Oracle Security Solutions for SAP Environments
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Operating System Security</td>
<td>3</td>
</tr>
<tr>
<td>Role-Based Access Control (RBAC)</td>
<td>5</td>
</tr>
<tr>
<td>Protecting Logins</td>
<td>5</td>
</tr>
<tr>
<td>Virtualization—Increase Security, Flexibility and Scalability</td>
<td>6</td>
</tr>
<tr>
<td>Organizational Security and Compliance</td>
<td>7</td>
</tr>
<tr>
<td>Configure and Manage the Software and Services</td>
<td>8</td>
</tr>
<tr>
<td>Summary</td>
<td>8</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>10</td>
</tr>
<tr>
<td>Oracle Identity Governance Suite</td>
<td>10</td>
</tr>
<tr>
<td>Oracle Access Management Suite Plus</td>
<td>12</td>
</tr>
<tr>
<td>Oracle Enterprise Single Sign-On Suite Plus</td>
<td>13</td>
</tr>
<tr>
<td>Oracle API Gateway</td>
<td>13</td>
</tr>
<tr>
<td>Oracle Secure Global Desktop</td>
<td>14</td>
</tr>
<tr>
<td>Oracle Directory Server Enterprise Edition</td>
<td>14</td>
</tr>
<tr>
<td>Oracle Mobile Security Suite</td>
<td>15</td>
</tr>
<tr>
<td>Summary</td>
<td>16</td>
</tr>
<tr>
<td>Database Security</td>
<td>17</td>
</tr>
<tr>
<td>Attack Scenarios and Protection Strategies</td>
<td>17</td>
</tr>
<tr>
<td>Encryption Technologies (Oracle Advanced Security)</td>
<td>19</td>
</tr>
<tr>
<td>Privilege Management (Oracle Database Vault)</td>
<td>22</td>
</tr>
<tr>
<td>Conclusion</td>
<td>25</td>
</tr>
</tbody>
</table>
Introduction

More often than not, talks about security solutions for SAP environments are talks about what have been called “security silos.” Administrators discover a security hole and discuss how to protect their systems. Vendors promote new security products or features. Managers wonder how relevant news about security breaches or new compliance regulations apply in their particular case.

None of them can be blamed. There is no single solution that could provide complete security for SAP environments. SAP tried to define what “complete security” means when they published the SAP Security Solution Map.¹ But this architecture clearly shows why no single vendor—including SAP—will ever be able to build and offer a complete solution:

- The model contains a layer called Infrastructure Security. “Infrastructure” means everything on top of which SAP applications run: from networks and servers to operating systems and databases. Infrastructure security is essential for the security of SAP environments: There is no point in spending a lot of time and money for SAP application security if the door of your data center is always open. On the other hand SAP cannot influence infrastructure security: SAP does not sell doors, and SAP applications do not even check during startup whether the door of your data center is locked.

- The model is called SAP Security Solution Map, and rightly so. But many managers and administrators are responsible for an enterprise IT environment, which also includes non-SAP applications. A holistic approach then calls for as many general security functions as

¹ The SAP Security Solution Map can be downloaded from http://scn.sap.com/docs/DOC-17098.
possible: functions that are implemented once and can handle all application requirements. The layer of these general functions can be called *Superstructure Security* (see Figure 1).

![General Security Model](image)

This model is less complex, but more general than the SAP Security Solution Map. Nevertheless, it can be used by SAP partners to describe the security solutions they offer and to define the role that every single product plays as an element of this architecture.

Oracle Corporation offers infrastructure as well as superstructure solutions that can be and are used by SAP customers. The following article discusses operating system hardening (Part I) and Oracle Database security (Part III) as essential elements of infrastructure security. It describes Oracle identity and access management solutions (Part II) and how they help implement superstructure security.
Operating System Security

Information is an essential asset for all companies and must be adequately protected. The information about the IT system (metadata), communication technology and organization should ensure that a server operating system is deployed, configured and managed to increase the security and reliability of the information in all kinds of data centers, which are the essential backbone of today’s work and business processes.

Today’s IT infrastructures reside on widely distributed private or public cloud centers with their networks commonly linked to the internet, providing intruders with readily available entry points to corporate systems and data.

The first step in creating a secure environment is securing the underlying operating system. Many security issues can be avoided if the operating system’s fundamental services are configured appropriately. Especially in the SAP environment it is essential to have a properly configured operating system in place, to be able to ensure all business components are securely deployed on top.

As a leading supplier for IT hardware and software platforms, Oracle has also provided specialized solutions, integration, operating systems, networking, built-in virtualization features, performance and support for SAP applications for many years.

Oracle offers two valuable and well-accepted operating systems for the SAP market: Oracle Solaris and Oracle Linux (see Figure 2). Both provide a comprehensive set of tools and technologies to protect IT environments and reduce security challenges associated with remote access and administration including network firewall control plus access control security policies. Deploying SAP Business Suite on Oracle Solaris or Oracle Linux platforms offers unparalleled enterprise-class functionality as well as performance, density, and energy efficiency.
The following strategies in this section cover the hardening security aspects (see Figure 3) of Oracle Solaris in SAP environments. Why use Oracle Solaris as an essential backbone for today’s enterprise applications?

**Defending:** With Oracle Solaris you can provide a strong assurance of system integrity and defend systems from unauthorized access.

**Enabling:** Oracle Solaris provides secure authentication of all active subjects and protects communications between endpoints.

