Formulate A Database Security Strategy To Ensure Investments Will Actually Prevent Data Breaches And Satisfy Regulatory Requirements

January 2012
# Table Of Contents

- Executive Summary .................................................................................................................. 2
- Most Database Security Implementations Have Gaps ............................................................... 6
- Focus On Monitoring Rather Than Prevention Leaves Companies Exposed ...................... 8
- Single-Vendor Integrated Database Security Platform Lowers Cost, Improves Integration And Protection .......... 8
- Key Recommendations .............................................................................................................. 10
- Appendix A: Methodology ....................................................................................................... 11
- Appendix B: Supplemental Material .......................................................................................... 11

© 2011, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-19ORUG]

---

**About Forrester Consulting**
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [www.forrester.com/consulting](http://www.forrester.com/consulting).
Executive Summary

With a growing number of internal and external attacks on corporate and government applications and stronger regulatory compliance enforcements, data security continues to be the top priority for organizations year after year (see Figure 1). Although many enterprises are taking stronger measures to protect their data, significant gaps still exist at the very core — the databases that house the corporate crown jewels. Many enterprises don’t have a comprehensive enterprise database security strategy that can defend against sophisticated attacks originating externally or internally, track sensitive data as it’s copied into multiple locations, or even meet the tougher emerging regulatory requirements. In addition, most companies tend to focus on detective controls rather than preventive measures when it comes to database security, making them highly vulnerable. By contrast, we found that companies that implemented a comprehensive and integrated database security solution with a strong emphasis on preventive measures achieved improved security controls, introduced a higher degree of automation across the enterprise, and were more confident in defending against attacks.

Oracle recently commissioned Forrester Consulting to conduct a study of how customers are approaching database security. Forrester conducted in-depth interviews with 15 enterprises in the US and Europe, each with more than 5,000 employees, covering financial services, healthcare, manufacturing, retail, telecommunications, public services, and media. The interviews were conducted with decision-makers and influencers for their firm’s enterprise wide data security strategies and purchases. Forrester found that all companies interviewed agreed that database security was critical to their organization, and most were investing more time and effort to improve database controls.

Key Findings

Forrester’s study yielded several key findings:

- **Most enterprises do not have a comprehensive database security strategy.** Although several of our 15 interviewees stated that they have an information security strategy covering high-level policies, governance, and risk mitigation, many have only basic database security practices. We find that most enterprises invest more on securing their networks and the application middleware tier, leaving their databases and critical application data exposed.

- **Most agree that database security doesn’t get the priority and investment that it needs, leaving the organization vulnerable.** Although more enterprises want to have more effective controls around their databases, our interviewees noted that security budget, organizational issues, and lack of resources often impede initiatives in this area. There is often a false sense of security based on the fact that databases are deep within the perimeter, harder to reach, and therefore are not vulnerable.
• Enterprises tend to focus on detective controls rather than take preventive measures for database security and may not be achieving the outcome expected. Many enterprises implement auditing and monitoring, but these are reactive approaches and cannot prevent attacks that result in data being compromised or stolen. Detection of a security incident is of course critical, but the focus on prevention will become increasingly more critical as more database attacks target intellectual property vital to the viability of the organization itself.

• Integrated database security platforms help lower costs and deliver enhanced security. Enterprises that had implemented point solutions from several vendors found that they had significant gaps in their security — often translating into audit deficiencies — and ultimately required more budget, as point solutions were replaced with single-vendor platform that provided better security at lower cost.

**Figure 1**
IT Security Priorities


**What Comprises A Comprehensive Database Security Strategy?**

A comprehensive database security strategy focuses on proactively protecting data from internal and external attacks, minimizing data exposure to privileged IT users, and securing all databases, including production and nonproduction. Most enterprises often focus on perimeter-based network security, offering the first line of defense, but growing complexity of the environment and sophisticated attacks are requiring enterprises to take a broader view of data security. Database security, which is the last line of defense for enterprise data, needs a greater focus than other layers of the application stack because it holds the crown jewels.
A key to building any successful and comprehensive database security strategy comprises of:

1. Understanding what data needs to be protected, such as credit card numbers, Social Security Numbers, customer data, personal identification information, protected health information, and IP.
2. Understanding applicable regulatory compliance requirements, such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and European Union regulations.
3. Performing an inventory of all databases, including nonproduction.
4. Discovering and classifying databases based on sensitivity of data.
5. Establishing security policies for all databases.
6. Converting the policies into actions and deploying them across databases.
7. Taking appropriate security measures, such as encryption, auditing, access control, monitoring, and data masking.
8. Looking for a comprehensive database security solution that can implement a robust database security at a low cost.

