

Office of Management and Budget (OMB) Introduces Regulations to Require Continuous Monitoring of IT Assets

In 2010 the Office of Management and Budget (OMB) enacted radical changes in Federal cybersecurity strategy. The goal of this initiative is to drive Federal agencies to implement an automated and proactive approach that is risk-based, cost-effective and provides for continuous security. These changes are defined in new FISMA regulations. Under the new regulations, agencies are required to:

- Implement software to support a program of continuous monitoring
- Feed their data to Cyberscope, an online software tool that reports how agencies are meeting the new FISMA requirements

The goal of continuous monitoring is to provide real time awareness of an agency's security posture, enabling agencies to address threats and to proactively remediate vulnerabilities before they can be exploited.

NETWORK VERSUS DATA CENTRIC APPROACHES TO CONTINUOUS MONITORING

As agencies formulate security plans, there are two approaches to consider:

- Network Centric
- Data Centric

Network Centric — The network centric approach focuses on providing defense at the periphery. Many agencies are interpreting the new FISMA regulations as a mandate to lock down all end points. This is a complex task involving additional firewall deployment, network scanning, and configuration and patch management at the device level. In an agency with tens of thousands of end points, this is a massive undertaking.

Data Centric — The data centric approach focuses on the data itself and where it lives – the database. Data centric continuous monitoring protects the data by identifying and fixing database vulnerabilities before they can be exploited. In an agency with hundreds of database instances, continuous monitoring at the database level is a much more automated and manageable task.

Which approach should Federal agencies adopt to provide continuous security? The answer is both. Federal agencies are the target of the most organized, sophisticated and well-funded attackers – Terrorists and Foreign state agencies. They are subject to the most advanced attack vectors. The failsafe approach is a defense in depth strategy that incorporates solutions and best practices from both network centric and data centric approaches. The new mission is to protect information and data, yet many organizations are starting out in the periphery, far away from where data lives. Federal agencies must prioritize continuous monitoring of the database. A logical approach focuses on the data at risk and starts from the inside, the database, and then works its way out to the end points.

“The main thrust of the updated law is its focus on data,” says Erik Hopkins, staff member of the Senate Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security. “What we care about is the protection of the information.”¹

Protecting data at the database layer offers several advantages that agency CIOs should consider.

A Federal agency may have hundreds of database instances versus tens of thousands of end points. Implementing continuous monitoring at the database layer is a significantly smaller scale effort than locking down all end points.

¹ Vanessa Jo Roberts, FEDTECH – Cybersecurity: Continuous Monitoring Is a Must. May 27, 2010.

Office of Management and Budget (OMB) Introduces Regulations to Require Continuous Monitoring of IT Assets 2

Protecting data at the database layer provides a higher level of protection against vulnerabilities that put sensitive data at risk. In 2009 and 2010 the Verizon Risk Team was commissioned by the U.S. Secret Service to document known data breaches. Verizon was able to identify over 428 million compromised records. Verizon attributed 92% of the data loss to attacks direct on the database.² These statistics highlight the protection limitations of periphery defenses:

- Most attacks occur using valid credentials.
- Many attacks from outsiders are highly sophisticated in nature and designed to take advantage of weaknesses in firewalls and web application code.
- The number of attacks coming from inside the firewall are the fastest growing category.

In summary, continuous monitoring at the database layer provides a broader range of protection, requires a smaller scale implementation, is faster to deploy, and costs less than continuous monitoring of all end points.

DATABASE SECURITY PROCESS CONTROL AND CONTINUOUS MONITORING

Matt Coose - Director of Federal Network Security, DHS states: "Agencies should automate what they can," and he points to four categories for which decent tools are available: Inventory management, configuration management, vulnerability management and patch management. "The standards are mature and the tools are out there. Agencies, at a minimum, need to get these foundational pieces in place."³

DbProtect with the Database Security Process Control methodology:

- Will enable Federal agency CIOs to meet and exceed the new OMB mandate for continuous monitoring.
- Will provide a broader spectrum of vulnerability protection than locking down end points.
- Will require less effort to implement and maintain than a program of locking down end points.

- Meets all related government compliance regulations.

