Pillars of Protection:
A New View of Enterprise Security

ORACLE WHITE PAPER | JULY 2018

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Introduction

At Oracle, security is our top priority. We take it seriously. We provide integrated security controls at each layer of the stack from the applications down to the operating system, virtualization and hardware, including storage. This means that Oracle Linux and Oracle VM provide security advantages over other Linux distributions and virtualization technologies. Oracle allows you to build pillars of protection for both private and public cloud deployments, providing a secure, low-risk foundation for your workloads.

Defending Your Business

Cyberattacks are on the rise. Whether you know it or not, you are in a cyberwar. You need to defend your business from attackers. However, building firewalls to keep bad actors out is not enough anymore. You need layers of protection in your data center and in the cloud. Tools like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are a necessary start but they aren't enough either. At every layer of your environment, you need to protect three things: people, the platform and your data. We call these the "Pillars of Protection." You need to engage all three pillars in order to protect your data center and cloud instances from cyberattacks.

For more on the lifecycle of a security breach, read the Anatomy of a Cyber Attack.

People

People are the Achilles' heel of cybersecurity[1]. People have been and continue to be the single largest source of cybersecurity incidents. While some may be "bad actors," generally, incidents are either the result of simple mistakes that create exposure to a cyberattack or information leak via social engineering. Training your people to handle sensitive data, systems, passwords, and account access is *critical* to success in cybersecurity.

However, training alone is not enough. You also need to protect your data and systems *from* people.

Oracle Secure Global Desktop helps you secure your systems by isolating users from the systems they are using. Oracle Secure Global Desktop provides *secure* access to virtual desktops which means your users are no longer directly connected to your servers. Instead, users have indirect remote access to the system via an Oracle Secure Global Desktop proxy system.

By isolating users, you are protecting your servers from malware attacks. When using Oracle Secure Global Desktop, users are in effect interacting with a screen image. When a key is pressed, or a mouse click occurs, that information is sent to a remote server that interprets it, and then passes the corresponding action to the system the user is virtually connected to. So, while it looks like they are typing and interacting with windows on the desktop of the systems, they are not actually connected to those systems.

This level of isolation allows users to stay outside your firewalls and still be able to work. Even if your user's systems are attacked by malware, the malware cannot be spread to the systems they are using inside your firewalls.

Also, the Oracle Secure Global Desktop gateway proxy tunnels its proprietary display protocol for interaction between the client/user system and the remote instance through SSL, therefore the attack surface is significantly reduced in the event the client system is exploited.

[1] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-internet-of-things.pdf

Now that you've protected your systems, you can improve the methods by which you provide the identity of your users by implementing Multi-Factor Authentication (MFA). MFA goes beyond the traditional username/password combination that has been problematic throughout the years.

There are three factors that can be provided to prove your identity: something you know (i.e. your password), something you have (i.e. a token provided by a dongle or app), and something you are (i.e. fingerprint or facial scanning).

MFA systems incorporate two or more of these factors into the authentication process. One of the most common MFA systems Oracle Linux provides is the ability to use smart cards as part of the authentication process. Smart cards provide physical authentication in combination with username/password (i.e. knowledge-based authentication). Regardless of the second factor, whether it be smart card, challenge/response cards or software, or using biometric scanning, introducing a second factor greatly increases the likelihood that the person being identified is actually who they say they are.

Once you implement MFA and are assured that only your employees are accessing your systems, you still face the threat of people having access to systems or data they shouldn't. Someone in product development shouldn't have access to your human resources databases, and someone from human resources shouldn't have access to your development systems.

Oracle Linux provides a "least privilege" model which helps ensure that only the data that a user needs is accessible to them. This model allows user access to be granted for only the required level necessary to perform an authorized action.

Finally, Linux Integrity Management can monitor and block accidental or malicious changes made to files. This helps prevent users from exposing data, either due to mistakes or intentional action, and can prevent potential data corruption. Combining Integrity Management with remote audit logging helps prevent an attacker from hiding their activities by preventing them from removing audit log entries.

Platform

The second pillar of protection is the platform. These are the physical and virtual machines in your data center, or any instances in the cloud. While people can be the root cause for the plurality of incidents, vulnerable systems contribute to a large portion of successful attacks.

One of the main reasons systems are vulnerable is that they are either not patched or not patched quickly enough. Systems continue to be unpatched across the globe. More than 110 unique Common Vulnerabilities and Exposures (CVEs) that had fixes available in 2007 were exploited in 2016[2]. This is a trend that has been consistent for many years.

