IMPERVA®

E-BOOK

Healthcare Cyber Security and Compliance Guide

Content

For Health Care the cost of a security breach has lept

282%

Healthcare Security and Cybercrime

The healthcare industry is quickly growing as a sweet-spot for hackers to steal large amounts of patient records for profit. The US Department of Health and Human Services website reveals that in 2015, over 111 million individuals' data was lost due to hacking or IT incidents in the US alone[1]. Furthermore, security incidents have soared 60 percent and the cost of a security breach leapt 282 percent in healthcare[2]. Hospitals are known to be a soft target, thus making it easy for hackers to gather large amounts of patient data in a single hacking effort. As cyberattacks and Internet threats continue to rise with the use of web-based healthcare portals and remote patient mobile technology, managing security and compliance across a distributed healthcare organization becomes a daunting task.

[1] Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information"

[2] "Why Healthcare Security Matters", 22 July 2015, SecurityWeek

What Really Matters–Securing The Data

Ultimately, hackers are motivated to steal patient healthcare records for profit. According to Reuters, a single stolen healthcare credential is worth $10 when sold on the black market, which is 10-to-20 times more valuable than a single stolen credit card[3]. Unlike stolen financial credit card data, healthcare data can be used to impersonate a person, to receive free healthcare, or file fraudulent claims. A typical healthcare patient record includes name, address, social security number, birth date and health history. With such a wide amount of personal data, a thief can open credit accounts or apply for medical care. While, a person's financial identity can be fully restored, healthcare data breaches have a much more personal and longer-lasting impact upon victims.

Cybercriminals use a variety of methods to profit from the healthcare industry. But, in the end, their ability to monetize is predicated upon either disrupting operations or stealing data.

A single stolen healthcare credential is worth 10-to-20 times more than a single stolen credit card

[3] "Your medical record is worth more to hackers than your credit card",24 Sept 2014, Reuters

Below are key areas of healthcare security that are directly addressed by Imperva cyber security solutions:

