Building a Database Security Program

Despite being our most important repositories for our most sensitive - and critical - data, the ongoing, multi-year spate of data breaches shows most organizations still struggle to effectively secure databases. From SQL injection attacks to administrator error or user abuse, organizations struggle to keep their data secure without hampering operations. While in some cases it's due to a lack of prioritization, in many situations it's more a factor of the difficulty of efficiently applying security controls in high performance, high priority, and highly complex systems. Securing a database (and associated applications) isn't nearly as straightforward as protecting a network or endpoint.

And nothing hampers our efforts more than a complete lack of industry-accepted database security process, never mind a framework for a complete program.

Database security encompasses a large number of processes managed by different teams- from DBAs, to security operations, to IT operations., to developers, to application owners Most companies run several types of databases, each serving different applications. Configuration and management is not applied consistently to all databases, rather each database is set to address specific security, compliance and business processing requirements, with dedicated resources directly proportional to the criticality of the service.

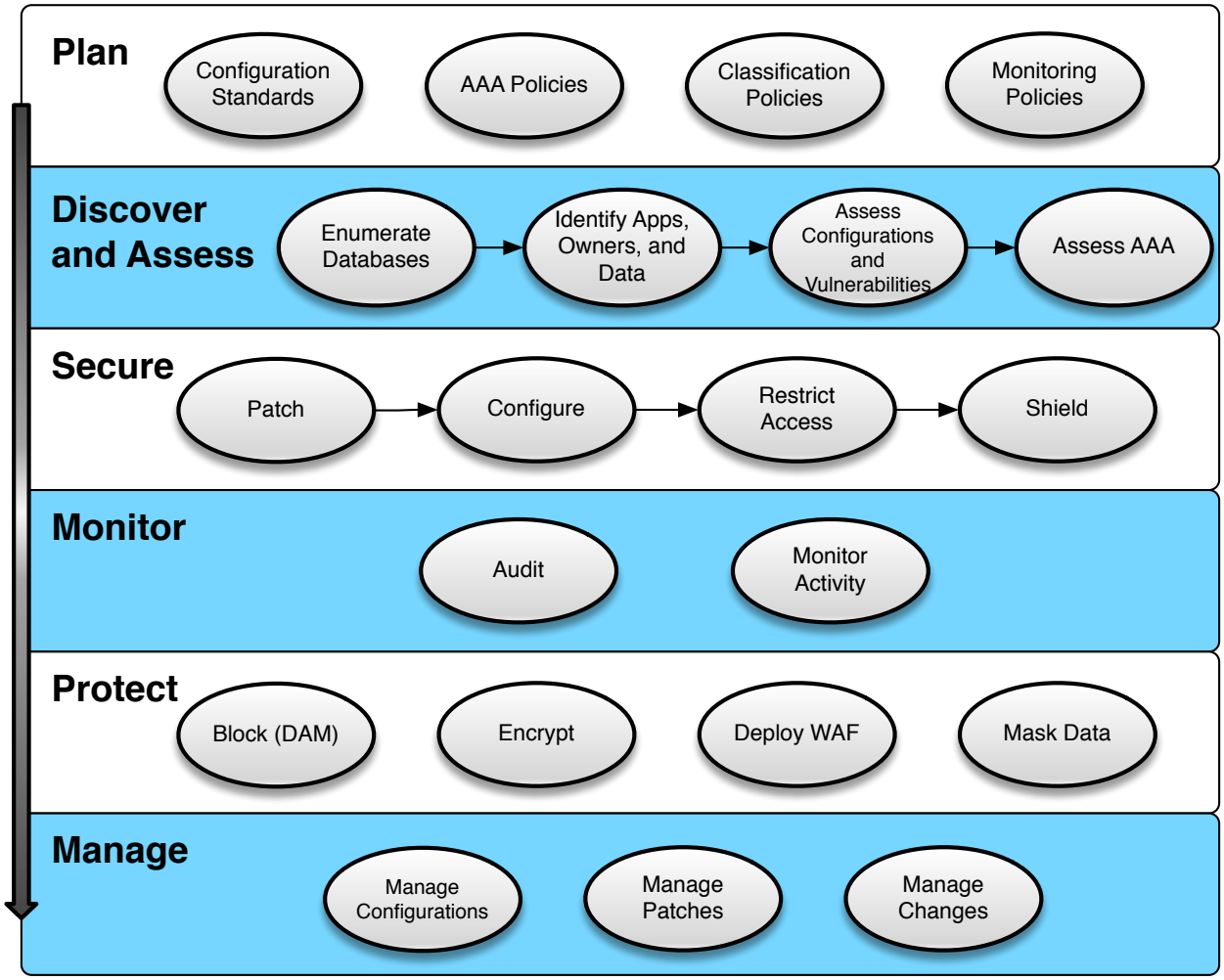
We at Securosis initially set out to build a lightweight metrics model for measuring the costs of database security. We quickly realized that not only were there no open, public frameworks for a database security program, the industry generally lacked even individual processes for standard database security tasks. It took us over 18 months of research, writing, and seeking public feedback to develop the processes, models, and metrics encompassed in this report. To our knowledge it is the first comprehensive database security program framework.

