USE CASE OVERVIEW

Seven Steps to Cost-Effective HIPAA Compliance

Trustwave®

The Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect patients' Personal Health Information (PHI). HIPAA's Security and Privacy rules outline the requirements for Electronically Protected Health Information (EPHI).

Title II of HIPAA includes the Privacy Rule which regulates the use and disclosure of PHI held by health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers. The HIPAA Security Rules specify the technical requirements to operationalize the Privacy Rule. These technical requirements include:

- Controlling and monitoring access to equipment containing health information.
- Limiting access to hardware and software to properly authorized individuals.
- Protecting information systems housing PHI from intrusion.
- Ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Documenting risk analysis and risk management programs.

The Importance of a Data-Centric Approach To HIPAA

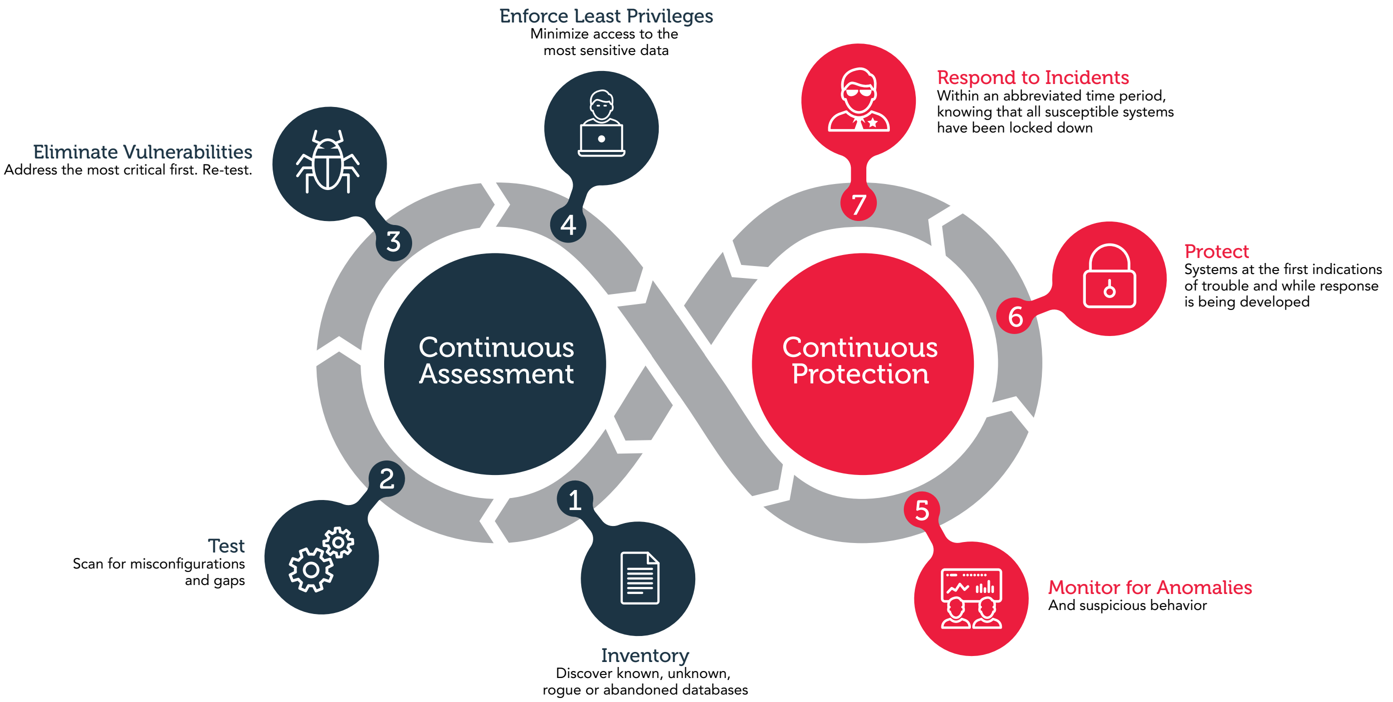
Many organizations start with a network-centric approach which focuses on the end points and periphery defense. While it's important to enact proper periphery defenses, they are ineffective at blocking today's most successful attacks:

- SQL injection vulnerabilities that provide direct access to the database.
- Malware introduced through phishing or other attacks via employee workstations, providing a jump off point to the database and PHI.
- Insider attacks.

