

CUSTOMER SUCCESS STORY – NESS TECHNOLOGIES



“The inability to achieve compliance can bring enterprise operations to a halt. Global enterprises, such as ours, which handle project sensitive and confidential information, are mandated to stay compliant ensuring that we have best practices in place to secure information access. IMAG’s effective and

innovative password management solution has enabled AperE to significantly reduce operating costs and enable us to meet regulatory requirements including BS-7799”.

**Director IT,
Ness Technologies**

ABOUT NESS TECHNOLOGIES

Ness Technologies (NASDAQ: NSTC) is a global provider of end-to-end IT services and solutions designed to help clients improve competitiveness and efficiency. Ness specializes in outsourcing, offshore, systems integration, application development, consulting, quality assurance and training. With 7,500 employees, Ness maintains operations in 16 countries and partners with numerous software and hardware vendors worldwide.

THE FIRST CHALLENGE: PASSWORD PROTECTION

Ness Technologies needed to add several new international certifications, such as ISO/IEC 27001 (formerly known as BS 7799), to provide a secure infrastructure for their growing customer base, which is a substantial task.

ISO/IEC 27001 and other standards including ISO/IEC 17799:2005, ISO/IEC 13335-1:2004, ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000, ISO/IEC TR 18044:2004 and the “OECD Guidelines for Security of Information Systems and Networks” require organizations to establish a process and implement controls that monitor and secure financial, personnel, and patient health care data.

To achieve regulatory compliance, Ness Technologies was required to maintain confidentiality of sensitive data, and also needed to ensure that best practices were implemented to secure information access. In addition, the company was obligated to manage mandatory documentation for quarterly fillings, which can be costly and result in decreased productivity as essential personnel are needed to gather and process this information.

THE SOLUTION – IMAG BY APERE

To Implement and Centralize Password Protection and Management

As is the case with most companies, Ness Technologies required users to establish passwords to access network resources. The passwords needed to be a minimum of eight characters long, could not be the same as the login ID or most commonly used information such as last name, maiden name, etc, and could not be a password that had recently been used. However, to avoid a password security breach and maintain maximum protection, passwords should be

Ness Technologies Challenges

- Establish a centralized process to provision users across various applications and perform password reset. The lack of a centralized process created accuracy, productivity and cost issues and this forces Ness Technologies to implement an elaborate manual process that takes as much as 7 business days.

Application Included

- Active Directory (AD)
- Oracle 9i, Oracle 10g
- Bug Tracking System (BTS)
- Time Entering System (TES)
- Solaris Server v10
- Red Hat Linux Server

- Use of the same user ID for different projects results in sharing the same user account which in turn is a compliance violation and a serious security threat.
- Add required international certifications to secure infrastructure,
- Establish a process and controls to monitor and secure financial, personnel, and patient health data
- Ensure that best practices were implemented to secure information access
- Implement, maintain and automate regulatory compliance requirements and reporting
- Maximize productivity and minimize expenses

AperE IMAG Solution

- Centralize password protection
- Establish identity consolidation process
- Automate password management
- Institute self service password mechanism

The Results

- IMAG delivered immediate value to Ness Technologies by successfully and rapidly facilitating the implementation, consolidation and management of user identities and their passwords.
- As a result, Ness Technologies was easily able to meet all required compliance regulations including ISO/IEC 27001, improve administrative productivity, and significantly reduce IT costs.
- IMAG enhanced the ease of managing shared users across multiple applications and networks for Ness, while improving security for regulatory compliance, and maximizing administrative and user productivity.

frequently changed, ideally at least every 15 days. Configurations in which common accounts are used across multiple projects, such as Ness Technologies, security and compliance can become an issue as personnel change responsibilities or leave the company. To properly manage these shared accounts, Ness Technologies needed to consolidate user identities and expand the password management mechanism by bringing key business applications under the compliance umbrella, including Oracle 9i, Oracle 10g, Time Entering System (TES) and Bug Tracking System (BES), Solaris Server, Redhat Linux, as well as Active Directory (AD).

The IMAG Identity Consolidation Process

Ness assembled an authoritative list of all employees including last name, first name and email addresses. In order to access various applications, some of these employees had multiple identities. Ness leveraged IMAG's unique RapidConnector Technology, which emulates the actions performed by an administrator to fetch, create, delete, enable, and disable, as well as password reset, to connect and gather the user information from all key applications in about 30 seconds. *RapidConnector Web™* was used for TES- Time Entering System and BTS- Bug Tracking System. As a result, all users were reconciled by IMAG's unique rule-based reconciliation process, user identities were mapped with an authoritative list that contained all required user information and the reconciliation process provided a reliable view of active and inactive users within the enterprise.

Implementing Password Management using IMAG

Upon completing the consolidation process, Ness Technologies now needed a simple and effective framework for centralizing password management. Aperere's IMAG combines the important benefits of identity management with the security framework of password management to deliver a unique and cost saving password self administration technology. With users across Oracle9i, Oracle 10g, TES and BTS now integrated under IMAG's Password Management process, each would receive an automated reminder to reset their password at pre-defined intervals. When reset by the user, these passwords are then checked against Ness corporate policies including length of (min, max), characters (special, lowercase, uppercase), etc.

In addition, network management personnel at Ness automatically receive email notifications, while IMAG logs security events, whenever passwords or accounts are changed; significantly enhancing network security at the company. IMAG also creates an audit trail of all reset passwords for simple and easy quarterly reporting by Ness IT administration, eliminating potential error and an expensive manual process which could take 1-2 weeks of audit preparatory time.

“The normal time-period to change a password is hours, but with IMAG’s Password Management Solution we are able to reset a password in two minutes, thereby greatly increasing our overall productivity.”

Director IT,
Ness Technologies

IMAG's Self Service Password Mechanism

Because Ness employees require immediate access to multiple applications, forgetting a password can impact their ability to work, resulting in an unnecessary call to the help desk. Ness needed to address this productivity issue by implementing a self service password mechanism in which the user could automatically reset a forgotten password. IMAG offered the self service password management services to allow employees to reset their passwords easily, increasing overall productivity and reducing the number of calls to their help desk.

The Results:

Aperere's IMAG delivered immediate value to Ness Technologies by successfully and rapidly facilitating the implementation, consolidation and management of user identities and their passwords. As a result, Ness Technologies was easily able to meet all required compliance regulations including ISO/IEC 27001, improve administrative productivity, and significantly reduce IT costs.

ABOUT APERERE

Headquartered in San Jose, California, Aperere was established by a group of experienced techno-entrepreneurs, and has been engaged in creating world-class products dedicated to offering state-of-the-art and yet cost-effective enterprise security solutions. Aperere offers the industry's first Identity Managed Access Gateway designed to address identity and data security issues while significantly reducing the management burden placed on IT staff.

US Headquarters

2635 North First St Suite 212
San Jose, CA 95134
Phone: +1-408-434-1001
Fax: 1-408.434.1002
E-mail: contact@apere.com

India Research and Development Office

Aperere India Pvt Ltd
Plot # 14, Huda Colony
Road # 02, Banjara Hills
Hyderabad - 500 033
Phone: +91-40-44308080
Fax: +91-40-44308