An Oracle White Paper

March 2013

Oracle Enterprise Transformation Solutions Series

Security in Depth Reference Architecture

ORACLE

Executive Overview

Data is one of the most valuable commodities in the business world today, and organizations continue to find more and more value in it. Unfortunately data also carries a certain amount of risk. According to research performed by the Ponemon Institute, the average cost for a breach of sensitive data is $214 per record[1].

Yet despite staggering financial losses, data breaches are still occurring. Science Applications International Corporation is facing a $4.9 billion lawsuit due to stolen backup tapes[2]. TJX Companies estimates their cost associated with a breach of their customer database to be $250 million[3]. The Verizon Data Breach Investigation Report for 2012 summarizes 855 incidents with over 174 million records in one year alone. And that is just what *they* have investigated.

So why are breaches still occurring? The answers often pertain to inadequate security controls, excessive privileges granted to internal users, and an over-reliance on network and perimeter security. Generally, organizations are still relying on traditional, network based security controls and have failed to truly adopt a secure in depth approach to securing their environment. It is likely that traditional exclusively network-based approach to securing IT environments will fail as organizations further adopt distributed computing paradigms such as cloud computing, and experience an ever-increasing need to support various forms of remote access and mobile devices.

The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to take a holistic approach to protect systems starting with sensitive applications and data. And, they need to protect these key assets from both external and internal threats.

This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached. It enables the right level of security, tailored to the

---

[1] 2010 Annul Study: U.S. Cost of a Data Breach, ©2011 Symantec Corporation

[2] SAIC hit with a second class-action suit, Jan 09 2012, WashingtonTechnology.com staff

[3] Breach of Network Security Rises; Manage Your Risk, Kutak Rock LLP

specific assets, yet in a consistent, flexible, and cost-effective manner that will allow the business to grow. And, it applies equally well with modern computing strategies such as service-oriented architecture, cloud computing, and mobile device access. This paper presents a security in depth reference architecture to address these challenges.

Introduction

Security today involves far more than just password protection, anti-malware solutions, and network encryption. It requires a continuous application of security measures to manage and control access to your most valuable electronic assets – your data. It requires the protection of data, from deep inside the datacenter all the way out to the end users, wherever they happen to be, regardless of the devices they happen to use. It requires security that follows the lifecycle of your data.

Despite best efforts to protect data, security breaches can still occur. Weak passwords, eavesdropping, unlocked devices, and phishing attacks can result in fraudulent activity. The architecture must provide capabilities to detect fraud, either before it can occur or as quickly as possible once it begins. It must support real-time forms of detection, post-incident investigation, and offline profiling and analysis for the purpose of uncovering new and emerging types of attacks.

While prevention and detection are both important facets of security, regulatory pressure also shapes security investments. Remaining compliant, and documenting continuous compliance, can drive up costs. Compliance requirements can also affect the way security is applied. They can mandate certain capabilities and practices that might otherwise be marginalized. While some capabilities are necessary to provide or manage security effectively, others are used to report on the state of security in order to demonstrate compliance.

This paper describes a security in depth reference architecture that addresses all three of these key aspects of security: data security, fraud prevention, and compliance enablement. It presents the reference architecture using both conceptual and logical views. This approach offers a clear separation between views that describe what capabilities the architecture provides and how those capabilities are realized. This paper also describes how the architecture conforms to well established architecture principles, and how it can be achieved using various security products available from Oracle.

Conceptual View

The conceptual view of the architecture, shown in Figure 1 below, brings together three key focus areas of security inside-out. Data security is of paramount importance, and is presented at the center of the diagram. It is flanked by fraud prevention and compliance enablement. Each focus area is described by a set of capabilities that are critical to that aspect of security.

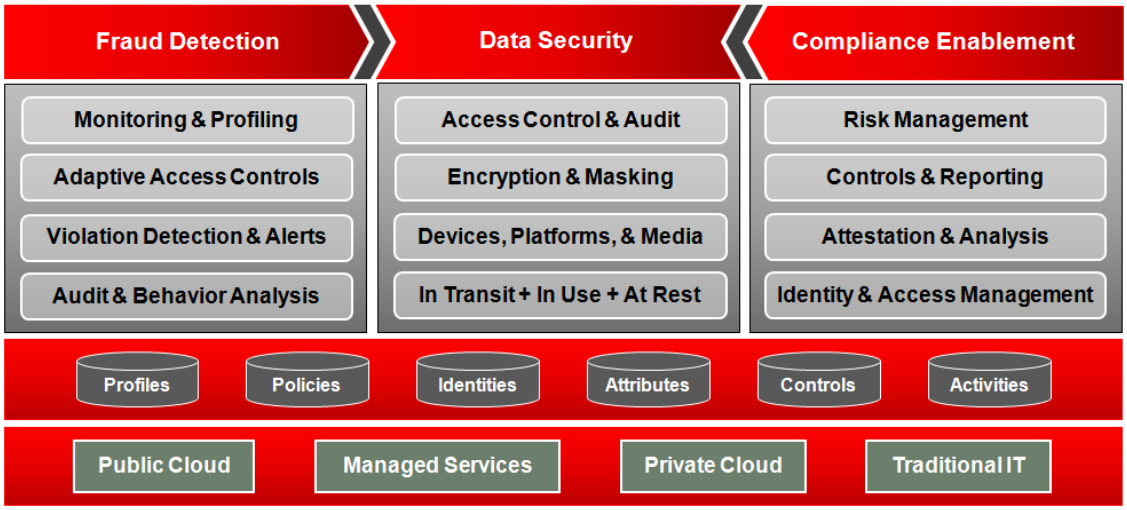

Figure 1: Security Conceptual View

Data Security

Data security is often characterized by the ability to ensure confidentiality, integrity, and availability. It aims to protect data from unauthorized disclosure and modification, while maintaining full availability to authorized users. Access control is critical to this endeavor in order to clearly define who the authorized users are, and to enforce confidentiality and integrity restrictions on enterprise data. User identities and attributes are used to determine access privileges, and access control policies determine what privileges are required to perform operations on the data. Auditing capabilities allow the organization to review operations that have been performed, to know when they were performed, and by whom.

Data confidentiality and integrity are also supported by encryption and digital signatures. Encryption protects data in transit, either via transport layer encryption (TLS), by message level encryption (e.g. XML-Encryption and WS-Security), or a combination of both. Encryption can also protect data at rest. It can be used to protect media such as disks and tapes from low level read operations that can bypass application or database access controls.

An effective data security architecture will protect data in all three states: in transit, in use, and at rest. Data security has become much more complex given the evolution of IT

environments from collections of disparate monolithic systems to integrated, distributed, networked, (and even Cloud-based) systems. Key to providing data security consistently and efficiently is the use of secure computing, database, desktop, and backup platforms. Secure platforms, configured and managed properly, provide the ecosystem necessary to protect data from the inside out. They provide the required security controls at every point in the processing chain, incorporating the latest standards, protocols, and algorithms, to help safeguard one of your most critical assets – your data.

