ORACLE

OPTIMIZED SOLUTIONS

An Oracle White Paper
March 2011

Oracle's Optimized Solution for CRM - A Business Case for Secured Siebel CRM on Oracle's SPARC T-Series

ORACLE

Executive Overview 1
Introduction to Security Standards Requiring Encryption 3
Payment Card Industry Data Security Standard (PCI-DSS): 3
Health Insurance Portability Act of 1996 (HIPAA)..... 3
Sarbanes-Oxley Act (SOX): 3
Complementary Technologies for an Optimal, *Secured* Siebel CRM . 4
Options for Accelerating or Offloading Cryptographic Workloads... 5
Integrated Cryptographic Acceleration on T-Series 7
Enabling Technologies..... 8
Complementary Technologies for Secured, Optimal Siebel CRM**Error! Bookmark not defined.**
Virtualization Technologies & Security**Error! Bookmark not defined.**
Conclusion 9

ORACLE

Executive Overview

Customer Relationship Management (CRM) is well understood among IT professionals as an application that rapidly becomes critical to an enterprise. Initially, a CRM installation is usually conceived as a tool for improving business efficiency in some singular, straightforward way. But as the CRM system operationally demonstrates its full range of capability, the organization becomes increasingly dependent upon it. Large volumes of data eventually get moved over to the CRM systems in support of new, larger projects.

Then comes the sudden, profound realization that all that data contains a substantial amount of proprietary or sensitive information. If improperly configured for security, a CRM system could become a business liability.

The very nature of CRM links an organization's prospects, customers and strategic partners together but requires sober consideration of issues relating to data privacy, data theft, contractual terms and legally-mandated standards compliance.

Unfortunately, secured configurations of any enterprise software are frequently considered unconventional, unnecessary or an impediment to administrative simplicity. Most IT managers think of security as introduction of risk, rather than a mitigation of risk.

Indeed, implementation of security methods, especially encryption, can introduce additional administrative overhead, require expensive additional hardware, prove an impediment for rapid deployment, or impose a massive decrease in hardware capacity.

But these problems are largely eliminated when deploying Siebel CRM on SPARC T-Series servers. SPARC T-Series servers include a special arithmetic unit optimized for executing cryptography at full CPU speed, mitigating performance concerns and eliminating the need for more equipment.

Combining this unique hardware capability with Oracle Solaris makes it easy to enable and continuously operate in a secured configuration with only a little effort and very little specialized knowledge on the part of the administrator.

This paper explains how deploying SPARC T-Series servers as the cornerstone of your secure CRM deployment mitigates risk while maintaining an advantageous TCO.

This is not a technical manual. For technical guidance and information for securing Siebel CRM, please refer to the installation and administrative guides.

Introduction to Security Standards Requiring Encryption

Many security standards and policies exist worldwide. These standards can be found at the city government level to provincial governments and regional administrations. Additionally, corporations and non-governmental organizations (NGO's) may adhere to security standards uniquely tailored for their needs. But many of the patchworks of IT security standards derive from more universal and well-recognized standards.

Several security requirements may apply to your business, depending on the nature of your enterprise. Below are a few of the most common examples:

Payment Card Industry Data Security Standard (PCI-DSS):

A standard imposed on those accepting major payment cards and processing credit card data. PCI's most noteworthy (and troublesome) rule involves data residing on disks or tapes. One of the most overlooked requirements stated in the PCI-DSS standard is the stipulation that remote administrative consoles for managing server applications must use encryption. This seemingly minor configuration can quickly "leech" performance from the server by imposing a fairly heavy cryptographic workload if the administrative console is dynamic or highly graphical in nature.

PCI-DSS compliance requires at least 128-bit encryption (SSL) in most cases and some PCI compliance officers recommend 256-bit encryption. Most likely, any new revisions to the standards will codify 256-bit as the requirement.

Noncompliance can result in massive fines but more importantly; credit card payments can be suspended, likely resulting in a profound disruption of business and financial losses.

