Security Inside Out

Oracle Security Solutions

April 2008

EXECUTIVE OVERVIEW

Information Security has changed radically in the last decade, and is more important today than it has ever been in the past. Security has become more visible as a business issue across all industries and affects organizations of all sizes. In the current environment a security breach has the potential to impact a business's bottom line - damaging its reputation, customer loyalty and profitability. Furthermore, compliance with governance and privacy regulations has put an unprecedented executive level focus on the need for strong security controls.

Managing security risks in today's environment requires an enterprise security framework, one that extends beyond traditional network perimeter measures to protect applications, middleware, and data infrastructures.

Oracle offers the industry's leading comprehensive best-in-class security solution, and the only one of its kind to enable a common security framework for applications as well as data. Oracle's ability to secure not just the Oracle database, applications, and middleware, but also all the leading enterprise applications and platforms (including SAP, IBM Web Sphere and others) enables customers to leverage and protect their existing investments. Oracle security solutions include:

- **Access Control Solutions**. Industry-leading access control solutions that span directory services, user provisioning, authentication and authorization, separation of duties, enterprise single sign-on, web services security, and identity federation.
- **Data Privacy Solutions.** Unique and cutting-edge data privacy solutions including privileged user access control, encryption for data at rest as well as data in motion, data classification, secure backups, and secure enterprise search.
- **Governance, Risk, and Compliance Solutions.** Comprehensive solutions for Governance, Risk and Compliance that include identity auditing and reporting, audit consolidation and risk & compliance process management.

INTRODUCTION

Information Security, Now a Business Issue

"Here's the primary reason we believe IT risk is a concern for LOB executives: the many public and painful disclosures, especially security breaches that have dramatically affected brand image and the financial health of many public companies. IT risk, specifically data security, has truly become a board-level discussion."

- AMR Research[1]

Over the last ten years, information technology has brought new levels of business opportunities and productivity gains. IT has become a strategic business growth engine, opening up doors to new customers, enabling new products and services, and improving customer experiences. However, as more and more business is driven across the Internet, it also places critical information beyond the safety of a data center.

Information security has changed dramatically in recent years. What used to be the domain of hobby hackers has now entered the attention of criminals looking to profit from online fraud. Hackers have become increasingly sophisticated in their attacks, often challenging technology to its limits. Previously one of the worst things that could happen was someone broke into your website and changed the front page – today you have to worry about them stealing your intellectual property and sensitive information about customers and employees, or even corrupting critical data needed to keep your business operational. Furthermore, as the Internet has grown in the amount of business conducted online, so has the frequency and number of threats that organizations are constantly faced with.

"21% of enterprises are worried about a decline in stock price [resulting from a security breach]"

—Forrester Research[1]

The fact that a security breach today makes front page news in mass publications such as the Wall Street Journal or New York Times has made business executives very sensitive to the security of their IT systems. According to Forrester Research, "21% of enterprises are worried about a decline in stock price [resulting from a security breach]"[2]. This has given information security a CEO and Board level awareness it never had before.

Another business issue that is top of mind for executive management today is regulatory compliance. The pressure to comply with regulations such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, SB 1386, and more is extreme, and the consequences of failing to do so are dire. Most compliance requirements are rooted in preventive controls. This makes Information Security the most strategic technical consideration for compliance issues.[3] Automating key tasks based on business policies not only improves security but also lowers the cost of meeting compliance requirements. These tasks include granting and revoking user access, enforcing separation of duties, generating audit reports, and periodically reviewing and attesting to the validity of user privileges.

It is no surprise that Information Security has now become a top priority for CIOs. A business inadequately protected from the constant barrage of threats and attacks risks losing a lot more than data. A single security breach could diminish business reputation, customer loyalty, and ultimately profitability. Information Security is no longer just a technology issue; it has become a critical business issue.

---

[1] AMR Research, *Governance, Risk and Compliance Spending Report 2008-2009,* 2008
[2] Forrester Research, *Aligning Data Protection Priorities With Risks*, April 2006
[3] AMR Research, 2005

Protection beyond the Network Perimeter

In the last few years a lot of attention has been placed on securing the network perimeter. This includes implementing technologies such as firewalls, VPNs, anti-virus, and anti-spam software. These are important controls that present a first line of defense.

"The most prevalent attack style, responsible for 39% of data thefts, was authorized users exploiting their privileges."