**Deploying:** Oracle Solaris offers an IT infrastructure stack that is well integrated; it is architected to interoperate with other security architectures. In addition, it provides ease of management, use of security features, independent assessment of security, and built-in virtualization with Oracle Solaris Zones.

**Compliance Enforcement and Auditing:** With Oracle Solaris, reports on configuration management for internal and regulatory security policies can be created. These reports are fully integratable into the Oracle Identity and Access Management (IAM) stacks.

![Figure 3. Operating system hardening steps.](image)

---

2 A complementary, but not SAP-specific, white paper on Oracle Linux hardening is available at [http://www.oracle.com/technetwork/articles/servers-storage-admin/tips-harden-oracle-linux-1695888.html](http://www.oracle.com/technetwork/articles/servers-storage-admin/tips-harden-oracle-linux-1695888.html).
Role-Based Access Control (RBAC)

Security administrators can apply fine-grained security policies at the application and user level using simple tools that restrict or grant specific system behaviors (such as program execution, file access, and network port control).

The privileges are discrete rights that can be granted to a command, a user, or a role. Role-based access control (RBAC), a feature of Oracle Solaris, reduces the security risk of intruder or regular user actions by implementing administrative hierarchies, constraining applications to specific actions, elevating administrative capabilities, and setting software restriction policies.

RBAC controls user access tasks that would normally be restricted to the root user. By applying security attributes to processes and to users, RBAC can distribute administrative rights among several administrations.

The isolation of administrative functions into grantable profiles removes the need for— and high risk of— anonymous and too powerful root access. Oracle Solaris access controls ensure applications run with the minimum access permissions needed to accomplish their tasks, limiting misbehaving applications or malware from impacting other applications on the system.

Users or applications with root access can make major changes to the Oracle Solaris operating system, Oracle database and SAP applications. With Oracle Solaris, administrators can secure the system by granting fine-grained privileges to users and applications, giving them the minimal access rights needed to perform specific tasks. The root user account is defined as a role and only users with appropriate privileges can assume that role. Any changes made are traceable to users, providing greater security and accountability.

Oracle Solaris is installed with a default Oracle Solaris security policy that is based on industry best practices. The administrative user is accessed via the RBAC system administrator role, and can use sudo and su commands, which provides:

- Limited network exposure, as SSH is the only network service enabled
- Limited auditing is enabled (logon, privilege escalation, logoff)
- Limited installation of packages (configure and manage the software and services)

Protecting Logins

Remote logins are initially limited to an authenticated channel through the Secure Shell (SSH) feature of Oracle Solaris for protected encrypted communications with other systems. This feature allows a user to log on remotely to a computer and transfer data between the local computer (client) and the remote computer (server) over a secure connection that SSH establishes. To increase the security when communicating with other systems, SSH should be used in place of other communication services such as telnet, RSH, and rlogin. SSH automatically encrypts and decrypts the information sent between the sender and the recipient and guarantees the integrity of the data. By providing strong authentication and cryptography, SSH creates a secure connection for communicating over an unsecured channel.

Oracle Solaris provides two building blocks for accelerated cryptography, the Oracle Solaris Cryptographic Framework and OpenSSL.
The cryptographic framework is used when encryption key management is important or the application has complex cryptography needs. Hardware and software cryptography is optimized at the machine code level to ensure the highest performance for these applications.

OpenSSL is provided for applications that typically do not have complex key management requirements. OpenSSL is typically used by open source applications and is the preferred library for secure HTTP traffic. OpenSSL can take advantage of hardware cryptography either through the cryptographic framework or directly using an optimized encryption engine.

Oracle Solaris components such as Secure Shell (SSH), ZFS, Kerberos, and Internet Key Exchange Protocol (IKE) use the cryptographic framework by default with no additional configuration needed to take advantage of high-performance cryptography on SPARC platforms.

Java code, Oracle Database, and Oracle Fusion Middleware are all automatically accelerated on Oracle Solaris by indirectly or directly using the cryptographic framework or the Oracle Database cryptographic pathway, or by being compiled to use SPARC instructions.

Virtualization—Increase Security, Flexibility and Scalability

Oracle Solaris server virtualization securely divides systems into smaller virtual servers, enabling administrators to place more applications on a single system. Secure, built-in virtualization services enable operating systems, networks, Oracle Database and SAP systems to be consolidated and used optimally for greater data center efficiency and thus take the advantage of a platform that constantly offers new features to address the difficult task of supporting large-scale mission-critical environments.

Oracle Solaris Zones enable organizations to isolate application components from one another. When used to consolidate applications or tiers on a single server, Oracle Solaris Zones can increase utilization rates and reduce data center complexity. The isolation of applications within zones prevents processes in one zone from monitoring or affecting processes running in another zone. Zones are virtualized operating environments that enable multiple applications to run in isolation from each other on the same physical hardware. Even a super user process from one zone cannot view or affect activity in other zones. By offering built-in virtualization, Oracle Solaris enables customers to maximize physical and virtual systems, network and data resources without adding significant overhead and complexity (see Figure 4).

As increasing numbers of users access SAP applications over a network, network virtualization allows administrators to allocate more resources to high-priority, high-bandwidth traffic, while more limited resources are assigned to low-priority traffic. Without adding network devices, network throughput is increased simply by scheduling and handling packets more efficiently.
Organizational Security and Compliance

Security is expanding from primarily technical issues (such as changing telnet to SSH) to organizational issues. Oracle Solaris eases the burden of organizational security by providing a compliant base platform supported by an ecosystem that supports higher-level security goals and major trends such as compliance enforcement and auditing.