Application Security's approach to Continuous Monitoring is Database Security Process Control. By controlling the database processes that impact the security of sensitive data, agencies can improve the protection of that data. By automating Database Security Process Control, agencies can reduce and control the costs of implementing Continuous Monitoring.

FIVE STEPS TO COST-EFFECTIVE CONTINUOUS MONITORING COMPLIANCE

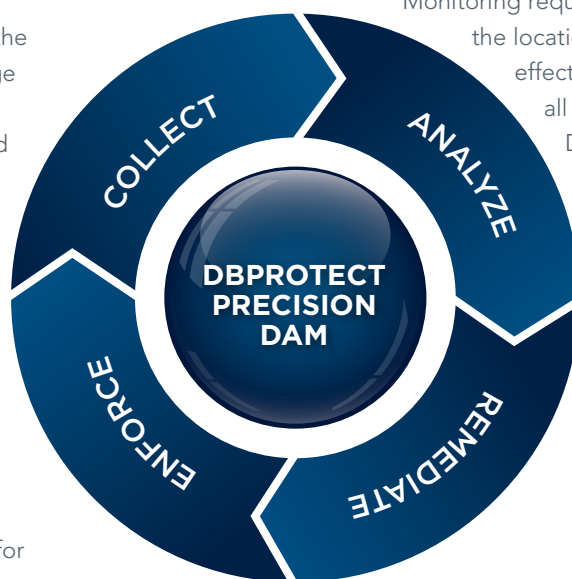
Step 1: Isolate Sensitive Databases

DISA STIG, the implementational guidelines for Continuous Monitoring requires agencies to identify and report on the location of all sensitive data. The first step to effective Continuous Monitoring is to isolate all databases containing sensitive data. The Database Discovery feature of DbProtect's Vulnerability Management generates a complete inventory of all databases deployed agency-wide. It identifies all production, test, and temporary databases, and more importantly, any unauthorized databases. DbProtect's Sensitive Data Discovery identifies and locates all sensitive data residing on those databases. DbProtect helps federal agencies to protect their sensitive data by:

- Ensuring all sensitive is located on authorized and secured databases
- Restricting access and use of sensitive data.
- Identifying and removing any unauthorized databases from their networks

Step 2: Eliminate Vulnerabilities

Default and weak passwords, misconfigurations, and missing security patches provide avenues of attack through database security to sensitive data. Continuous Monitoring requires agencies to ensure that all databases are configured in accordance with DoD guidelines and to identify and remediate any database vulnerabilities exposing sensitive data. DbProtect Vulnerability Management provides unparalleled database vulnerability assessment, allowing



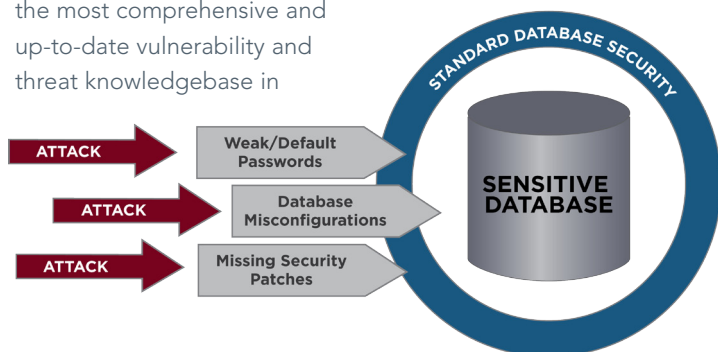
2 Verizon 2010 Data Breach Report. A study conducted by the Verizon Risk Team in cooperation with the United States Secret Service. July 2010.

3 Vanessa Jo Roberts, FEDTECH – Cybersecurity: Continuous Monitoring Is a Must. May 27, 2010.

Office of Management and Budget (OMB) Introduces Regulations to Require Continuous Monitoring of IT Assets 3

organizations to identify and eliminate vulnerabilities and fix misconfigurations that put their customer data at risk.

Vulnerability Management is driven by a powerful policy development engine that begins with a proven DISA STIG compliant template. DbProtect’s policy development is fed by the SHATTER Knowledgebase, the most comprehensive and up-to-date vulnerability and threat knowledgebase in



the industry. Each check in the SHATTER knowledgebase provides clear and detailed remediation instructions to insure that the vulnerabilities exposing customer account data are fixed in a timely manner.