—Forrester Research[3]

However, what organizations are finding today is that these controls are simply not adequate. Several factors are contributing to the urgent need to secure applications and data beyond the network perimeter:

- **Internal Threats:** Increasingly a major source of attacks on information systems is stemming from internal threats. Insiders (and those with ties to them) with malicious intent are often able to gain access to sensitive systems and compromise their confidentiality or integrity. According to Forrester Research, "The most prevalent attack style, responsible for 39% of data thefts, was authorized users exploiting their privileges."[4]
- **SOA Adoption**: Web Services present a strong business case for business agility and reduced development costs. However, since Web Services are in their purest form plain text messages transported over standard HTTP protocols they can filter through firewalls and expose sensitive data.
- **Partner Extranets:** Online integration with partners has become a necessity for businesses, often granting partners insight into critical information systems through dedicated extranets. This opens up yet another potential back door for attacks to infiltrate all the way to applications and data.

It has thus become vital for organizations to look at an enterprise information security strategy that encompasses applications, middleware, and data beyond the network perimeter. This is driving spending behavior. Many industry analysts are predicting that a big portion of new investments in IT security will be towards data security issues, not perimeter security.

"According to the *2007 Annual Study: Cost of a Data Breach:* Data breach incidents cost companies $197 per compromised customer record in 2007, compared to $182 in 2006. "

- Ponemon Study[5]

Information Security Today

As critical as information security is today, industry solutions remain immature. Point solution vendors abound, oftentimes small and with questionable viability. Similarly, these solutions oftentimes will not work together and may address an issue that is application or platform specific. Rare are solutions that can be applied across one's entire IT infrastructure, helping to secure both infrastructure and business applications.

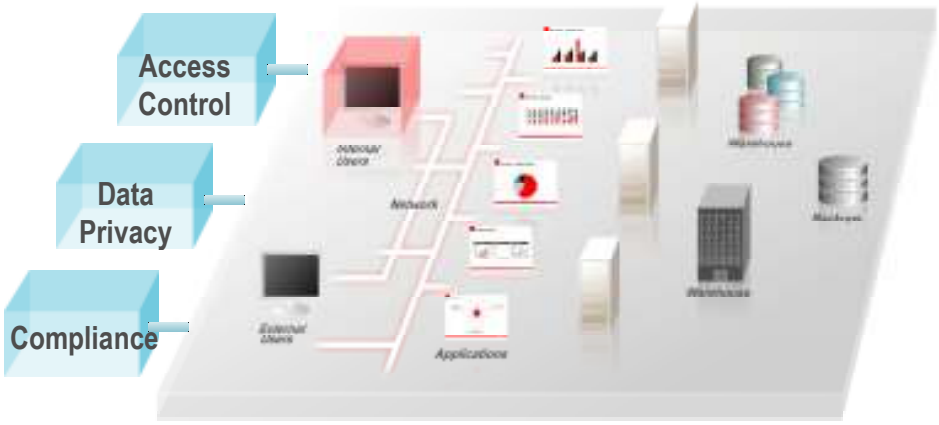
Similarly, many solutions are limited in nature today. They focus on detecting an anomaly (known as a detective control) versus preventing it from happening in the first place (known as a preventive control).

---

[4] Forrester Research, *Aligning Data Protection Priorities With Risks*, April 2006
[5] Ponemon Press, *Ponemon Study Shows Data Breach Costs Continue to Rise,* Nov 2007

THE SOLUTION – AN INTEGRATED SECURITY FRAMEWORK

An effective enterprise security strategy requires a holistic approach based on a framework that extends across applications, middleware, and data stores.



The major components of such frameworks fall into three primary areas: Access Control, Data Privacy, and Compliance.

Access Control

The enforcement of security policies restricting who has access to what, when, and from where constitutes the primary goal of any security architecture. A centralized framework ensures such policies are consistently applied across all applications and systems, whether contemporary web-based, client/server, or legacy systems. Access control entails the following functions:

- **Authentication:** Validating a user's identity. This could take several forms from the simplest username/password combination to stronger authentication schemes such as token cards and biometrics.
- **Authorization:** Once validated, enforcing which resources this user has access to across the enterprise systems. Authorization policies that are centralized and applied across the enterprise provide superior security.
- **User Provisioning and Identity Administration**: Managing security policies for thousands of users across hundreds of applications is a daunting task. Manual administration of such is not just costly, but also presents security challenges, as human errors are inevitable. Easing administration through automated user provisioning and de-provisioning, self-service user functions (such as password resets), and delegated administration dramatically reduces costs and improves security.
- **Role Management:** Once users have been provisioned, management of data across users, organizations, global locations and reporting structures becomes an additional complicated challenge. User, groups and roles

created to abstract privileges need to be properly managed. The need arises to set up role lifecycle management, business and organizational relationships, and resources.

