally propagate throughout an entity’s enterprise, what types of data the malware is searching for, whether or not the malware may attempt to exfiltrate data, or whether or not the malware deposits hidden malicious software or exploits vulnerabilities to provide future unauthorized access, among other factors,” HHS advises.



**SEE OUR
BLOG**

To learn the circumstances under which covered entities don’t have to follow through with a breach notification.

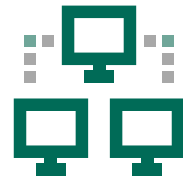


4 Stage DLP Road Map



DISCOVERY DLP

Start with Discovery DLP to identify everywhere PHI is located. Discovery DLP proactively scans your network, including laptops, servers, file shares and databases to deliver a comprehensive analysis of where PHI resides and where you're most at risk. Most data discovery solutions require an agent installed on the device being scanned.



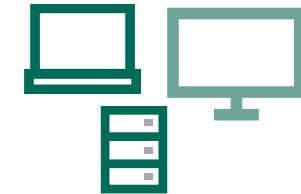
NETWORK DLP

Network DLP is the foundation for data protection in healthcare systems. Network DLP inspects all network traffic - including email, Web, File Transfer Protocol, Secure Sockets Layer - then enforces policies to ensure PHI doesn't leave your network. Deployment is typically easier than endpoint DLP. A physical or virtual appliance is configured for network traffic to pass through for inspection. Policy based actions include: allow, prompt, block, encrypt, reroute, and quarantine.



CLOUD DLP

Cloud DLP enables your organization to adopt cloud storage while maintaining the visibility and control you need to comply with data and privacy regulations such as HIPAA. Cloud DLP scans cloud storage repositories and delivers an accurate picture of what PHI and other sensitive data is in the cloud. Cloud DLP sees PHI as it is being put into the cloud and can perform a cloud storage audit or remediation. It is typically deployed via API integration with the cloud storage providers.



ENDPOINT DLP

Endpoint DLP gives you greater visibility into how PHI is used on the endpoint, and controls egress of PHI to USB devices. Endpoint DLP uses purpose-built software agents that are installed on laptops, desktops, servers and communicate with the management console. Deployment involves installing the agent on machines where protections is desired.



A Proven PHI Protection Framework

Done right, DLP provides the foundation for a straightforward compliance framework that combines people, processes, and technology to prevent breaches.



First Stage: Analyze & Control Risks To Regulated Data

Compliance and protection start with understanding your risks. Deploy Network DLP to identify, analyze and control risks to regulated data such as PII, PHI, PCI.

Discover, monitor and control PII/PHI/PCI that is being:

- Emailed out of your organization
- Transferred out of your organization in unencrypted FTP
- Copied to USB devices or burned to CDs or DVD
- Uploaded to the cloud

Second Stage: Train Employees On Security Policies In Real Time

Employees are your biggest risk. Use DLP to prevent user actions that put your organization's data at risk and educate users in real time on the appropriate handling of regulated data.

If a user potentially violates a policy:

- Display prompts
- Request justification
- Educate users with positive reinforcement (Gamification)

Third Stage: Assess & Iterate Security Policies

You can't improve what you don't measure. DLP provides a mechanism to continuously assess, iterate and improve security policies and procedures.

- Regular review of risk and policy enforcement
- Rebuild trending
- Tune classification and policies



HEALTHCARE CASE STUDY

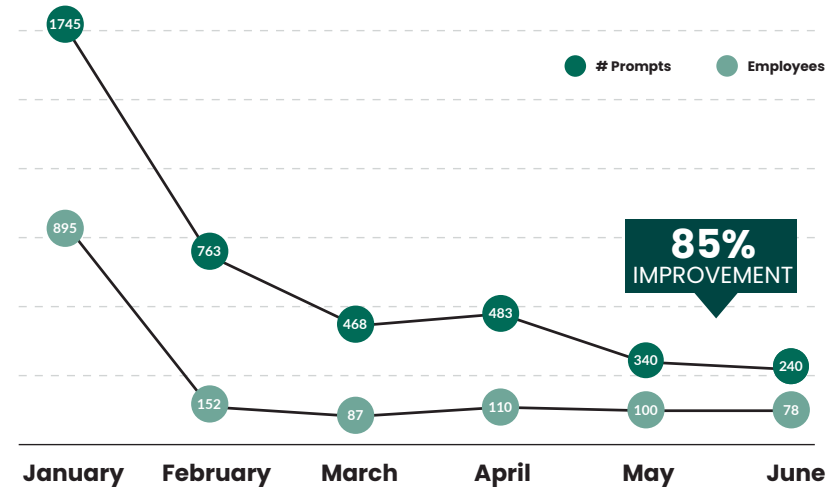
Real-Time Education Drives Security Awareness

