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 occur non-stop worldwide.

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

Security breaches have evolved from being the work of hobbyists and amateur hackers to becoming a professional operation of organized multibillion dollar enterprises. Where hobbyists were only aiming at testing, the intent of current enterprises is more criminal, that is, information theft. Selling stolen information is highly lucrative and has become equally, if not more, profitable than drugs. Cybercrime is big business.

Cyber attacks cost businesses $400 to $500 billion a year and cause extensive damage. The damage take on varied forms but all lead to a decline in company earnings and value. For example:

- 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 which affects all vertical industries across geographies. Security experts estimate that 95% of all customers have been breached, although they might not know it yet.

Consequently, companies now have to satisfy new security-related regulations imposed by governments in response to these threats, such as:

- 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 in patching systems. The complexity is particularly true in a hybrid infrastructure that most enterprise environments use.

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 before. The customer has the responsibility to designate a time period to test the patches and ensure they do not break the rest of the operations. 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 systems' probability of being penetrated.

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

In short, in a heterogeneous data center, patch management is a nightmare.

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. However, in urgent circumstances, critical fixes are also made available outside of the monthly schedule as necessary.

- In SRUs, all updates and security fixes are pre-bundled. Thus, SRUs are applied as a unit.
- Security updates apply to all the 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. Patching is run with a single command. Similarly, rollbacks are also a one-step operation. Both patching and rollbacks require only a single reboot. Therefore, very little system downtime is involved.
- A critical patch update is published every quarter that lists all new security fixes in Oracle products, including Oracle Solaris SRUs and Solaris 10 patches.

With Oracle Solaris systems, patching is efficient. A system administrator is able to patch 16 times as many Oracle Solaris 11.1 systems as one who manages non-Oracle systems.

System security threats have made frequent and timely patching a reality. In the era of cybercrime, the adage "if it ain't broke, don't fix it" is an unwise philosophy. Instead, "patch early and patch often" is a best-practice approach to secure the data center. With Oracle Solaris systems, this practice is no longer a daunting experience.

Unprotected Company Data

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

Typically, security protection is focused on "defending the perimeter", that is, protecting the network from intrusion. In one survey, 52% of respondents claim that their databases are the most vulnerable to an attack, compared to only 34% claiming the same about their network layer. The same survey also indicated that 67% of security resources is allocated to secure the network, while 15% is spent on data protection.

A secure network is a vital component to guard against attacks. Spending continues towards the deployment of intrusion detection systems, anti-malware, and network firewalls. However, in the age of globalization, industries encompass 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, and achieving a completely secure perimeter is virtually impossible. If a network does get 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. It is worthy to note that 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 code 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.

Also, 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's 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 using Oracle Solaris systems benefit equally from both at the same time.

Security: An Oracle Solaris Differentiator

Part No: E89596

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E89596

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.

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.

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 ce 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.

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 Xeon 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, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

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.

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.