From policies to generating audit reports we believe we've managed to lay out straightforward processes for all major database security tasks. This executive summary may be under 10 pages, but the full report <link before we post> clocks in at 80 pages and contains 6 major phases with 21 subprocesses and dozens of operational metrics. Since that material is so dense, we realized we also needed to release this lightweight, process-oriented version that's more consumable. This *Executive Summary* includes the entire framework, high level processes, and identifies the key metrics we consider most important.

These steps are by no means gospel, but the processes and metrics should encompass all of your database security activities. Some of you might use everything included, while others are just starting, but the key to deriving value out of this project is to use the provided framework as a reference to improve your own processes, while picking the metrics that make the most sense for you.

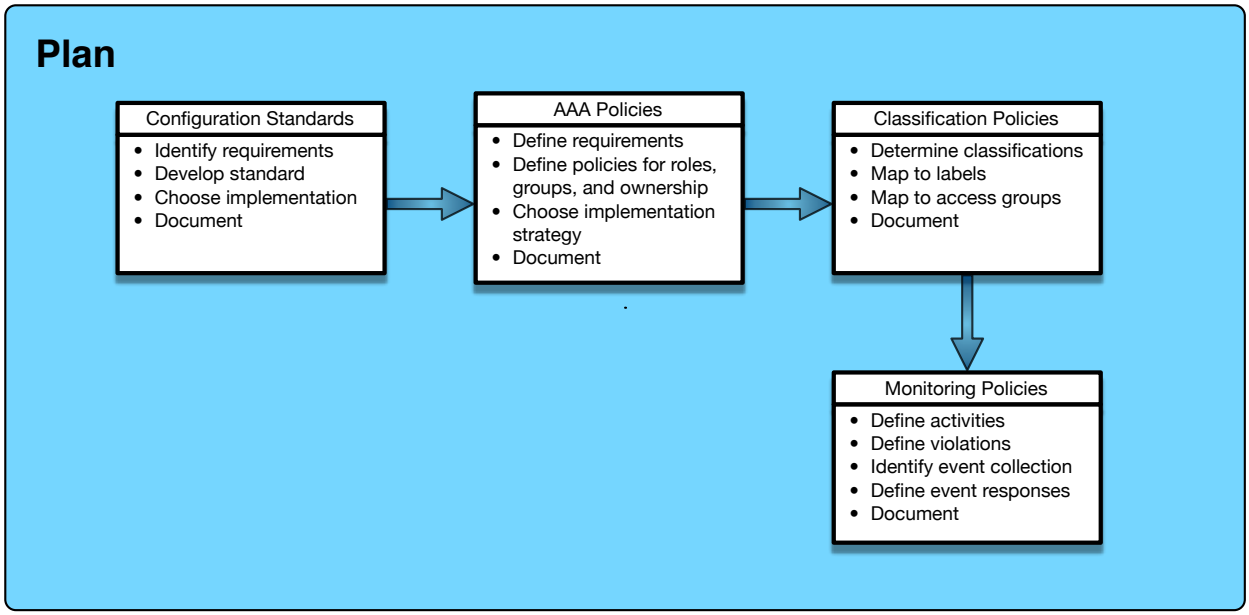
The value of any research is in how you use it to improve your operations and day to day activities. Use what makes sense and forget the rest.

The Securosis Database Security Program Framework



The Plan Phase

This phase encompasses the major planning and policy development steps. These high-level policies are designed to guide the rest of your program and will save time and costs later, because instead of having to start from scratch for every database, you have a base to either directly comply with, or to adjust as necessary for specific systems. Just make sure you document any deviations from the baseline, especially if the database is within a compliance scope. Key metrics from the planning phase are centered on establishment of access control policies, specifically for mapping logical roles to business functions, mapping administrative duties and defining access and authentication mechanisms.