Fraud Detection

While data security mechanisms are designed to manage access to data, they must rely on other controls to help ensure the identity of the end user. If a user's password is guessed, a device is compromised, or a session is hijacked, then fraudulent activity may occur. Likewise, if a privileged user has, or gains, "back door access" to IT systems, then traditional data security access controls may be bypassed. Also, if a user accumulates an excessive amount of privileges over time, then efforts to establish a segregation of duties can be thwarted.

Fraud detection is comprised of both preventative and detective controls. Preventative controls actively monitor user activity and exert security measures when conditions exist that indicate a potential for fraud. The conditions may be a departure from normal behavior, e.g. using a new device or logging in from a foreign country. In such cases, access controls may automatically adapt to the threat and require stronger forms of authentication, such as challenge/response questions.

Fraud conditions may also be related to a set of ordinary activities that are suspicious when viewed together in a given sequence. In the financial sector this may apply to a pattern of financial transactions that could resemble money laundering. In such cases the system may suspend accounts and send alerts when such potential violations are detected.

Fraud detection often relies on behavior profiles or rules to discern normal from suspicious behavior. The profiles and rules may be defined manually based on specific criteria, or they may result from the collection and analysis of activities that serve as a normal baseline behavior pattern.

Detective controls may also be applied as another measure of security. They provide the ability to perform audits and analysis based on ad-hoc criteria. They can be used to perform "what-if" analysis, look for specific trends, investigate the actions of suspicious users, etc. The administrative audit and analysis capabilities provide a backstop for fraud detection that either has not yet been defined or has not yet been codified into a purely run-time preventative security control.

Compliance Enablement

A key aspect to any security strategy is the ability to achieve the proper level of security for a given IT environment. Too little security has obvious drawbacks. Too much security can result in wasted IT spend, poor system performance, reduced productivity, and loss of agility. Each organization must evaluate risks, set goals and objectives, and track progress on achievements over time. This promotes a much more consistent, top-down focus on security. The efforts are rooted in objectives that are recognized as important to the business, and are therefore supported by the business.

Often in the past security goals and objectives for a business or industry were quite discretionary. Over time several regulations have been established to mandate certain levels of security, particularly pertaining to sensitive data such as personal information, financial information, credit cards, health records, etc. Organizations are now required demonstrate compliance with various regulations. The efforts to manage risk, implement security controls, track progress, and report on security issues have become a requirement rather than merely a best practice.

To meet these requirements organizations need to ensure that they have proper security policies in place as well as the security controls to manage and enforce them. Often they turn to automating controls as much as possible to improve efficiency and consistency. Finally, it is important to be able to report on the effectiveness of these controls over time to prove ongoing compliance.

An integral part of compliance enablement is the ability to demonstrate data security in terms of access controls and privileges. Not only must access controls be in place, but the organization must be able to attest to who has access to what, and when. User identities and privileges must be properly managed in a manner that not only establishes the proper segregation of duties, but also enables historical auditing and analysis. Identity and access management plays a crucial role in governance and auditing of compliance issues.

Logical View

The high level logical view of the architecture, presented in Figure 2, illustrates how the concepts of data security, fraud detection and compliance enablement fit together in a multi-layered architecture. A more detailed logical diagram is provided for each concept individually in subsequent sections.

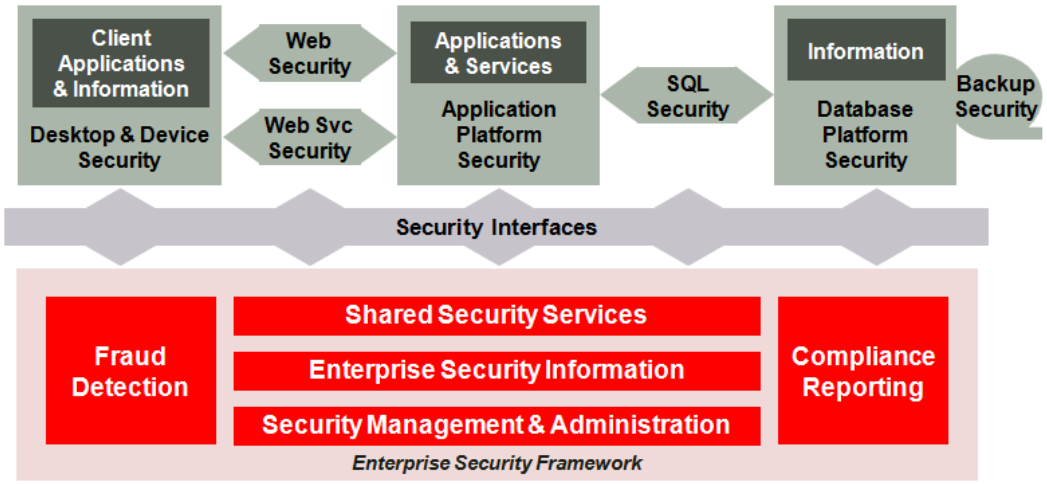

Figure 2: High Level Logical View

The high level view is basically comprised of three main parts: a series of platforms and infrastructure that apply and enforce security controls (across the top), a common enterprise security framework used to consistently manage and govern security (across the bottom), and a set of standard security interfaces that enable communication between security components (in the middle).

The use of secure computing platforms and inter-communications throughout the processing chain is paramount to a successful defense in depth security strategy. It enables each node in the chain to inject security controls as deemed necessary to protect data in use, in motion, and at rest. Data is protected from end to end, from the end user devices through all processing nodes, networks, queues, and databases, all the way to offline backup media.

The enterprise security framework consists of three main layers: a shared set of security services, security information, and components that support management and administration. It also includes components that address fraud detection and compliance enablement. Security services include authentication, authorization, single sign-on (SSO), and attribute services. Security information includes identities, credentials, attributes, roles, policies, privileges, etc.

In order to maximize interoperability, interfaces between security components should be designed to embrace open standards as much as possible. Standards such as SAML, XACML, LDAP, WS-Security, TLS, and SPML are recommended as part of the architecture.

The following sections offer more detailed views into data security, fraud detection, and compliance enablement by further elaborating on these high level architecture constructs.

Data Security Logical Architecture

The data security logical architecture, presented in Figure 3, is focused on securing data from the inside out. It implements access controls, encryption, and auditing components in a manner that protect data from both external and internal threats.

