

# ORACLE PARTNERS

## PARTNER INDEX

- Q SOFTWARE
- THE WERCS
- PRICEWATERHOUSECOOPERS
- ALERTENTERPRISE
- CYBER-ARK

To download Oracle and Oracle Partner white papers on Security and GRC, please visit: [www.oraclewhitepapers.com](http://www.oraclewhitepapers.com)

## THE FOLLOWING SECTION HIGHLIGHTS.

The Oracle Enterprise Security and Governance, Risk, and Compliance Initiative is one of the first global technology vendor and service provider initiatives of its kind, recognizing that customers across the globe are increasingly viewing information security, and governance, risk and compliance (GRC) as a critical long-term investment in sustainability. Available to select members of the Oracle Partner Network who deliver security and/or compliance solutions or services complementary to Oracle applications and infrastructure software, the initiative helps create a partner ecosystem offering world-class, integrated, comprehensive solutions and services that provide customers best-of-breed solutions at lowest total cost of ownership.

### Proven to Cut Oracle's JD Edwards World line of Applications Security Costs by Up to 80 Percent

**Q** Software is the only Oracle Certified Partner that provides security, and governance, risk, and compliance (GRC) solutions for JD Edwards World customers. Q Software is Oracle's selected enterprise security and GRC global partner for JD Edwards World line of applications.

Q Software security management solutions are certified by Oracle and recommended by both Oracle and leading audit firms.

We also support JD Edwards EnterpriseOne Financial Management and Compliance Console and complement it with our own comprehensive compliance reporting solutions.

More than 250 customers tell us we cut their security costs by up to 80 percent. No wonder we have the security solutions of choice for Oracle's JD Edwards customers.

To learn how you can cut your security costs, visit [www.qsoftware.com/cutmycosts](http://www.qsoftware.com/cutmycosts)



FOR MORE INFORMATION VISIT | [www.oraclewhitepapers.com/reg/52508](http://www.oraclewhitepapers.com/reg/52508)

### Providing Global Regulatory Compliance, Hazard Communication, Sustainability, and REACH-Compliant Solutions

**R**ecipe-based process manufacturers that are required to comply with global regulations by creating hazardous materials documentation can benefit from the The Wercs automated software application suite. The Wercs also provides the necessary tools to comply with Europe's REACH legislation.

Founded in 1984, The Wercs, Ltd. is the established global standard of software tools that automate the authoring, distributing, and managing of material safety data sheets (MSDS) and other hazard communication documents. The Wercs solution provides the most advanced global functionality to help businesses succeed in the international marketplace. Our multilingual solution and integration and monitoring of more than 2,800 global regulations, extensive REACH functionality, and support offices around the world makes our best-of-breed solution a preferred choice for leading manufacturers around the world.

For more information on ensuring regulatory, hazard communication, and REACH compliance, visit us at [www.thewercs.com](http://www.thewercs.com) or call 1.800.572.6501.



FOR MORE INFORMATION VISIT | [www.oraclewhitepapers.com/reg/52387](http://www.oraclewhitepapers.com/reg/52387)

# PricewaterhouseCoopers: The Big-Picture Approach to Identity and Access Management

Over the last decade, many organizations have attempted to address identity and access management (IAM) issues by implementing a variety of solutions. In general, however, these have been point solutions that focused on specific areas, which led to fragmented and redundant security processes and systems—an approach that has often proven to be complex and costly, particularly in the face of increasing compliance requirements.

In recent years, however, Oracle security solutions have enabled companies to use address IAM issues in a more comprehensive manner, with an application suite that covers the entire range of IAM activities. A holistic IAM solution enables an organization to effectively manage user access across the enterprise and serves as an enabler to lines of business and strategic partners. Effective user management helps automate the process of provisioning and deprovisioning users as they are hired, terminated, or transferred. In addition, a comprehensive user management solution provides the ability to monitor and review (or test) change history, user permissions, and authorization, all of which are critical for sustaining compliance.

To help companies take full advantage of these solutions, PricewaterhouseCoopers (PwC) works with clients to take an integrated, big picture approach to Oracle's security applications and IAM. "That's critical, because security cannot be addressed effectively in a piecemeal fashion," says Gary Loveland, a principal at PricewaterhouseCoopers.

PwC's tools and methodologies have been developed through years of experience in the field. The firm has one of the largest security practices in the world—a global team of some 3,200 security professionals working in all major markets. PwC has built security infrastructures for 14 of the Fortune 25 and performed security assessments and/or implementations at more than three-quarters of the Fortune 500. PwC also draws on its relationship with Oracle. The firm is an Oracle Certified Advantage Partner, and the two companies collaborate in areas such as governance, risk, and compliance; corporate performance management; and security.