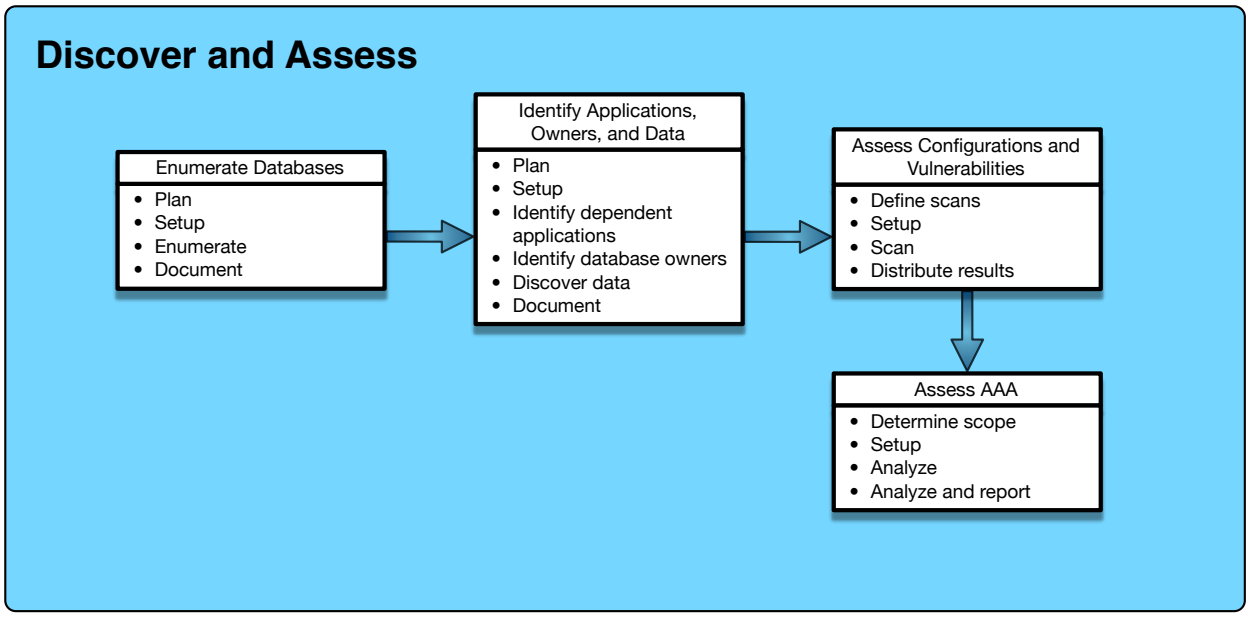


Key Metrics		
Time to determine configuration standards requirements	Time to map logical roles to bus functions	Time to determine monitoring requirements
Time to determine classification scheme		

The Discover and Assess Phase

In this phase we identify databases; determine what applications and business units they support; assess them for vulnerabilities; and evaluate authentication, authorization, and access controls. Enumeration is really the linchpin step which differentiates a series of one-off projects from a database security *program*. It's what allows you to prioritize and manage deficiencies based on data, rather than assumptions.