Comprehensive auditing and reporting on an environment can help detect unusual behavior before an event occurs. Understanding the status of a running system can reduce the risk of a data theft event. Records generated are application defined and report on what applications developers decide to log. It is not appropriate to treat logs as fully trusted sources of data. Although logs can be used as a very helpful diagnostic step, a compromised application can change generated log events.

Instead, analysis of risk should be performed using tamper-proof auditing data that is administrator controlled and kernel mediated. By default auditing is enabled on Oracle Solaris for key events (such as login and privilege escalation). However, there are many classes of audit data available to record. A unique capability of Oracle Solaris is the ability to tag administrative files and record any changes in the audit log. This administrative edit command is a simple mechanism to record any privileged configuration edits.
Compliance reporting itself does not increase security or reduce risk, but it is an administrative mechanism designed to reduce risk and ensure that internal or external security and privacy requirements are being met. All the effort required to produce compliance reports could be better spent in doing activities that do make a functional difference.

Configure and Manage the Software and Services

Installing new software packages or patches is a potential source of corrupting user provisioning, network services and libraries. Eliminating unnecessary software packages, services, applications and network protocols minimizes possible avenues of attack.

Similar to minimizing software, restricting services to only those required for the server to deliver application services can help to eliminate potential avenues of attack.

The Service Management Facility (SMF) is a feature of Oracle Solaris that provides a uniform mechanism to manage system and application services (enable, disable, refresh, restart, and so on) on Oracle Solaris. SMF improves the availability of a system by ensuring that essential system and application services run continuously even in the event of any hardware or software failures. SMF is one of the components of the wider Oracle Solaris predictive self-healing capability.

To increase the security on the operating system, software packages associated with a service that is not in use should be removed or disabled.

Attackers have generally moved on from attacking operating systems and instead are focusing the majority of their energy in compromising applications that are easier targets. Multistage compound attacks build upon a single exploitation that is then used to subsequently find weakness across the network.

It is critical to limit damage of malware or misbehaving applications. On Oracle Solaris this can be accomplished using a combination of the following:

- Application security policies
- Immutable zones, a mechanism where zones have limited access to the local file system (designed for web applications that connect to remote databases and logging server)
- Address space layout randomization to protect against application buffer overflow exploits
- Cryptographically signed executables ensuring Oracle Solaris utilities are provided by Oracle
- Package integrity validation where files and executables obtained via the packaging system match what is installed on disk

Summary

Protecting organizations and data from reputation or fiscal harm requires advanced platform security features to protect data, isolate applications, limit user actions, and report on system activities. With virtualization features that target cloud and large enterprise environments, Oracle Solaris is designed to solve the most challenging issues customers face when deploying and managing a modern data center infrastructure. By running SAP applications on Oracle Solaris, IT organizations can create cost-
effective, robust, enterprise solutions that offer high performance, increased flexibility and security, and improved decision support.
Identity and Access Management

Today's businesses demand an ever-increasing focus on identity and access management (IAM) solutions to be able to understand who has physical and logical access to their facilities, networks and information. The major drivers behind this security trend are mixed and virtualized OS, application and database deployments with different user management engines, B2B – service-oriented architecture implementations, cloud computing, mobile computing (such as BYOD), IT governance, risk and compliance policies/rules, and new Internet paradigms such as Internet of Things (see Table 1). All of this needs to be seen in a coherent SAP ERP security approach with the needed flexibility to also integrate other third-party platforms which are used to establish full end-to-end business processes and transactions over all available business layers. Oracle Identity and Access Management Suite exactly fulfills this kind of demand.

### TABLE 1. NEW TRENDS TRANSFORMING IDENTITY AND ACCESS MANAGEMENT

<table>
<thead>
<tr>
<th>MOBILE</th>
<th>CLOUD</th>
<th>SOCIAL</th>
<th>INTERNET OF THINGS</th>
<th>PLATFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>• BYOD complicates privacy</td>
<td>• On premise, private, public apps</td>
<td>• Users want to use social ID</td>
<td>• Millions, billions of devices connecting</td>
<td>• Simplification,edefragmentation</td>
</tr>
<tr>
<td>• Enterprise and personal data</td>
<td>• Identity for SaaS apps</td>
<td>• Simplify registration and marketing</td>
<td>• Generate massive data</td>
<td>• Address full identity lifecycle</td>
</tr>
<tr>
<td>• Poor device, app, &amp; data security</td>
<td>• Cloud-based access portals</td>
<td>• Lack of trust in social login</td>
<td>• Need real time policy decisions, security and lifecycle management</td>
<td>• Reduce total cost of ownership</td>
</tr>
<tr>
<td>• Unified approach: ios, Android, ...</td>
<td>• Fragments identity</td>
<td>• Disconnect between social login and local accounts</td>
<td></td>
<td>• Remove latency &amp; integration errors</td>
</tr>
</tbody>
</table>

