



CUSTOMER SUCCESS STORY

# Large Healthcare Organization Protects Patient Data with Imperva

## Company Background

This network of hospitals is one of the largest nonprofit healthcare systems in the country. The system employs more than 50,000 people across dozens of hospitals and academic medical centers in six states. To deliver on its mission, the organization is bringing healthcare to patients, wherever they are—in the clinic, on mobile devices, or telephonically.

## The Challenge

Today, data plays a vital role in improving patient care—from diagnostics to treatment and illness prevention. Like all healthcare organizations, this one must balance its clinicians' needs for on-demand access to patient data against the risk of a data breach.

“These days, a health record is more valuable on the black market than a social security number,” says the organization’s director of information security and data protection. “It is our responsibility to keep patient data secure so that patients can have confidence that not only are they getting the best treatment, but that they’re going to be protected.”

And, with more than 400,000 people in the health system, there’s a lot of data to protect. Patient data is used at every step of the patient care experience, resulting in a sprawling environment that spans structured data, unstructured data, and data stored in the cloud.

“We are a healthcare organization, so every single database has the potential to have some type of protected data in it,” adds the director of information security and data protection. “When people are pulling data into an Excel file, they’re not thinking about where they’re storing it or what might happen to it. They just see the data that they’re going to use to make patients’ lives better. They don’t understand all of the risks.”

In January 2016, the health system began a multiyear project to better protect patient data across the organization. “We had industry-standard products for firewall security, intrusion prevention, and endpoint management security,” says the director of information security and data protection. “But we were not necessarily data focused. Our goal was to reposition the organization to be very operationally secure.”

The organization engaged Imperva partner Network Consulting Services, Inc. (NCSI) to begin work developing a cybersecurity strategy and framework for protecting patient data in its many forms and for mitigating data breach risks. The team initially planned to implement application protection first, intending to get web application firewall and DDoS protection up and running quickly. But, in the early days of the project, a data security incident forced the group to reevaluate its priorities.

“Perimeter protection is much sexier than database protection because it’s an easy win for management,” explains a security consultant at the organization. “We saw that we need to take a long-term approach to ensure that data is managed responsibly, so we shifted gears to start by looking at our highest areas of risk first.”

## IMPERVA SOLUTION

This healthcare organization uses Imperva Data Security to protect patient data from unauthorized access.

## BENEFITS

- **Ability to monitor data access and detect threats in real time:** Imperva Data Security uses machine learning and behavior analytics to distill 45 billion event alerts per day down to 150 critical alerts, making it easy to identify and act on critical threats.
- **Significant cost avoidance:** With a fraction of the alerts being sent to the SIEM, the organization can avoid millions of dollars in Splunk licensing fees.
- **Fast time to value:** Using the FlexProtect licensing model, the healthcare organization only had to purchase licenses for the database servers. All the underlying Imperva virtual architecture for the organization’s environment could be designed, built, deployed and tested before the agents were fully deployed.
- **Simplified compliance reporting:** Automated dashboards and reports make it easy for the healthcare organization to demonstrate compliance and pull reports on who is accessing a given database for a specified time range.

## The Solution

In the wake of the incident, the organization had a singular focus: protect its “crown jewels” and then systematically expand coverage to all its databases. NCSi worked with the health system to roll out a multi-phased data security maturity model, beginning with its most critical assets.

Within three months, 20 key database servers were covered by Imperva Data Security while the security team built the architecture to support the full deployment of 15 business-critical applications and over 780 database servers. Under Imperva’s FlexProtect licensing model, the organization only had to purchase licenses for the database servers. This enabled all of the underlying Imperva virtual architecture for the organization’s environment to be designed, built, deployed and tested before the agents were fully deployed.

## The Results

Imperva Data Security uses machine learning and behavior analytics to distill 45 billion event alerts per day down to 150 critical alerts, avoiding millions of dollars in Splunk SIEM license fees and making it easy to identify and act on real risks.

REDUCTION IN EVENT ALERTS FROM

DOWN TO

**45 Billion**

**150 Critical**

“Without Imperva’s analytics engine, the number of alerts that are generated is overwhelming,” explains the director of information security and data protection. “You can’t do anything about them because it is just paralyzing. As we change the rules, things get clearer and clearer and the policy set gets better and better. It becomes consumable and actionable.”

With Imperva Data Security, the security team can now monitor data access and detect threats in real time. The stats are impressive, but, more importantly, the team has gained the confidence that they are catching the most critical threats and mitigating data breach risks more effectively.

“I don’t worry about whether something is getting past us anymore. Imperva’s analytics engine looks at usage and patterns of usage to help us focus our time on what matters most,” says a security consultant at the organization. “That’s what really sold us on Imperva.”

Imperva Data Security also provides the organization with automated dashboards and reports, making it easy for them to pull reports on who is accessing a given database for a specified time range. Those reports also make it easy to demonstrate compliance.

“We don’t do something just to meet compliance guidelines, we do it because it’s the right thing to do for the business,” says the director of information security and data protection. “In this case, we are doing the right thing and we are meeting compliance guidelines.”


**“I don’t worry about whether something is getting past us anymore. Imperva’s analytics engine looks at usage and patterns of usage to help us focus our time on what matters most.”**

Director of Information  
Security and Data Protection

## Looking Ahead

As the organization enters the final phases of the maturity model, the team knows that their work will be ongoing. Like any other business, this health system is constantly changing. Every day, data volumes grow, and new applications are brought on or retired. And as cybercriminals become more sophisticated, the system must also adapt to the evolving threat landscape.

“In my position, you never really sleep well at night, because as long as there’s an internet connection and a human being, a breach can happen,” says the director of information security and data protection. “With NCSi and Imperva, we feel very confident in the high alerts that we get. Nothing gets by us on the databases that we are monitoring.”



**“With NCSi and Imperva,  
we feel very confident  
in the high alerts that  
we get. Nothing gets  
by us on the databases  
that we are monitoring.”**

Security Consultant

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 [866] 926-4678  
[imperva.com](https://www.imperva.com)