In its IAM engagements, PwC looks well beyond the implementation of the technology, helping companies develop an overall security strategy. "We work with clients to define where they are, where they want to be,

and how they are going to get there," says Loveland. "This enables them to deal proactively with security, rather than just react to events." PwC also helps clients address the all-important people and process issues that are key to effective security. "We do security assessments every day—and usually we find that security problems have little to do with the technology itself," Loveland says. "Security has to be a people, process, and technology effort, and we help clients bridge any gaps across those areas."

Overall, PwC helps ensure that security is not tackled in a vacuum, and that IAM initiatives are tied to the client's business needs. That might mean, for example, balancing compliance requirements with business objectives such as improved operational effectiveness and reducing operating costs, or creating a reusable, service-based security platform that offers greater efficiency and flexibility.

The goal of such efforts, says Loveland, "Is first and foremost to increase security and reduce risk." But the PwC approach also targets broader benefits, such as enhanced user productivity, an improved ability to handle mergers and acquisitions and the integration of partners, and enhanced speed-to-market for new applications.

In addition, companies often achieve greater control over costs through reduced help desk and user-administration workloads, more-rapid provisioning of new users, and greater economies of scale that result from the consolidation of the IT infrastructure. A holistic approach to IAM can also enable better compliance processes due to improved control of information access, uniform enforcement of access policies, and a consolidated view of user access information. And it can help contain compliance costs by simplifying processes and reducing overlapping efforts.

"By combining PwC's in-depth regulatory, compliance, and industry knowledge with Oracle's comprehensive suite of technology solutions, companies can significantly reduce the time and effort normally involved in solution deployments," sums up Loveland. "And they can gain a streamlined, enterprisewide approach that enhances security and helps address their business issues."

Gary Loveland, a principal based in Southern California, leads PwC's security and IdM practice in Oracle environments. He can be reached at [gary.loveland@us.pwc.com](mailto:gary.loveland@us.pwc.com)

## AlertEnterprise: Filling the Security Gap

**M**ost organizations today pay careful attention to security in their IT systems, applications, and databases. Typically, they also keep a close eye on physical security and environment, health, and safety (EHS) issues at plants and facilities. Nevertheless, says Mark Feldman, COO at AlertEnterprise, they are often operating with a significant and exploitable blind spot.

“Physical and logical security systems are functionally separate and rarely integrated. That creates the single largest and most overlooked gap in enterprise security,” says Feldman.

AlertEnterprise helps companies bridge that gap with solutions that integrate physical access control systems and IT infrastructure and applications to deliver real-time global controls, security, and compliance with governing policies, practices, and regulations.

By linking those physical and logical systems, the company’s solutions enable enterprises to detect and resolve “blended threats” in real time. “The most insidious risks may not individually trigger an alert in any one system,” says Feldman. “But in combination, they can create a risk that may defy detection.

“For example, a person may have authorization to order the scrapping of inventory,” Feldman explains. “Carrying out this authorized task would not trigger an alert. That person may then use legitimate badge access to enter the warehouse containing the scrapped inventory after hours, which would also not in itself trigger an alert. However, these actions in combination create a risk of fraud and theft, and you need to link the physical and logical security systems to correlate them and identify the risk.”

AlertEnterprise offers two solutions that address such issues: AlertAccess and AlertAction.

AlertAccess is an access enforcement solution that uses rules-driven, automated risk analysis to grant secure, role-based access to IT applications, physical locations, and corporate assets. It provides policy-compliant global provisioning and deprovisioning and is designed for tight integration with enterprise resource planning, human resources, and legacy systems, as well as environmental health and safety databases. This helps ensure both that the right employees are getting the right access and only that access, and that their safety and well-being can be monitored from a risk and threat standpoint.

“If you are provisioning various IT applications, physical locations, and assets such as laptops or BlackBerrys, an automated analysis will determine whether you are creating any risks,” says Feldman. “If you are introducing a risk, the system won’t let you go any further unless you add a mitigating control for that risk.” For example, the system may forbid an accounts-payable clerk from having access to a room where checks are kept unless a supervisor is also present.

Alert Access provides workflow and configuration tools that accelerate safe provisioning and avoid productivity lapses due to lack of proper access. It can work either as a standalone solution or with existing identity management and physical access control systems, including Oracle Identity Manager. “If you have Oracle Identity Manager and you want to add both automated risk analysis and provisioning to physical locations, there is a seamless integration between our system and Oracle Identity Manager,” says Feldman.