Oracle Identity Governance Suite

Oracle Identity Governance Suite delivers a converged, comprehensive platform for identity administration, access request, role lifecycle management, access certification, closed loop remediation and privileged account management for mixed platform deployments. This product enhances regulatory compliance by enforcing and attesting to regulatory requirements (such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and KonTraG) associated with identifying who has access privileges to sensitive, high-risk data on SAP and non-SAP system (see Figure 5) by offering a direct integration into the SAP GRC stack. It also eliminates potential security threats from rogue, expired and unauthorized accounts and privileges, which goes hand in hand with privileged account management allowing root users (administrators) to gain access to sensitive applications in a timely manner, while providing sufficient audit trails about their activities. Oracle offers this converged solution with the Oracle Identity Governance Suite: Oracle Identity Manager (OIM), Oracle Identity Analytics (OIA), and Oracle Privileged Account Manager (OPAM) work together to create a complete governance process for the enterprise.
Oracle Identity Manager (OIM) is a highly flexible and scalable enterprise identity administration system that provides operational and business efficiency by providing centralized administration and complete automation of identity and user provisioning events across enterprise as well as extranet applications. It manages the entire identity and role lifecycle to meet changing business and regulatory requirements and provides essential reporting and compliance functionalities. Its seamless integration with Oracle Identity Analytics (OIA) and Oracle Privileged Access Manager (OPAM) ensures consistent enforcement of identity-based controls, reducing ongoing operational and compliance costs. OIM offers dedicated connectors for SAP ERP (ABAP and Java), supports special SAP HCM scenarios, and integrates into SAP BusinessObjects Access Control (V5.3 and V10) for SAP-specific Segregation of Duty validations.

Oracle Identity Analytics (OIA) software provides enterprises with the ability to effectively achieve and manage access compliance and automate critical identity-based controls. It also allows roles to be defined, certified, and assigned, and then continues to deliver value throughout the user access lifecycle by:

- Providing a complete view of access-related data that includes the user’s access; the “who, why, and where” of that access; whether the access violates defined SoD policies; and activity associated with the access
- Automating the entire process of certifying and reviewing access and removing inappropriately assigned access
- Providing evidence that access is being defined according to established policies
- Enabling changes in access based on changes in users’ roles to minimize the disruptive effects of change on user productivity

OIA allows the usage of the SAP Org-Structures as the basis for the development of a central enterprise-wide business role model with integratable cross segregation-of-duty checks over all assigned systems accounts (SAP and non-SAP). The OIA functionality will soon be completely merged into Oracle Identity Manager and offered as a single product.
Oracle Access Management Suite Plus

In the last years, access management has covered application and web service security focusing primarily on authentication, authorization and audit. This has extended to new levels of protection. For example, enterprises need to provide employees with access to company resources from personal mobile devices. Similarly, some organizations need to grant customers access to applications on the basis of the user’s identities on social networking sites. And most organizations need to manage sign-on to cloud services as they would for on-premise applications. Further, organizations are being transformed by the need to provide end-to-end, standards-based security services to their applications, data, web services, and cloud-based or software-as-a-service (SaaS) applications.

Such business demands are driving organizations to externalize security services, integrate with partners, and evaluate the risk of internal and external transactions. Oracle Access Management Suite Plus addresses these challenges with a complete solution for controlling access to applications, data, web services, and cloud-based services across and beyond the enterprise. The package includes the following main features:

- Authentication (for example, WebSSO), authorization and audit for applications such as SAP NW Enterprise Portal
- Extending access management artifacts to mobile devices (for example, single sign-on for native mobile applications on iOS and Android)
- Extending access management artifacts to mobile devices to clouds (for example, Single Sign-On Portal)
- Integration with social networks through standards like OAuth
- Federated identities
- Fine-grained authorization for internal and external resources
- Proactive fraud prevention and authentication security
- Real-time risk analytics and risk-aware, multifactor authentication
- Comprehensive security for web services and SOA infrastructure
- Integration into the Oracle API Gateway
- Security token service (STS) for secure identity and token propagation
- Single sign-on for “fat clients” / Enterprise Single Sign On

Oracle Access Management Suite (OAM) works with existing heterogeneous environments in the enterprise, with agents certified on hundreds of web servers and application servers as well as applications. Especially in the SAP world, Oracle Access Management Suite is able to provide a full WebSSO solution for SAP NetWeaver Enterprise Portal deployments that are used in conjunction with other third-party web applications.

Furthermore, Oracle Identity Federation (OIF) significantly reduces the need to manage partner identities and lowers the cost of integrating with partners through standards-based federations. Oracle Identity Federation offers a cross-domain and cloud-ready single sign-on solution for a variety of application platforms including SAP ERP on the basis of highly accepted market standards such as the Security Assertion Markup Language (SAML).
Oracle Adaptive Access Manager (OAAM), as part of the Oracle Access Management Suite Plus, offers innovative, comprehensive features to help organizations prevent fraud and misuse of online resources. By strengthening existing authentication mechanisms with risk-based challenge methods and by providing real-time risk analysis, OAAM provides a unique multi-factor authentication solution (see Figure 6). In addition, OAAM’s risk analytics features help security experts to preemptively detect fraud and abuse across multiple channels of access. OAAM layers additional security measures on top of existing authentication to strengthen browser and mobile application login flows. These security layers include user device tracking, location profiling, transactional risk analysis, risk-based identity verification, and behavioral profiling.

Figure 6. Oracle Adaptive Access Manager in action.

Oracle Enterprise Single Sign-On Suite Plus

Oracle Enterprise Single Sign-On Suite Plus securely eliminates the need for users to remember and manage passwords for virtually any application, web or non-web. With OESSO Logon Manager, employees sign on to Windows and OESSO Logon Manager does the rest. As they launch their other applications, OESSO Logon Manager automatically logs them on with each application’s password. It can be installed on corporate computers and is also accessible via a website from any non-corporate computer—anywhere, anytime. It also includes a secure, reliable, but also simple integration for all SAP power users on the basis of the SAP GUI for Windows. In comparison to other available solutions in this market segment, OESSO is also the first enterprise-class strong authentication solution with no server infrastructure (no datacenter deployment—just desktop based), making it inexpensive and independent from any in-house proxy or gateway component.

