CLABBY ANALYTICS

Research Report

Securing Data: Advanced Methods and Tools

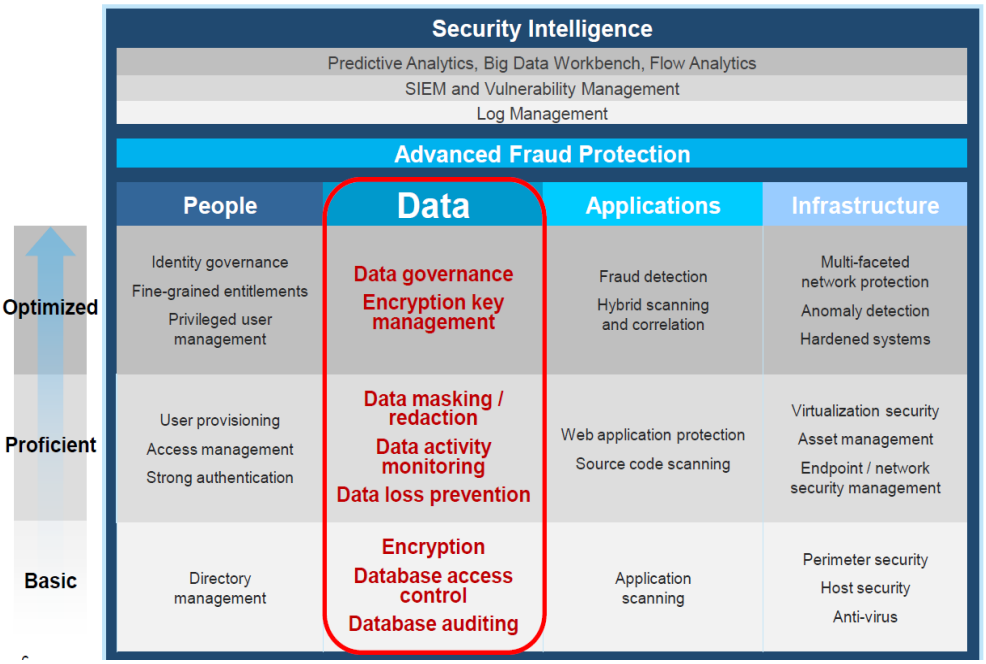
Introduction

Over the past year data breaches have generated negative publicity for several large corporations including Target Corporation, Home Depot, and Apple (more specifically, within the Apple cloud) as personal identifiable information (PII) was stolen from thought-to-be-secure enterprise data-bases. These breaches have highlighted the need for enterprises to become more aggressive and vigilant in securing PII and other data sources. Accordingly, enterprise information technology (IT) buyers are now implementing broader security strategies that include:

- Using predictive analytics to improve systems security;
- Installing software that can protect against data loss, monitor data activity, mask and redact data, govern data and protect encryption keys;
- Installing software to scan applications and source code, and to provide hybrid scanning and correlation as well as fraud detection; and,
- Focusing on people management with stronger authentication, access management and user provisioning as well as privileged user management, fine grain entitlements and identity governance.

This evolving, more sophisticated security/data protection landscape is illustrated in Figure 1.

Figure 2 – How Data Fits into a New, More Comprehensive Security Hierarchy



Source: IBM Corporation – September, 2014

This *Research Report* focuses on what enterprises can now do to better protect data. When it comes to data protection, it is our perspective that, to date, enterprises have largely focused on encryption, database access controls, and database auditing. But we are now seeing increased focus on data masking/redaction, data activity monitoring, data loss prevention, data governance, and encryption key management. To illustrate what is now possible in data protection we examine IBM's Guardium product set, part of IBM's comprehensive Infosphere data management environment.

Readers should be aware that this report is the second in a series of three reports on advanced security methods and products. Earlier this year Clabby Analytics published a report entitled: "IBM's Smarter Counter Fraud Initiative: A Comprehensive, Unique and Aggressive Approach to Real-time Fraud Prevention" in which we discussed some of the activities taking place at the applications layer (in column three of Figure 1) that bring application security beyond application scanning to new levels of proficiency. Our next advanced security report will focus on more advanced security for the infrastructure layer – particularly on cloud security and security intelligence.

The Market Situation

The motivations for implementing better data protection are both financial and have to do with corporate reputation. From a financial perspective, consider Target Corporation's data breach (the second largest breach in history). There are over 90 lawsuits pending on the Target breach, with a potential of a hundred billion dollars in claims at risk. As for damage to corporate reputation, as a result of this breach, Target sales immediately dropped to their lowest level in three years after the company's security breach. Further, Target's reputation was damaged due to the loss of customer PII credit card data – causing customers to lose confidence in the company. For more about the huge legal risks involved in failing to protect data, consider listening to this in-depth Absolute Software webinar hosted by CIO.