Forrester recommends a comprehensive database security strategy should comprise of three key pillars.

**Foundation Pillar Comprises Of Discovery, Classification, AAA, And Patch Management**
Without understanding where and how your sensitive data is used, data security can be very challenging. The foundation pillar stresses on discovery and classification of sensitive data and having a robust authentication, authorization, and access control framework. In addition, all critical databases should be patched on a regular basis to eliminate known vulnerabilities. Understanding which databases contain sensitive data is a key requirement for any database security strategy. Enterprises should take a complete and ongoing inventory of all databases, including production and nonproduction, and ensure authentication, authorization, and access control is enabled for all critical databases. To establish a strong database security foundation, enterprises should use:

- Database discovery and classification that provides information on which databases to focus.
- Authentication, authorization, and access control for database access.
- Patch management that protects against known vulnerabilities.

**Detection Pillar Comprises Of Auditing, Monitoring, And Vulnerability Assessment**
All changes to sensitive data should be logged to provide the ability to answer audit questions should a need arise such as “who changed what data?” and “when was it changed?” Auditing and monitoring offer compensating controls when preventive measures are not enabled. In addition, vulnerability assessment reports gaps in database environment, such
as weak passwords or excessive access privileges. To support regulatory compliance standards, such as PCI, HIPAA, SOX, and EU, and improve data security, enterprises should track all access and changes to sensitive data. Data and metadata in databases can be accessed, changed, or even deleted in seconds. Detection pillar provides a detailed audit trail of database activities and provides details on vulnerabilities. Detection layer security includes:

- Auditing and alerting on data anomalies and access by privileged users.
- Security monitoring and real-time intrusion prevention to protect database against threats.
- Vulnerability assessment to check for integrity and configuration of databases.

Preventive Pillar Comprises Of Data Encryption, Data Masking, And Database Firewall

This pillar focuses on preventing unauthorized access and protecting against attacks. Preventive security measures include: 1) network and data-at-rest encryption; 2) data masking for nonproduction databases to prevent data exposure to developers, testers, and other non-production users; 3) database firewall to prevent threats such as SQL injection attacks or privilege escalation from even reaching databases; and 4) change management to enable a formal procedure to manage changes in production. The goal is to prevent unauthorized access to and exposure of private data. Preventive measures include:

- Database and network encryption to protect production databases and applications.
- Data masking to protect data in nonproduction databases.
- Database firewall ensures real-time protection from SQL injection attacks, among others, and ensures that if unauthorized users break in, it can protect data by blocking connection or access in real time.

Figure 2
Three Pillars Of Database Security

Most Database Security Implementations Have Gaps

Enterprises, for the most part, still rely on network security to protect their databases. Although this may prevent very basic intrusion to database infrastructure, network security cannot protect the data in databases. Especially as more and more attacks against databases exploit legitimate database access by compromising applications and user credentials. Today, attacks on digital information are more sophisticated, occurring from remote locations on the Web and in lighting speeds that make it difficult to detect and respond before the attacker has gotten away with the data.

Although most of our interviewees have a data security strategy, many don’t have a database security strategy that ensures complete protection of critical databases and prevention of attacks. Unlike database security that primarily focuses on databases, data security is broader, covering databases, midtier, applications, infrastructure, and network — the entire technology stack. Most databases are vulnerable to some form of attack, but without strong security processes and technologies in place, they are soft targets. While all enterprise DBMS products offer basic security features — enterprises still need strong policies and procedures to protect data. Database security is not just about enabling auditing and monitoring, it’s about establishing a comprehensive strategy that prevents unauthorized access to data from hackers, applications, and even privileged database users.

We found in the interviews that most enterprises don’t have an enterprisewide database security strategy that truly focuses on preventing database breaches. Some have a very basic security strategy that only caters to a particular geographic region or certain applications. Regardless of how sophisticated their strategy, most of our interviewees agreed they are not doing enough in securing their databases. Rather pessimistically, they indicated that only a breach will cause people to pay closer attention; until then, database security will not get the priority it needs.

“"For security regulations, we’re complying at minimum levels. If there was an incident, [regulators] would demand to see the how and why [of the incident]. I don’t know if we can provide that level of insight.” (IT manager, US — manufacturing)

Based on the interviews, the current state of database security deployments revealed:

- **Most know that they are not doing enough when it comes to database security.** We found that most enterprises focus more on network- or application-level security and less on databases, even though databases hold the crown jewels. Database security is addressed on an ad hoc basis typically in response to an infrequent audit. More enterprises would like to improve database security but often lack budget earmarked for higher visibility projects, understanding, or management focus.