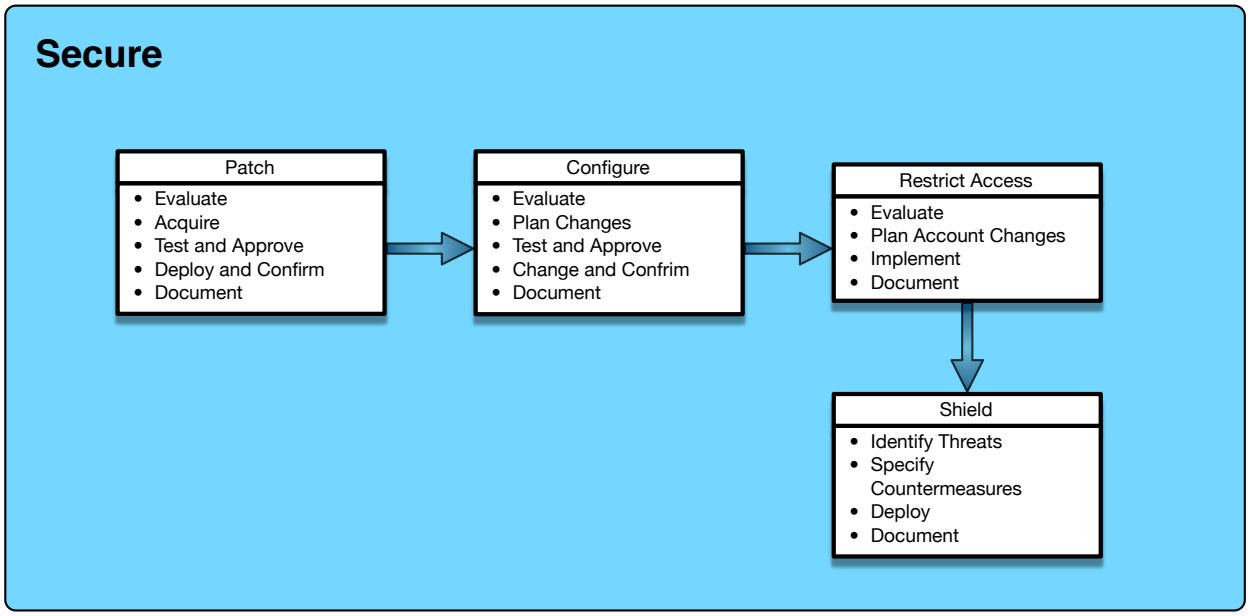
Key metrics derived from the research include effort to discover databases, cataloging application dependencies, determining your configuration requirements, and scanning databases for patches, vulnerabilities and settings.



Key Metrics		
Time to discover databases	Time to assess database configuration and vulnerabilities	Time to catalog application dependencies
Time to collect and assess users and entitlements		

The Secure Phase

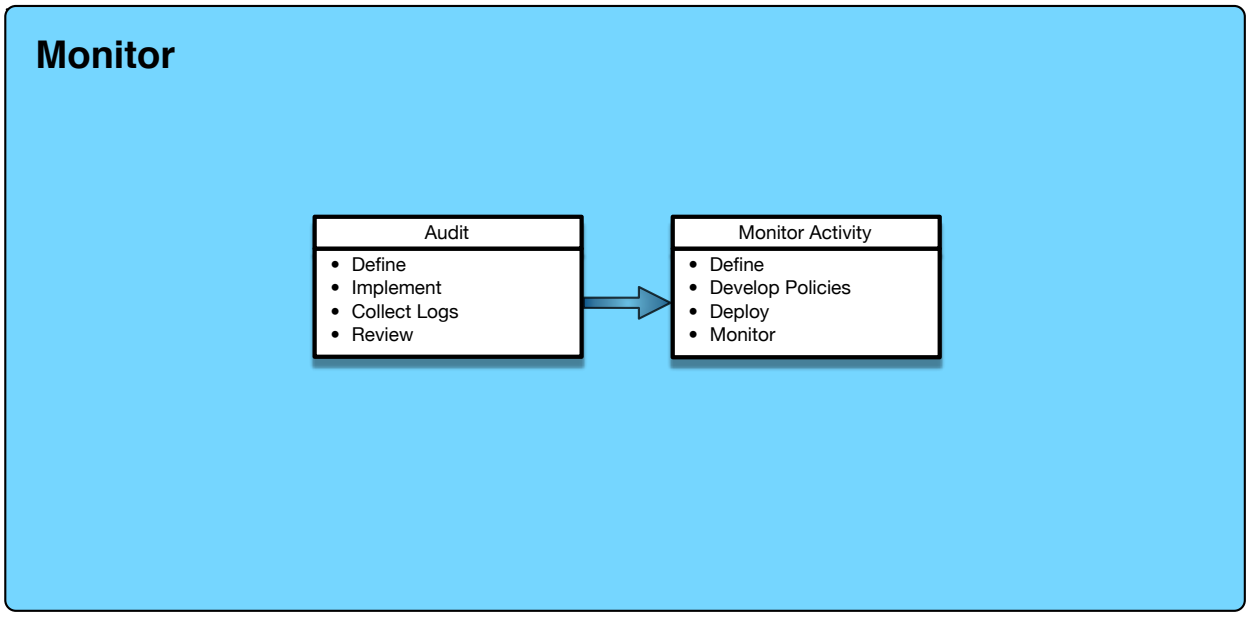
In the Secure phase we fix whatever problems we found in the Discover and Assess phase: missing database patches, configuration changes, access control settings, and shielding the database from known attacks. Key cost metrics are dominated by installation and verification of patches, and setting user, administrator and service account settings to match policy. Databases serving web applications also require significant investment in threat assessment and planning security counter-measures.