Oracle API Gateway

Companies worldwide are actively deploying service-oriented architecture (SOA) infrastructures using web services, both in intranet and extranet environments. While web services offer many advantages over traditional alternatives (such as distributed objects or custom software), deploying networks of interconnected web services still presents key challenges, especially in terms of security and management. Oracle API Gateway is a software solution that provides application-level routing (based on source, target, sender identity, and XML message type); XML conversion, validation and threat scanning; XML acceleration; security (selective encryption and signature of XML messages, decryption
and signature validation); monitoring (response time, logging, and alerting); and governance (service access and usage).

Oracle API Gateway is tightly integrated with Oracle Access Manager, Oracle Entitlements Server, Oracle Web Services Manager, and Oracle SOA Suite to provide transport- and application-level security across all layers involved in web services requests. It primarily provides first line of defense in the DMZ. Oracle API Gateway is designed to secure, accelerate, and integrate all types of traffic between web services requesters and web services providers. It can be deployed standalone or as an integral component of a strategic enterprise SOA infrastructure, interfacing with enterprise service bus such as SAP NIF Process Integration Engine (SAP SOA Engine), enterprise management, and identity management platforms.

Oracle Secure Global Desktop

Oracle Secure Global Desktop is a secure remote access solution providing access to applications running on Microsoft Windows, Linux, Oracle Solaris and mainframe servers, from a wide variety of popular client devices, including Windows PCs, Macs, Linux PCs, and tablets such as the Apple iPad and Android-based devices. Oracle Secure Global Desktop allows administrators the freedom to use a single solution to provide secure access to a variety of applications and desktop environments resident in the data center. Oracle Secure Global Desktop leverages open standards such as HTML5, and provides industrial-strength security and encryption. It integrates with corporate standards such as the Lightweight Directory Access Protocol (LDAP), UNIX passwords, Pluggable Authentication Modules (PAMs), Oracle Internet Directory, and Microsoft Active Directory.

Oracle Secure Global Desktop also comes with a secure gateway that enables access from anywhere, and helps eliminate costs of maintaining VPN infrastructure. It supports users connecting to the applications they need from inside and outside the corporate firewall (for example, SAP GUI or SAP NW Portal). This means users are free to work from any location. But this freedom also extends to the device choice. With the broad supported client list that Oracle Secure Global Desktop offers, users are free to connect from whichever device they choose, without consideration of the client platform. So, for example, users can access Windows applications on iPads, or access Linux applications from Windows laptops. And because Oracle Secure Global Desktop offers session persistence, users can jump between devices, resuming sessions on different devices without interruption.

Oracle Directory Server Enterprise Edition

Oracle Directory Server Enterprise Edition is the only high-performance directory server to provide a core directory service with embedded database, directory proxy, synchronization with Microsoft Active Directory, and a web console to manage your software all in one package. It includes key components that together provide a complete directory service:

- Directory Server for core directory service with embedded database
- Directory Proxy Server for load balancing, high availability, data distribution capabilities and additional security enforcement point
• Identity Synchronization for Windows for identity data, password, and group synchronization between Microsoft Active Directory and Oracle Directory Server Enterprise Edition

• Directory Server Resource Kit for tuning and optimizing directory service performances

• Has been LDAP certified for integration with SAP NetWeaver

Oracle Mobile Security Suite

More and more employees bring their own devices to work (BYOD) and use them to get access to internal and publicly available applications (apps) over the enterprise intranet. In addition they share files and data inside and outside of the office. This is a difficult security situation for every IT department because of the missing visibility and control over the devices. It is well known that companies have to mobilize their enterprise web apps with native applications, but the current development model is expensive and not practical enough. Companies are looking for a cost-effective, scalable, secure and simple framework to develop, deploy, manage, customize, authenticate and provision mobile applications on the fly.

Oracle Mobile Security Suite offers IT departments a way to enforce data leakage protection policies while at the same time offering secure access to internal applications—without the use of a virtual private network (VPN) connection. This software adds a complete new isolation level for all corporate data within an end-user-owned mobile device and allows companies to easily mobilize any enterprise data across iPhone, Android and Blackberry natively in just 30 minutes. It is based on a container concept by which the product sets up a secure sandbox on the end-user mobile device. Enterprise applications or other third-party applications can be trusted by the Oracle Mobile Security Suite, and are considered at that point to be containerized and secured the same way as are the native Oracle Mobile Security Suite apps. All applications will be accessed based on the included secure web tunnel through the Oracle Mobile Security Suite gateway, providing access to internal-only applications including, for example, SAP AG ERP mobile apps which are specifically developed for mobile and smart devices.
Figure 7. Oracle Identity Governance Suite—Core solution components.