A data-centric approach mitigates these attacks by protecting data where it lives – the database. Securing the organization's databases begins by adopting an overarching framework that directs the security processes that impact Personal Health Information. Trustwave works with hundreds of healthcare organizations to secure PHI by adopting a seven-step continuous protection approach to database security.

Trustwave DbProtect is an enterprise-class database security risk and compliance solution that helps organizations operationalize data-centric security. DbProtect helps organizations quickly identify and reduce risk, enforce the Principle of Least Privilege and protect sensitive data across all of their databases both on premises and in the cloud. DbProtect identifies all known production, test, and temporary databases, and more importantly, any unknown, rogue (and therefore unsecured) databases.

Seven Steps to Cost-Effective HIPAA Compliance


Enforce Least Privileges
Minimize access to the most sensitive data
4
Eliminate Vulnerabilities
Address the most critical first. Re-test.
3
Respond to Incidents
Within an abbreviated time period, knowing that all susceptible systems have been locked down
7
Protect
Systems at the first indications of trouble and while response is being developed
6
Continuous Assessment
Continuous Protection
2
Test
Scan for misconfigurations and gaps
1
Inventory
Discover known, unknown, rogue or abandoned databases
5
Monitor for Anomalies
And suspicious behavior

Step 1: Inventory Databases

HIPAA requires healthcare organizations to implement policies and procedures to prevent, detect, contain, and correct security violations. The first step to effective HIPAA compliance is to inventory all databases containing Personal Health Information. Discover, classify and prioritize known databases on your network and in the cloud. Discover unknown databases that are potentially unsecured and out of compliance.

DbProtect helps organizations protect their PHI by:

- Ensuring all PHI is located on authorized and secured databases.
- Restricting access and use of PHI.
- Identifying and removing any unauthorized databases from their networks.

Step 2: Test

Ensure that your database security strategy, configurations and settings are in line with the latest HIPAA policies and standards. Once policies are in place, perform an analysis to associate risk scores with the findings of your vulnerability assessment to help focus efforts where you stand to make the most impact (e.g. reduce the most urgent risk).

Trustwave DbProtect helps you automate and accelerate this process, making it easier to discover, classify and prioritize your organization's databases that contain sensitive information whether cloud-based or on premises.

Step 3: Eliminate Vulnerabilities

Compliance with the HIPAA Security Rules can seem like a daunting challenge for small and large healthcare organizations alike. On top of that, the healthcare industry continues to be a major target for cyber criminals looking to exfiltrate patients' personal information for purposes of identity theft. In 2018, the healthcare sector saw 15 million patient records compromised in more than 500 breaches, three times the amount seen in 2017, according to the Protenus Breach Barometer. This trend is increasing in 2019, with 25 million patient records breached by midyear.

Default and weak passwords, misconfigurations, and missing security patches provide avenues of attack to PHI. HIPAA specifies implementing policies and procedures to prevent, detect, contain, and correct security violations. It requires healthcare organizations to perform periodic technical evaluations in response to environmental and operational changes affecting PHI.

Once your databases have been inventoried and scanned, the next step is to mitigate risk and address compliance concerns at the database level. Trustwave DbProtect Vulnerability Management has powerful database scanning capabilities. Your team benefits from unprecedented Insight to identify and eliminate vulnerabilities and fix misconfigurations that put your organization's PHI at risk. With built-in policies, powered by Trustwave SpiderLabs® threat intelligence, you benefit from up-to-date vulnerability and threat information. Each check in the Knowledgebase provides your team with clear and detailed remediation instructions to ensure that the vulnerabilities exposing sensitive data are fixed in a timely manner.