Data Protection – The Focus Is Now on Discovery, Masking, Redaction, Monitoring and Blocking

To date, much of the action in the security marketplace has been focused on securing the computer systems perimeter from external threats, using authentication and authorization monitoring software to protect against internal as well as external threats, and protecting data through encryption. Much work still needs to be done to "harden" information systems in order to protect against threats – work such as deploying multifaceted network protection, anomaly detection, virtualization security, asset management and endpoint/network security management. These are all topics that will be examined in our follow-on report on advanced methods of protecting computing infrastructure.

As for protecting data, Clabby Analytics has seen a major shift in the security marketplace as enterprises are now investing more heavily in advanced tools that help protect data. For years encryption methods have been used to protect data-on-the-fly (over networks) in order to make reading that data extremely difficult for hackers. But the major breaches described earlier have shown that even more needs to be done to secure both systems and data. What we are now seeing is increased investment by enterprises in tools to mask, redact, monitor and block/quarantine data.

The Approach

As enterprises endeavor to improve data security several decisions need to be made. First, enterprises need to understand the risk and value of their data, in other words data security assessment and planning needs to take place. Some data does not need stringent protection, while PII data needs the utmost protection. To understand the level of protection that should be afforded

to different types of data, enterprises need to perform value-risk mapping. During this process IT managers and administrators need to work closely with line-of-business management to discover and classify data in their information systems domain.

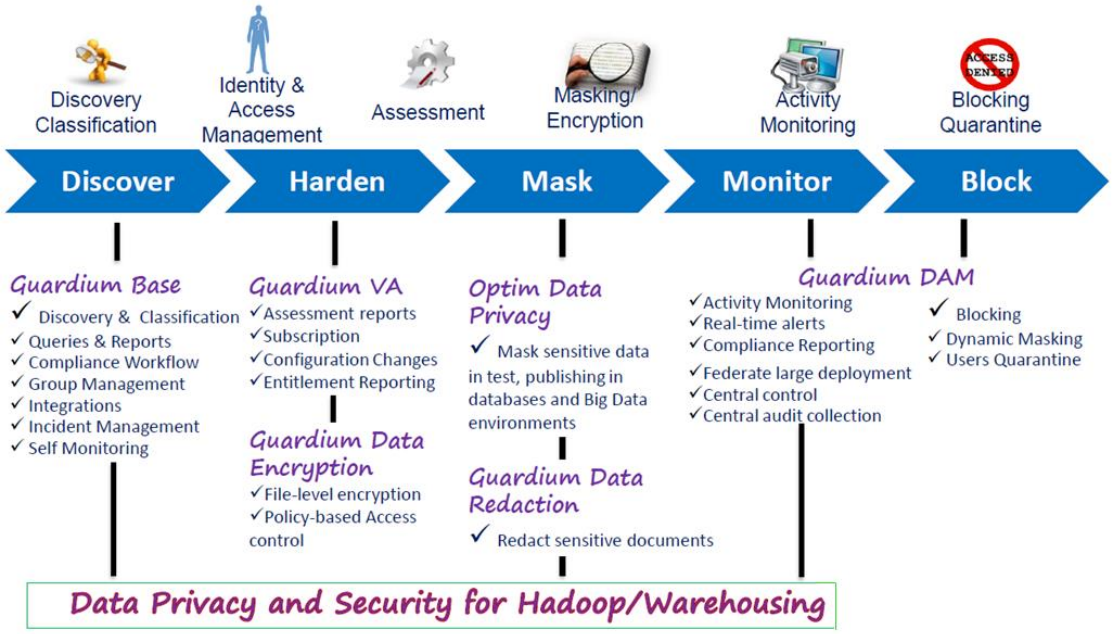
Once data has been classified according to risk level, enterprises can then take steps to protect that data. To do this IT management (usually database administrators) use tools to mask, redact, or encrypt their high priority, must-be-protected data. Data masking is a method of creating a structurally similar version of data by changing certain data elements while information is changed in order to protect the original privacy data. Using this approach structured sensitive information is replaced with realistic but fictional data that is still usable for such tasks as testing, application development, or trend analysis. With redaction, unstructured sensitive information is covered or deleted from view of unauthorized users. With encryption , sensitive information is garbled with an algorithm, and it is only decipherable with the use of a key. This activity provides broad thereat protection against lost or stolen media, unauthorized file sharing, and against abuse by privileged users. The goal during this phase is to reduce risk by cleansing or obfuscating sensitive data. Additionally, vulnerability assessments need to take place regularly; and entitlements need to be reevaluated and cleansed to maintain a tolerable data risk level. This is also known as hardening the data.