Health Insurance Portability Act of 1996 (HIPAA)

HIPAA standards operate on the principle that information systems containing individual patient health information must be safeguarded against unauthorized access. Since its adoption in the United States in 1996, HIPAA's specific regulations involving the proper handling of patient information have held up well. Notably, HIPAA requires the encryption of any data flowing over an open network.

HIPAA compliance requires a 128-bit level of encryption for the transport of sensitive documents and data over networks.

Noncompliance can result in prison and a fine up to $25,000 per year.

Sarbanes-Oxley Act (SOX):

Sarbanes-Oxley is a legal mandate requiring all publicly held US companies to adhere to certain guidelines in maintaining the security of financial information.

SOX specifies the well-recognized ISO/IEC 27002 information security standard as a best practice for attaining compliance. The ISO 27002 standard advocates extensive use of cryptographic means to secure data.

Cryptographic requirements are set at the 128-bit level and 256-bit is suggested.

Noncompliance can result in extremely large fines and prison for key executives.

Complementary Technologies for an Optimal, *Secured* Siebel CRM

Oracle's most proven and cost-effective solution for Siebel CRM 8 workloads is a highly consolidated design based around Oracle's SPARC T-series servers, the Oracle Solaris operating system, and Oracle's Sun Storage technologies, as shown in Figure 1.

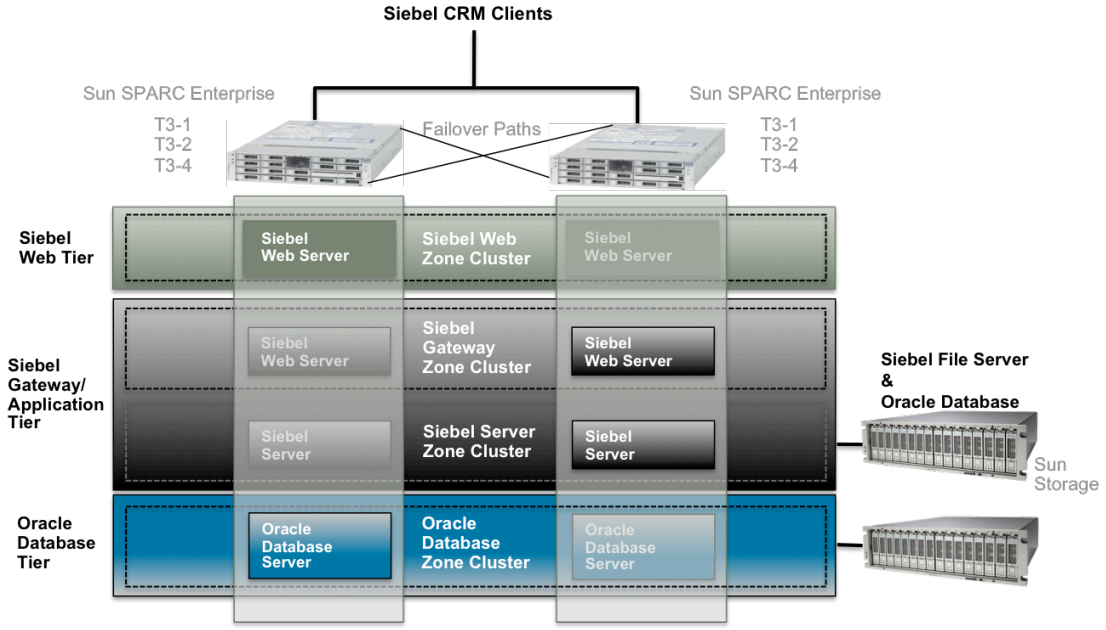

Figure 1. The Siebel CRM consolidated architecture for T-Series optimized for performance and low TCO

At the heart of the solution are Oracle's built in, no added cost virtualization technologies — Oracle Solaris Containers or Oracle VM Server for SPARC (formerly known as Logical Domains) — that enable such a flexible deployment and industry leading efficient operation.