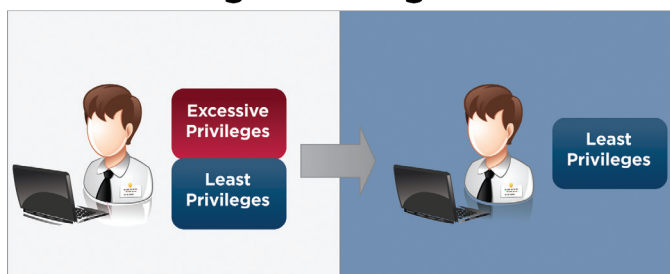
DbProtect’ Risk Analysis maps vulnerabilities to risk level and security impact. This helps agency to prioritize their remediation plans and ensure the most serious threats to sensitive data are addressed quickly.

Step 3. Enforce Least Privileges

Over time, users accumulate more privileges than they need to do the job. This can lead to Segregation of Duties (SoD) violations that enables an insider to access or steal sensitive data. Continuous Monitoring specifically requires that access to sensitive data be restricted by need-to-know basis. It requires identifying and mitigating Segregation of Duties conflicts, along with the implementation of a program of Least Privileges.

DbProtect Rights Management provides a detailed view of an agency’s data ownership, access controls, and rights to sensitive information. Rights Management enables the agency to enforce the Principle of Least Privileges – grant only the

Rights Management



privileges that users need to do their jobs. It allows you to restrict database access to a business need-to-know basis and mitigate against Segregation of Duties conflicts. Rights Management also provides an audit trail on how privileges were granted, to help prevent against future privilege escalation.

Step 4. Monitor for Deviations

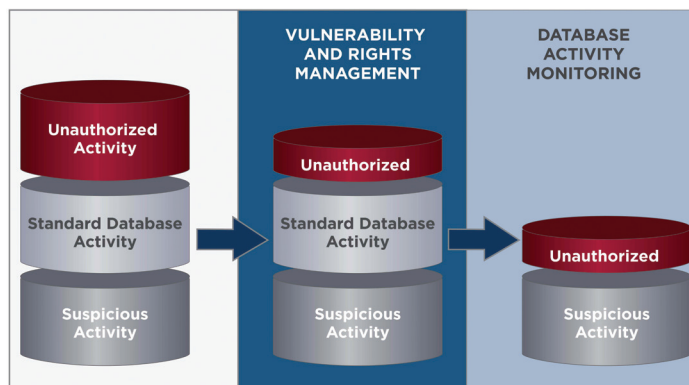
Continuous Monitoring requires agencies to track and monitor all access to sensitive data and immediately report on any suspicious or unauthorized activity. DbProtect Database Activity Monitoring (DAM) meets Continuous Monitoring requirements by:

- Validating remediated vulnerabilities
- Monitoring unremediated vulnerabilities to ensure they are not being exploited
- Monitoring privileged user activity to ensure they are not engaged in any unauthorized behavior
- Monitoring for any new avenues of attack

DBProtect’s unique approach to Database Activity Monitoring is precision monitoring. Precision monitoring employs DbProtect’s powerful policy development engine to streamline monitoring operations to focus on any suspicious activity threatening sensitive data. DbProtect’s precision DAM solution can be customized to a fine level of granularity: a specific activity, performed by specific user, accessing a specific data, in a specific database.

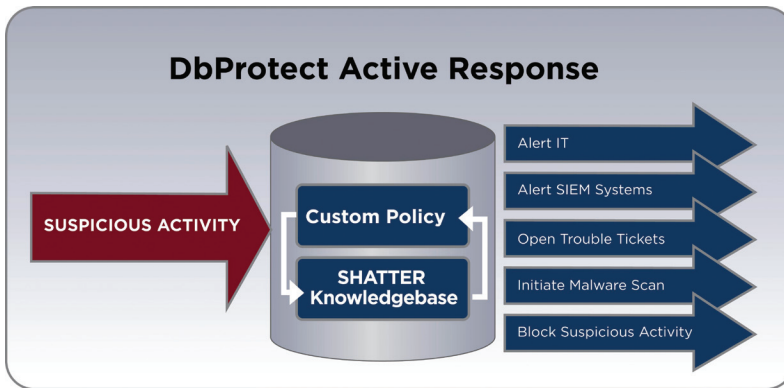
Backed by the same SHATTER knowledgebase that drives DbProtect Vulnerability Management, DbProtect DAM reduces risk and offers best-in-class data protection and PCI DSS compliance reporting.