**Summary**

Provisioning, privileged access request and approval management, role management, and compliance products evolved independently of each other, which led to companies implementing multiple products from multiple vendors as point solutions to address these needs (see Figure 7). As regulatory and provisioning requirements continue to grow and change, such multi-vendor solutions only increase the complexity and costs of managing and integrating these products. As a result, enterprises are in an inevitable position of having to rely heavily on each of these vendors for support and also committing significant resources to governance efforts for integration and manual processes with little assurance that they will prove successful. Recent research also has made it evident that organizations can save up to 48% in overall costs deploying a single-vendor platform solution when compared to deploying multi-vendor point solutions. Therefore Oracle with its single, converged IAM platform is the right partner for all heterogeneous multi-vendor application and operating system deployments. Oracle’s IAM suite of products can serve as a starting point and basis for a non-silo-based and highly flexible SAP IAM solution.
Database Security

If a user wants to read or update data in an Oracle Database that is used as a data store by an SAP application, the first and obvious way is to use the interfaces provided by SAP’s applications. From an Oracle Database perspective, this is the easiest case, because all questions—Which people should be able to access the data and which people should not? Which part of the data should a particular person be able to access? What exactly should this person be able to do with the data?—are asked and answered by SAP’s user and privilege management with the possible support of identity and access management solutions provided by Oracle. This means: All legal data accesses are managed by identity and access management, and there is not much the Oracle Database could or would need to add, as long as there are only well-behaved users.

Attack Scenarios and Protection Strategies

Putting this statement the other way round, we get this rule: Oracle's database-related security features and options help prevent data accesses which bypass the SAP applications, use non-SAP tools to access SAP data, and are at least potentially illegal.

Attack Scenario 1: Network Sniffing

Attackers could use a sniffer tool to capture data while they are in transit (see Figure 8). This would allow them to intercept sensitive data like logins and passwords, table and column names, and even actual table data (such as social security numbers, credit card numbers and other personally identifiable information) going to or coming back from the database server.

Encrypting data in transit prevents this sort of activity. Therefore, the first data protection technology, implemented in the Oracle Database\(^3\), provides network encryption. In this context, network encryption means: Oracle software installed on both the SAP application server and Oracle Database server machines encrypts data before and decrypts them after they are sent over the network.

Attack Scenario 2: Database File Copies

Attackers could also steal a copy of the database files and read the files directly (see Figure 9). Of course, these files are not simple text files, so a lot of knowledge about SAP’s data model and Oracle’s data storage algorithms would be required. So it is difficult. But it is not impossible.

Therefore data at rest needs to be protected as well. With Transparent Data Encryption—a set of technologies provided by Oracle Advanced Security—data are not stored as plain text, but in a coded

---

\(^3\) As of June 2013, the use of network encryption no longer requires an Oracle Advanced Security license, but is included in Oracle Database 11g as well as 12c.
form. Therefore the information in the data files looks like nonsense and is completely meaningless to everybody who tries to read the data files directly.

**Attack Scenario 3: Direct Database Connect**

But there is yet another “unusual” way to the data. Privileged database users—like database administrators—can use DBA tools and directly connect to the database, thus bypassing SAP’s security checks (see Figure 10). The first aspect that needs to be understood when considering this scenario is that encryption does not help against this kind of threat. If someone is able to connect to the Oracle database using a sufficiently privileged account, and if he or she is then able to build an appropriate `SELECT` statement and send it to the database, then Oracle will generously deliver the result set to this user. And if the data is encrypted on disk, then Oracle will even decrypt them, because from an Oracle Database perspective the request sent by this user seems to be a perfectly valid request.

The second aspect that needs to be understood is the reason for Oracle’s behavior. As a database user, you can be granted object privileges and system privileges. There are many different kinds of objects in a database, but average database users as well as people who want to steal data are only interested in tables, so for simplicity’s sake we will assume that database “objects” means just “tables”. An “object privilege” for a table, then, means that you are allowed to access the data in that table. A system privilege, on the other hand, means that you are allowed to manipulate the database structure. You may add disk space to (or release it from) the database, you may create new tables (or drop old ones), you may add an additional column to an existing table. Now, in traditional databases (including Oracle Database), if you were explicitly granted a sufficient number of system privileges, you implicitly received object privileges for all tables as well. For decades people found this quite natural and unproblematic. Only recently companies began to ask: Is it really necessary and is it really desirable that a database administrator, who is supposed to manage the database structure, is by default able to read (and even change) all data in the database?

So the third aspect that needs to be understood is that the third scenario requires a new privilege management strategy in the database. This strategy should continue to provide system privileges and object privileges, but it should get rid of implicitly granted object privileges. In other words: A “normal” database user needs object privileges only, and a database administrator in most cases needs system privileges only. If there is a reason why the database administrator should be able to access the data as well, then he or she—as everybody else—should be granted the required object privileges explicitly.

This is exactly what Oracle Database Vault does. It replaces the traditional, somewhat clumsy privilege management strategy with a new, more flexible one. It eliminates all implicit grants and instead provides a means to explicitly define access rights as well as the circumstances under which they are effective. This goes far beyond traditional user–privilege or user–role correlations. Oracle Database Vault allows companies to implement and enforce concepts such as the segregation of duties or the four eyes principle.

Putting the pieces together, it can be said that all data accesses using SAP’s applications are handled by SAP, so there is not much Oracle can or needs to do. However, if people use other strategies to access the data in your database, there is not much SAP can do, and this is exactly when the security features
implemented in Oracle Database and Oracle Database options can help you protect your data. Encryption prevents people from directly reading the database files. Oracle Database Vault prevents people from accessing the data via standard database tools.

Encryption prevents people from directly reading the database files. Oracle Database Vault prevents people from accessing the data via standard database tools.

Figure 8. Database Security—Oracle Network Encryption.

Encryption Technologies (Oracle Advanced Security)

Encryption technologies in Oracle Advanced Security protect both data in transit and data at rest.