SITUATION: The company is one of the largest managed healthcare providers in North America. Despite spending more than \$1M annually on HIPAA compliance training, an internal audit identified a significant risk of non-compliance. The training had failed because it was a specific event not reinforced through ongoing processes. Remote users were not diligent about using the company's VPN, where data protection controls were enforced.

SOLUTION: The company's auditors recommended stricter controls, both on and off the corporate network. The company needed to change user behavior when interacting with sensitive data, reinforce existing policies as data was used, and create a culture that held users accountable for their actions. Digital Guardian helped by enforcing connections through the company's VPN, applying policies in real time based on network awareness, and prompting users who violated data use policies. Users are presented with a prompt screen that requires them to acknowledge the appropriate company policy and provide justification to continue.

RESULTS: Within six months, the healthcare provider reported an 85% decrease in prompts to users, indicating a significant increase in both policy awareness and secure employee behavior.

UNAUTHORIZED TRANSMISSION OF PHI DATA



WATCH A VIDEO

Watch a video on driving security using real-time user



Part Six

Business Case For DLP



Making The Case For DLP To Hospital Boards

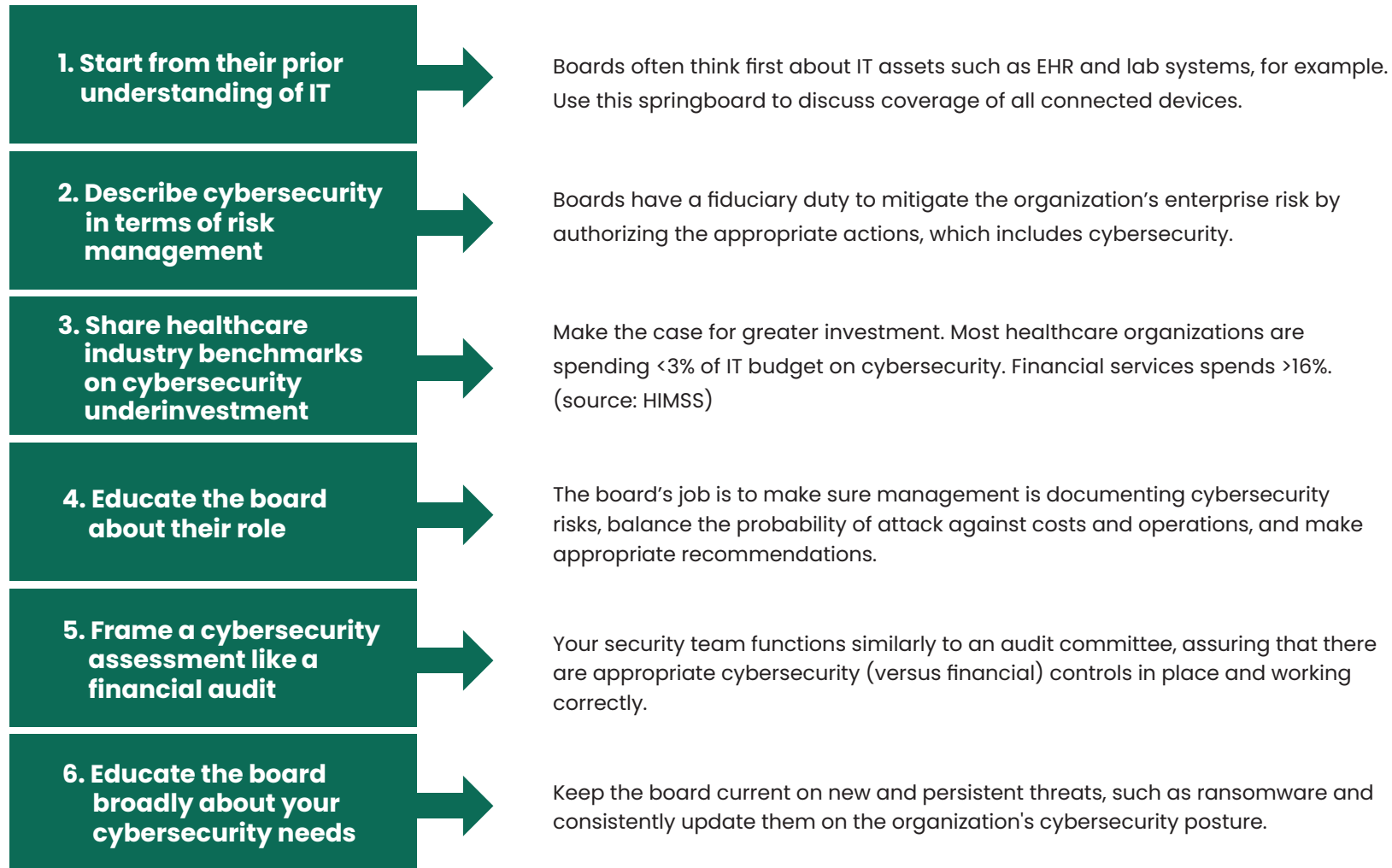
Healthcare cybersecurity is no longer just an IT issue. Management as well as hospital boards need to understand the deeper issues and necessary measures to prevent data breaches.