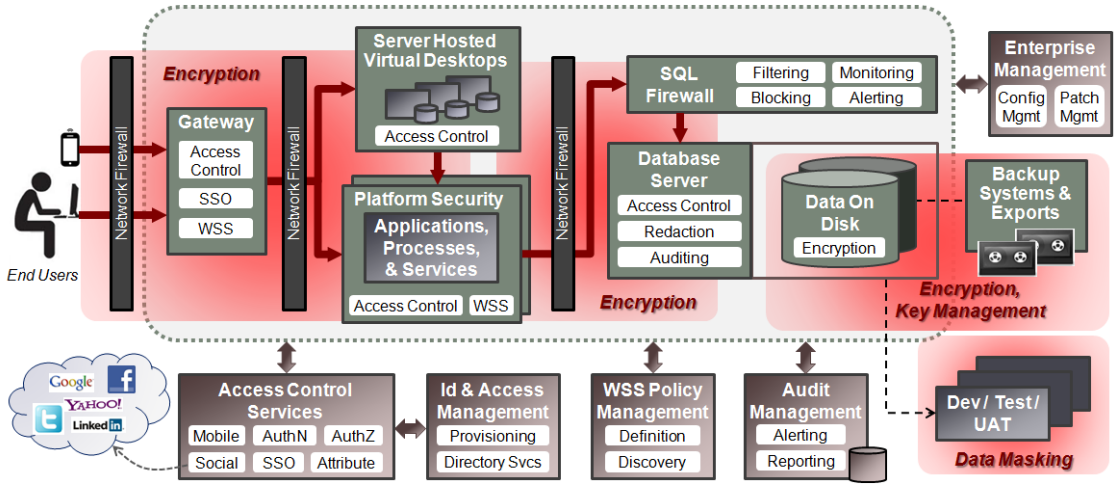

Figure 3: Data Security Logical Architecture View

Central to the architecture is a secure database management system (DBMS) that controls access to data via programmatic interfaces as well as by privileged users. The DBMS supports programmatic access control at the row and/or column level. Row level controls can be used to implement label security, e.g. access based on classification labels applied to data. It can also be used as a safeguard against improper access in single-schema multi-tenancy database environments which are frequently used in Cloud Computing.

Row and column access controls can also be used to filter or redact data based on the privileges of a user. This permits the deployment of common data services that serve multiple types of consumers. Redaction rules are administratively controlled and audited.

Access controls are also applied to administrative functions performed by privileged users. They allow the configuration of privileges based on administrative role, and can enable administrative functions without providing access to the actual data. Access can also be maintained on tables and schemas, providing further segregation of administrative duties. In addition, the identity and access management component provides the capability to manage and track administrative user access by issuing one-time passwords for administrative access.

Access control is applied at other layers of the architecture as well. When end users attempt to access data, their requests pass through several components that perform authentication and/or authorization. For instance, the gateway intercepts requests in the network DMZ, handles user authentication, and supports single sign-on (SSO). Applications, processes, and services may be configured to accept SSO tokens or require their own form of authentication.

The identity of the user can be passed along from one component of the architecture to another in order to authorize (grant or deny) requests and to identify users for auditing purposes. Each platform adds an additional layer of security, transparent to the end user.

A key element of the architecture is the use of common access control services. The gateway, application platforms, and database platforms all leverage the same set of services. This not only provides consistency in the way security is applied across the data center, but also enables a seamless environment that can be holistically managed. It allows security controls to be injected into the processing chain without worry of introducing problems that often stem from inconsistencies in the management of security information across platforms and services.

The authentication service can be driven by identities and credentials that are managed internally, or by those maintained elsewhere in the cloud. Internal identity management is recommended for access to sensitive information, business processes, and services. However, access to some applications and data may be provided using common social media credentials. This encourages new customers to acquaint themselves with products and services without the need to set up new user accounts – often an impediment to establishing a new business relationship.

Encryption is also an important aspect of data security. While encryption is frequently used to protect data in transit across public networks, it should also be used internally depending on information sensitivity. The data security architecture supports encryption between all components of the architecture. This can be accomplished using transport layer security (TLS), message level security, (such as XML-Encryption within Web Service Security), or a combination of both. Encryption is handled by the platforms, allowing it to be configured easily, and eliminating the need to provide such functions with custom-developed code.

Encryption is also used to protect data at rest. Data can be automatically encrypted when it is stored to disk or backup media. This protects the data from disclosure that could occur through the use of disk or tape scanning tools. Disk encryption is performed during write operations in a way that greatly minimizes latency, making it virtually transparent to the end users. In addition, key management techniques are used to enable the easy rotation of encryption keys and the management of large numbers of keys across backup devices.

To further protect data where encryption is not possible, the architecture supports data masking. This allows sensitive information to be transposed in a manner that will not hinder ordinary database operations, such as maintaining referential integrity and data type constraints. Data values are changed yet conform to schema requirements, allowing database

extracts that ordinarily contain sensitive data to be used for development and testing purposes.

The architecture also includes components that provide monitoring, filtering, alerting, auditing, and reporting capabilities. The database firewall provides both active and passive security controls to protect the database from inappropriate access. It is used to actively filter out SQL requests that are deemed unsafe, such as nested statements that are typically used in SQL Injection attacks. It can also passively monitor SQL traffic, generate reports, and send alerts.

Auditing is recommended on all databases, particularly where sensitive information is stored. It enables the tracking of information access and changes as well as administrative operations that could be used to compromise data security. Given the large number of databases an organization might maintain, the architecture includes a centralized audit management and collection point. This allows auditing to be managed consistently and efficiently across the enterprise, and it enables audit records to be stored in a secure location where reporting and analysis can be performed.

In this architecture data security extends from the database all the way out to the end user. One way of doing this is by maintaining end user data inside the organization as opposed to maintaining it on end user devices. Server hosted virtual desktops are included to surface end user applications and data on end user devices virtually, rather than physically. Users can move from one device to another, in and out of the data center, while their data and applications remain safe and secure behind network firewalls. Virtual sessions emulate the flexibility and autonomy of a standalone environment, but avoid the security and maintenance issues an organization often faces when managing data and applications across hundreds or thousands of laptops and PCs.

Management of the architecture and platforms is also included in the security architecture. A common management platform is defined that provides access to platform configurations, logs, and settings. The management platform also provides a way to manage configurations and patching across the whole environment. This makes it easier to ensure that critical security patches are being installed on all platforms and that configurations are maintained according to recommended security practices.

Fraud Detection Logical Architecture

The fraud detection architecture, shown in Figure 4, enhances data security by adding both preventative and detective security controls. The architecture builds upon the platform and database security components (introduced in the previous section) and adds several components that are used to detect fraudulent activity.