Protecting Data in Transit: Oracle Network Encryption

In SAP environments, users do not directly connect to the Oracle Database server. They connect to an SAP application server instance, and the SAP application server instance in turn connects to the Oracle Database server. So, in this case, the application server instance is the Oracle client, and Oracle’s network encryption encrypts all data traveling between application server and database server.

Oracle’s network encryption requires Oracle software, which is not installed on end-user devices. Therefore it can only encrypt/decrypt data travelling between SAP application server and Oracle Database server machines. Additional technologies or products must be used to protect the communication between SAP users and SAP application servers.

However, people can not only try to read data in transit, they can also try to intercept and modify them. Therefore, in addition to network encryption, Oracle Advanced Security also supports crypto-checksumming to ensure data integrity.
Both encryption and crypto-checksumming are completely transparent to the application, and in both areas the system administrator can choose between several algorithms. The function encrypts payment card numbers before they are stored in the database and decrypts the card numbers while the document is processed (for example for authorization purposes). In transactions, the system displays only a masked number. This encryption function, however, is limited to credit card numbers. As the Oracle database is not aware that these data are encrypted nor how they are encrypted, the use of this function may result in negative side effects such as the inability to perform range scans.

Oracle Transparent Data Encryption (TDE) is applied to data in the files which make up the production database (as opposed to backup files, which will be discussed in the next paragraph). As the name indicates, TDE is transparent to the application; no application changes are required. Starting with SAP NetWeaver version 7.20, you can use BRSPACE to set the encryption attribute on a tablespace level. BRSPACE can also be used to manage the wallet, which stores the encryption keys.

Transparent Data Encryption comes in two flavors. The first one, which had already been available in Oracle Database 10g, is called Column Encryption, because you select just a few of the many SAP tables.
or even individual columns of these tables that contain sensitive data and encrypt them. Everything else remains unencrypted. The second one, called *Tablespace Encryption*, is new in Oracle Database 11g. It allows you to encrypt complete tablespaces, which may contain hundreds, thousands, or tens of thousands of tables.

The hardware encryption feature provided by some recent CPUs can be used for tablespace encryption (but not for column encryption), an additional plus. Hardware cryptographic acceleration for TDE tablespace encryption is available with Intel® CPUs with AES-NI, a set of New Instructions for the Advanced Encryption Standard. Oracle Database 11g Release 2 TDE tablespace encryption automatically detects and leverages the hardware-based cryptographic acceleration for decryption of data. With Oracle Database 11.2.0.3, hardware crypto acceleration support is extended to Oracle Solaris 11x64 on Intel CPUs with AES-NI, as well as Oracle Solaris 11 for SPARC. Hardware cryptographic acceleration for TDE column encryption is not supported.

The storage nodes in Oracle Exadata Database Machine provide hardware-based cryptographic acceleration based on Intel® Xeon® CPUs with AES-NI, delivering a near-zero performance impact for TDE tablespace encryption. Companies no longer have to choose between security and compliance on one side and high performance computing on the other side. With Oracle Database 11g Release 2, the tablespace keys for TDE tablespace encryption, or table keys for TDE column encryption, are available to the intelligent storage cells where encrypted data is now decrypted before Smart Scan is applied.

TDE tablespace encryption and Oracle’s compression technologies allow encryption of compressed data. TDE tablespace encryption can be combined with Oracle Advanced Compression in single instance and Oracle Real Application Clusters (Oracle RAC) deployments. Because Oracle Database applies compression before encryption, encryption has no negative impact on the compression ratio.7

**Protecting Data at Rest: Oracle Backup Encryption**

Especially if you decide to use column encryption in your production database, you may want to increase the security level of your database backups, as it is generally much easier to steal backups of the database files than the production database itself. Therefore, the third set of features in Oracle Advanced Security is related to backup encryption.

If you simply backup your database files, only those columns that are encrypted in the production database files are encrypted in the backup copies. However, combining Oracle Recovery Manager (Oracle RMAN) and Oracle Advanced Security, whole backup sets (that is, all data) can be encrypted.8

---

7 For details see SAP Note 974876 (Section 1.5).
8 For details see SAP Note 1324684.
Oracle Database Vault is an option that extends the functionality and the power of Oracle Database privilege management. Oracle Database Vault has been certified by SAP for use with all SAP applications.

Access Control Components

As described previously in this paper, Oracle Database Vault is designed to protect your data against insider threats by enabling you to define very flexible access policies. Access control components are the pieces that are used to build access policies. Two groups of them can be distinguished. The concept of realms constitutes a group on its own. It is the basis for everything else.

- **A realm** is basically a container for database objects. As in the previous section, we will only consider tables and neglect all other kinds of objects for simplicity’s sake. A database can contain many tables, but it would be very cumbersome to define a complex security policy for every single table. On the other hand there is no guarantee that the same policy would be appropriate for all tables. That is why Oracle Database Vault supports the concept of realms. A realm is a group of tables to which the same access policy applies. So as the first implementation step you create one or more realms, and as the second step you assign every single table to its appropriate realm.

The second group comprises the concepts of factors, identities, rules, rule sets, command rules, and secure application roles. These are the building blocks that you use to create access policies for your realm(s).

- **A factor** is an attribute of a data access (or an attempted data access) that can be determined automatically by the database server. Examples include the IP address, the day of the week, and the time.

- The problem with factors is that they are just simple facts. In most cases there are too many possible values (IP addresses, access times), and in all cases they don’t mean much. Identities, therefore, add...
meaning to those values, and in most cases they do this by defining a very small number of possible
types. For example, the IP address could indicate that the user is working in the data center,
somewhere else inside the company network, or outside of the company network. Days of the week
can be working days or weekend days. An access time could be within typical working hours or
outside working hours.