Denial of Service (DDoS) Protection

Web Application Security

Data Security

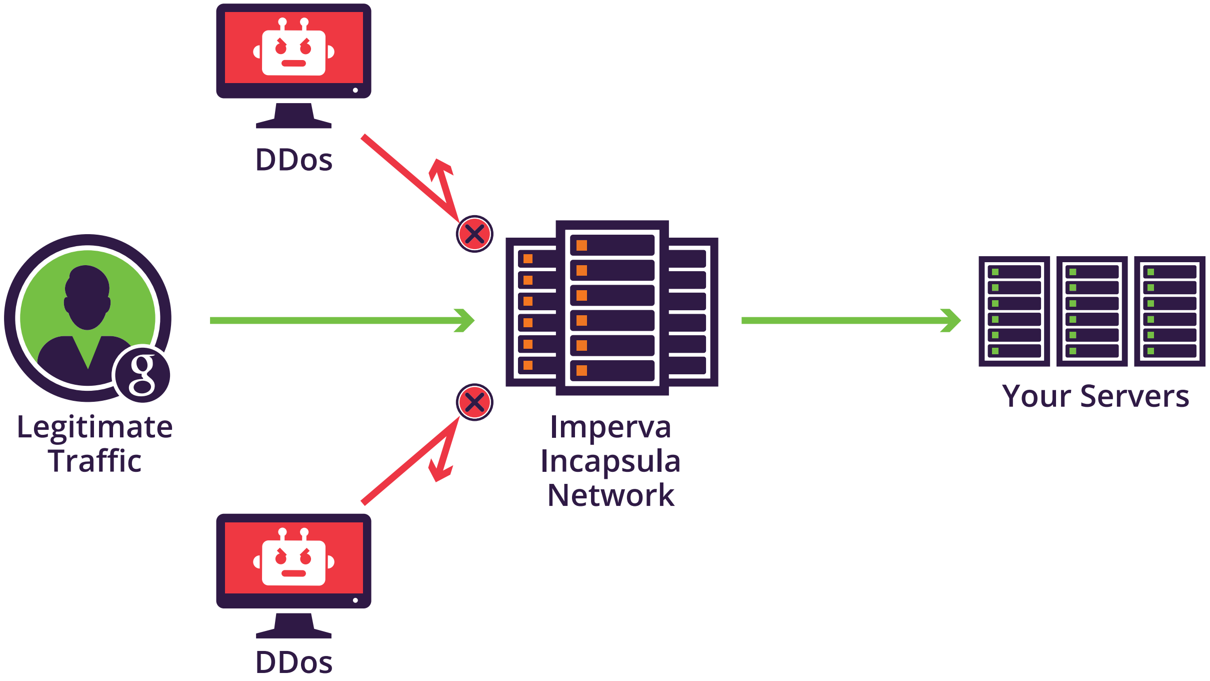
Insider Threats

Regulatory Compliance

USE CASE	BENEFIT
Denial of Service (DDoS) Protection	Shield critical online assets from a wide range of DDoS attacks with an always-on, scalable service
Web Application Security	Protect online patient portals and Internet-connected medical technologies from account takeover and vulnerability exploits
Data Security	Identify security violations and protect data at the source
Insider Threats	Detect and mitigate data abuse by malicious, careless and compromised insiders
Regulatory Compliance	Meet compliance and audit mandates for HIPAA, PCI, and FDA; automate reporting

Defend Against Denial-of-Service Attacks (DDoS)

DDoS attacks are designed to compromise the availability of healthcare patient portals and client websites. These attacks cause slow website response times and prevent customers from accessing an institution's public website. As healthcare organizations continue to build their online presence and adopt Internet connected medical technologies and online exchanges, DDoS attacks will continue to be of major concern. DDoS attacks are a top concern in 2016 along with ransomware and malware as the top three cyber threats facing healthcare organizations today[4].



[4] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016, Ponemon Institute

Application layer attacks growing more advanced

The percentage of bots know how to pass standard security challenges grew 6x from last quarter to almost 37%[5]

Network layer attacks are becoming more sophisticated

1 out of 3 network layer attacks combined high bandwidth and high packet rates[5]

While a primary motivation of DDoS attacks is extortion, they also serve as a diversionary tactic for criminals attempting to steal money or healthcare data. DDoS attacks result in business disruption, reputation damage, lost revenue and reduced customer confidence.

Take for example, the recent hackers purportedly representing the hacktivist group Anonymous, who hit Boston Children's Hospital with phishing and DDoS in protest of the controversial custody case of Justina Pelletier, who was being kept a patient at Boston Children's Hospital as a ward of the state against the wishes of her parents. This DDoS attack targeted the hospital's servers and hampered hospital operations for a week.

Imperva helps healthcare organizations shield critical online assets against DDoS attacks by:

- **Protecting against a wide-range of DDoS attacks** including layer 3/4 volumetric attacks, low and slow attacks, and layer 7 application attacks.
- **Scaling bandwidth on-demand** to absorb peak attack traffic which can be 10-to-100 times greater than standard Internet traffic levels.
- **Monitoring application and network traffic** to detect and stop malicious users and requests.

[5] Imperva Incapula Q3 2015 DDoS Report

Web Application Security

Online patient portals, health information exchanges (HIE), and cloud applications are considered prime targets for cyber criminals because they can provide direct access to sensitive data inside a healthcare organization. Juniper Research suggests that the rapid digitization of consumers' lives and enterprise records will increase the cost that breached organizations will pay for data breaches to $2.1 trillion globally by 2019[5]. Internet accessible patient portals and HIEs are compromised using two distinct types of attack vectors: access control attacks and application vulnerabilities.

The rapid digitization of consumers' lives and enterprise records will increase the cost that breached organizations will pay for data breaches to $2.1 trillion globally by 2019.[6]

JUNIPER RESEARCH

Access control attacks involve the use of stolen credentials to gain unauthorized access to customer accounts. Account takeover is usually the first step to committing fraud. Once criminals have successfully hijacked a customer's bank account, they can commit fraudulent transactions or steal personally identifiable information (PII) to enable fraud.

Cyber criminals also exploit application vulnerabilities. Many online and mobile healthcare applications are custom-developed applications created by an in-house application development team or third-party developers. When vulnerabilities are found in these applications, it can take months to develop, test and implement code fixes. That also leaves the web application exposed to attackers for months.

The following Imperva solutions helps healthcare organizations protect against web attacks:

- **Imperva SecureSphere Web Application Firewall (WAF)** defends against a wide range of web application attacks including account access control and technical attacks like SQL injections. Implementing a WAF also enables healthcare organizations to virtually patch application vulnerabilities to reduce the exposure time from months to days.
- **Imperva Threat Radar** global threat intelligence improves detection accuracy and security operations by identifying new attack vectors and blocking known malicious sources.