Key Metrics		
Time to install and verify patches	Time to install configuration changes	Time to create new roles, remove accounts, and adjust memberships
Time and cost to deploy countermeasures		

Monitor Phase

The Monitor phase serves two purposes: to satisfy compliance requirements, and to improve security. Key metrics include determining which transactions, objects and users were critical, time to review auditing and monitoring reports, and the cost of any supporting monitoring tools.

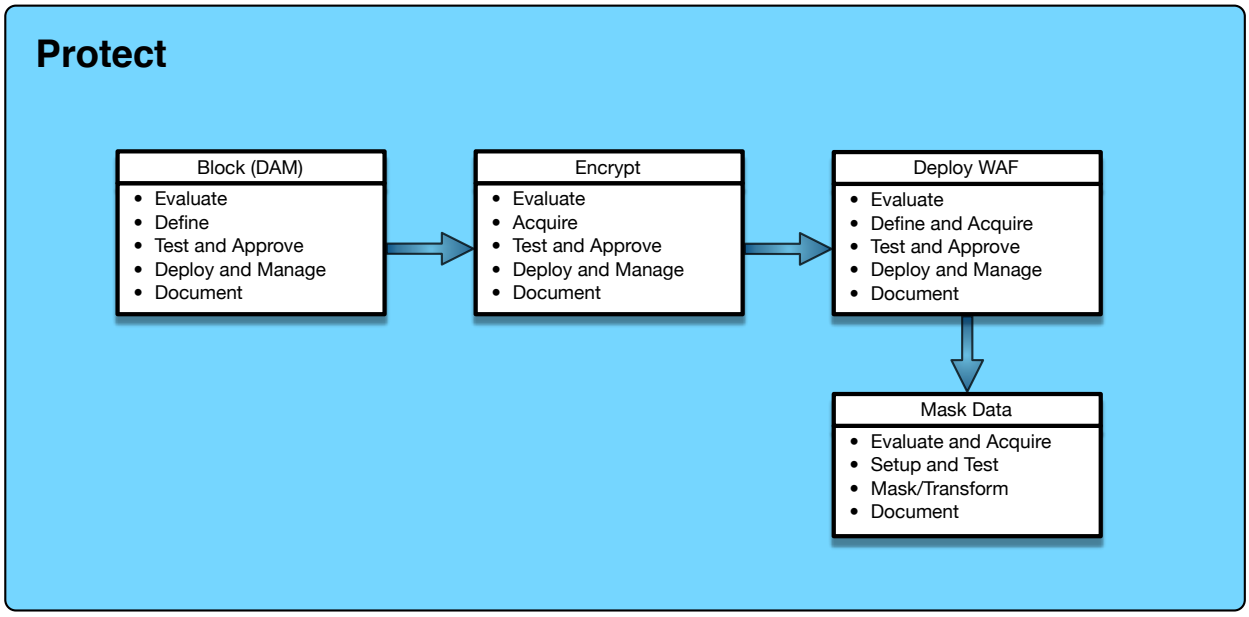


Key Metrics		
Time to determine audit events	Time to review auditing and/or monitoring reports	Cost of audit/monitoring tools
Time to generate compliance reports		

Protect Phase

The purpose of the Protect phase is to implement active security controls to block attacks, protect stored data, and scrub/obfuscate production data for use in testing environments. In this phase we start implementing active security controls that change the functioning of the database and can interfere with business process if not implemented properly.