Precision DAM



Step 5: Respond to Suspicious Behavior

DBProtect’s Active Response provides an additional layer



SUMMARY

New regulations from the Office of Management and Budget mandates that Federal agencies implement a proactive program of continuous monitoring to protect sensitive data assets. Many agencies are taking a more traditional network centric approach, attempting to lock down their end points. Agency CIOs also need to take a data centric approach and protect the data where it lives – in the database. Application Security’s DbProtect provides comprehensive Database Security Process Control.

DbProtect:

- Will enable Federal agency CIOs to meet and exceed the new OMB mandate for continuous monitoring.
- Will provide a broader spectrum of vulnerability protection than locking down end points.
- Will require less effort to implement and maintain than a program of locking down end points.
- Meets all related government compliance regulations.
- Integrates with Cyberscope to provide real-time reporting.

of protection around sensitive data. Active Response can be configured to take action when an unauthorized and suspicious database activity is detected. Active responses can be customized to a fine level of granularity: a specific activity, performed by specific user, accessing a specific data, in a specific database.

DbProtect’s SHATTER knowledgebase, for example, contains information on the latest SQL injection attacks. When DbProtect recognizes an SQL injection statement, Active Response can:

- Send an alert to IT Security
- Notify the SIEM system to correlate database activity with web application logs
- Initiate a malware scan to remove the SQL injection code.

DBPROTECT AND CYBERSCOPE

DbProtect provides real time alerts, reporting and analytics. It is designed to integrate and share data with other systems in a security, risk and compliance ecosystem. As proof, DbProtect shares data with:

- Enterprise Database Audit Management systems – Oracle, Microsoft, Sybase and IBM
- Enterprise SIEM and IT GRC systems – ArcSight, McAfee, RSA, R-sam and Archer
- Enterprise Service Management systems – IBM Tivoli, HP and BMC

DbProtect will integrate with and provide real-time data within the Cyberscope framework.

For more information contact Application Security toll free at 866-927-7732 or visit our website at www.appsecinc.com.

5 Key Steps to Database Security Process Control

In order to effectively secure their databases, organizations must address five critical requirements:

- 1. Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
- 2. Eliminate Vulnerabilities:** Identify and fix vulnerabilities that exposing the database on a continual basis.
- 3. Enforce Least Privileges:** Reset user access controls and privileges to allow access to only the minimum data required for employees to do their jobs.
- 4. Monitor for Deviations:** Implement appropriate policies and monitor for any and all activity that deviates from normal and authorized activity.
- 5. Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

Summary of Requirements

	Isolate Sensitive Databases Database Discovery w/Sensitive Data Discovery	Eliminate Vulnerabilities Vulnerability Management	Enforce Least Privileges Rights Management	Monitor for Deviation Database Activity Monitoring	Respond to Suspicious Activity Active Response
Identify and report on location of sensitive data — DG0107	✓				
Security Configuration Compliance (ECSC) Ensure databases are configured in accordance w/DoD guidelines		✓			
Vulnerability Management (VIVM) Identify and remediate vulnerabilities		✓			
Access Need-to-Know (ECAN) DG0122, 0123, 1038, 0776, 0069, 0053			✓		
Separation of Duties and Least Privilege (ECLP) — DG0080, 0119, 0120, 0121, 0005, 0008, 0085, 0086, 0063, 0077, 0040, 0041, 0116, 0124			✓		
Restrict privileged account access to privileged users — DG0040, 0041, 0116, 0124			✓	✓	
Restrict use of privileged accounts for privileged functions — DG0004, 0042, 0051			✓	✓	
Audit Record Content (ECAR) — DG0145				✓	
Immediately report on any suspicious or unauthorized activity — DG10161				✓	✓

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world’s most comprehensive database security knowledgebase from the company’s renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

**APPLICATION
SECURITY, INC.**[®]
www.appsecinc.com