Virtualization Technologies & Security

Using one or both of these virtualization technologies, Siebel CRM 8 services in each tier can run in isolation, without impacting service execution in other tiers. System resources can also be allocated and reassigned to each tier as needed.

That there is no added cost for the use of these virtualization technologies in a consolidated Siebel CRM architecture is not their greatest benefit when implementing a secured configuration. Oracle's enterprise virtualization technologies ideally fit into the overall design is mostly a matter of compatibility and close relationship to the underlying hardware and the Oracle Solaris OS. Both virtualization technologies introduce very little performance penalties on virtualized machines as a result. Either virtualization technology provides a direct means for VMs to access hardware-assisted cryptographic capabilities to run workloads at near-native speed.

Typically, virtualization gets in the way of a VM accessing a CPU's special features directly. Most, if not all, approaches for getting VMs to accelerate or offload crypto workloads to a specialized coprocessor will likely meet with degraded performance, reduced scalability potential, reduced functionality or complete lack of functionality at the hardware, OS, hypervisor or virtual machine level.

For instance, one may add a specialized card to an x86 server to ease the burden of cryptography, but the hypervisor won't likely recognize it and make its capabilities available to virtual machines. Or, one may retrofit a similar type of card to a enterprise-level server and find it works well, but must be allocated in whole to a single VM, wasting a great deal of computing potential.

In any case, the most ideal technical arrangement is virtualization capability fully aware and able to exploit specialized hardware features. In the Oracle T-Series servers, the cryptographic processor is built in to the CPU of the server itself, and is designed from the ground up to work with Oracle Solaris, and all virtualization features enabled by that operating system. This is a unique benefit over pure software layer cryptographic systems through being "virtualization aware" and running at full internal CPU "wire speed", allowing for impressive comparable performance.

Oracle Solaris Containers

Containers are a no-cost virtualization mechanism that can isolate application services within a single instance of Oracle Solaris, enforced by kernel level separation between each container. Oracle Solaris Containers are designed so that faults in one container have no impact on applications or service instances running in other containers. Containers are an OS-level type of virtualization, making it inherently hardware-aware, OS-aware and highly compatible with anything the underlying Oracle Solaris OS can address. In addition, it imposes very little performance penalty on its virtual machines while being extremely quick to set up and provision.

Oracle VM Server for SPARC.

Native to Oracle chip multi-threading (CMT) processors like the SPARC T3, this technology allows multiple tiers to be consolidated easily using isolated domains, without additional cost. Each domain runs a completely independent copy of Oracle Solaris, and there are no licensing fees for additional OS copies. Oracle VM for SPARC is a hypervisor type of virtualization designed to fully encapsulate virtual machines by abstracting the hardware's resources. This approach allows for extremely fine-grained resource allocation and other advanced features. As opposed to many types of hypervisors that need to be installed or retrofitted onto some sort of server storage, Oracle VM Server for SPARC is built into the firmware of the platform to insure optimum functional circumstances.

Options for Improving Cryptographic Workload Performance

Accelerator or Offload PCI cards

While crypto cards are fairly accepted and somewhat popular in the IT industry, they suffer from intractable technical disadvantages.

Chief of these disadvantages is their inherent performance disadvantage by way of their position in a system. Cards reside on a bus, a decidedly slower and less direct placement in relation to the CPU.

While the card itself may be able to crunch through huge amounts of cryptographic work, it must still move that data across the bus. Under intense workloads, with multiple cards, it is perfectly conceivable to consider the burden all this bus traffic will have on the overall system performance, as well as showing increased needless power consumption with those multiple cards running at full speed, but not delivering full performance.

Also troublesome is the necessary consideration that an addition of a card to a system is an addition of complexity, and therefore an introduction of risk.

While these other problems can certainly vex a deployment making use of cards, they are essentially a performance consideration. More importantly, Siebel CRM architects may simply dismiss the option of a card altogether if their design involves the use of hypervisor-type virtualization. Hypervisors, such as those commonly used on x86 platforms, are usually not compatible with such add-ons and it's generally considered bad practice to run virtualized cryptography-type workloads over the PCI bus.

