Security: An Oracle Solaris Differentiator

November 2020

Part No: E89596

This article describes the security threats that enterprise systems face and how Oracle Solaris systems address those threats.

A Look at the Security Landscape

Today, security is a paramount and urgent business concern. More and more products and services connect individuals to the network in increasing numbers and with greater ease. Online transactions are commonplace. Network traffic of vast amounts of data occurs non-stop worldwide.

This increasing business interconnectivity has changed the nature of security, the underlying threats, and the countermeasures to address the risks.

Security breaches have evolved from being the experiments of amateur hackers to being information theft by professional operations. Selling stolen information and ransoming access are highly lucrative. Cybercrime is big business.

Cyber attacks cost businesses $400 to $500 billion each year. The following are just some of the ways that businesses are damaged:

- In the short term, direct loss of customer, employee, and company data and digital assets.
- In the longer term, negative branding and further loss of customer trust. Companies that have been penetrated are at a competitive disadvantage.
- Exposure to lawsuits, penalties, and other legal liabilities.

The frequency of reported attacks shows the widening reach of cyber criminal activity that affects all industries across geographies. Security experts estimate that 95% of all customers have been breached, although they might not know it yet.

Increasingly, companies must satisfy new security-related regulations such as the following:

- Security measures as a requirement for conducting business.
- Stiff penalties for security failures.
- Required response times in the event of a breach.

Oracle's Security Solutions

Oracle's security offerings are unique from those provided in other products by their respective vendors. Oracle owns the entire stack, encompassing both the hardware and software components. Therefore, Oracle can employ cross layer and in-between layer engineering to truly implement a defense-in-depth solution against cyber threats. These enhancements are further extended in the capabilities that have been engineered into Oracle SPARC and Solaris products.

The purpose of the defense-in-depth strategy is threefold:

- Prevent attacks.

  Oracle systems use encryption and redaction, masking and subsetting, as well as controlling all privileged user credentials to shield themselves from attack.
- Detect security breaches.

  Oracle systems perform active monitoring, auditing, and reporting to record suspicious activity.
- Administer all the security-related system components.

Being the owner of the total stack, Oracle offers integrated administrative tools such as key management, privilege and data recovery, and configuration management to efficiently administer security.

According to an analysis, 82% of all reported attacks is caused by the following vulnerabilities:

- Abuse and misuse of credentials (50%).
- Unpatched or poorly configured systems (19%).
- Unprotected data (15%).

The following sections discuss how Oracle Solaris security solutions are designed to specifically address these vulnerabilities.

Abuse and Misuse of Credentials

One hundred percent of all cyber attacks target user names and password credentials. These are the keys that enable entry to a company's infrastructure and its digital assets and intellectual property. The extent of the monetary losses due to theft of personal and company information reaches billions of dollars.

To minimize this vulnerability, Oracle Solaris systems run an array of technologies such as the following:

- Immutable systems and virtual machine technology
- Role based access controls
- Secure by default installation
- Verified boot

In combination, these technologies secure and protect user credentials by blocking malware from gaining a foothold in the data center.

System immutability minimizes administrator mistakes by preventing even superusers from writing files on the system and making configuration changes. If changes are required, these occur on the next layer down and are visible because they are audited. With verified boot, only signed boot and kernel modules can run on the system, and unauthorized or unsigned software fails. Therefore, malware code cannot alter system configurations.

Additionally, system administrators, database administrators, and others who have privileged access are granted limited rights that are directly related to their specific tasks. These rights be can controlled by time, date, and system name so that authorized system and data access are restricted only to defined days and times. Thus, 24/7 access is granted only to the most essential roles rather than to all administrators.

Role based access controls are complemented by fine-grained auditing. With remote auditing, audit records are kept elsewhere than on the system being monitored. Therefore, hackers cannot tamper with audit trails to remove evidence of a breach.

These security controls are available on all Oracle Solaris systems.

Unpatched or Poorly Configured Systems

Unpatched systems are open doors into the data center. Of the reported penetration through unpatched systems, 99.9% occurred at least a year **after** vulnerabilities were identified and published and the patches had been made available to plug those security holes.

Failure to patch systems promptly despite official threat notices is largely due to the complexity of patching systems. The hybrid infrastructures that most enterprise environments use are particularly complex.

In a generic environment, systems and software are assembled from a variety of sources. Accordingly, patches for each layer of the stack are supplied by different vendors. Typically, vendors provide their own vendor-specific tools to apply their patches.

In this scenario, a customer deals with multiple but autonomous patches that have not been tested to run together. The customer has the responsibility to designate a time period to test the patches and ensure they do not break the operation of the system. Testing can take a significant amount of time. If failures occur during testing, patching would be delayed while emergency fixes from vendors are also tested to identify potential impacts. Postponements in applying patches increase the probability of the systems being penetrated.

The customer is also in charge of rolling out the patches to production. In a generic environment, a smooth rollout is not guaranteed. Rolling back the patches can become as complicated as the patching itself.

In short, in a heterogeneous data center, patch management can be very challenging.

Oracle Solaris security fixes, together with other feature updates, are released through support repository updates (SRU releases) and, for earlier OS versions, through patches. SRUs are released monthly. In urgent circumstances, critical fixes can made available outside of the monthly schedule.

- In SRUs, all updates and security fixes are pre-bundled. Thus, SRUs are applied as a unit.
- Security updates apply to all layers of the stack: applications, database, OS, virtualization, and firmware.
- These updates are tested to guarantee that they work together seamlessly before they are released.
- Only one tool is employed. System update (patching) is accomplished with a single command. Similarly, rollback also is a one-step operation. Both update and rollback require at most a single reboot. Therefore, very little system downtime is involved.
- A critical patch update is published every quarter that delivers all new security fixes for Oracle products, including Oracle Solaris SRUs and Solaris 10 patches.