87%

of healthcare organizations
indicate that information security
is a critical business priority



6 Steps For Making The Case To Your Board





Part Seven

Buying DLP

To guide you in your data protection journey, this section offers some tips and then a detailed evaluation matrix that can serve as a starting point for your decision making process.



How To Evaluate DLP Solutions

Here Are The Steps We Commonly See As Enterprises Evaluate DLP Vendor Solutions

- 1. Research Initial Vendor Set.** Hundreds of vendors offer some form of data protection. We recommend identifying and applying a set of filters to narrow down your organization's choices. One common filter is identifying whether the vendor supports all of your operating environments. Another guide used by many organizations is the Gartner Magic Quadrant report for Enterprise DLP. Peer research is a valuable source of information.
- 2. Reach Out to Vendors with a Plan.** After you create the short list, it is time to contact the vendors. Have a list of use cases or critical business needs. This process can be as structured as you need it to be to satisfy your internal organization.
- 3. Consolidate Responses.** Gather the key stakeholders and seek to build consensus around which vendors have the best ability to solve your problems.
- 4. Narrow Choices Down to Two Vendors.** Based on RFP scores or rankings, you should be able to eliminate all but two vendors that can be engaged for on-site presentation and risk assessment.
- 5. Conduct Pilot Tests.** Request pilots from both vendors, or from a single finalist as selected from on-site meetings.
- 6. Select, negotiate, purchase.** After pilot testing has concluded, take the results to the full selection team. Begin negotiating with your top choice.

Gartner®



Get a complimentary copy of the 2016 Gartner MQ for Enterprise DLP



View webinar recording on 2016 Gartner MQ for Enterprise DLP



Vendor Evaluation Criteria

Here are specific key criteria to consider in healthcare system environments.

- 1. Breadth of Offerings.** Are Discovery, Network, Cloud, and Endpoint all offered with the ability to consistently apply policies?
- 2. EHR Integration.** Can the vendor demonstrate integration with your EHR?
- 3. Deployment Options.** Are on-premises and managed service options offered?
- 4. Deployment.** How long does it typically take to deploy the solution in healthcare systems?
- 5. Management.** How many FTEs are required to manage it?
- 6. Pre-Built Policies.** Does the vendor provide pre-built policies for healthcare environments?
- 7. Healthcare Experience.** How long has the vendor been in the healthcare market? How many healthcare systems have deployed the solution? Can they provide healthcare references that have deployed with your EHR system?



Get the Data Protection
Vendor Evaluation Tool Kit
(includes RFP template and
Vendor Evaluation Scorecard)



Part Eight

Digital Guardian Purpose Built For Healthcare



Why Healthcare Systems Choose Digital Guardian

Digital Guardian believes that data protection products for regulatory compliance are often needlessly complex to implement and difficult to manage, leading to unplanned costs, delays and diminished ROI. Digital Guardian for Compliance has taken a different approach.