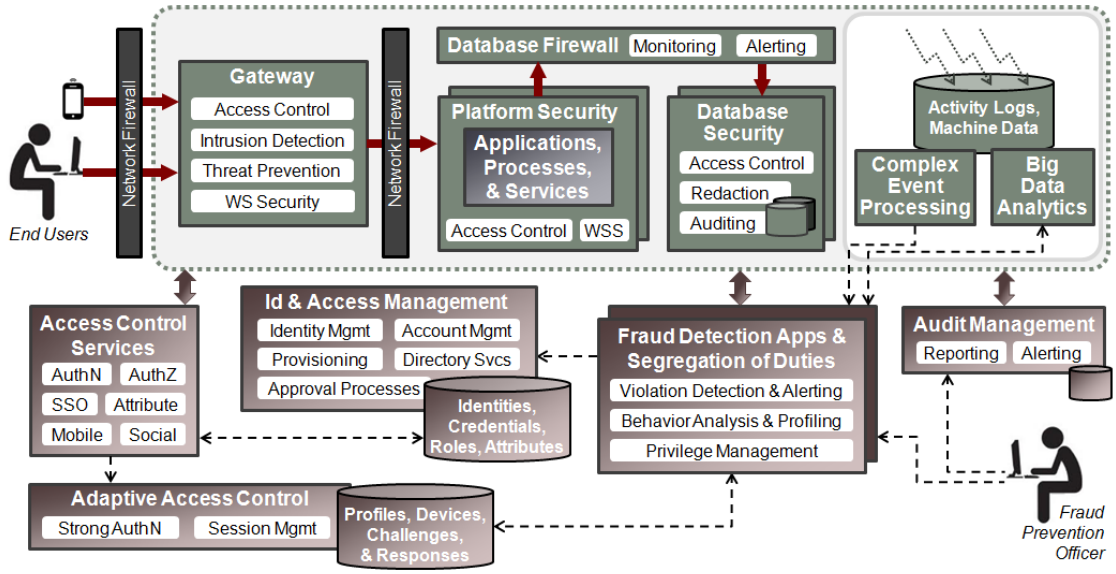

Figure 4: Fraud Detection Logical Architecture View

Beginning with end user access, the gateway component adds fraud detection capabilities by examining inbound requests. It can inspect messages and payloads looking for potential signs of hacking. Common attacks, such as malformed content, recursive payloads, and cross-site scripting, can be thwarted before they result in any actual fraudulent activity. The gateway is designed to handle multiple delivery channels such as standard HTML, Web Services, and mobile devices.

Once a request clears the gateway further scrutiny is applied to the authentication routine. An adaptive access control component has been added to the architecture to enhance the access control services. It examines the context of the authentication request, taking into account factors such as device identification, time of day, IP address, previous failed login attempts, etc. If conditions appear normal, then authentication will proceed as usual. However, if conditions are questionable, then a stronger authentication mechanism may automatically be triggered. Likewise if conditions are unacceptable, e.g. a blocked user id or unacceptable country of origin is found, then authentication is rejected entirely. Many users are familiar with this feature; when logging into a site with a device they've never used they are challenged with questions that must be answered correctly in order to continue. This is known as knowledge based authentication (KBA).

The adaptive access capability demonstrates a key advantage of implementing platform security and common security services. Since all platforms provide access control, and access control is provided via a common enterprise service, adaptive access can be incorporated and managed across the enterprise from a single point in the architecture. Fraud detection is universally applied across all data sources and access channels.

Sometimes fraud is committed by legitimate end users of the system. Often it is the result of users having privileges to perform functions beyond the scope of their assigned roles. Similarly, fraud can result from assigning users multiple roles that are meant to be kept separate as a means of monitoring and safeguarding operations. For example, the initiator of a purchase may require approval from a manager. If one individual is assigned both privileges, then that safeguard is eliminated. Such circumstances can easily occur when users move from one position to another within the organization and privileges are accumulated rather than properly managed.

The architecture includes a component for managing user privileges. It works in conjunction with identity and access management infrastructure to maintain proper segregation of duties. Privileges are managed across enterprise applications from a common governance platform. Access rights are then provisioned to LDAPs, databases, applications, etc.

Fraud detection also applies to administrative user activities. A user with administrative privileges may attempt to manipulate the system for personal gain. This may include creating false accounts, entering data via administrative interfaces, and removing records to conceal fraudulent activity. The architecture addresses this concern using a combination of administrative account management and auditing capabilities.

Identity and access management provides the capability to manage administrative accounts. It does so by controlling the passwords to applications, services, middleware, databases, and operating systems. When a privileged user requires access, the system will generate and set the password for the target asset, and then provide the password to the user. When the user is finished with the asset, the system will reset the password on the target asset. This helps with fraud detection by tracking access via group administrative user accounts down to individual users.

An important part of the architecture is a robust audit management system. It collects audit records that include such activities and securely manages them apart from individual databases. It manages the types of records that are collected and applies the audit profile across all databases. Further, it supports the reporting and analysis of audit records across multiple databases.

Fraudulent activity, once it occurs in the system, can be detected via a number of means. Some are geared towards recognizing predictable patterns, while others are meant for ad hoc investigation and analysis. The architecture includes components to support both forms of fraud detection.

In certain industries where incidents of fraud are common, applications are available to help monitor and track patterns of activity that tend to be suspicious. These applications provide

an easy way to cover many of the known fraud use cases for a particular industry. The architecture positions them as fraud detection applications, although they may serve other purposes as well. The applications interact with other applications, processes, services, and databases as needed in order to monitor for known fraud-related activities.

In addition to supporting known forms of fraud, the architecture includes components that enable an organization to analyze and investigate new and emerging threats. Big data analytics represents the analysis of large data sets such as activity logs and machine generated data. It can be used to correlate patterns of behavior that represent fraud in an attempt to recognize when a problem is about to occur.

Once a pattern has been identified it may be codified into an automated response. For instance, if a credit card appears to be compromised then the account can be locked before any additional charges are authorized. The complex event processor is used to monitor activities for a specific pattern. It triggers an alert or a process to lock the account when the suspicious event pattern occurs.

Compliance Enablement Logical Architecture

The architecture for compliance enablement, shown in Figure 5, supports efforts to manage compliance activities and to demonstrate results. It leverages several components that are vital for data security and fraud detection, and highlights some new capabilities specific to compliance enablement.

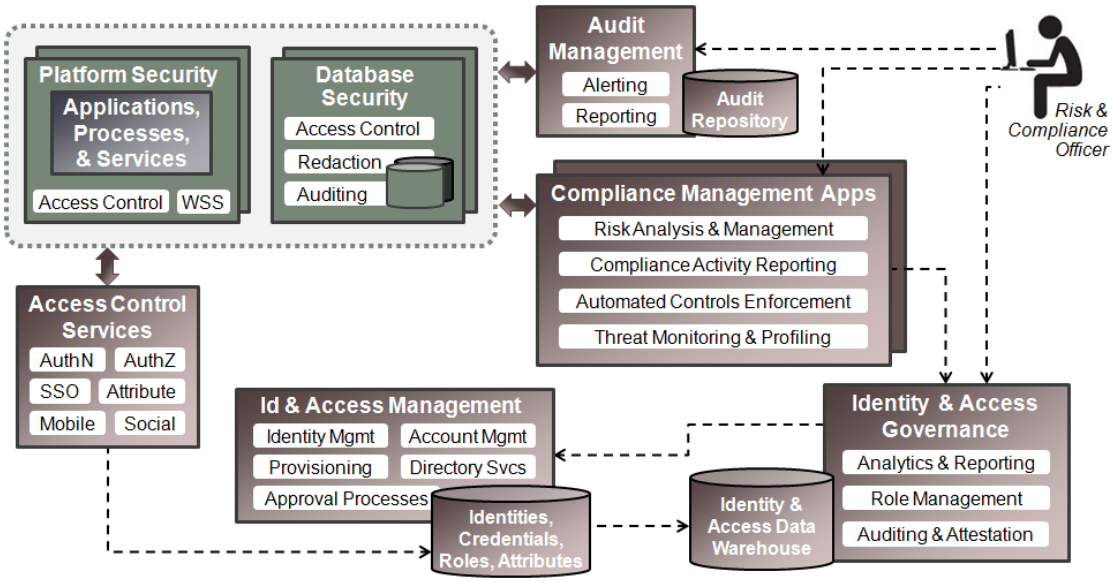

Figure 5: Compliance Enablement Logical Architecture View

Access control and auditing are important characteristics that underpin the architecture, enabling security to be applied and demonstrated at each layer of the architecture. As described in previous sections, platform security, database security, access control services, identity management, and audit management provide these capabilities. Without a consistent and comprehensive approach to access control and auditing, instituting and demonstrating compliance would be unachievable.