[6] "Cybercrime will cost businesses over $2 trillion by 2019', 12 May 2015, Juniper Research

Safeguard Sensitive Data

Given the vast amounts of data healthcare organizations collect and process, data security should be a top priority. In a well-publicized 2015 healthcare breach, hackers gained access to 80 million records that contained personal information on current and former members, the largest cyber attack ever disclosed by a healthcare provider.[7]

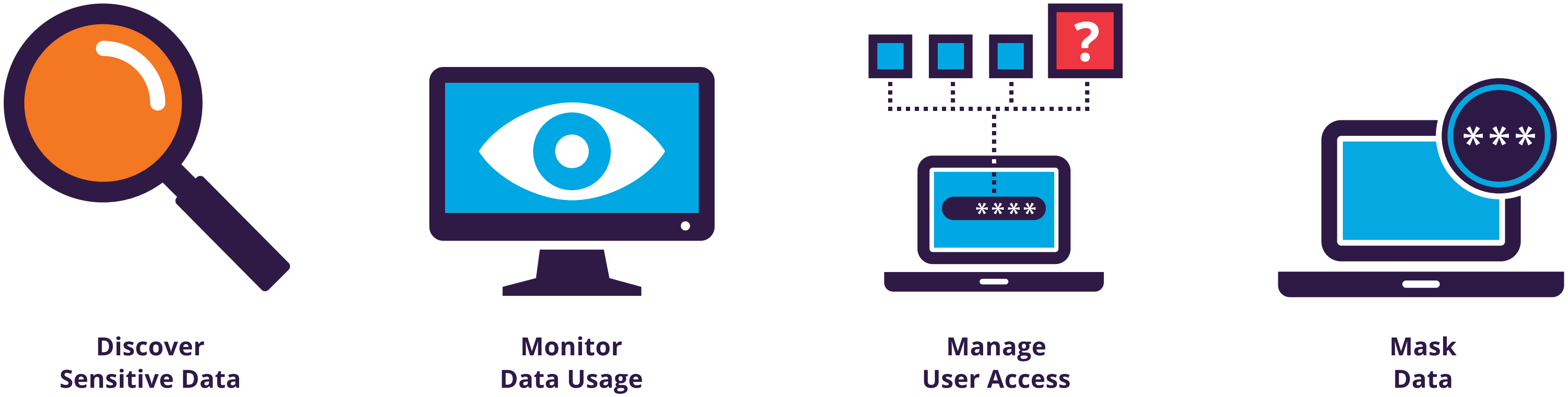
Many organizations have implemented perimeter security, data loss prevention, intrusion prevention/detection systems and endpoint protection, but healthcare organizations' complex IT environments adds new data security requirements to protect data at the source. Multiple relational and non-relational data stores, instances and versions (often from different vendors), and geographically distributed systems that require coordinated policies, monitoring and enforcement leave gaps between systems and applications, leaving these data stores vulnerable to attack.

Furthermore, cyber criminals employ multi-stage attacks, leveraging compromised credentials, obtained via malware and phishing campaigns, to infiltrate the secure perimeter. Once inside, they look for privileged user accounts to elevate their access privileges and move laterally until they find the data they're after. Proactive security monitoring deployed at the data level is the last opportunity to stop an in-progress data attack.

[7] "Hackers breach Anthem; 80m exposed", 4 February 2015, Modern Healthcare

Imperva helps health-care organizations safeguard data by:

- **Discovering where sensitive data lives–in the cloud and on-premises.** The first step in protecting data is knowing where an organization's sensitive data is. Automated discovery and classification are the only reliable way to routinely and consistently discover and classify new or modified database instances containing sensitive data.
- **Monitoring data usage activity across a broad range of data stores.** While databases are a prime target for criminals, sensitive data exists in many types of systems–databases, Big Data platforms, SharePoint portals and file stores. And this data lives both in the cloud and on-premises.
- **Managing user access.** Attackers look for easy opportunities to access sensitive data. They target privileged user accounts, users with excessive access rights and dormant user accounts. To limit lateral movement of attackers and reduce the risk of data breach, healthcare organizations must proactively monitor privileged users, identify users who have excessive privileges and deactivate dormant user accounts.
- **Masking data in non-production environments.** Data masking reduces the attack surface by eliminating sensitive data in non-production environments. Rather than creating copies of sensitive data for test and development teams or for market research purposes, healthcare organizations can enable these groups by replacing sensitive data with realistic, fictional data.