**DIGITAL
GUARDIAN IS
DEPLOYED IN
MORE THAN**

100 

HEALTHCARE SYSTEMS

 **FREE
DOWNLOAD**

Digital Guardian for Healthcare solutions sheet

 **FREE
DOWNLOAD**

4 Ways DLP Can Help You Meet More Stringent HIPAA Compliance



HEALTHCARE CASE STUDY

Plug The Leaks

SITUATION: St. Charles Health System (SCHS) of Oregon completed a security risk assessment that found PHI leaking via the Internet and unencrypted email.

SOLUTION: SCHS implemented Digital Guardian's compliance solution for on-going data discovery, data monitoring and blocking. The solution provides DLP protection for all SCHS facilities across 3 hospitals, 20 clinics and nearly 3,000 caregivers. Preloaded with HIPAA-compliant policies, Digital Guardian began returning value immediately after being turned on. "Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away", said Steve Scott, InfoSec Manager. According to Scott, responding to alerts and refining policies, as management identifies new data to be registered, is all that's required from him and his team. He finds himself spending less than 30 minutes a day with the system.

RESULTS: SCHS can effectively enforce regulations while educating physicians, employees and partner providers about risky behaviors. "Our strategy is about changing employee and business associates' behavior through the policies we've set-up. We use Digital Guardian to supervise and reinforce the behavior," said Scott..



Since implementing this DLP solution, we find people are much more careful with the organization's sensitive data. We can give functionality back to our users knowing that our data is being properly handled and protected.



- Steve Scott
Information Security Manager
SCHS



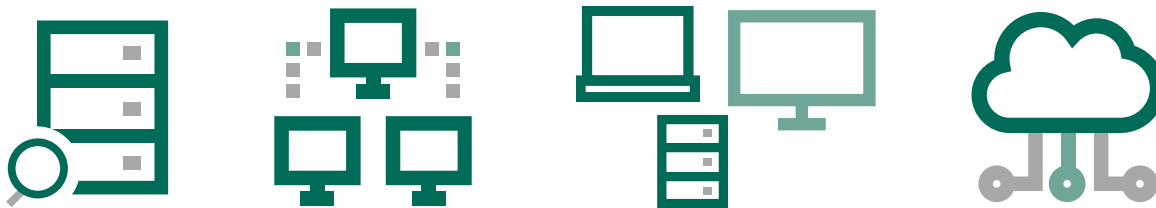
Read the full case study here



DLP On The Network, On Endpoints & In The Cloud

Digital Guardian for Compliance enables healthcare organizations to effectively discover, monitor and control PHI, whether on the network, in use on desktops or laptops, at rest in databases and on network servers – or stored in the cloud.

Our Cloud Data Protection allows healthcare organizations to adopt cloud storage while maintaining the visibility and control they need to comply with privacy and data security regulations.



 **FREE
DOWNLOAD**

Digital Guardian for
Compliance solutions sheet

 **FREE
DOWNLOAD**

Digital Guardian for
Compliance Technical
Overview white paper



The Lowest False Positive Rate

Our Database Record Matching fingerprinting technology is the industry's most accurate for identifying and controlling PHI. By focusing on protecting PHI, we provide hospitals with the absolutely lowest false positive rate of any technology available.

For example, rather than triggering on any 9-digit number, the policy is triggered only by the SSN of a specific patient, and only when detected in combination with the Patient Name or Patient ID. This allows healthcare IT teams to focus on the real risks.



Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away.



- Steve Scott

*Information Security Manager
Saint Charles Health System*



Why Database Record Matching is the Most Effective Method for Protecting PHI white paper



Fully Integrated With The Leading EHRs

Digital Guardian for healthcare is integrated and tested with the leading EHRs.



Digital Guardian for Healthcare solutions sheet



A Leader In The Gartner Magic Quadrant

- “Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported.”
- “The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor...”
- “...Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option.”

Gartner 2016 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016 , Brian Reed and Neil Wynne.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Digital Guardian.