In today's complex environment, access control needs to be applied across a wide variety of systems spanning web applications, client/server applications, databases, web services, operating systems, and storage systems. Only a system built on open standards and with a commitment to supporting heterogeneous environments is capable of handling such demanding requirements.

Data Privacy

Ensuring confidentiality of sensitive information is critical to any organization. Any compromise of information about your business, customers, employees, or partners could lead to very costly consequences. Information needs to be protected from prying eyes everywhere it lives and wherever it travels - across the web, network, applications, databases, and storage.

Privileged users in an enterprise are one factor that can lead to data leaks and compromises. This can occur when individuals with privileged administrator access (i.e. DBA) or other super users intentionally or unintentionally use their status to access information that they were never intended to view. It is not uncommon that developers, system administrators, QA teams, and others have full unrestricted access. Restricting their privileges to just what they need to their jobs greatly helps lower risk.

Protecting Personally Identifiable Information (PII) is vital, yet increasingly challenging. Many attacks today are targeted explicitly at acquiring such information from corporate systems. This data needs to be protected equally while in transit on the network or while at rest in a database or on tapes and backup storage. Selectively encrypting only sensitive portions of a data set, such as a database column containing credit card numbers, ensures minimal performance and storage overhead typically associated with data encryption. Classifying data based on sensitivity and controlling access according to classification is also a highly effective approach to ensuring data privacy. Finally, adding a security layer to enterprise search results prevents confidential information from being inadvertently revealed.

Governance, Risk and Compliance

A rapidly growing list of governance and privacy regulations has placed tremendous pressure on CIOs to tighten up security around the house. Today Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, FFIEC, SB 1386, and HSPD-12 are just some of the regulations organizations face. These requirements are not restricted to the shores of the United States; in fact global organizations doing business in the U.S. must also meet Sarbanes-Oxley requirements. Increasingly, European and Asian governments are requiring their own compliance measures, including Basel II, EU Privacy, and Japanese SOX. Each regulation requires an

examination of an organization's business practices with specific measures that need to be adapted to be compliant. Auditors, both internal and external, require irrefutable proof that these measures are working and their list of additional measures seems to be ever growing.

Initially, many organizations faced with looming deadlines, implemented manual processes to pass compliance audits. However, these have quickly taken their toll costing millions of dollars in incremental spend and precious resources diverted off important projects. To make matters worse, several organizations still failed their audits, and those that did pass had to immediately start the cycle over again for the next audit.

Achieving sustainable compliance cost-effectively is a goal for most businesses today. Effective solutions are those that not only help automate compliance controls and processes; they are also flexible enough to adapt to meet changing requirements. Key functionality required here includes:

- Separation of Duties across people & roles in organizations
- Effective collection & management of large audit data volumes
- Powerful reporting and analytic capability
- Process & content alignment with major regulations

BEST-IN-CLASS SECURITY SOLUTIONS FROM ORACLE

Security has been part of Oracle's heritage since its very beginning. For decades Oracle products have had security designed into them from the start. A series of non-stop industry firsts including the first trusted database, the first network encryption, the first virtual private database, and the first transparent data encryption have earned Oracle a reputation for building secure products. Coupled with an industry-leading 19 governmental security evaluations for the database alone, has made Oracle the choice for "security aware" organizations.

Today, Oracle offers security solutions that help enterprises protect information at all levels, across all systems, within the enterprise and beyond the firewall.

Comprehensive, Industry Leading Solutions

With solutions spanning access control, data privacy, and compliance management, Oracle leads the industry with the most comprehensive information security architecture. Best-in-class products such as Oracle Access Manager, Oracle Role Manager, Oracle Identity Manager, and Oracle Database Vault, recognized by industry analysts as leaders in their spaces, make this an unbeatable solution; one you can trust will cater to your information security challenges today, and have you prepared for those that might arise in the future.