Even if you are patching your systems, it may be taking months to do so because patching a system is hard. Patching an entire data center is nearly impossible to do quickly. There are a lot of variables to consider before a system can be patched. Things like:

1. Is the patch available for the version of the operating system (OS) that is being run?

   Often, the system is running an older version of the OS. If the system is running an out of support version of the OS, a patch may not exist.

[2] Verizon Data Breach Investigations Report, 2016

2. Does the patch impact the software running on the system?

   Very few operating system vendors test their patches using real-world applications and data. For example, the community version of the Stack Clash vulnerability fix (CVE-2017-1000364) caused some issues with some enterprise software applications, and the fix needed to be re-released.

3. Does the patch work with the server's particular version of the hardware?

   The exact revision of hardware may change during the production of a server model. This can lead to incompatibilities in one system, while another "identical" system may not have issues with the patch.

4. When is the server available to be taken offline for patching?

   Often, patching a system means the system must be down to perform the patch, and it typically must be rebooted for the changes to take effect. In today's 24/7/365 business world, a system may be allowed only 2-3 hours of down time per year, if at all, depending on the demands of the line of business that runs the applications on the system.

Taking these variables into consideration for one system is difficult enough. Doing the analysis, planning and action required to execute a patching plan across 10,000 systems is extremely challenging.

Traditionally, IT philosophy has been to deploy servers and only touch them again if they break but the era of "If it ain't broke, don't fix it" is over. Continuing to apply this philosophy today is at best waving a white flag of surrender and at worse inviting invasion. You must patch your data centers, and not just your "edge" systems. Act as if the bad guys are already in your data center because they may already be there, whether you are aware of it or not.

Oracle Linux has several unique capabilities to help you address these issues. Only Oracle Linux provides zero downtime patching for kernel and selected user space libraries via Oracle Ksplice technology.

Ksplice is a proven enterprise-class capability of Oracle Linux. It allows you to apply a security or stability patch to the OS kernel and the critical libraries while the system is running, and the patch takes effect immediately. Ksplice can also be used to apply security and stability fixes on the Oracle VM hypervisor. Meaning, you can patch your guest VMs and your host too. If you're using containers, Ksplice patches are automatically applied to the host kernel, so all your containers are patched as well. All without downtime.

Each Ksplice patch, called a splice, is tested extensively with Oracle Applications and Oracle Database to help ensure that the splices are rock solid for your most intensively used production systems. Additionally, Ksplice can be easily configured to automatically patch your systems as new splices are released, allowing you to rest assured that your systems have the most recent security fixes installed on them.

If you use Oracle Enterprise Manager or Spacewalk to manage your data center, you can push the Ksplice patches out to all systems, greatly simplifying patching and significantly reducing the time it takes to remediate security vulnerabilities. Additionally, both Oracle Enterprise Manager and Spacewalk allow you to execute the OpenSCAP compliance testing tool across managed systems, allowing you to validate that your systems continue to meet your compliance requirements.

But, even if you are actively patching your systems, they can still be vulnerable. Patching, while critical to remaining secure, doesn't solve the problem of being vulnerable. There are two reasons for this:

1. The bugs at the heart of many Common Vulnerabilities and Exposures (CVEs) have been in the code base for years before they were discovered and fixed. There have been many CVEs that were published (i.e. the bug was found and fixed by vendors) as much as 10 years after the bug was introduced into the code base. Heartbleed is an excellent example of such a bug. The Heartbleed bug was introduced into

SSL 10 years before it was discovered. That means that you, and everyone else, were vulnerable to attack for 10 years before there was a fix available.

2. There are far too many CVEs discovered and fixed to patch them all. In 2016 alone, there were 6,435 newly published vulnerabilities[3]. Of those, 2,469 (38%) of them had CVSSv3 score of 7.0 or higher.

Whenever code is installed on a system, there is the potential for unknown vulnerabilities to be there waiting to be exploited. While “white hat” hackers work to identify these vulnerabilities, so they can be fixed, there are still far too many vulnerabilities to be able to keep up. Sometimes, even after a CVE is published, there still isn’t a fix for it.

More importantly, preemptive mitigation technologies need to be applied to help reduce exposure to potential vulnerabilities.

This can be achieved with a security solution that provides layers of protection. Each layer represents additional hurdles for an attacker to overcome, thus slowing down or potentially frustrating an attack. On many popular x-86-based systems, Oracle Linux helps prevent exploitation from occurring.

Oracle Linux provides tamper evident software by cryptographically signing all RPM packages. This means that you know if the package being installed has been modified in any way. It also means that you can prevent installation of any software not properly signed. At boot time, as the OS is loaded, it can be verified via secure boot that what is about to be run is what is expected to run. When you enable secure boot, no unsigned kernel modules are allowed to run on the system, which significantly reduces the risk of malware infecting the operating system.

