

Automating Database Security Controls

Databases hold the most critical information within an organisation, and so require a tightly orchestrated range of **controls to secure and audit their usage.**

Many such controls are manual, making them very expensive and time-consuming to manage, and have difficulty keeping pace as application versions, staff members and threats constantly evolve.

Automation of database security controls, meanwhile, can dramatically increase the efficiency of security enforcement, assure compliance to mandates such as PCI & SOX, and improve working practices. Without it, organisations struggle to maintain intelligence around what databases exist, how they are patched, who has access to them, and what individual access policies allow. The problem is compounded within multi-vendor database environments.

Being able to accelerate security and compliance enables organisations to drive down costs but also decrease the risks inherent with managing databases. Organisations seeking to protect themselves from attack by the implementation of controls can minimise risk and effectively secure their database assets through automation.

AUTOMATED IT RATING: 4.7

This advisory describes the process and impact of automating database security controls.

- **Situation Analysis (Before & After Automation)**
- **The Business Criticality of Automating Database Security Controls**
- **Automation Impacts**
 - **Running Costs**
 - **Time/Labour**
 - **Space & Power**
 - **Decision Making**
 - **Uptime**
- **Implementing Automation**
- **Fortinet Solutions**

Situation Analysis

Before Automation

- The organisation invests massively in time-consuming and inefficient processes and specialist skills in order to manually enforce its database controls.
- The developing and constant tuning of a comprehensive control model for database security/access may also be inconsistent and inefficient.
- The number of databases in deployment, the users privileged to access them, and the extent to which that access is managed are not fully understood by the organisation. IT professionals are likely to be unaware that this is in fact the case.
- Security patching for databases may not be up to date, and the organisation struggles to understand the extent of this problem.

- Compliance mandates governing database security are a significant distraction to the IT department, diverting strategic and tactical resources away from services development and delivery elsewhere within the organisation.
- Even with a robust control model in place, and efficient processes for enforcement, the organisation struggles to respond to the dynamic nature of the database environment (e.g. changing roles of individual users, new technology versions, evolving compliance standards, extent/posture of new threat and vulnerability profiles). As such, the organisation's best-laid plans rapidly unravel over time into an unworkable and potentially insecure status.

After Automation

- The organisation maintains an accurate picture of its database estate via an intelligent and automated process, and is able to address internal/external auditors with an authoritative perspective on database vulnerability posture at any given time.
- Despite constant change to the database environment, its users and its prevalent threats, the database control model continues to be enforced without the need for prolonged or time-consuming manual intervention.
- The organisation is significantly more confident of the security of its databases, and of having its automated multi-vendor patching cycles completely up-to-date at all times.
- The IT team is less distracted by compliance anxieties and the constant need for intervention in database control and enforcement. This directly benefits the organisation's other more progressive IT-driven business goals.

The Business Criticality of Database Security Controls

All organisations use databases, relying and trading upon the value of the data they hold. Controlling access, alerting leaks and breaches and adapting to rapidly changing technological demands are therefore of vital business importance. In highly regulated industry sectors such as financial services, the business criticality of database security controls is almost unparalleled.

Establishing a control framework is the first part of the challenge and one that consumes significant resources and expertise. The second and concluding part of the challenge is enforcing those controls; arguably the larger and more critical undertaking. Here, multi-disciplinary teams spend enormous amounts of time grappling with the most dynamic of technology environments; environments that they typically have only cloudy visibility into.

The answer is to implement a system to automate and manage these processes, ensuring budgets and resources are used efficiently, and that the ultimate goal of optimum security is met continually.

Automation Impacts

Running Costs

HIGH 😊

An automated database security control solution dramatically undercuts the running costs of the manually-driven equivalent, while enabling a series of new and valuable capabilities. The biggest cost saving that can be achieved through automation relates to the amount of time freed up by stripping away unnecessary manual processes.

In addition, some solutions are converged with other related capabilities such as improved logging and event management. Deploying a logical suite of automated processes, available in a single form-factor, can reduce or eliminate the need to purchase or maintain separate solutions.

Time/Labour

HIGH 😊

Automation of database security controls removes the labour burden of multiple time-consuming processes.

One example is the auto-discovery of every database on the network, regardless of subnet boundaries, and the automated determination of user privileges, user behaviour profiles, database version updates, and patching status. A manual process capable of achieving the same level of accuracy would consume a huge amount of skilled resources; indeed, such a large amount that many organisations may decide against it.

The other main group of processes relates to enforcement of the database controls model. Rather than task database analysts to write new scripts in response to perceived vulnerabilities, this process can be fully automated, freeing up time for other more strategically valuable tasks, and improving accuracy and prioritisation. Database analysts typically focus their skills within a limited number of operating systems and applications, necessitating the duplication of script-writing tasks within a multi-disciplinary (often multi-departmental) team. Automation enables those specialised skills to be used more progressively.

Space/Power

MED 😐

The overall potential efficiencies of this approach are outstanding; however there is a limited impact on space and power in the datacentre.

A good automated database security control solution should be able to support databases within a virtualised environment, safeguarding the space/power saving virtualisation/consolidation strategy being pursued. Moreover, an agentless operation option can further reduce the load on database operation.

Decision Making

MED 😐

This automation approach provides a crystal-clear visibility of the database environment that many organisations will never have encountered before. This will enable similarly precise decision making practices, particularly concerning the development and enhancement of database functionality, scale and user control.

Real-time enforcement, reporting and alerting against whatever comprehensive database control model is applied, will also inform the compliance process; enabling organisations to provide auditors and assessors with exactly the validation they require, presented in the format they need.

Uptime

HIGH 😊

This approach fundamentally enhances the security posture of an organisation, safeguarding compliance to critical regulations and promoting its integrity and public commitment to data protection.

This approach will rarely 'displace' existing solutions of a similar ilk, but instead adds robust layers of added security control to an organisation's most critical assets.

Implementing Automation

Implementation of tools to automate database security controls can be accomplished almost immediately, particularly in terms of initial vulnerability assessment. Following simple installation, the ongoing management of such a system is extremely straightforward; supported by a centralised, web-based management application.

Unlike equivalent manual processes which struggle to keep pace with the dynamic database environment, the beauty of an automated approach is its capacity to tirelessly meet those challenges.

The vendor-independent flexibility of such a solution is extremely important, as is the flexibility to either facilitate the development a new control model, or to enforce an imported set of control criteria.

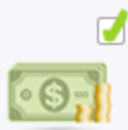
Fortinet Solutions

Fortinet is a leading provider of network security appliances and the leader of the unified threat management (UTM) market worldwide. Fortinet's award-winning portfolio of security gateways, subscription services, and complementary products delivers the highest level of network, content, and application security for enterprises of all sizes, managed service providers, and telecommunications carriers, while reducing total cost of ownership and providing a flexible, scalable path for expansion. For more information, visit www.fortinet.com

Click [here](#) to download a free trial of FortiDB software version for automated database security controls.

Click [here](#) to download the FAQ guide on FortiDB.

Click [here](#) to download the FortiDB datasheet.



SLASH COSTS

- Cut management costs associated with database security enforcement
- Further reduce opex spent on developing control models



SAVE MAN-HOURS

- Free up skills for innovation
- Eliminate time consuming practices
- Eliminate duplication of activity



CUT SPACE/POWER

- Supports virtualised environments
- Agentless option reduces database load



BETTER DECISION-MAKING

- Gain and maintain an accurate picture of database estate
- Enforce controls and react to alarms in real-time
- Become less distracted by compliance anxieties



BOOST UPTIME

- Achieve optimum database security
- Add layers of security controls to your most critical data assets