On other enterprise platforms, cards might work just fine with the hypervisor but cannot be partitioned and allocated fractionally. Essentially, one card must be allocated to one VM, limiting how many VMs with cryptographic capability can operate to the number of card slots available, and therefore decreasing business agility in responding to emergent or unexpected cryptographic demands needed by other instances of the OS running elsewhere in the system.

Network Load Balancers/SSL Accelerator network appliances.

Network load balancers (NLB) can be found in many datacenters mostly as a means of distributing work among a pool of servers in order to increase redundancy and increasing capacity. But many of these NLBs can do a double duty as cryptographic offload engines. They operate by intercepting incoming encrypted data over the network, decrypting the data and passing it on to the application server "in-the-clear." It works in reverse for outgoing data encryption. Some of these appliances dispose of the NLB functionality altogether and operate only as a cryptographic offload engine.

In principle, these appliances are simply preprocessors designed to lighten the load on the application server.

While the network appliance approach for handling cryptographic workloads may be straightforward, it adds substantial physical footprint to any project and negatively impacts most of the gains of server consolidation by drawing additional power, requiring more cooling and specialized administration.

On-CPU cryptographic units

Since their inception, SPARC T-Series CPUs have included a special arithmetic unit ideally suited to computing cryptographic workloads.

This is not to say that SPARC T-Series remains the only product to place specialized cryptographic provisions on-chip. X86 chipmakers have taken notice of the SPARC advantage and have begun placing cryptographic enhancements on their CPUs as well.

However, no enterprise server hypervisor software currently claims or indicates virtual machine support for the new on-chip cryptography available in certain x86 current-generation CPUs. Even

when that support comes, x86 CPUs with cryptographic enhancement are limited to one SIMD (Single Instruction Multiple Data) crypto unit per core. Presently, that adds up to six total. The new SPARC T3 CPUs, by contrast, possess sixteen crypto units on the chip. This allows roughly twice the density of virtual machines making full use of cryptography, while imposing minimal overhead. Increased density and capacity at the virtual layer result in less hardware and ultimately less TCO.

Integrated Cryptographic Acceleration on T-Series

Understanding the complex deployment scenarios that typically result from the need to keep information secure, Sun and then Oracle created the SPARC T1, T2, T2 Plus and T3 processors—CPUs that are targeted at throughput applications and are equipped with built-in hardware cryptographic units to simplify and accelerate cryptographic operations. The processors combine chip multiprocessing and hardware multithreading with an efficient instruction pipeline to enable chip multithreading. The resulting processor design provides multiple physical instruction execution pipelines and several active thread contexts per pipeline.

To meet the ever-increasing demand on cryptographic operations, the SPARC T2, T2 Plus and T3 processors use a unique System-on-a-Chip (SoC) design that incorporates additional cryptographic features as well as on-chip I/O and on-chip 10 Gigabit Ethernet networking capabilities to help improve performance (Figure 2).