Identity and access governance takes identity management one step further by providing the tools that are necessary for a compliance officer to audit and attest to access privileges across the organization. It uses an identity and access data warehouse to store historical access privilege data. This offers the ability to view access rights across various points in time. It also enables analysis and reporting based on varying dimensions such as user hierarchies, function and data hierarchies, and time period hierarchies.

Governance also extends to the definition and management of enterprise roles, which can be used to manage access to functions and data. The governance component feeds into identity management in order to support the provisioning of role and privilege changes to identity stores.

The architecture also positions applications that are specifically designed to support compliance management and reporting. These applications provide a common foundation for managing risk and compliance documentation, assessment, analysis, and certification. They are used to manage and track compliance-related activities and automate governance process management and security controls monitoring. The applications enable real-time event escalation and reporting.

Architecture Principles

The logical architecture presented in this paper supports several well established security architecture principles, including:

- Defense in Depth
  The defense in depth strategy advocates the use of multiple defense mechanisms, in various forms, in multiple layers, in order to protect one's resources as opposed to a single barrier or perimeter. It aims to win the war of attrition rather than rely on the strength (or vulnerability) of a single barrier.

  The architecture promotes a defense in depth strategy in several ways. First, it recommends the use of secure platforms for all information processing and storage. Each application layer (web tier, application tier, database tier, etc.) is expected to enforce the necessary forms of security.

Second, it promotes security at multiple layers of the processing stack, i.e., network layer security, host security, application security, and data layer security. Specifically, access control and encryption are applied throughout the architecture in different layers.

And lastly, it provides a common security infrastructure that ties all these layers together. Each layer can draw from the same security services and identity and access information, enabling a seamless secure flow of information throughout the system.

- Least Privilege and Segregation of Duties

  Least privilege and segregation of duties are popular ways to minimize the risk of malicious or fraudulent activity. With least privilege, each user has only the privileges they need to do their job. Access to all other functions is denied. Segregation of duties creates a separation of privileges in order to avoid conflicts of interest. It also helps guard against any one individual having too much power, which translated into a security context equates to an accumulation of privileges that can manifest undesirable consequences.

  The architecture addresses these principles through a holistic approach to identity and access management. The enterprise security framework includes components to manage, analyze, and govern security privileges. The output of analysis is fed into the identity and access management system, which in turn is used to drive the authentication and authorization services. Since all information processing and storage platforms use these common services, the least privilege and segregation of duties initiatives are propagated out across the IT landscape.

- Security as a Service

  Security as a service is a central tenant to the security architecture. It involves the use of common security services, wherever possible, to support all functions related to security. The intent is to promote the rationalization of security functions and consolidation of information used to make security decisions.

  One of the main drivers of this principle is the emergence of distributed computing initiatives. Service-oriented architecture (SOA), business process management (BPM), and cloud computing are all prime examples of technology strategies that embrace and promote distributed computing. A disjointed approach to security will quickly break down and become unsustainable as the degree of interoperability increases. Security services solve this problem by offering a consistent foundation to build upon.

  Security as a service also recommends the use of services and infrastructure over custom code. This helps to reduce threats related to coding errors made by developers who are often not well versed in security technologies. It also moves the management and administration effort for security away from code maintenance and places it into infrastructure that can be more easily configured, audited, and managed.

Oracle Product Mapping

This section describes how the logical architecture can be implemented using security products that are available from Oracle. The relationship between architecture components and products is not intended to reflect a one-to-one mapping as some products have multiple features. Likewise, some components will map to multiple products that support different technologies or unique sets of capabilities.

The list of products presented in this section is not intended to represent the entire suite of products available from Oracle. Rather, they represent a best match to the scope of the architecture that is addressed by the conceptual and logical views. Additional products are available to handle other aspects of security. For more information on Oracle security products, or further information on product features, please consult the Oracle website or an Oracle product specialist.

Data Security Product Mapping

Figure 6 illustrates how Oracle products map onto the architecture for data security.

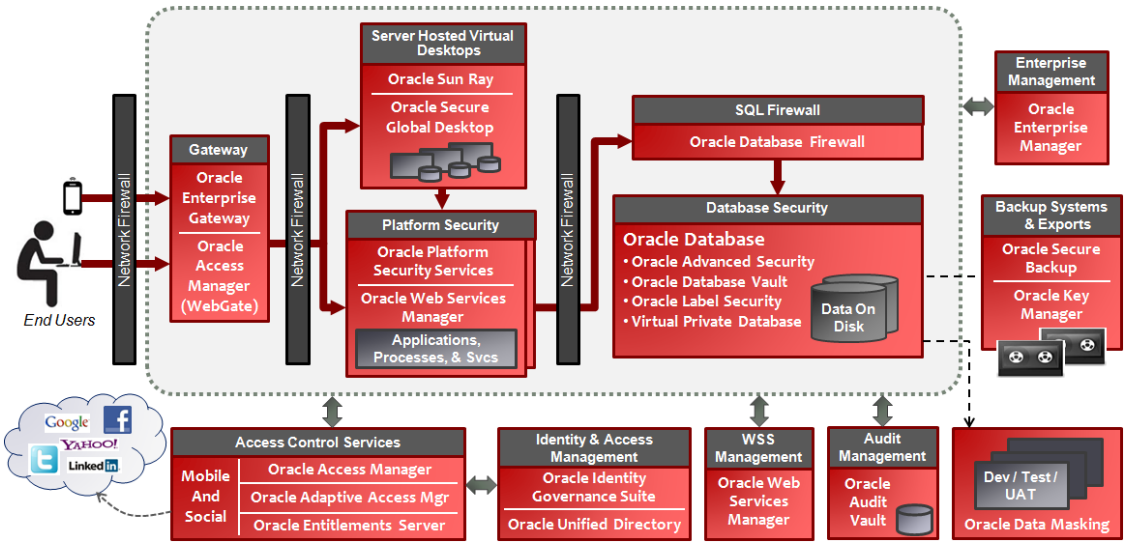

Figure 6: Data Security Product Mapping

The gateway, deployed in the DMZ, represents a logical component that is comprised of one or more products. **Oracle Enterprise Gateway** is designed to secure SOA deployments, either in house or in the cloud. It handles web service and REST traffic and provides many features including access control, auditing, message validation, threat detection, and auditing. **Oracle Access Manager** is used to support standard web based access control and SSO. It includes

agents that are deployed on the Web servers that work in conjunction with an access management server. The agents are logically considered part of the gateway in this architecture while the access management server (deployed in a secure network tier) helps to constitute the access control services.