Next, file labeling allows fine-grained control over who has access to a file and the access rights they have to that data. This prevents users from being able to read, write, or modify data that they are not authorized to access.

Another critical capability is being able to establish baseline software and best practices across your data center and cloud deployments. To assist you in achieving this, Oracle provides pre-built VM templates as well as the capability for you to build your own.

Oracle also provides pre-built containers on Oracle Container Registry, simplifying the process of building a secure cloud environment in your data center or in a public cloud.

Data

The third pillar is your data. In 2016, the average cost per record of data stolen was $158[4]. The cost per record by industry ranged from $88/record for government (public sector data) to $355/record in the healthcare industry. In 2016, the cost of stolen data to the healthcare industry was more than $325,000/minute[5].

Traditionally, protecting the data center, and therefore the data, meant protecting the network with firewalls, network intrusion prevention systems and network intrusion detection systems. While it’s critical that these things are done, it is simply insufficient to protect your data.

Let’s use the analogy of a medieval castle: castles were built to keep invaders out and protect the people inside. They had vast walls surrounding them. However, castles were also living cities, and needed ways to interact with the outside world. So, every castle had at least one gate. The gate allowed for commerce, it allowed farmers to get to their fields, and it allowed visitors. The gate was always a weak point, but it wasn’t the only weak point.

[3] http://www.cvedetails.com

[4] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report

[5] 1,378,509,261 records in 2016; 2622/minute; 35% are healthcare; 2622*.35 = 917.7 records/minute*$355/record = $325,783.5/minute

Much like the castles of old, your data center is protected at the perimeter with a wall (a firewall). However, you need to conduct commerce. Medieval castle developers punched large holes in the perimeter defense, building gateways for commerce. In the data center or cloud, the analogous structure would be a web gateway. However, just like some citizens could be witting or unwitting bad actors inside the castle, the same is true for the systems, laptops and users in your business.

How do you protect your data inside your castle when there are enemies both within and without? You need to encrypt it. However, the data in most data centers isn't even encrypted while it is at rest, on disk. In 2016, 96% of all data stolen wasn't encrypted.

Oracle Linux gives you what you need to protect your data. It starts with state-of-the-art PKCS#11v2.40 algorithms. You can then encrypt the data at rest with Ext4 built-in file system encryption or use EncryptFS. You should also encrypt the data in motion. Oracle Linux can automatically accelerate Java applications, Oracle Database, SSL/TLS and custom applications with built-in hardware crypto engines, and it integrates with KMIP-compliant key management servers, protecting your data at rest and in motion.

Additionally, Oracle Linux is in the process of completing FIPS 140-2 level 1 certification, which validates the algorithms it uses for accuracy. You can find out more about Oracle Linux FIPS 140-2 certification on our website and on the NIST Cryptographic Module Validation Program website.

Evaluate and Validate Your Security Posture

As clients move their sensitive information, data, and business operations to the cloud, the platform on which these critical applications run must be proven to be secure.

The Oracle Linux Security Assessment (OLSA) is a practical exercise focused on detecting areas of potential security vulnerabilities in your data center and identifying strategies to mitigate those potential vulnerabilities. The assessment focuses on the platform but also examines surrounding system components including storage, network, and applications. The assessment provides a view into some of your compute processes and policies, with the goal of promoting successful approaches to mitigate potential security risks.

Conclusion

The operating system you use can have a significant impact on your business. Oracle Linux provides unique, state of the art security technology that allows you to protect the three pillars of protection and stay ahead of cyberattacks. Oracle Secure Global Desktop helps you protect your people. Ksplice can automatically patch your platforms. Automatic cryptographic offload and FIPS certification assist you in protecting data with confidence.

Get more information about Oracle Linux Security and our Security Assessment Services or contact your Oracle Linux representative to see how Oracle Linux can help you protect your people, platforms and data.

VAST is an IT service company that helps businesses manage the cost and complexity of their on-premise, hybrid and multi-cloud environments. VAST services address complex cloud, infrastructure, information governance, data protection, security and business continuity challenges. VAST is a certified partner of Amazon Web Services, Azure, GCP, CloudHealth, VMware, Veritas, Oracle, Nutanix, and others. **VAST is 2018 Oracle Linux Partner of the Year.**

For more information and to purchase Oracle Linux or Oracle Linux Support, contact VAST at 800.432.VAST or email us at info@vastitservices.com.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

VAST
IT without Limits™