An Oracle White Paper
December 2010

Strengthening Information Technology Security for the Nation’s Energy Infrastructure
Executive Overview

Record high prices for crude oil, dwindling fossil fuel reserves, and increasing geopolitical instability in the Middle East have put the spotlight firmly on security in the energy industry. Computer security breaches in energy companies pose a double threat, endangering corporate data privacy as well as the stability of the domestic oil and gas supply and national energy grid infrastructure.

One major area of information technology (IT) security concern is password protection of energy company systems and applications. With decentralized operations extending to remote oil fields and distant offshore drilling platforms, field personnel at a rig are often casual about sharing passwords, which creates the potential for unauthorized access to applications and sensitive datafiles. In addition, oil field personnel rely on access to IT systems to get their jobs done. When employees a thousand miles away from the main office forget their passwords, their productivity is severely compromised, and the resulting delays in a password reset translate directly into a bottom line loss.

Oracle Enterprise Single Sign-On Suite Plus is the industry’s leading enterprise single sign-on (ESSO) platform upon which an enterprise can build a full suite of single sign-on solutions addressing all their password-related authentication requirements. Used by three of the world’s largest oil companies, Oracle Enterprise Single Sign-On Suite Plus is rapidly becoming the energy industry’s standard for sign-on and authentication, with more than 250,000 licenses sold worldwide.

With Oracle Enterprise Single Sign-On, network administrators can quickly and efficiently provision and manage passwords from a central point of control across multiple time zones. This results in increased productivity and enhanced IT security at every office, rig, pipeline, and platform.
Oil and Gas Market Dynamics

To truly understand the importance of securing enterprise systems in the oil and gas industry requires a review of key market dynamics.

- **Oil and gas are America's most precious, most limited, and most vulnerable national resources.** Despite being the most precious and most limited national resources, oil and gas are completely controlled, not by the federal government, but by hundreds of private firms—major and junior oil and gas companies responsible for exploration, production, and refining.

- **America's appetite for oil is nearly insatiable.** One out of every four barrels of oil produced in the world is consumed in the United States. Over the past 50 years, nearly 40 percent of total U.S. energy has been supplied by burning oil. About 13 percent of America’s daily oil supply comes from the Persian Gulf states. Without Middle Eastern oil, the U.S. economy would come to a grinding halt. The Persian Gulf produces 18 percent of the world’s oil, so any disruption to this supply could precipitate a severe shortfall, sending the price of oil higher. The U.S. military spends about US$50 billion annually safeguarding oil supplies in the Persian Gulf. Continued geopolitical instability throughout the Middle East and ongoing threats of global terrorism threaten the stability of the Persian Gulf oil supply—and could send oil prices soaring on a moment’s notice.

- **China's booming economy is creating increased Asian demand for fossil fuels.** Between now and 2025, oil consumption in Asia is expected to increase 3 percent annually, with more than one-third of this increase coming from China alone. To meet the growing energy demands of its population of 1.3 billion, China has decided to run pipelines between Xinjiang and Kazakhstan. These pipelines will be vulnerable to attack from hostile minority groups.

- **The oil and gas industry is dependent on IT systems for efficient operation.** Studies show that the ability to monitor and manage upstream oil and gas operations in real time, regardless of location, can cut operating costs for the U.S. hydrocarbon processing industry by US$4 billion to US$8 billion, as well as increase overall output by 2 to 6 percent.

- **The oil and gas industry spends US$0.25 per barrel of crude on IT.** Of the US$0.25 per barrel of crude spent on IT, the oil and gas industry spends US$0.16 on back-office products and services. An article in the *Journal of Petroleum Technology* reports: “A growing number of professionals within the industry are implementing advanced-support mechanisms that address infrastructure security.”

- **The vulnerability of oil and gas companies to computer attacks is real and costly.** One oil and gas company noticed that several thousand barrels of oil were missing. Auditors discovered the cause: manipulation of the network. The company had to replace the missing barrels and incur the resulting revenue loss.

As these market drivers clearly indicate, oil and gas are limited, precious resources that affect every nation. Any impact on the supply chain for these resources has the potential to create global instability. Given the critical role IT plays in this process, the need for powerful application and network security cannot be understated.
Enterprise Single Sign-On: A Single Point of Control

In an oil and gas company, the refining and distribution network could extend thousands of miles, with hundreds of locations in dozens of countries—from remote drill sites in isolated fields to platforms in the middle of the ocean. As incredible as it sounds, energy companies can run between 5,000 and 8,000 different applications, with some having as many as 26,000 applications. IT, of course, must remain firmly in control of access to applications and data.