Platform security is provided using a combination of **Oracle Platform Security Services** (OPSS) and **Oracle Web Services Manager** (OWSM). OPSS is an extensible Java-based security framework that provides a wide range of security capabilities for Java EE platforms, such as **Oracle WebLogic Server**, as well as Java SE environments. It includes a plug-in framework and libraries to handle security capabilities including authentication, SSO, authorization, auditing, credential mapping, identity assertion, encryption, and digital signatures. OWSM is an agent-based web service security component. It works in conjunction with OPSS and the web service request interceptors built into WebLogic Server. The OWSM agents handle all functions related to web service security, such as token creation and validation, message encryption, and signing. OWSM includes a web service security policy management server, which is positioned in the architecture under WSS management.

Oracle offers two solutions for server hosted virtual desktops. **Sun Ray Software** is a client/server solution that improves data security by centralizing management, data, and applications in the data center. It provides access to virtual desktop environments from nearly any location and reduces the complexity and operational costs incurred by traditional PC deployments. Client side devices include Sun Ray Clients, PCs, laptops, and tablets. **Oracle Secure Global Desktop** provides secure access to centralized, server-hosted Windows, UNIX, mainframe, and midrange applications from a wide variety of popular client devices, including Windows PCs, Mac OS X systems, Oracle Solaris workstations, Linux PCs, thin clients, and more.

Access to the data tier is provided via a SQL firewall. **Oracle Database Firewall** monitors database activity on the network in real time to help prevent unauthorized access, SQL injections, privilege or role escalation, and other external and internal attacks. It can block, substitute, alert and pass, or log unauthorized SQL statements to the databases it protects.

Database security is provided by options and features of **Oracle Database**. **Oracle Advanced Security** (OAS) performs network encryption to/from the database and transparently encrypts data as it is stored on disk, disk backups, and exports. Disk encryption can be performed on the entire tablespace or specific sensitive columns. It does not require changes to the application. OAS also supports multi-factor user authentication, including PKI, Kerberos, and RADIUS-based strong authentication solutions.

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. It allows you to create realms composed of the database schemas or database objects that you want to secure. You can further secure the realm by creating rules, factors, identities, rule sets, and secure application roles. In addition, you can run reports on the activities these components monitor and protect.

Oracle Label Security enables row-level access control. It controls access to the contents of a row by comparing that row's label with a user's label and privileges. Administrators can add selective row-restrictive policies to existing databases by means of the graphical interface provided by **Oracle Enterprise Manager Database Control**.

Virtual Private Database, a feature of Oracle Database, allows security administrators to assign unique access policies to tables. Access policies can specify custom rules for specific rows and columns of a table. Data is redacted based on the evaluation of policies and run-time parameters.

Security is extended to development and test environment through the use of **Oracle Data Masking.** Oracle Data Masking allows organizations to generate realistic and fully functional data with similar characteristics as the original data to replace sensitive or confidential information. It applies masking definitions to columns in a staging database. The results can be exported and used for development and testing purposes.

Data protection for tape and cloud storage is provided by two **Oracle Secure Backup** offerings. Oracle Secure Backup, centralized tape backup management, provides high performance and heterogeneous data protection in distributed UNIX, Linux, Windows, and Network Attached Storage (NAS) environments. Oracle Secure Backup Cloud Module provides an integrated Oracle Database backup to Amazon S3 cloud (Internet) storage. In addition, **Oracle Key Manager** is available to centrally authorize, secure, and manage all of your encryption keys, reducing exposure of sensitive data and ensuring reliability and security. It encrypts data as it is being recorded onto StorageTek tape drives and protects against both on-premise and off-site data loss.

Access control services are provided by **Oracle Access Manager**, **Oracle Adaptive Access Manager**, **Oracle Entitlements Server,** and **Oracle Access Management Mobile and Social**. The Oracle Access Manager's server works in conjunction with the gateway agents (mentioned previously) to provide user authentication, SSO, and coarse grained authorization services. Oracle Adaptive Access Manager (OAAM) automatically adapts the strength of authentication based on contextual information pertaining to user access. For example, when a user attempts access from a suspicious location or a new device, or when access is attempted from multiple locations in a short period of time, OAAM will require stronger

forms of authentication such as KBA. Oracle Entitlements Server externalizes and centralizes fine-grained authorization policies for enterprise applications, web services, and data. It allows access decisions to be based on more detailed conditions such as real time contextual information and environment variables. Oracle Mobile and Social extends access control and SSO to mobile devices. It connects mobile access to the access control services so that existing security services can be leveraged by mobile devices. It also enables user authentication via social network authentication APIs.

Identity and Access Management is included to control and govern security information such as user credentials, attributes, role assignments, and access policies. This information underpins the access control services. **Oracle Identity Governance Suite** is a combination of three integrated products that fulfill this purpose: **Oracle Identity Manager**, **Oracle Identity Analytics**, and **Oracle Privileged Account Manager**. Oracle Identity Manager handles the approval and provisioning processes for identity management. Oracle Identity Analytics provides capabilities to support role management, auditing, attestation, and analytics of security information. Oracle Privileged Account Manager enables organizations to control access to privileged accounts by managing the creation and revocation of account passwords. Users are required to check-out and check-in passwords in order to gain access to administrative accounts. Directory services, used to organize, persist, and access security information, are provided by **Oracle Unified Directory**.

Audit management is handled by **Oracle Audit Vault**. It automates the consolidation of audit data into a secure repository which includes audit policies, access control, audit alerts, and reports. With Oracle Audit Vault database audit settings are centrally managed and monitored.

Management of Oracle products across the architecture is handled by **Oracle Enterprise Manager**. Oracle Enterprise Manager provides comprehensive management solutions to help streamline IT operations with plug-ins for operating systems, hosts, databases, middleware, security, network, servers, and storage. It also provides bi-directional connectors for popular management frameworks including IBM Tivoli, HP OpenView, and Microsoft MOM, as well as connectors for popular service desks including BMC Remedy.

Fraud Detection Product Mapping

The architecture for fraud detection can be implemented by several products, as shown in Figure 7.