Powerful reporting provided in DbProtect helps perform risk analysis to map vulnerabilities to risk level and business impact. This analysis helps organizations and cloud providers to prioritize their remediation plans and ensure the most serious threats to sensitive data are addressed quickly.

Step 4. Enforce Least Privileges

Getting on a regular program of assessing technical vulnerabilities and misconfigurations can greatly reduce risk. Assessing users' access and what they have done and can do with the data should also be done in parallel, to further strengthen your defenses.

Over time, users accumulate more privileges than they need to do their job. This can lead to segregation of duties violations that enable an insider to make fraudulent changes or steal PHI. HIPAA specifically requires implementation of policies and procedures to ensure that all members of its workforce have appropriate access to PHI and to allow access to only those persons that have been granted access rights to PHI.

Trustwave DbProtect Rights Management provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. Rights Management enables the organization to enforce the Principle of Least Privileges – grant only the privileges that users need to do their jobs. It allows organizations to restrict database access to a business need-to-know basis and mitigate against shared accounts. Rights Management also provides an audit trail on how privileges were granted, to help prevent against future privilege escalation.

Step 5. Monitor for Anomalies

HIPAA requires organizations to implement mechanisms that record and examine activity in information systems that contain PHI and to regularly test security systems and processes. Database activity monitoring is a critical component of a mitigating breaches and meeting HIPAA requirements.

Trustwave DbProtect Activity Monitoring enables your organization to meet HIPAA requirements and reduce risk and data loss by:

- Validating remediated vulnerabilities.
- Monitoring unremediated vulnerabilities to ensure they are not being exploited.
- Monitoring privileged user activity to ensure they are not engaged in any unauthorized behavior.

Step 6: Protect

As a database security best practice, we recommend the definition of a policy-based monitoring methodology that meets your specific security and audit requirements and provides a compensating control for known vulnerabilities. A policy-based database activity monitoring solution utilizes vulnerability, configuration and user data, united by a comprehensive vulnerability and threat intelligence knowledgebase, to produce accurate, efficient monitoring policies resulting in a manageable set of actionable security and compliance alerts.

Trustwave DbProtect detects, alerts and takes corrective action against suspicious activities, intrusions and policy violations.

Step 7: Respond to Suspicious Behavior

Time is of the essence when it comes to breach response. The average total cost of a data breach is $3.9 Million USD and the average breach lifecycle is 279 days. Organizations that contained a breach lifecycle to within 200 days saved a total of $1.2 Million USD (What's New in the 2019 Cost of a Data Breach Report). Healthcare organizations should look for a database security solution that enables them to take immediate action when suspicious activity is detected or when policy violations occur.

DbProtect Active Response provides an additional layer of protection around sensitive data in the cloud. Active Response can be configured to take action when an unauthorized and suspicious database activity is detected. Active Response can be customized to a fine level of granularity – a specific activity, performed by a specific user, accessing specific data, in a specific database.

For example, when DbProtect recognizes a SQL injection statement, Active Response can:

- Send an alert to IT Security.
- Notify the SIEM system to correlate database activity with web application logs.
- Initiate a malware scan to remove any injected code.
- Take scripted action, such as lock an account, drop a connection, block suspicious activity, and more.

Summary

Attackers are increasingly targeting personal healthcare data across the globe. Relational databases and big data stores at healthcare organizations are a prime target for attackers because of the large amounts of sensitive information about personal identities and medical histories stored within them. More than ever before, organizations need to implement a rigorous defense-in-depth approach to security that includes protecting data where it is stored – in the database. An effective database security program, as outlined in this paper, requires commitment and discipline across the organization. Instituting a proven methodology and identifying the individuals directly responsible for delivering on the program objectives will prevent the over-extension of resources and succeed in establishing effective security controls around your most prized possession – your data.

For more information: www.trustwave.com