Detect Insider Threats

Inside jobs have been around for as long as business has existed and insider threats continue to be a major security concern for today's healthcare organizations. 92% of healthcare IT decision-makers reported that their organizations are vulnerable to insider threats, and 49% felt extremely vulnerable.[8]

Whether they're motivated by monetary gain or damaging a company's reputation, these individuals are already inside your perimeter defenses. They are employees, contractors and partners that have legitimate access to your valuable data. While the malicious insiders get most of the limelight, it's critical to keep in mind that insider threats extend beyond the disgruntled employee and include compromised and careless users. According to the Verizon DBIR, 76% of data breaches involve stolen or exploited user accounts[9]. That's why insider threats are one of the most difficult to detect.

92%

of Healthcare

IT decision-makers reported that their organizations are vulnerable to insider threats.[8]

[8] 2015 Vormetric Insider Threat Report, Vormetric, May 2015

[9] "Verizon Data-Breach Investigation Report (DBIR), May 2013, Verizon

Detect Insider Threats

No discussion of insider threats would be complete without looking at privileged user access. Privileged users are perhaps the biggest risk when it comes to insider threats. The very nature of their roles and the often unfettered access to critical systems and sensitive data, make system administrators and DBAs prime targets for attackers. Compromising privileged user credentials essentially gives criminals the keys to the kingdom.

To detect and contain insider threats, Imperva enables healthcare organizations to:

- **Gain visibility into who is accessing data.** While many healthcare organizations trust their employees, they must also verify that trust is well placed. Real-time monitoring of all user access, including privileged user access, to databases and files on premises or in the cloud gives IT visibility into which users are accessing what data.
- **Analyze user behavior.** Establishing a baseline of "normal" user patterns via big data, dynamic profiling, machine learning and peer group analytics allows IT to identify anomalous data access. For example, a DBA typically accesses database A between the hours of 9 a.m. to 5 p.m., and then suddenly starts accessing database X between 2 a.m. and 4 a.m. In this scenario, user behavior analytics would detect and prioritize this anomalous data access.
- **Monitor privileged user access:** Proactive monitoring of all privileged access to databases, files and cloud applications helps healthcare organizations keep a watchful eye on system administrators and DBAs and protect critical IT assets from advanced cyber attacks.
- **Eliminate excessive access rights:** Healthcare organizations can reduce the risk of insider theft by granting access to sensitive data on a business need-to-know basis.
- **Mask data in non-production environments.** Data masking reduces the unnecessary spread of sensitive data and enables organizations to implement least privilege by replacing sensitive data with realistic, fictional data.

Streamline Audit and Compliance

Regulatory and industry compliance are major drivers of security investment for healthcare organizations. While compliance is certainly not security, compliance can provide a solid foundation for an information security program. After all, many of the data protection and privacy mandates are intended to protect consumers by ensuring proper security controls are implemented.

Compliance remains a daunting challenge for healthcare organizations. Security requirements are found within a broad set of regulations and mandates, including HIPAA and PCI. Healthcare organizations require automated, continuous compliance across ever-changing regulations and a dynamic IT environment.

Imperva provides industry cyber security leading solutions that help healthcare organizations streamline database audit and compliance.

Imperva has powerful centralized management and reporting solutions that unify security operations to simplify distributed management. Imperva solutions support environments ranging from a single location to those with multiple lines-of-business, geographic locations or data centers.

Advanced web application, database security, and file server security products that offer a wide range of features comprise the suite of Imperva cyber security solutions that protect healthcare organizations. Imperva secures sensitive patient data in three key areas: data security, insider threats, and web applications.

While compliance is certainly not security, compliance can provide a solid foundation for an information security program

Streamline Audit and Compliance - Database Security

REQUIREMENT	REGULATIONS	IMPERVA CAPABILITIES
Database Security	HIPAA 164.308 (a)(5) Login Monitoring; 164.312 (a)(1) Access Control PCI 10 Security Logging and Monitoring	Database Activity Monitor • Audit all access to patient data in databases • Alert and block unauthorized access • Login event logging and monitoring
	HIPAA 164.308 (a)(1) Protection from malicious software; HIPAA 164.312 (c)(1) Integrity PCI 6 Maintain Vulnerability Assessment Program	Database Assessment • Assess database vulnerabilities • Discover and Identify database objects housing patient data • Discover newly created databases and database objects holding ePHI
	HIPAA 164.312(a)(1) Access Control PCI 7 for Access control Addresses; PCI 8.5 for Inactive User Accounts	User Rights Management for Databases • Identify users with excessive rights • Support database user rights review
	HIPAA 164.312 (a)(1) Access Control HIPAA 164.308 (a)(5) Information Access Management PCI 7 Restrict Access PCI 8.5 Implement Strong Access control	CounterBreach • Consolidated view analyzes user access behavior across database, file, and cloud application data • Establish a baseline of typical user access to database tables and file shares • Detects and prioritizes anomalous activity