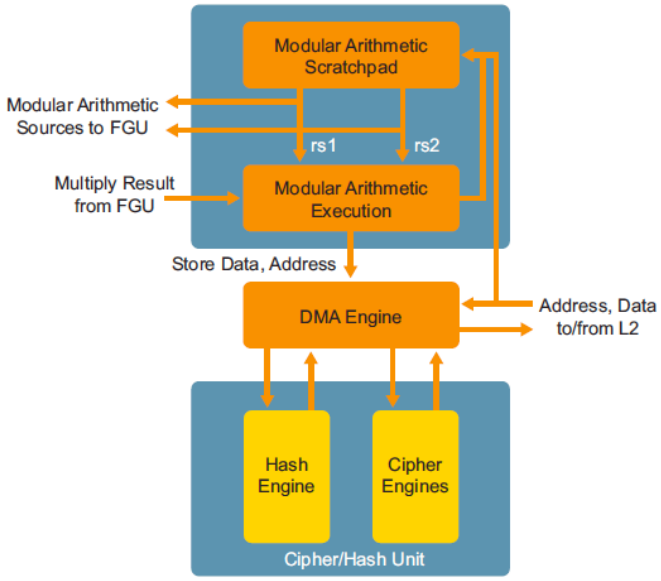

Figure 2. The Modular Arithmetic Unit

Rivest Shamir Adleman (RSA) operation is an important component of the Secure Sockets Layer (SSL) full handshake. Each core of the SPARC T1, T2, T2 Plus and T3 processors includes a Modular Arithmetic Unit (MAU) that supports RSA and Digital Signature Algorithm (DSA) operations. RSA operations utilize a compute intensive algorithm that can be off-loaded to the MAU. Indeed, the MAU is capable of sustaining 14,000 RSA-1024 operations per second on a system with an SPARC T1

processor, more than 30,000 RSA-1024 operations per second on systems with an SPARC T2 processor and over 40,000 RSA-1024 operations per second on the SPARC T3. Moving RSA operations to the MAU speeds SSL full handshake performance and frees the CPU to handle other computations.