  “"I don’t think we are taking enough measures to prevent breaches. It’s an ongoing process. Yes, we do tick the boxes, we can show that it is secure, and it goes quiet for a while . . . . But it’s healthier to make sure we progress.” (Manager/technical lead, UK — consumer manufacturing)

- **Most don’t have an enterprise database security strategy.** Many have a data or information security strategy but typically don’t extend that to their databases. Forrester estimates that only 20% of enterprises have some basic database security strategy that addresses the risks to their critical databases. Without a database security strategy in place to address risks in a systematic way, enterprises are taking on risks that they may not even be aware of and can be vulnerable to attacks and regulatory audit failures.
“Our data security strategy focuses on securing networks and having strong authentication and access control to data. We don’t have a specific strategy for databases. However, we do believe that, going forward, we need to have a comprehensive strategy. In fact, we are now putting some plans together to have one by this year.” (IT director, — healthcare insurance)

- Most enterprises use native database security features but are looking for more advanced solutions. We find that most enterprises have implemented native database security features for basic authentication, access control, and auditing. Native auditing especially is often used as a compensating control by organizations that haven’t put in place preventive controls such as encryption, privileged user controls, data masking, and other controls required for regulatory compliance.

“For database security specifically, we rely mainly on the native database features and functionality but are evaluating additional solutions going forward since we don’t feel that we are sufficiently protected, especially in the light of recent attacks on government installations.” (Network management manager, US — government)

- Many are concerned about growing attacks on various businesses, especially increasing evidence of intellectual property theft and industrial espionage. With increasing number of attacks this year, more enterprises are concerned about such attacks.

“Most of our IT security budget and focus are around networks and applications, although some go into database security, but that’s not sufficient, and we know it. I am sure a breach will cause people to pay closer attention to database security, but for now, we are keeping our fingers crossed.” (CIO, US — manufacturing)

- Many don’t spend security budget wisely. Many companies interviewed claimed that security budget was between 8% and 10% of the overall IT budget. Although the percent has not grown over the past year, many were expecting an increase given the rise of security breaches this year. Forrester sees that most don’t spend on the right tools and technologies to execute a comprehensive data security strategy. Some organizations put very strong emphasis on network- and application-level security, which often leaves the backdoor open for hackers to break in into databases. In addition, enterprises need to consider consolidation of databases to bring down the cost of database security.

“With the amount of security budget we have, we cannot secure each and every database that we have, and the management knows about it. We are trying to balance our security projects with the budget, and that’s hard to do. I am hoping that in the coming years the management can realize the risk and can increase the spending so that we can have a better sleep at night.” (VP of IT, US — travel and hospitality)

- Most enterprises acknowledge they run a high-risk database environment because they focus exclusively on detection. Many enterprises have database auditing and monitoring in place, but these solutions only help them to find out about “who accessed the sensitive data?” or “when was the data accessed?” Detective controls cannot block attacks and unauthorized activity in real time.

“Our key focus from day one on database security has been around database monitoring for our critical databases. Given the growing threats to corporate systems, we are now starting to put a strategy together to not only focus on elaborate monitoring measures but also put in place security solutions that can protect in real time. We are definitely moving from being reactive to proactive.” (IT manager, US — financial services)
• **Single-vendor comprehensive database security solutions offer greater benefits.** We find that enterprises that choose a single-vendor database security platform that provides all the capabilities needed for a comprehensive database strategy including encryption, real-time intrusion prevention, database auditing and reporting, multifactor authorization, masking, and secure configuration management often have better security, lower cost, and improved integration.

“We shifted to a single vendor from multiple security vendors. Our old system wasn’t very secure, and it was homegrown. It was too difficult to integrate with multiple vendors and provide a robust security framework. We opted to get full service with one vendor.” (CIO, US — manufacturing)

---

**Focus On Monitoring Rather Than Prevention Leaves Companies Exposed**

Many companies that we interviewed had some level of database auditing and monitoring capability implemented for many of their critical databases. Native database auditing and monitoring features that came with the DBMS product were typically deployed by most, while some had additional solutions from third parties or database vendors. Interestingly enough, many companies rely on network firewalls and application-level access control in conjunction with database monitoring to “prevent data breaches.” Unfortunately of course, this approach does not actually provide real-time protection — attacks exploiting legitimate access to the database, such as SQL injection attacks or direct access circumventing applications using stolen credentials, can easily get through.