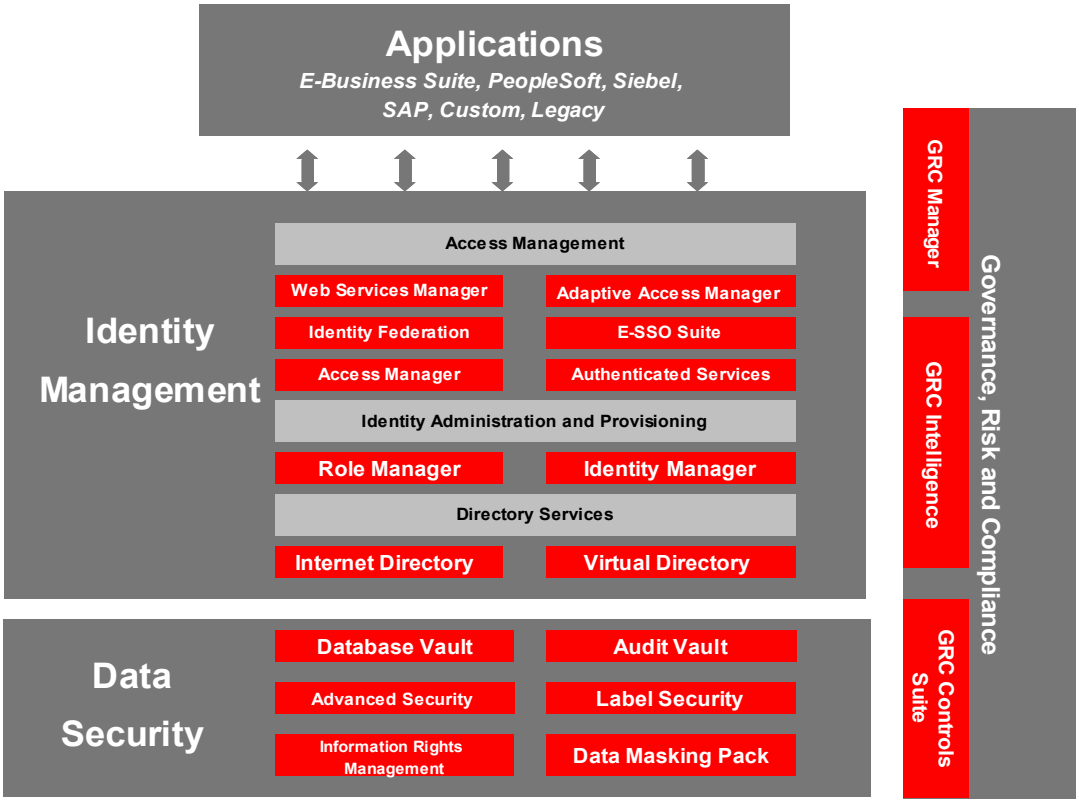
Common Integrated Security Across Applications And Data Infrastructure

The ability to secure all your applications, middleware, and data systems with a single common framework is unique to Oracle. Having a single view of activities across the enterprise provides improved security, lowered costs, and faster compliance.

Hot-Pluggable and Open

Built on open standards, Oracle's security architecture integrates with all leading applications, platforms, and systems. Protect your existing investments, securing them against constantly evolving threats and enabling unhindered business growth.

ORACLE SECURITY ARCHITECTURE



Oracle Security Architecture – A Complete Integrated Framework

Access Control Solutions

Oracle's industry-leading access control solutions span directory services, user provisioning, authentication and authorization including single sign-on for legacy applications, web services security, and identity federation. Specific products include:

- **Oracle Access Manager**
- **Oracle Adaptive Access Manager**
- **Oracle Role Manager**
- **Oracle Identity Manager**
- **Oracle Enterprise SSO**
- **Oracle Identity Federation**
- **Oracle Web Services Manager**
- **Oracle Internet Directory**
- **Oracle Virtual Directory**
- **Oracle Authentication Services for Operating Systems**

Data Privacy Solutions

"Oracle is leading the pack of database makers with the new access restriction features...Microsoft, IBM, and Sybase don't have anything like this."

—ZDNet[6]

Oracle offers unique and cutting-edge data privacy solutions for privileged user access control, encryption for data at rest as well as data in motion, data classification, secure backups, and secure enterprise search. Specific products include:

- **Oracle Database Vault**
- **Oracle Advanced Security**
- **Oracle Label Security**
- **Oracle Secure Enterprise Search**
- **Oracle Data Masking Pack**
- **Information Rights Management**

Governance, Risk, and Compliance Solutions

Oracle offers a comprehensive solution set for governance, risk, and compliance by combining risk reporting and analytics, policy and process management, and controls enforcement. Specific products include:

- **Oracle GRC Intelligence**
- **Oracle GRC Manager**
- **Oracle GRC Controls Suite**
- **Oracle Audit Vault**

[6]ZDNet, *Oracle wants to rein in database admins,* April 25, 2006

CONCLUSION

Information Security is a top priority for any CIO today. The increasing sophistication and frequency of threats makes this a challenging task, one that can only be conquered through an integrated enterprise security strategy and architecture. Oracle offers the most comprehensive and best-in-class security framework for access control, data privacy and compliance management for Oracle as well as non-Oracle environments. To learn more about Oracle's Security Solutions, visit **oracle.com/security**.

Security Inside Out – Oracle Security Solutions
April 2008
Author: Hormazd Romer

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