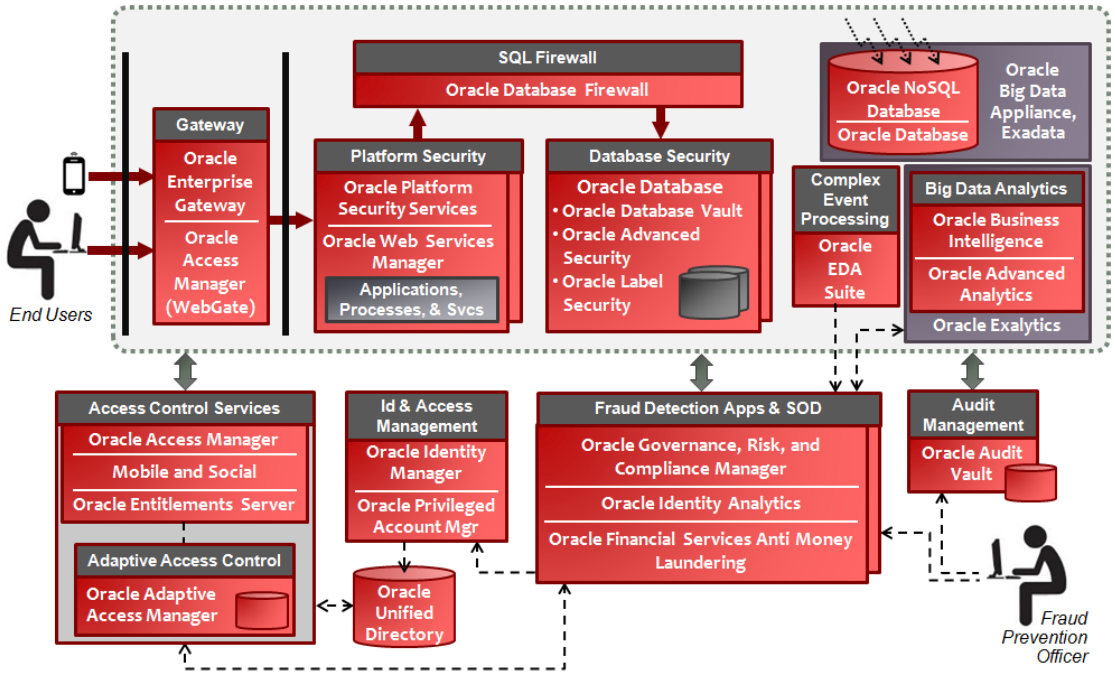

Figure 7: Fraud Detection Product Mapping

The architecture includes several components that are shared with the data security architecture; therefore the product mapping is also shared. The common components include:

- The gateway is comprised of **Oracle Enterprise Gateway** and **Oracle Access Manager**. These products help with fraud detection by monitoring and/or preventing access to resources from suspicious sources, and by providing audit and alert capabilities. For instance, Oracle Enterprise Gateway will detect malicious content and block SOA requests. Oracle Mobile and Social can recognize and prevent access from unregistered mobile devices. And all three products work in conjunction with adaptive access controls to detect suspicious access attempts.
- Platform security (**Oracle Platform Security Services**), SQL Firewall (**Oracle Database Firewall**), audit management (**Oracle Audit Vault**), and **Oracle Database** security products and features all provide auditing and alerting capabilities that are necessary for fraud detection. In particular, Oracle Database Firewall actively screens SQL requests for SQL Injection attacks – a very common attack vector with Internet facing applications. Whereas Oracle Database Vault and Oracle Audit Vault help protect from fraud that can occur from inside the organization by restricting privileged user activities and auditing their actions.
- Access control services, comprised of **Oracle Access Manager**, **Mobile and Social, Oracle Entitlements Server**, and **Oracle Adaptive Access Manager**, also carry forward from data security. Oracle Adaptive Access Manager is highlighted in this architecture

view for its ability to support fraud detection via access profiling. It monitors contextual information such as location, time of day, and IP addresses. When a user attempts access outside of normal parameters, then stronger forms of authentication are automatically applied.

- **Oracle Identity Manager** helps to avert fraud by properly maintaining access privileges that support the segregation of duties (SOD). Oracle Identity Manager is a comprehensive identity management system that includes provisioning, approval workflow, integration with identity stores and applications, reconciliation, notification, password policy management and reporting. It integrates with many different directory servers from Oracle and other vendors, as well as various operating systems and popular packaged applications.
- **Oracle Privileged Account Manager** helps prevent fraud that can occur via administrative accounts such as root, sysadmin, etc. It eliminates the potential for fraud resulting from having passwords that are known to more than one person at a time, or passwords that remain the same for long periods of time. Privileged users are issued newly created passwords when they need to access the system. The passwords are reset once the user is finished with their work on the system.
- **Oracle Unified Directory** provides a comprehensive set of directory solutions for high-performance enterprises and carrier-grade environments. It includes scalable, industry leading LDAP directories for identity information as well as directory synchronization and virtualization capabilities.

Fraud detection also includes components and products that have not previously been described. Highlighting this architecture are offerings used to collect, analyze, audit, report, and maintain privilege assignments. **Oracle Identity Analytics** organizes access privileges into a data warehouse that facilitates the attestation and governance of end user privilege and enterprise-level role assignments. It provides an enterprise-wide view of roles and privileges across IT technologies. In addition, **Oracle Governance, Risk, and Compliance Manager** automates SOD enforcement across enterprise applications. It focuses on application-level role and privilege assignments as they pertain to specific business functions. Edge-to-core coverage of access controls prevents SOD conflicts from arising and applies least-privilege principles to protect sensitive information.

Oracle also provides applications that have been designed specifically to support fraud detection, such as **Oracle Financial Services Anti Money Laundering**. This application, available as a part of the **Oracle Financial Services Analytical Applications** offering, provides automated surveillance of all accounts, customers, correspondents, and third parties in transactions across all business lines. It allows organizations such as banks, brokerage firms, and insurance companies to monitor customer transactions, providing a holistic view of all transactions and activities.

Fraud detection via the collection and analysis of Big Data is also supported by Oracle. The **Oracle Big Data Appliance** is an engineered system that combines optimized hardware with the most comprehensive software stack. It is a high performance system specifically designed to collect and organize large quantities of data. The software stack includes a NoSQL database, a full distribution of Cloudera's Distribution with Apache Hadoop (CDH), an open source distribution of the statistical package R for analysis of unfiltered data, and tools for operating and managing the system.

Once data of value has been found, it is frequently moved from the NoSQL database to a relational database or data warehouse where more sophisticated analytics and data mining can take place. Oracle Database is shown on the architecture as this data repository. **Oracle Big Data Connectors** (not shown) are used for data integration with the Hadoop Distributed File System (HDFS).

Oracle Business Intelligence and **Oracle Advanced Analytics** provide analysis, reporting, alerting, and data mining capabilities. They feed fraud notifications and alerts into applications and dashboards used by fraud prevention personnel. Oracle Business Intelligence is available as a standalone software solution, and as part of an engineered hardware and software analytics solution, **Oracle Exalytics**. Oracle Exalytics combines Oracle Business Intelligence with Oracle Times Ten in-memory database, Oracle Essbase multidimensional OLAP server, and industry leading hardware and networking, to create a high performance in-memory analytics solution.