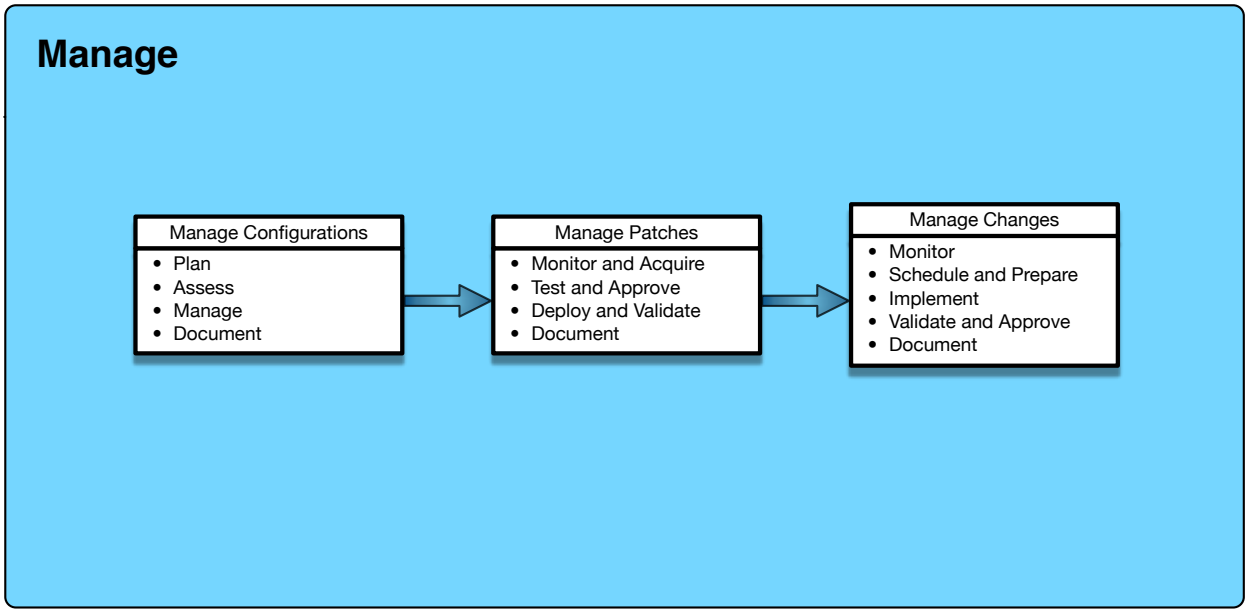
Key metrics are focused in the deployment of encryption, masking and activity blocking technologies, whereas web application firewalls required significant management time.



Key Metrics		
Time to manage DAM incidents	Time to deploy encryption	Time to integrate encryption with applications
Time to deploy and configure WAF	Time to create data masking plan	

Manage Phase

The Manage phase is an ongoing process used to keep systems compliant with policy. These three sub-phases help us keep our systems configured securely and up to date, and allow us to track changes ranging from settings to user accounts. Key metrics were heavily weighted toward pre-installation preparation, and the post installation validation - of any changes to the database environment. This includes configuration, patching and upgrades.



Key Metrics		
Time to assess configuration changes	Time to test and evaluate patches	Time to validate patch installation
Time to validate implemented changes		

Getting Started

There are many operational steps and associated metrics in this project. We recommend organizations start small, and likely focus on areas involved in compliance. Database discovery, assessment (especially configuration and vulnerability), auditing/monitoring, and encryption tend to be the top compliance concerns and are likely activities you are already involved with. Another common area is assessing and managing user entitlements. All of these also happen to be areas where security and database teams tend to have to work together.

The steps to introduce this approach to your organization are pretty straightforward and very replicable.

1. Pick a place to start.
2. Map the process.
3. Choose the metrics.
4. Collect the data.
5. Analyze the data.
6. Adapt the process.

Then go back to Step 1, with another subset of your database security operational processes. We don't mean to oversimplify things, but it's not hard. Your organization just needs the commitment to systematically collect data and adapt the processes based on what the data tells you.

Finally, the authors of this report would like to encourage additional open, independent, community research and analysis projects in IT and security metrics. Utilizing a transparent research process enables new kinds of collaboration capable of producing unbiased results. We are investigating other opportunities to promote open research and analysis, particularly in the areas of metrics, frameworks, and benchmarks. If you have any suggestions as to additional research opportunities, feel free to drop us a line at info@securosis.com.

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog <http://securosis.com/blog>, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by Application Security Inc.

About AppSec:

Founded in 2001, Application Security, Inc. (AppSec) has pioneered database security, risk, and compliance solutions for the enterprise. AppSec empowers organizations to assess, monitor and protect their most critical database assets in real time, while simplifying audits, monitoring risk, and automating compliance requirements.

As the leading provider of cross platform solutions for the enterprise, AppSec's products – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – deliver the industry's most comprehensive database security solution. With over 2,000 customers in 42 countries, AppSec is headquartered in New York City and has offices throughout North America and the United Kingdom.

For more information, please visit www.appsecinc.com.

Contributors

The following individuals contributed significantly to this report through comments on the Securosis blog and follow-on review and conversations:

'ds'

Russell Thomas

Copyright