2016 Gartner Magic Quadrant For Enterprise Data Loss Prevention



 **FREE DOWNLOAD**

Gartner 2016 MQ for Enterprise DLP



Resources At A Glance

Title	Type	Link
St. Charles Health Case Study	Case Study	https://info.digitalguardian.com/rs/768-OQW-145/images/case-study-st-charles-healthcare.pdf
Fortune 50 Energy Company Case Study	Case Study	http://info.digitalguardian.com/rs/digitalguardian/images/energy-division.pdf
Jabil Managed Security Program Case Study	Case Study	http://info.digitalguardian.com/rs/digitalguardian/images/Jabil-manufacturing-MSP-case-study.pdf
Breaches Affecting 500 or More Individuals	HHS Report	https://ocrportal.hhs.gov/ocr/bleach/bleach_report.jsf
What's the Value of a Stolen X-Ray? More Than You'd Think	Blog Post	https://digitalguardian.com/blog/whats-value-stolen-chest-x-ray-more-you-d-think
Pediatric Clinic Breach affects 16,000 in Texas, Underscores Insider Threat	N/A	N/A
A Hospital and its Technology Partner Share \$90k HIPAA Fine	Blog Post	https://digitalguardian.com/blog/hospital-and-its-technology-partner-share-90k-hipaa-fine
Time to Stop the Bleeding on Medical Device Security	Blog Post	https://digitalguardian.com/blog/time-stop-bleeding-medical-device-security
Latest HIPAA Settlement Underscores Medical Device Risk	Blog Post	https://digitalguardian.com/blog/latest-hipaa-settlement-underscores-medical-device-risk
451 Research: The Data Loss Prevention Market by the Numbers	Analyst Report	https://info.digitalguardian.com/451-data-loss-prevention-market-by-numbers.html
Dan Geer on 5 Myths Holding Your Security Program Back	eBook	https://info.digitalguardian.com/ebook-five-myths-holding-your-security-program-back.html
4 Ways DLP Can Help You Meet More Stringent HIPAA Compliance	Executive Brief	https://info.digitalguardian.com/executive-brief-four-ways-data-loss-prevention-can-help-meet-more-stringent-hipaa-enforcement.html
Simplifying Your Data Protection Program for Quick Wins	Video	https://youtu.be/vFWKTj9-v2E
2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention, Gartner	Report Download	https://info.digitalguardian.com/gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html
Gartner on the 2016 Enterprise DLP Magic Quadrant Report, Featuring Gartner	Webinar rebroadcast	https://info.digitalguardian.com/webinar-on-demand-gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html
Data Protection Vendor Evaluation Toolkit	Evaluation tool kit	https://info.digitalguardian.com/data-protection-vendor-evaluation-toolkit.html
Digital Guardian for Healthcare solutions sheet	Solution Sheet	https://info.digitalguardian.com/rs/768-OQW-145/images/digital-guardian-DLP-for-healthcare-systems.pdf
4 Ways DLP Can Help You Meet More Stringent HIPAA Compliance	Executive Brief	https://info.digitalguardian.com/executive-brief-four-ways-data-loss-prevention-can-help-meet-more-stringent-hipaa-enforcement.html
St Charles Healthcare System	Case Study	https://info.digitalguardian.com/rs/768-OQW-145/images/case-study-st-charles-healthcare.pdf
Digital Guardian for Compliance solutions sheet	Solution Sheet	https://info.digitalguardian.com/rs/768-OQW-145/images/DG%20for%20Compliance%20-%20Datashet%20-%20Draft%204.pdf
Digital Guardian for Compliance Technical Overview white paper	Technical Overview	https://info.digitalguardian.com/rs/768-OQW-145/images/DG%20Compliance%20-%20Tech%20overview.pdf
Why Database Record Matching is the Most Effective Method of Identifying Regulated PHI	Whitepaper	https://info.digitalguardian.com/why-dbrm-is-the-most-effective-method-of-identifying-regulated-phi.html
Digital Guardian for Healthcare solutions sheet	Solution Sheet	https://info.digitalguardian.com/rs/768-OQW-145/images/digital-guardian-DLP-for-healthcare-systems.pdf
2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention, Gartner	Report Download	https://info.digitalguardian.com/gartner-2016-data-loss-prevention-magic-quadrant-analyst-report.html

FORTRA™

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.