After data has been assessed and properly secured and protected it is necessary to constantly monitor data in order to ascertain exactly what is happening with that data directly. (It is believed that part of the failure at Target was in this phase of data management – Target apparently had monitoring tools in place but they were not used properly and did not address access to their data repositories). In this phase, monitoring tools are used to generate real-time alerts on unauthorized/unusual data access. Also, privileged users are monitored; data leakage is checked; breach detection is performed and a threat profile is created and monitored. Using monitoring information centralized forensic analysis can be easily conducted to analyze data activities across the enterprise – and compliance processes can be automated. Further, if critical tampering is underway, enterprises have the ability to block and quarantine users such that the sensitive data is not compromised. To do this, real-time data breach prevention and real-time privacy protection tools are used.

A Closer Look at IBM's Data Protection Offerings

InfoSphere is IBM's name for its family of data integration, data warehousing, master data management, big data and information governance product offerings. Within this product family, IBM's Guardium is the name of the product set that provides data protection facilities. As shown in Figure 2 (next page), Guardium consists of a group of products that can perform discovery classification, identity and access management services, data assessment, tools that mask or encrypt, data activity monitoring tools and tools for blocking/quarantining access to specified data.

Figure 2 – The Guardium Product Set



Source: IBM Corporation – September, 2014

Guardium Base – Discover

Notice in Figure 3 that IBM describes a hierarchy of activities that need to take place in order to secure data (discover, harden, mask, monitor and block). As described in the previous section, enterprises need to start their data protection journey by understanding what and where their data is – and what its risk level is. IBM's Guardium services in the base product help IT managers discover and classify data – as well as some other basic operational requirements such as managing incidents and self-monitor activities. Queries on data activities can also be issued and reports can be derived as part of Guardium Base's monitoring/reporting functionality.

Guardium VA and Guardium Data Encryption – Harden

Guardium VA and Guardium Data Encryption can be used to assist in hardening information systems environments. Guardium VA can be used to create periodic vulnerability assessment reports automatically. It centrally check every database infrastructure (OS and Database Server) for possible miscofigurations or needed patches. An important part of these configuration checks is for understanding the privileges related to the sensitive data, which are surfaced with the entitlement reports. It keeps up to date with the latest vulnerabilities by using a subscription service. Guardium Data Encryption provides non-intrusive centralized strong file-level encryption as well as policy-based access control.

Optim Data Privacy and Guardium Data Redaction – Mask

Optim Data Privacy is a data masking tool that masks sensitive data for application testing or development, or by publishing masked data in database and Big Data environments. Guardium Data Redaction is exactly what its name implies – a tool for redacting sensitive documents.

Guardium DAM

Guardium DAM provides both monitoring and blocking services. From a monitoring perspective it conducts data activity monitoring, issues real-time alerts, automates compliance reporting, helps federate large deployments, offers centralized control and central audit collection facilities. From a blocking perspective, Guardium DAM performs blocking, dynamic masking and allows for user quarantines.

Also noteworthy in the monitoring category is kernel-level monitoring. When it comes to data security, most enterprises want to know who accessed what, where, and when. IBM has built an operating system kernel-level monitor that tracks system/data-source activities – and that can't be bypassed. Importantly, this monitor has no performance impact on a given system because there is not a need to turn on native database logging. And it is extensible to handle a large number of diverse databases.

IT managers who are considering buying services from cloud service providers should consider getting their cloud service provider to install a kernel-level monitor. Failing that, network monitoring is another method for tracking behavior – but, because IT managers don't necessarily know where an application will be hosted in the cloud, off premises monitoring can be difficult. So, if possible, cloud managers should be encouraged to install kernel-level monitoring capabilities.

