northdoor
Store IT · Protect IT · Use IT

Four easy steps to compliance:
How a Northdoor client took control of database security

Is your sensitive corporate data protected?

With more people working from home, businesses in regulated industries should look at how well they are controlling access to sensitive personal and financial data.

Data is the most important and valuable corporate asset; a major breach can bring an organisation to its knees and cause irreparable damage to its reputation. With the GDPR in force, businesses also face large financial penalties for exposing customer data. Businesses in healthcare, financial services and other heavily regulated industries must also abide by regulations such as HIPAA and PCI DSS.

Historically, companies have tended to invest primarily in cyber security measures that protect the perimeter of the corporate network. But given that more than half of threats come from inside, this leaves a large potential attack surface.

Understand the risks and penalties

Many organisations today have a complex mix of on-premises and cloud systems, with databases storing valuable and sensitive information spread across multiple sites and technologies, potentially under different governance standards and regulatory regimes, and accessed by multiple people and systems. Each database will have multiple development, test, and backup environments; for ease of use, these may be less securely protected than the production environments.

At Northdoor, we have helped many UK organisations take back control of their sensitive data, cutting their risk of costly breaches, and improving their standing with auditors. We know the approaches that work best, compiled here into a 'how-to' guide based on a recent client engagement.

Our client - a major international health insurance company with a worldwide customer base-holds sensitive information on customers' health and finances. It knew that unauthorised access to data had occurred in the past but did not have full visibility into exactly what data had been accessed, or what had been done with it.

Meeting GDPR, HIPAA and FSA audit standards was difficult and time-consuming, because although most employees access data through applications with rigorous security controls, the databases themselves can be directly accessed by technical users with privileged credentials.

Our client needed to understand the who, what, where, when, and how of all access to structured information held in its most mission-critical databases.

1. Gain executive sponsorship and line-of-business commitment

Technology is clearly going to be an enabler for addressing database security, but the internal impetus and business case must come from the business.

For our client, the project began with corporate governance and line-of-business teams identifying the company's needs.

These were:

- provide better protection against the rising threat of data breaches
- enable more detail and visibility for auditors
- save time and effort in reporting and audit
- deliver intelligent real-time alerts on suspect user actions to the IT security team

Very early in the project, the internal teams gained buy-in and commitment from senior executive sponsors, ensuring that all the internal Business Units would spend the required time explaining their requirements.

2. Choose the right technology platform - and partner

Our client reviewed the market for database-protection solutions and determined that IBM Guardium Data Protection - an established solution with support for numerous database platforms - would best meet its needs. Based on advice from IBM, the client called in Northdoor as recognised UK experts in designing and deploying database-protection solutions. We rapidly set up a proof-of-concept environment, brought in representative databases, and showed the client how the solution would meet its needs around monitoring and reporting.

Market-leading database-protection solutions are highly configurable - and none more so than IBM Guardium Data Protection. That is great for businesses, but it means that they are not plug-and-play solutions. You need a partner who can tease out the business requirements and map those precisely to system policies.

3. Understand and map the business requirements

The key success factor in designing a database-protection solution is taking the time to understand the requirements from all stakeholders. In this recent client engagement, we worked closely with each of the client's application management teams to dig into their needs and design the appropriate policies in Guardium. Our consultative approach and ability to understand the business as well as the technology were crucial.

4. Test, engage, support

On the technical side, Guardium needs only limited input from IT administrators during the initial deployment. For this client, that meant just a couple of hours per database. Where you really need to spend time is on testing the policies, engaging with the application owners and business users to ensure that their needs are being met, and then ensuring that the knowledge about managing and refining the solution is absorbed by your organisation.

In this client engagement, Northdoor contributed 200 days of services over a period of eighteen months from the initial proof-of-concept through to knowledge transfer. This included extensive testing for each environment to ensure a fit-for-purpose solution.

Taking the next steps

With the new solution live ahead of their last major audit cycle, our client received positive feedback from auditors. Today, all application service managers receive a mixture of daily, weekly and monthly reports on database access for approval. The security team are also proactively engaged via real-time alerts sent out by Guardium to allow them to investigate potential security threats at the point of impact. Rolling up these reports for auditors is then fast and easy. Beyond the gains in time, the company now has far greater confidence in its ability to identity and analyse potentially unauthorised access to or use of data.

For many clients, the next step would be to extend the solution with enhanced analytics capabilities. IBM makes this easy with its CloudPak for Security offerings, which include the ability to deploy Guardium Insights, which creates a data lake containing every connection ever made to any database, on premises or in the cloud. So not you can not only report on individual incidents, but also look at longer-term trends - something that auditors are often very keen to see.

The AI engine in Guardium Insights builds up profiles on the behaviour of connected applications and privileged users, enabling the solution to create alerts when it identifies changes in behaviour or outliers from the norms.

Why Northdoor?

Whether you want to improve security for on-premises databases or deploy a full hybrid-cloud cyber security environment on IBM CloudPak for Security, Northdoor combines technical expertise with business experience. We know from long experience that IT security projects sink or swim based on the ability to get engagement and commitment from business stakeholders: so you need a partner that can speak their language as well as understand the technology.

Get in touch today to find out how Northdoor can help you protect business-critical databases against misuse and solve your audit worries.