“Until someone actually attacks our databases directly, the focus on database security is likely to remain low. We believe our first line of defense, which includes network- and application-level security, is sufficient to defend against real-time attacks. Although we do monitor our databases to track access and abuse, I know that if our first line of defense gets penetrated, our databases could be vulnerable.” (CIO, manufacturing)

Forrester defines database security monitoring as “the process and technology of monitoring activity in a database for unauthorized access including fraudulent purposes to support compliance requirements such as SOX and PCI.” Whereas, prevention is “the process and technology of taking proactive measures to prevent attacks of sensitive data in real time.” Both are equally important, but prevention should definitely be the top priority for everyone.

“Prevention is definitely even more important than monitoring, which can be passive, whether it’s a firewall and it’s more advanced, on a database level and on a network level.” (IT manager, US — financial services)

---

**Single-Vendor Integrated Database Security Platform Lowers Cost, Improves Integration And Protection**

An integrated and comprehensive database security platform provides better integration and in-depth defense, lowers cost, and improves security. It integrates processes and technologies cohesively to deliver a robust security framework, providing a 360-degree protection from internal and external attacks. The integrated platform covers detective and preventive measures to support heterogeneous applications and databases. Enterprises should look at a single vendor to:
• **Improve database security internally and externally.** An integrated and comprehensive solution delivers a powerful security framework that ensures all components, layers, and processes work together to defend against attacks. It provides a well-integrated security system that offers defense in depth against all types of internal and external threats to a database.

“We are vigilant about external attacks; we’ve had attack attempts from nonfriendly companies and countries. . . But the database, especially from the internal side, if we had a rogue employee, that’s a pretty good hole.” (IT manager, US — manufacturing)

• **Lower software and support cost.** Security from multiple vendors can help address point requirements but lack the comprehensiveness and integration, which typically outweighs any functional benefits and overall increases IT security cost. On the other hand, an integrated and comprehensive security solution from a single vendor lowers costs while actually providing better overall security.

“We like dealing with a single vendor. We are now obtaining all of our database security tools from a single vendor. We negotiated pretty heavily based on products and services they provided, and we were able to get significant discount. Single vendor also helps to deploy solutions quickly, get better support, and minimize issues.” (IT director, US financial services)

• **Scale to support hundreds and thousands of databases.** Integrated and comprehensive database security solutions are often easier to scale to hundreds and thousands of databases, especially those offered by the same DBMS vendors who are used to customer requirements regarding performance, scalability, and accuracy.

“There’s an economy of scale when dealing with a single vendor. . . It makes integration a lot easier, [and] we are keeping the single vendor as a major selection factor.” (Information security officer, US — financial services)

• **Easier to integrate existing systems and processes.** Information security policies that need to be deployed across various solutions become simpler and manageable.

“Integration is a big key for us with the applications. Cost is another big key. We’d like to go with a single vendor if possible, just for support purposes. We try to be consistent when we make a decision. We get better price, less training, and less people need to be involved. We try to standardize and have a single business partner for applications.” (IT manager, US — manufacturing)

“It’s not a surprise we went with our preferred vendor’s tool because it was a package they could bring in and integrate it with our existing many apps really well.” (IT director, US — insurance)
KEY RECOMMENDATIONS

Database security has become critical for all enterprises to defend against growing attacks and meeting various regulatory requirements. Forrester’s in-depth interviews with decision-makers and influencers for their firm’s enterprisewide data security strategies and purchases yielded several important observations:

- **Prevention should be a top priority.** Although database monitoring is essential to track data access, it doesn’t prevent hackers from stealing information. Enterprises need to start looking at making the most of their investments by implementing preventive controls to defend against real-time threats.

- **Focus on an enterprisewide database security strategy.** A comprehensive database security strategy ensures investments are not ad hoc and address the three key pillars — foundation, detection, and prevention across the critical databases. Don’t just focus on one or two critical databases, but on all databases that store sensitive data — in other words, all your databases. Discover and classify your databases, noting which ones hold private and sensitive data such as credit card numbers and Social Security Numbers. Make database security part of the database infrastructure.

- **Single vendor solutions offer stronger security and can lower cost.** When looking for a database security solution, look for vendors that offer a comprehensive set of technologies to support your entire database security strategy and offer capabilities for data masking, encryption, auditing, monitoring, firewall, vulnerability assessment, access control, and patch management. We find that a single vendor solution offers stronger security and lower cost and helps avoid cobbiling together point solutions.
Appendix A: Methodology

In this study, Forrester interviewed 15 organizations in the US, Canada, and the UK to evaluate their current enterprise database security strategies. Survey participants included decision-makers in the CIO, IT director, and IT manager roles. Questions provided to the participants asked about their current database security efforts, budget, tools, and roles. Respondents were offered a gift card and data roll-up as a thank you for time spent on the survey. The study began in May 2011 and was completed in August 2011.

Appendix B: Supplemental Material

Related Forrester Research