AlertAction, meanwhile, is a visual threat-detection solution that combines real-time, intuitive alerting, geo-spatial monitoring, and online action scripts for fast remediation of access threats and EHS events throughout the enterprise. Its time and space mapping of access and other sensor-triggered events (such as temperature, pressure, humidity, etc.) combined with Web service data (such as weather, fire, emissions, etc.) provide location intelligence and intuitive understanding to support rapid responses to problems. For example, says Feldman, “AlertAction will give you satellite views of your locations around the world and allow you to drill down to plant-level sensors or IP cameras to see and assess the situation, as well as deploy first-responders.”

Both solutions provide clear audit trails, analytics reporting, and automated processes such as reaffirmation to verify adherence to policies and regulations. Finally, the solutions are based on a service-oriented architecture, which facilitates cross-platform functionality, integration with legacy systems, and unobtrusive integration in IT landscapes and with physical access control systems and other data sources.

Overall, says Feldman, “These solutions make it possible to do what has traditionally been a very difficult task—bringing together the two worlds of physical and logical security. That means companies can do a better job of identifying potential threats that otherwise fall through the cracks.”



## Cyber-Ark: Securing Privileged Identities and Oracle Databases

Today, IT security breaches are a growing problem that can have significant operational, financial, and compliance ramifications. Often the greatest threat is close at hand—increasingly the breaches are coming from an organization's own employees, as evidenced by the growing number of insider incidents. According to a recent Computer Emergency Response Team (CERT) study, more than 80 percent of insider breaches were traced to users with privileged access to systems within the internal infrastructure.

For many companies, the privileged identities that provide administrators with wide-ranging access to systems, applications, and databases are a weak point in internal security. The risk comes in part from the fact that these identities are meant to be shared by many users and are generic in nature, so systems don't track who is logging into them. Additionally, an enterprise may have tens of thousands of them—they are found on virtually every piece of hardware and software in an organization. Furthermore, these accounts are nearly impossible to disable, because they provide the main method for managing these systems.

To help companies address this problem, Cyber-Ark offers its award-winning Enterprise Password Vault (EPV), which provides a centralized solution to secure and manage all of an organization's privileged accounts—even application identities embedded in scripts and connectors. Part of a suite of Cyber-Ark security products, EPV creates a multilayered information security infrastructure that helps companies efficiently personalize, manage, and automate privileged accounts while providing the security, flexibility, detailed tracking, and identity-auditing capabilities that are typically missing from today's various encryption-only solutions.

Cyber-Ark is a member of the Oracle PartnerNetwork. EPV integrates out of the box with Oracle Identity Management, enabling the Oracle solution to be the central point for managing and provisioning all identities, including both traditional end-user targets and the privileged administrative and application identities used by network administrators.

In addition, EPV complements the Oracle Database Vault, enhancing the management and personalization capabilities of database administrators. In essence, says Adam Bosnian, vice president of products, strategy, and sales at Cyber-Ark, "The solution enhances security by acting as a front end to Oracle's products, so an organization knows who is accessing their data-

bases and systems, while improving auditability, workflow automation, security, and manageability."

At the heart of EPV is Cyber-Ark's patented and ICISA Labs-validated secure digital vault technology, which provides high levels of security for privileged passwords—or any type of highly sensitive information—both at rest and during transmission. Digital vault technology includes a Federal Information Processing Standard 140-2-validated cryptography module (with advanced encryption standards encryption), and meets payment card industry requirements. "We create an electronic safe haven in the network so that regardless of the overall network or security surrounding it, the privileged accounts are always secure and available, eliminating the traditional tradeoff between accessibility and security," says Bosnian.

Building on this foundation, the EPV solution also provides

- A Web-based interface that provides a single console for accessing and managing privileged accounts throughout the enterprise
- The Central Policy Manager, a module that automates and instantly changes passwords for the thousands of databases, servers, network devices, and applications within an infrastructure
- Auditing compliance capabilities, such as built-in entitlement reports and the ability to track time, date, personalized identity, changes, and logging history
- The scalability to manage tens of thousands of privileged administrative and application accounts across multiple networks and geographies
- Seamless integration with Oracle Identity Management, providing a complete solution for managing all the identities within an organization

EPV supports an exceptionally wide variety of platforms, including UNIX, Linux, AS/400, MVS, and Microsoft Windows operating systems; Oracle and other databases; firewalls, network devices, and routers; and key systems such as LDAP, Active Directory, and more. The solution's unique architecture enables companies to dynamically support any other third-party or in-house systems, devices, and applications.

With EPV, Oracle users can enhance security, reduce risk, and improve compliance while reducing the workloads associated with managing privileged identities. "Companies need to have this kind of rock-solid control over their most critical accounts and systems," says Bosnian. "Together, Oracle and Cyber-Ark help them meet that challenge."