Streamline Audit and Compliance - File Security

REQUIREMENT	REGULATIONS	IMPERVA CAPABILITIES
File Security	HIPAA 164.308 (a)(5) Log-In Monitoring HIPAA 164.312 (a)(1) Access Control PCI 10 Track and monitor access PCI 11.5 File Integrity Monitoring	File Activity Monitor • Security Logging and Monitoring • File Integrity Monitoring • Audit access to patient medical records stored in files and spreadsheets • Offers tamper-proof audit trail • Alert and block unauthorized access of patient data
	HIPAA 164.312 (a)(1) Access Control HIPAA 164.308 (a)(5) PCI 7Access Control PCI 8.5 Inactive User Accounts	User Rights Management for Files • Access-Control • Inactive User Accounts • Identify users with excessive rights • Support user rights review and approval processes • Automate reporting on user rights access to patient data
	HIPAA 164.312 (a)(1) Access Control PCI 10 Track and monitor access	CounterBreach • Consolidated view analyzes user access behavior across database, file, and cloud application data • Establish a baseline of typical user access to database tables and file shares • Detects and prioritizes anomalous activity

Streamline Audit and Compliance - Web Application Security

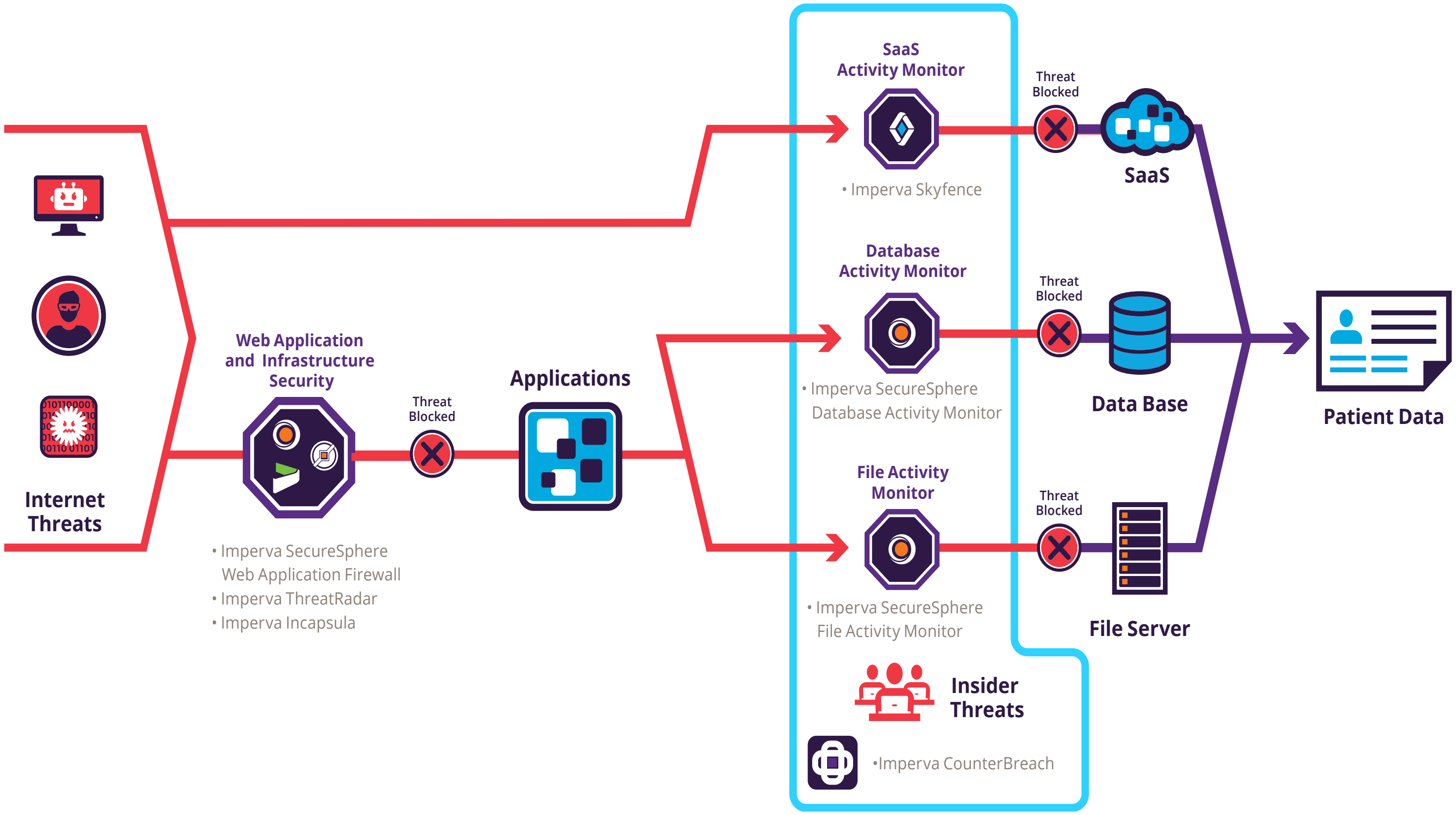
REQUIREMENT	REGULATIONS	IMPERVA CAPABILITIES
Web Application Security	HIPAA 164.308 (a)(4) Information Access Management HIPAA 164.312 (c)(1) Integrity Controls PCI 6.6 Vulnerability Management	Web Application Firewall • Web Application security • Protection against zero-day application and OWASP Top 10 attacks • Integration with code-scanner for vulnerability management • Virtual patching for web applications
	HIPAA 164.312 (c)(1) Integrity Controls PCI 6.6 Vulnerability Management	Skyfence • Enforce controls on sanctioned and unsanctioned cloud applications • Assess risks of cloud applications, pinpoint compliance gaps, and protect user accounts and data in the cloud • Monitor and analyze data usage, administrator activity, and API activity while preventing account-centric threats
	HIPAA 164.312 (c)(1) Integrity Controls PCI 6.6 Vulnerability Management	Incapsula • Cloud-based application delivery service that protects websites while increasing performance • Guards web applications against from OWASP top 10 web attacks like SQL injection and XSS • Includes web application firewall to thwart hacking attempts, DDoS attacks, and web traffic acceleration • PCI-certified cloud application delivery service meets PCI 6.6 mandate for web application firewall requirements
