IMPERVA®

CASE STUDY

Imperva And Blue Cross Shield of Tennessee, A Trusted Cybersecurity Partnership for The Healthcare Industry

BlueCross BlueShield

Business Problem

All health insurers face a daily challenge of safeguarding the private health information of their members and associates. In addition to serving the best interests of these constituents, insurers are also subject to various regulatory requirements relating to the privacy of personal information.

Two prominent regulatory requirements result from the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and new requirements of the Centers for Medicare & Medicaid Services (CMS). Both are intended to help secure the private healthcare information of consumers.

HIPAA regulation 164.312(a)(1) Access Controls states that organizations handling private patient information must:

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights ..."

In addition to HIPAA regulations, BCBST is also subject to ongoing security and privacy requirements from the CMS. These requirements are independent of HIPAA, but related in that they specify levels of security measures regarding private patient information.

Business Approach

Accomplishing the goal of proactively protecting the private information of members and partners would require a broad effort inside the company, touching the people, processes, and potentially technology that BCBST used to secure and manage the infrastructure.

In order to leverage this internal effort and to streamline the process of demonstrating compliance, the BCBST team linked their efforts related to HIPAA and CMS compliance. The team chose to implement a set of security guidelines specified by CMS in a document titled "Acceptable Risk Safeguards." By meeting this standard of security readiness, BCBST would be able to serve the best interests of their constituent base and demonstrate the appropriate regulatory compliance.

Technology Challenge

BCBST had built a security infrastructure that was comparable with current practices in the healthcare industry, and a substantial element of this protection involved a reliance on traditional enterprise firewalls. This technology provided a means to exclude all but previously approved and documented network traffic. However, application and database attacks that use the allowed protocols cannot be seen by traditional

BlueCross BlueShield

Background

BlueCross BlueShield of Tennessee (BCBST) is an independent, not-for-profit health benefits company. BCBST is the 11th largest of the Blue plans, serving the healthcare needs of more than 4.6 million people.

Founded more than a half-century ago, BCBST is the state's leader in health care financing. Today, millions of Tennesseans turn to the company for health plan coverage, insurance products and services that help protect their health – and their financial security.

enterprise firewalls. Also, traditional enterprise firewalls do not track the appropriate information to recognize malicious application activity. As a result, BCBST had no means to monitor and alert on malicious traffic that used legitimate protocols.

Technology Approach

In July of 2004, BCBST's technology team kicked off a project intended to provide protection for all aspects of the BCBST web and database infrastructure. The key requirements that the technical team identified for the project were:.

1. **Complete Solution** – BCBST needed to find a technology that protected across the entire infrastructure. Specifically, any solution would need to cover both the web applications and the associated databases.
2. **Low Infrastructure Impact** – Any technology deployed should not impact existing applications or infrastructure elements. Especially important was avoiding delays due to a solution that required changes in existing applications, infrastructure or processes.
3. **Low Operational Impact** – Any technology deployed should not impose an excessive burden on the operations team, particularly minimizing ongoing maintenance and avoiding impact on organizational processes.
4. **Deployment Support** – It was important to be able to find a turnkey solution to be able to deploy in time to meet the requirements.

Why Imperva?

The BCBST team chose the Imperva SecureSphere Dynamic Profiling Firewall to address the technology aspects of application and database security. SecureSphere is deployed in the internal and external network monitoring the traffic from protected systems and protecting them from attacks.

SecureSphere and Imperva addressed each of the four key requirements laid out by the technical evaluation team:

1. **Complete Solution** – SecureSphere's Unified Architecture addresses the complete problem of securing both applications and databases at BCBST.
2. **Low Infrastructure Impact** – SecureSphere offered the flexibility of deploying in non-inline mode so that the solution could be quickly tested and deployed in the production network without requiring any changes to existing applications, infrastructure or processes.
3. **Low Operational Impact** – Dynamic Profiling automates the process of deploying and maintaining up to date security at BCBST, removing the tuning overhead introduced by other potential solutions.
4. **Deployment Support** – Imperva delivered a turnkey solution package that allowed BCBST to implement in time to meet their compliance obligations.

> *"Imperva's product gives us the ability to address possible security vulnerabilities without being heavily dependent upon our vendors' timeframe and resources. We now spend less time on issues such as software changes and can direct more energy on protecting our members' data and company information."*
>
> SHARON BLACK,
> SR. MANAGER OF INFORMATION SECURITY
> BLUECROSS BLUESHIELD

> *"Web and database communication has become integrated into nearly every BCBST production system. So protecting our Web applications and databases is a key element in safeguarding the private health information of our members and partners."*
>
> CHRIS LEVA, CIO
> BLUECROSS BLUESHIELD

Imperva Solution

SecureSphere is currently protecting BCBST's entire online presence (www.bcbst.com), which includes portals for members, employees, providers and brokers. SecureSphere is also protecting a variety of internal and external applications as well as database systems from a variety of vendors. BCBST plans to deploy SecureSphere enterprise-wide to protect all web and database servers in the infrastructure.

An important benefit of the SecureSphere deployment architecture has been the flexibility to use inline and non-inline deployment for appropriate stages in the process. Because of this flexibility, BCBST has been able to quickly realize the benefits of SecureSphere without putting the IT infrastructure at risk.

> *"Our selection team considered a variety of products to help us deliver additional protection for our member and partner data. Imperva provided an excellent solution that fit into our architecture and covered both our application and database environments."*
>
> RUSSELL EUBANKS,
> INFORMATION SECURITY ANALYST