With Oracle Enterprise Single Sign-On, Suite Plus, application use can be tracked and reported. The solution leverages the common look and feel of application logon requests on the client, regardless of the back-end operating systems, databases, or hardware platforms. The platform intelligently recognizes and responds to application logon requests as they present themselves to users. By eliminating scripts, connectors, and wrappers, Oracle Enterprise Single Sign-On can work regardless of the various application versions that might be deployed or the network or application latency. This frees the enterprise from the limitations of the “authentication silos” built into various enterprise applications.

An Ideal Authentication and Provisioning Solution

There are several reasons why Oracle Enterprise Single Sign-On is particularly well suited to the needs of the energy industry.

- **Reduced customization costs.** Oracle Enterprise Single Sign-On works well with popular applications right out of the box, eliminating the need for programmers to write custom code and scripts to integrate with legacy applications. Energy companies typically have very large applications sets, making it cost prohibitive to create custom scripts.

- **Two-factor authentication.** The energy industry has embraced advanced, two-factor authentication. Oracle Enterprise Single Sign-On is designed to work with tokens, smartcards, biometrics, and other authentication hardware.

- **Rapid roll-out.** Energy companies can have thousands of geographically dispersed users, adding complexity to deployment. Oracle Enterprise Single Sign-On can be rapidly and efficiently deployed using any standard deployment software.

- **Higher-level security.** Because users do not have to remember multiple passwords, Oracle Enterprise Single Sign-On complex application credentials can be used—randomly generated user IDs and passwords—for greater security. This provides added protection for geoscientific surveys, proven and probable reserves data, pipeline pumping stations, process controls, and other sensitive databases and mission-critical infrastructure.

- **Integration with industry-standard platforms.** IT in the energy industry has largely standardized on Microsoft Active Directory. Oracle Enterprise Single Sign-On is designed to work on open standards and, consequently, runs on Active Directory as well as any other LDAP v2/v3 compliant directory.
Maintaining an Audit Trail

Oracle Enterprise Single Sign-On provides interfaces to network and computer logons and sign-on to applications, enabling users to log on one time with a single password. ESSO has already been implemented by almost half the major energy companies worldwide.

After users are logged on, Oracle Enterprise Single Sign-On serves whatever application they open the correct complex application credentials—transparently and automatically. The solution eliminates the need for users to remember and manage multiple usernames and passwords for their applications, while allowing administrators to manage password policies.

Oracle Enterprise Single Sign-On provides IT administrators with comprehensive reports on password-related activity. The solution captures, in real time, data identifying who is accessing what applications and when. By publishing the audit trail to appropriate management consoles, Oracle Enterprise Single Sign-On compiles a total view of user activity. This allows system administrators to correlate historical access data to the access rights originally granted, ensuring that security policy is maintained over time.

A Platform for Advanced Authentication

Security concerns are prompting many companies today to move from simple authentication, which uses only a password, to advanced or strong authentication. Advanced authentication typically requires two forms of authentication. One is something the user knows, such as a password. The other is something the user either has—an authentication device such as a token or smartcard—or something the user is—a biometric such as a retinal scan or fingerprint.

With two-factor authentication, for example, security for the network is essentially doubled by requiring users to present not one but two forms of identification: a password and an authentication device. Without both the password and the hardware, users cannot access all their applications (in graded two-factor authentication, a user who has lost a smartcard but remembers a password can get limited access to the network until a new card is received).

Oracle Enterprise Single Sign-On includes Oracle Authentication Manager, which allows organizations to use any combination of tokens, smartcards, biometrics, public key infrastructure (PKI), and passwords to control access to their applications. As a result, the solution can extend network security through various forms of advanced authentication.

Oracle Enterprise Single Sign-On integrates seamlessly, providing granular control over the level of authentication required to access specific applications. This makes it easier to implement advanced authentication strategies without locking your enterprise into specific authentication device vendors or technologies.
Case Study: An Integrated Energy Company

An integrated energy company with annual sales in the billions of dollars implemented Oracle Enterprise Single Sign-On to enable advanced authentication throughout the enterprise. Oracle Enterprise Single Sign-On encompasses users in hundreds of countries and more than a thousand offices, using thousands of applications. Individuals granted access to the network include company employees, independent contractors, joint venture partners, and other third-party users. These users access applications through local and wide area networks, remotely via a virtual private network and Citrix, and by using 802.x wireless devices and smartphones.

The company’s advanced authentication system requires two identification factors to gain network access: a smartcard and a personal identification number. The system architecture includes Schlumberger’s Identity Process Security Platform card management system, a Microsoft Active Directory infrastructure containing user information, Oracle Enterprise Single Sign-On, and a PKI with certificate authority built on Microsoft Windows.