Cybercrime and other system security threats have made frequent and timely patching a necessity. With Oracle Solaris 11, system update incurs minimal downtime.

Unprotected Company Data

The final target of cyber theft is the company's data.

Typically, security protection is focused on "defending the perimeter": protecting the network from intrusion. In one survey, 52% of respondents said that their databases are the most vulnerable to an attack, while 34% said their network is the most vulnerable to an attack. The same survey found that 67% of security resources are allocated to secure the network, while 15% of security resources are spent on data protection.

A secure network is a vital component to guard against attacks. Spending continues toward the deployment of intrusion detection systems, anti-malware, and network firewalls. However, in the age of globalization, industries span multiple countries across the globe. Outsourcing is common practice. Company data centers are in multiple locations. More recently, businesses are turning to cloud computing and services. These developments have made the network very large. If a network is breached, then other protections need to be in place between the attacker and company data.

One protection is encryption. In Oracle Solaris systems, encryption protection begins in the firmware and extends across to kernel software, application software, and database.

A general objection to encryption is performance overhead. No such penalty exists with Oracle Solaris systems running on SPARC.

Oracle implements industry standard algorithms and optimizes their performance on the SPARC chip. With on-chip technology, algorithms are executed on the chip rather than on the CPU. Because cryptography

is automatically offloaded when the algorithm is available on the chip, the processor becomes free for applications and the database to use, which accelerates their performance. The SPARC processor has more on-chip cryptography than any other processor.

The Silicon Secured Memory feature of SPARC processors adds another security layer through hardware monitoring of software access to memory. By protecting memory, it can prevent invalid operations to application data, effectively blocking malware from exploiting software vulnerabilities such as buffer overflows. This SPARC feature is faster than traditional software-based detection tools and has no impact on performance.

Encryption is built in to ZFS and SDN networking, and data is protected whether in motion or at rest. The operating system is integrated with Oracle Key Manager to secure all your keys in one place.

In summary, Oracle hardware and software technologies provide full capabilities to encrypt everything, everywhere, all the time. On Oracle Solaris systems, data protection and encryption security can be activated by default without requiring additional hardware investment.

Conclusion

In Oracle systems, security is part of the design, "built in, not bolted on." Security-in-depth enables companies to quickly meet their security compliance requirements. At the same time, performance is not sacrificed in favor of security. Businesses that use Oracle Solaris systems benefit equally from both at the same time.

Security: An Oracle Solaris Differentiator

Part No: E89596

Référence: E89596

Restrictions de licence/Avis d'exclusion de responsabilité en cas de dommage indirect et/ou consécutif

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Exonération de garantie

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Avis sur la limitation des droits

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Avis sur les applications dangereuses

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Marques

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Inside sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Epyc, et le logo AMD sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Avis d'exclusion de responsabilité concernant les services, produits et contenu tiers

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Date de publication et mention de la version préliminaire de Disponibilité Générale ("Pre-GA")

Version préliminaire de Disponibilité Générale ("Pre-GA") : 15.01.2020

Avis sur la version préliminaire de Disponibilité Générale ("Pre-GA") de la documentation

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère public ou privé :

Cette documentation est fournie dans la Version préliminaire de Disponibilité Générale ("Pre-GA") et uniquement à des fins de démonstration et d'usage à titre préliminaire de la version finale. Celle-ci n'est pas toujours spécifique du matériel informatique sur lequel vous utilisez ce logiciel. Oracle Corporation et ses affiliés déclinent expressément toute responsabilité ou garantie expresse quant au contenu de cette documentation. Oracle Corporation et ses affiliés ne sauraient en aucun cas être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'utilisation de cette documentation.

Mention sur les informations confidentielles Oracle

INFORMATIONS CONFIDENTIELLES ORACLE. Destinées uniquement à un usage autorisé. Ne pas distribuer à des tiers.

Avis sur la reconnaissance du revenu

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère privé :

Les informations contenues dans ce document sont fournies à titre informatif uniquement et doivent être prises en compte en votre qualité de membre du customer advisory board ou conformément à votre contrat d'essai de Version préliminaire de Disponibilité Générale ("Pre-GA") uniquement. Ce document ne constitue en aucun cas un engagement à fournir des composants, du code ou des fonctionnalités et ne doit pas être retenu comme base d'une quelconque décision d'achat. Le développement, la commercialisation et la mise à disposition des fonctions ou fonctionnalités décrites restent à la seule discrétion d'Oracle.

Ce document contient des informations qui sont la propriété exclusive d'Oracle, qu'il s'agisse de la version électronique ou imprimée. Votre accès à ce contenu confidentiel et son utilisation sont soumis aux termes de vos contrats, Contrat-Cadre Oracle (OMA), Contrat de Licence et de Services Oracle (OLSA), Contrat Réseau Partenaires Oracle (OPN), contrat de distribution Oracle ou de tout autre contrat de licence en vigueur que vous avez signé et que vous vous engagez à respecter. Ce document et son contenu ne peuvent en aucun cas être communiqués, copiés, reproduits ou distribués à une personne extérieure à Oracle sans le consentement écrit d'Oracle. Ce document ne fait pas partie de votre contrat de licence. Par ailleurs, il ne peut être intégré à aucun accord contractuel avec Oracle ou ses filiales ou ses affiliés.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

ORACLE