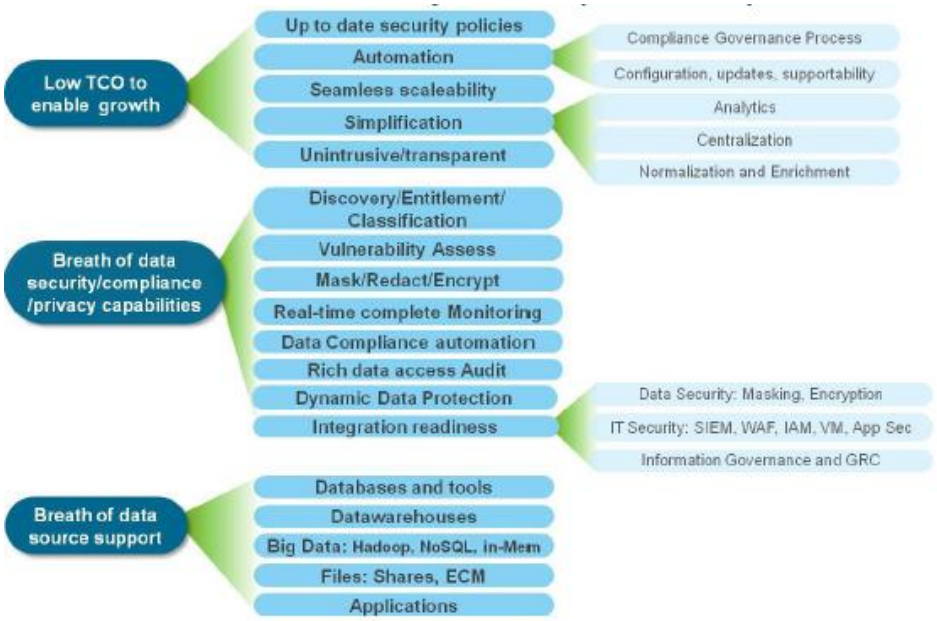
Data Privacy and Security for Hadoop/Warehousing
IBM's Data Privacy and Security for Hadoop/Warehousing is a convenient bundle that performs three functions: 1) discovery; 2) masking; and, 3) monitoring, specifically for Big Data or Data Warehouse environments; it protects sources and data; and it provides identification of sensitive data (discovery and classification) services.

Guardium Data Security and Compliance
Also worthy of note (but not illustrated in Figure 2) is IBM's InfoSphere Guardium Data Security and Compliance appliance, which is part of the InfoSphere Guardium architectural base. This appliance is comprised of a single, integrated virtual appliance that can be used in cloud configurations or on premises, it can dynamically scale, it enforces segregation of duties for database administrators, and it eliminates the need for native audit logs. It also offers a prepackaged vulnerability knowledge base and can generate compliance reports. The primary uses for this appliance are for data activity monitoring and for vulnerability assessment.

Integration is Key
As was the case when we published our fraud detection/prevention report, the *integration* of IBM's security product offerings is a key differentiator. In figure 3 (next page) IBM claims that its data security offerings help minimize total-cost-of-ownership (TCO) costs – and the big reason that IBM makes this claim is due to product integration and ready automation. IBM's Guardium offers an extremely broad set of services ranging from discovery and vulnerability assessment through masking/redaction and include monitoring and control tools – and all of these products have been integrated where appropriate to simplify use. IBM uses dashboard interfaces where to integrate these products with one another to create a seamless and comprehensive means to protect data. By integrating its various data protection products IBM is able to simplify the management of data, thus lowering TCO.

In addition to product integration/simplification, IBM's ability to automate compliance actions helps drive down TCO. Particularly noteworthy in Figure 3 is the governance aspect (upper right) of IBM's data protection offerings. Various compliance standards (such as Sarbanes/Oxley, Payment Card Industry, …) require that information be properly managed, properly secured and stored for long periods of time. Over the years IBM has implemented automated compliance routines that help enterprises comply with compliance standards.

Figure 3 – Integration Is a Key Differentiator



Source: IBM Corporation – September, 2014

Summary Observations

Until recently, we have seen enterprises take a piecemeal, siloed, reactive approach to systems security. Most enterprises usually start by securing the perimeter (using firewalls); then adopt antivirus software; then adopt authentication/authorization software – and finally, these enterprises secure their data using encryption techniques. Over the past year, however, we have seen a decided shift in enterprise security buying behavior – notably, a shift toward improving data protection using more advanced tools and methodologies. We attribute recent large scale security/data breaches as a major driving force behind this change in adoption patterns.

In this report we used IBM's Guardium of product offerings to provide an example of the broad range of data protection facilities, products and tools that are now available in the computer marketplace. But we also chose Guardium because it of its level of integration. With Guardium, IBM offers a comprehensive data security and privacy environment with the widest range of supported data sources and packaged application available on any platform in the industry. Further, as we noted in the previous section, compliance is important – and IBM offers support for dozens of compliance standards as well as pre-written scripts and reports that ensure that compliance requirements are being addressed.

As previously mentioned, this report is the second in a series of security reports. The first report deals with how security can be improved at the application level. This report deals with how data can be better protected. And our final report will deal with how infrastructure can be made more secure. All of these reports are available (or will be made available) on our Website at: www.ClabbyAnalytics.com.

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 846-6662