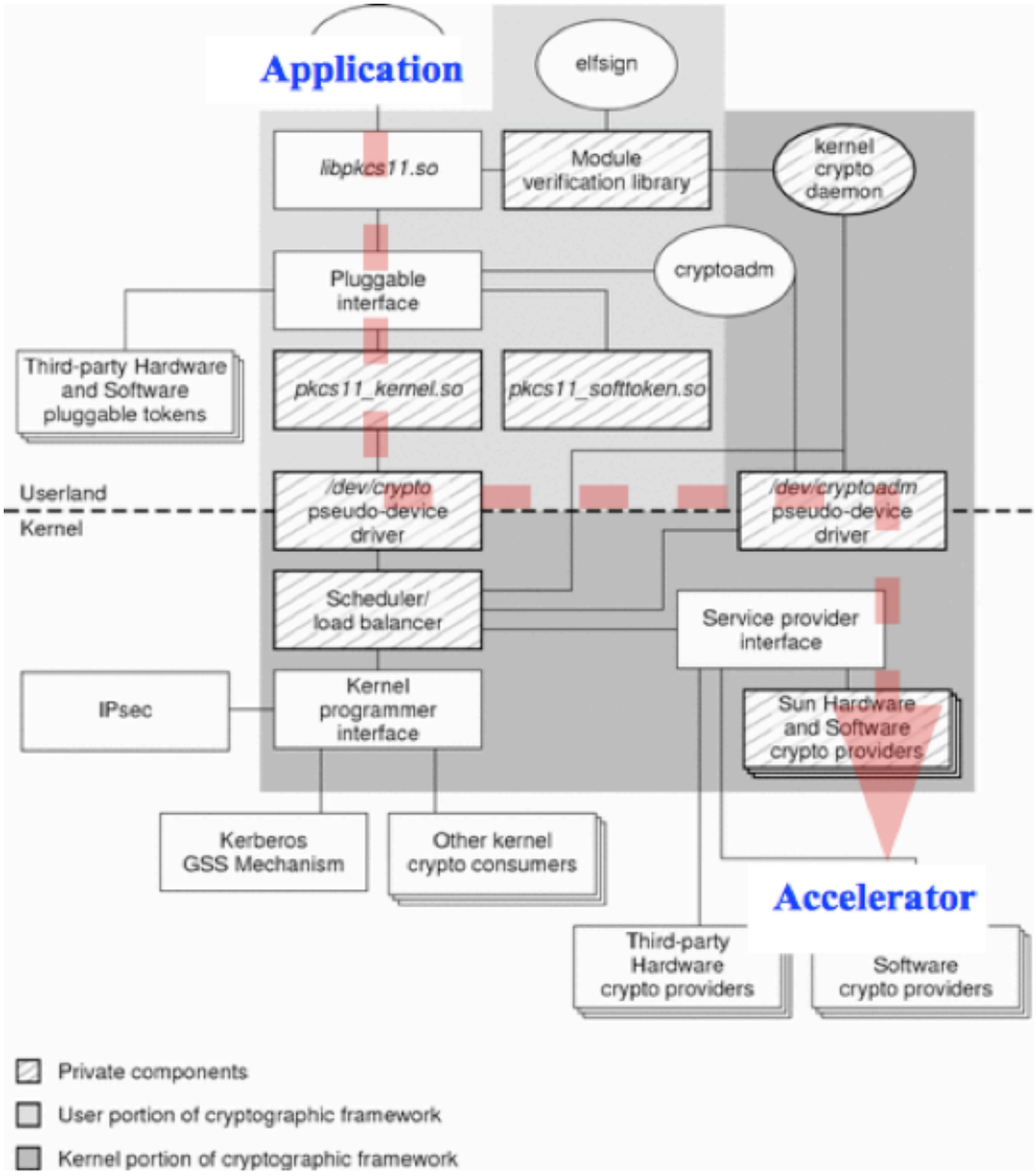

Figure 3. Overview of cryptographic workload management for SPARC T1, T2, T2+ and T3 CPUs

Enabling Technologies

The cryptographic capabilities of the SPARC T1, T2, T2 Plus or T3 processors can be accessed via the Solaris Cryptographic Framework (SCF). SCF provides cryptographic services for kernel-level and user-level consumers, as well as several software encryption modules.

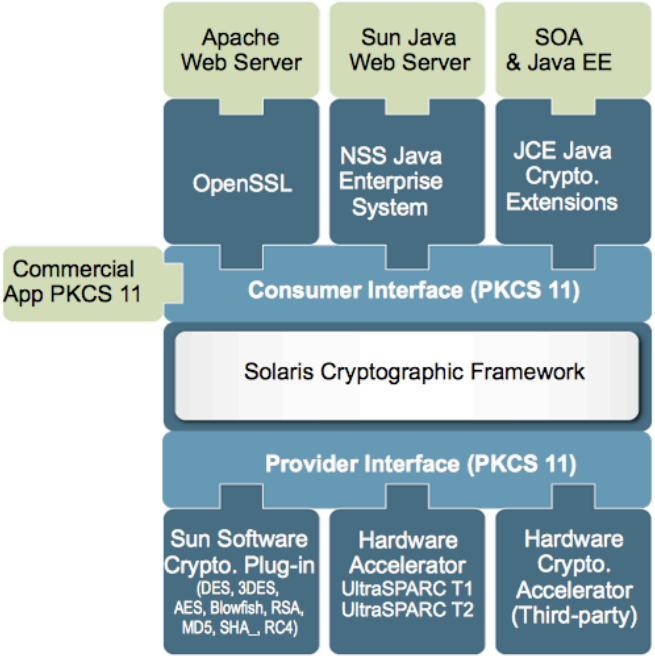

Figure 4. Accessing hardware cryptography assist from software

SCF continues to include Kernel SSL proxy (KSSL), which off-loads SSL processing from user applications and enables them to transparently take advantage of hardware accelerators, such as those available in SPARC T1, T2, T2 Plus or T3 processors.

Conclusion

As IT operational cost pressures converge with stringent security requirements, only Siebel CRM deployed on Oracle SPARC T-Series servers can retain a tightly consolidated profile and high performance throughput while implementing a secured configuration.

A secured configuration on the SPARC T-Series requires no additional equipment, no specialized training or any type of functional compromise as compared to competitive offerings.

The introduction of the new Oracle SPARC T3-1 server, with its increased thread count, doubled capacity for virtualization and myriad other evolutionary improvements, serves to cement Oracle's position as the leading provider of high-performance, cost-effective end-to-end integrated CRM solutions.

A Case for Securing Siebel CRM with
Hardware-assisted Cryptography
March 2011
Author: Chad Prucha

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.
This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0110

Hardware and Software, Engineered to Work Together