- Identities can be used to build rules. A rule could say: It is allowed to access the tables in this realm, if
  the user is inside the company network, if it is a working day, if the attempt happens between 8 am
  and 6 pm.

- Rule sets are combinations of rules. As usual, rules can be combined using logical AND and OR
  operations: Access is allowed (a) if it is a working day OR (b) if it is a weekend AND the IP address
tells us that the user is inside the company network. A realm and a rule set assigned to this realm are
the minimal form of what we initially called access or security policy. The expression multi-factor
authorization, which is used in some papers, means exactly the same thing. When you design an access
policy, you are not restricted to one factor (ultimately: one rule), but you can combine as many
factors as necessary to determine whether or not the attempted access should be allowed.

- A command rule is a special kind of rule. As the name suggests, it is related to a specific command: An
  ALTER TABLE operation is allowed, if it is a working day, but not if it is a weekend day.

- Secure application roles are database roles that are or are not enabled by the database system (that is, a
  PL/SQL procedure) after evaluation of a specific rule set.

Management and Monitoring

As discussed so far, the access control components are just concepts. If you really want to make use of
them—that is, if you want to build an access control policy—you need a tool to make that happen.
Oracle Database Vault provides an administrative console called Oracle Database Vault Administrator for
managing realms and rule sets. This application allows security managers to configure an access control
policy through a user-friendly interface. Database Vault Administrator is also used in SAP
environments. There is no additional or alternative tool provided by SAP.

After implementing an access control policy, you will want to monitor how it works (what it does and
what people do). Therefore, Oracle Database Vault comes with an auditing feature, which allows you to
track both successful and failed attempts based on different characteristics (in particular realms, factors,
and rule sets). In addition, Oracle Database Vault provides predefined reports which allow you to check
the consistency of your access policy as well as security violation attempts. And, of course, there is a
user-friendly interface that allows you to design additional reports.

SAP-Specific Security Policy

Oracle Database Vault, as sold by Oracle, is just a tool box. It is true that it comes with predefined
realms and roles, but those are realms for system tables (such as the Oracle Database data dictionary or
the tables that Oracle Database Vault needs itself) and very general (if fundamental) roles (such as the
distinction between database administrator and security administrator). These predefined components
allow Oracle Database Vault to be functional and allow you to use it, but they do not protect your
application data. That is because Oracle does not know anything about your applications and your data. Oracle can only give you a toolbox, and it is up to you to determine your security requirements and translate these requirements into an access control policy.

But there is an important difference. As long as customers use home grown applications, it is simply inefficient for Oracle to care. If, however, tens or hundreds of thousands of companies use a certain standard application and the security requirements of all these companies are (at least to a certain point) identical, because they are results of the application design, then it makes much more sense for Oracle to analyze the requirements and implement a basic security policy. Oracle has actually done this, saving hundreds of companies the time that is needed to implement the boring basics of an application-specific security policy, and protecting these companies from forgetting to implement some of the basics. As of today, Oracle provides a whole family of predefined application-specific Oracle Database Vault policies, and Oracle Database Vault for SAP is a member of this family.

This means: Considering Oracle Database Vault for SAP, you should distinguish between three levels. The first level is just the toolbox, which allows you to work with Oracle Database Vault. The second level is a predefined access control policy which covers the basic requirements of SAP applications. Finally, if the predefined policy does not cover all your requirements, there is a third level which allows you to modify or enhance the predefined policy.

What exactly does Oracle Database Vault for SAP do? What exactly does “application-specific security requirements” mean? Here are just a few examples:

- Some aspects are obvious and similar to policies appropriate for other applications. For example, a dedicated SAP realm needs to be created and the database objects that contain the SAP data need to be assigned to this realm. Also certain database users should no longer be able to connect using applications other than those provided by SAP.

- But there are more specific aspects. For example, it is typical for SAP applications running on top of an Oracle database that the BR*Tools family of administration tools are used to manage the database. Therefore, an SAP-specific security policy needs to make sure that even after installation and activation of Oracle Database Vault all BR*Tools operations are still possible and work as expected.

- It is typical for SAP systems that SAP Support needs to perform remote connects. Therefore, a SAP-specific security policy needs to create a dedicated database user for SAP Support. This account may be (and by default is) disabled, but it can be easily enabled whenever this is necessary. And, of course, enabling and disabling this account needs to be audited.

- It is typical for SAP systems that customers can use an ABAP and/or a Java stack. Therefore, a SAP-specific security policy needs to distinguish between data accesses via the ABAP and the Java stack.

More details and best practices can be found in SAP Notes 1355140, 1597194, and 1502374.
Conclusion

Oracle delivers secure infrastructure and superstructure solutions through a wide range of products, processes, and technologies to help prevent unauthorized access to confidential information, reduce the cost of managing users, and facilitate privacy management. Built on an innovative modern architecture that blends extreme scalability with rich user experience, Oracle offers a best-in-class suite of identity management solutions that allow organizations to simplify identity lifecycle management and secure access from any device for all enterprise resources. Oracle also provides a comprehensive portfolio of security solutions to ensure data privacy, protect against insider threats, and enable regulatory compliance. Oracle Solaris and Oracle Linux security technologies protect data, applications, users, and the operating system itself from a variety of external and internal threats which reduces risk and prevents breaches. Having pioneered many of the security features described in this white paper, Oracle has also set security standards for SAP environments.