Implementation Overview

The advanced authentication implementation works as follows:

- Each employee receives a smartcard. User information is embedded in two of the card’s three chips.
- The smartcard is integrated with Oracle Enterprise Single Sign-On.
- Digital certificates for logon, encryption, and digital signatures for all authorized users are stored in the Oracle Enterprise Single Sign-On database.
- The system handles both building and network access with a single solution. Employees must insert their smartcard at the door to gain entry to their building.
- After they are at their desktop, employees insert their smartcard into a card reader on their PC or laptop, then enter a one-time password to activate the card management system.
- The card management system asks a series of questions. Correct answers prove employee identity.
- Oracle Enterprise Single Sign-On binds the card to the end user. It downloads to the card’s third chip a set of digital certificates for logon, encryption, and digital signatures.
- For added security, Oracle Enterprise Single Sign-On also binds the end user’s identity certificates stored on the smartcard to its list of application passwords.
- After activation, the card logs users onto the network and their desktops.
- With the desktop logon now downloaded onto the card, the smartcard is the only credential needed for end users to access network resources.

It is important to note that user application passwords are stored in an encrypted database in Oracle Enterprise Single Sign-On, and not on the smartcard. Therefore, if a smartcard is lost or stolen, the person coming into possession of the badge does not possess any of the user’s application passwords.
The overall system implementation cost was US$50 per user for the cards, card readers, and software. According to the company’s IT department, return on investment was immediate, and included a 70 percent reduction in the nearly 4,000 password resets the business was performing each month. In addition, this company is considered “critical infrastructure” under the federal government’s Department of Homeland Security, and their advanced authentication system demonstrates compliance with the Homeland Security Presidential Directive—a federal mandate to establish secure and reliable forms of identification to access both federally controlled buildings and networks.

Benefits of Enterprise Single Sign-On

With Oracle Enterprise Single Sign-On, users can access all their applications, databases, and systems using a single, easy-to-remember password. So they can gain immediate access to drilling data, production reports, and other critical information in a more-secure, controlled environment.

Better Passwords

User-created passwords are often derivatives of names, Social Security numbers, and birthdays. These “obvious” passwords make it easy for unauthorized users to gain access to enterprise applications and data. With Oracle Enterprise Single Sign-On, users are only required to remember one password, which can be a more-complex system-generated password that is more resilient to attack.

Fewer Help Desk Calls

Authorized users frequently lose or forget their passwords. This places significant burden on IT support to provide replacement passwords. Analyst firms estimate that a password reset call to the help desk costs between US$25 and US$40 per call. This adds up to millions of dollars each year for some enterprises. Oracle Enterprise Single Sign-On customers eliminate password resets by 70 to 90 percent, reducing IT costs and freeing IT budgets.

Increased Compliance

Concerns about ineffective password systems and lax password security have led to many regulations calling for improved password security, for example, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act. By implementing ESSO—either standalone or integrated into an identity management system—network administrators can control password policy from a single point of control, without worrying about increased help desk costs from password resets.

Improved Productivity

Lack of quick and easy access to applications can adversely affect productivity and profitability in oil and gas exploration and production. For example, if geologists in the field are locked out of test well datafiles they need because they forgot their primary password, then the drilling of a new production well might be delayed. Or worse, the geologists might make a drilling error that creates an unwanted fracture and diminishes the output of the new well.
Oracle Password Reset—part of Oracle Enterprise Single-On Suite Plus—allows field personnel to regain access to their computer and the corporate network by resetting their own passwords directly from the Windows logon prompt on their locked-out workstation—without having to call the help desk or go to another workstation.

Oracle Provisioning Gateway—also part of Oracle Enterprise Single Sign-On Suite Plus—allows system administrators to directly distribute user credentials, usernames, and passwords. The administrator can add credentials for new applications and new users, as well as modify or delete old credentials within the solution. When provisioning a new user on a network, the administrator can place the user’s credentials directly into their Oracle Enterprise Single Sign-On account, so the user never knows or touches them.

Conclusion

Securing the IT infrastructure in use by oil and gas companies is critically important. Oracle Enterprise Single Sign-On Suite Plus provides authentication and password protection that several of the world’s largest oil and gas companies use today. Using this solution, these companies can

- **Enforce accountability.** Track application use and provide an audit trail.
- **Ensure safe and reliable access.** Authenticate credentials properly to ensure reliable and secure access to process systems.
- **Lock down applications.** Apply the strictest password policies for each application, preventing unauthorized users from gaining access.
- **Deploy single sign-on.** Authorized users can log on to all applications with a single, secure, easy-to-remember password or by using an authentication device.
- **Encrypt passwords in real time.** Secure and protect every application and credential at all times.
- **Enhance security.** Protect network and data from hackers, thieves, and saboteurs.