		ThreatRadar • Crowd-Sourced threat intelligence aggregates attack data from third-party security leaders and Imperva SecureSphere WAF customers worldwide • Increases detection and protection of web applications by quickly identifying new attack vectors and blocking malicious sources • Streamlines security operations by automatically blocking web requests based on user reputation, botnets, account takeover attempts, and reconnaissance.

Imperva Provides Industry Leading Cyber Security Solutions to Healthcare

Imperva is a leading provider of cyber security solutions that protect business-critical data and applications in the cloud and on-premises. Healthcare organizations around the world rely on our solutions and experience to protect their data and applications.

Our cyber security solutions enable healthcare organizations to discover assets and risks, then protect their most valuable information–customer patient records, accounts and transactions and financial records. We also help healthcare organizations comply with the myriad of stringent data protection regulations and mandates, as well as enforce policies, entitlements and audit controls.

Our Solution



Our solutions include:

- Imperva SecureSphere: a comprehensive cyber security platform that includes web, database and file security
- Imperva CounterBreach: a multi-layered security solution that protects enterprise data from theft and loss caused by compromised,
  careless and malicious users
- Imperva ThreatRadar: an advanced warning system that stops emerging threats before they impact your business
- Imperva Camouflage: a data masking solution that reduces risk exposure by replacing sensitive data with realistic fictional data
- Imperva Incapsula: a cloud-based application delivery service that protects websites and accelerates their performance for the best possible user experience
- Imperva Skyfence: a cloud access security broker (CASB) that provides visibility and control over sanctioned and unsanctioned could apps

For more information,, please visit www.imperva.com/go/healthcare

© 2016, Imperva, Inc. All rights reserved. Imperva, the Imperva logo, SecureSphere, Incapsula, ThreatRadar, Skyfence and CounterBreach are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders. eBook-Healthcare-0716-rev1

imperva.com

IMPERVA®