Fraud conditions that can be programmatically identified are configured into a complex event processor. The processor monitors activities, such as those associated with Big Data, looking for the predefined patterns of activity. **Oracle EDA Suite** includes a complex event processor to support this event-driven fraud detection architecture capability.

Compliance Enablement Product Mapping

Figure 8 illustrates how Oracle products map onto the architecture for compliance enablement.

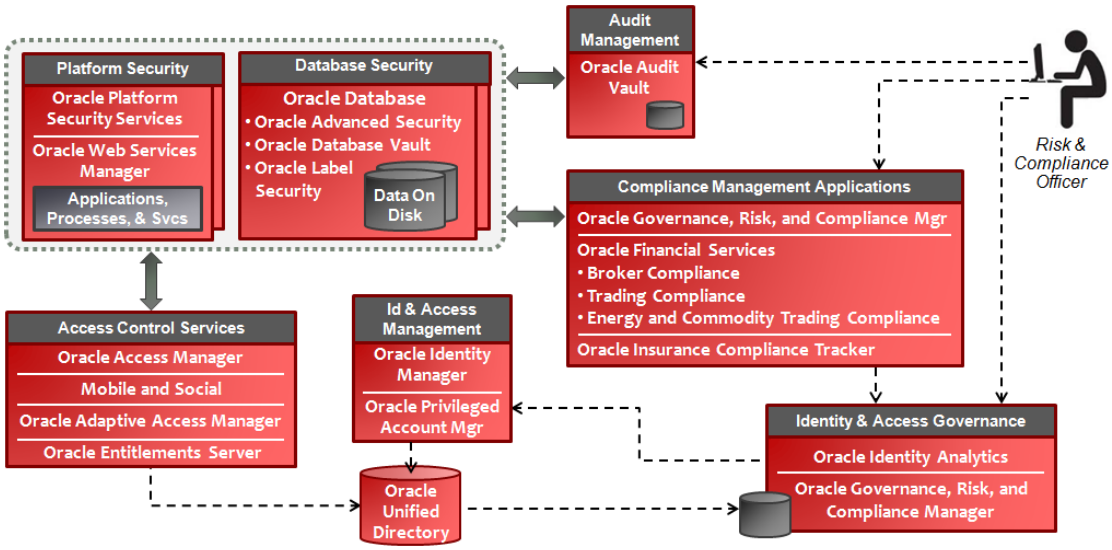

Figure 8: Compliance Enablement Product Mapping

As shown, Oracle provides several applications that are designed to help companies manage their compliance activities. **Oracle Enterprise Governance, Risk, and Compliance Manager** (Enterprise GRC Manager) provides a common foundation for managing risk and compliance documentation, assessment, analysis, and certification, allowing organizations to address multiple regulatory requirements. It creates a consolidated view of compliance, risk and internal controls that allow for centralized monitoring, reporting, and management. Enterprise GRC Manager highlights key risk and performance indicators via executive-level dashboards that can drill down to detailed evidence in source systems.

Oracle also provides applications that are designed for regulatory compliance within specific industries. They help to manage and automate specific activities that relate to current regulatory requirements. For instance**, Oracle Financial Services Trading Compliance** uses pattern recognition techniques to monitor trading and market making activities for potential cases of market abuse. **Oracle Financial Services Broker Compliance** can monitor customer suitability, trading abuses, and broker selling practices, to identify problematic activities related to customer interactions. It alerts analysts and investigators with a context of business data and historical information with which they can streamline analysis and resolution. **Oracle Insurance Compliance Tracker** provides insurers with end-to-end automation of state filings, including pre-population of filing forms, automatic conversion to PDF, and an up-to-date knowledge base for the latest information on state filing regulations.

The architecture also includes several components that are shared with the data security and fraud detection architectures, such as:

- Identity and access governance is provided by **Oracle Identity Analytics**. It offers the ability to collect, analyze, audit, report, and maintain privilege assignments across the IT environment.
- Audit management is provided by **Oracle Audit Vault**. It centralized the management and collection of audit records across all Oracle databases in the IT environment.
- Platform security (**Oracle Platform Security Services**), and **Oracle Database** security products and features provide auditing and access control capabilities that are necessary to enforce and support compliance enablement.
- Access control services, comprised of **Oracle Access Manager**, **Mobile and Social, Oracle Entitlements Server**, and **Oracle Adaptive Access Manager.** They leverage a common set of credentials, privileges, and access policies to provide a consistent means of authentication and authorization.
- Identity and access management is handled by **Oracle Identity Manager, Oracle Privileged Account Manager,** and **Oracle Unified Directory**. Oracle Identity Manager handles user and access provisioning, approval workflows, integration with identity stores and applications, reconciliation, notification, password policy management, and reporting. Oracle Privileged Account Manager provides access to administrative accounts by issuing and resetting account passwords. Oracle Unified Directory includes scalable, industry leading LDAP directories for identity information as well as directory synchronization and virtualization capabilities.

Conclusion

Most businesses currently focus on securing their network and endpoints. Spending on security continues to rise in response to increases in the number and complexity of external threats. Yet the number and scale of security breaches continues to rise, as does the cost of dealing with these breaches.

Oracle's security in depth architecture helps you prevent, detect, and respond to threats. It focuses on the most vital asset – your data. It starts from deep within the organization, protecting data at rest, in use, and in transit. It combines robust, proven application and database platform security, the latest in standards and technologies, versatile security services, and advanced monitoring and management capabilities, to produce a secure and cost effective solution.

The architecture presented in this paper provides a blueprint for security. It follows the most widely adopted security principles and best practices, and it describes a scalable architecture that addresses aspects of security that are critical to all organizations – data security, fraud detection, and regulatory compliance.

Though the architecture is designed to be vendor- and product-neutral, Oracle's depth of expertise in databases, applications, middleware, and hardware makes it the vendor of choice for securing these assets. Oracle provides market leading products across the entire IT stack and is a leader in identity and access management solutions.

In addition, Oracle provides expert consulting services to help customers with their security needs. Their understanding of security architecture, technologies, and strategy, coupled with their experience with Oracle products, makes them a valuable resource for all phases of planning and delivery. Please contact your local Oracle services representative to learn about how Oracle can help you achieve your security goals.

Further Reading

IT Strategies from Oracle

IT Strategies from Oracle (ITSO) is a series of documentation and supporting material designed to enable organizations to develop an architecture-centric approach to enterprise-class IT initiatives. ITSO presents successful technology strategies and solution designs by defining architecture concepts, principles, guidelines, standards, and best practices.

This document on security architecture highlights several aspects of security that are presented in the Oracle Reference Architecture (ORA) Security document. ORA Security is a comprehensive security architecture document complete with concepts, standards, and architecture views. It is included in the ITSO collection. Please consult the ITSO web site for a complete listing of materials in the ITSO series.

Other References

Further information about the products and services described in this paper can be found on Oracle's web site at: http://www.oracle.com/us/products/index.html

Security In Depth Reference Architecture
Release 3.0

March 2013

Author:
Dave Chappelle
Global Enterprise Architecture Program

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together