Pillars of Protection

A holistic view of enterprise security

July 27, 2023

Public

Purpose statement

This document defines the three things (people, platform, and data) you need to protect each layer of your environment and explains how you can build pillars of protection using the security advantages of Oracle Linux and Virtualization.

Disclaimer

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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 in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Introduction

At Oracle, the security of our customers' data is the top priority. That's why integrated security controls have been designed into each layer of the stack, from the applications down to the operating system, virtualization, and hardware components, including servers, host adapters, and storage. This means that Oracle Linux and Virtualization 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 foundation for your workloads.

Defending your business

Cyberattacks are on the rise, and 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 necessary, but they aren't enough. 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 to protect your data center and cloud instances from cyberattacks.

People

People are the Achilles' heel of cybersecurity. People have been, and continue to be, the single largest source of cybersecurity incidents. A recent study suggests that as much as 74% of security breaches involved a human element.[1] While some may be "bad actors," generally, incidents are either the result of simple mistakes that create exposure to a cyberattack or information leaks via social engineering. Training your people to handle sensitive data, systems, passwords, and account access is critical in cybersecurity.

However, training alone is not enough. You also need to protect your data and systems from the people element. 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 a username/password (i.e. knowledge-based authentication). Regardless of the second factor, whether it be a 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 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. For example, 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, due to mistakes or intentional action, and can prevent potential data corruption.

[1] Verizon 2023 Data Breach Investigations Report

Combining integrity management with remote audit logging helps prevent an attacker from hiding their activities by preventing them from removing audit log entries. Read the technical paper to learn how to use the Advanced Intrusion Detection Environment with Oracle Linux Automation Manager to install, configure, create baselines, and run detection reports.

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 some 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. Known vulnerabilities dating back to 2017 are still being exploited by attackers, according to a report by Tenable.[2] This trend 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 running?

   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. 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 caused issues with some enterprise software applications and the fix needed to be re-released.

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

   The exact revision of hardware may change during the hardware lifecycle. 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 hundreds or thousands of 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. Customers with an Oracle Linux Premier Support or an Oracle Cloud Infrastructure subscription can help increase the security, reliability, and availability of their Oracle Linux and Ubuntu systems by applying critical security patches to Linux kernels, without rebooting, using Oracle Ksplice. Moreover, Ksplice for Oracle Linux provides zero-downtime patching for critical user space libraries (`glibc` and `openssl`) and known exploit detection which automatically sends an alert if an attacker attempts to

[2] Tenable 2022 Threat Landscape Report – A guide for security professionals to navigate the modern attack surface

exploit selected patched vulnerabilities. In addition, Oracle Ksplice has been designed to interoperate with commonly used vulnerability scanners. These security scanners can recognize and incorporate patches applied through Ksplice, which helps to ensure more accurate and comprehensive vulnerability reporting for better compliance.

Ksplice Inspector is a free online tool that can show you a list of available patches that you can apply today with Ksplice without any downtime. Proactively identifying security vulnerabilities with Ksplice Inspector is an important step to help you assess the cybersecurity risks you are facing today.

If you use Oracle Linux Manager or Oracle OS Management Hub to manage your Oracle Linux instances in 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, Oracle Linux provides the Security Content Automation Protocol (SCAP) packages, 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 a prime 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 2022 alone, there were 25,227 newly published vulnerabilities. Of those, 3,266 (13%) of them had Common Vulnerability Scoring System (CVSS) score of 7.0 or higher.[3]

Whenever code is installed on a system, there is the potential for unknown vulnerabilities to be there waiting to be exploited. While ethical 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 Arm and x86 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 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 their access rights to the 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.

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

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. The average cost of a data breach is expected to reach $5 million in 2023[4].

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 insufficient to protect your data.

Using 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 to enter. The gate was always a weak point, but it wasn't the only weak point.

Just like medieval castles, your data center is protected at the perimeter with a wall (a firewall). However, openings were created in the castle walls as gateways to conduct commerce. Similarly, in a data center or cloud environment, a web gateway serves as the equivalent structure. However, just as there could be both intentional and unintentional threats within the castle, the same holds 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.

Oracle Linux enables you to protect your data. It starts with UEFI secure boot. You can then encrypt the data with cryptographic libraries included with Oracle Linux to protect data that is stored or that is being transmitted. 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.

The Federal Information Processing Standard (FIPS) 140 is a cryptographic standard developed by the National Institute of Standards and Technology (NIST) in the United States for the protection of sensitive but unclassified data. FIPS 140 specifies security requirements for cryptographic modules that encrypt and decrypt data, securely generate cryptographic keys, perform hashing, execute key agreement using industry standard protocols, and generate or verify digital signatures.

Oracle has performed FIPS 140-2 validations of cryptography included in Oracle Linux 7 and Oracle Linux 8 on x86-64 and aarch64 platforms. Oracle Linux 9 cryptographic module validation for FIPS 140-3 is in progress at the time of this writing. Visit Oracle Security Evaluations to learn more details about the Oracle products that have completed FIPS security certifications and those that are in progress.

[4] Acronis Cyber Protection Operation Center Report: Cyberthreats in the second half of 2022 – Data under attack

Security implementation

As customers move their sensitive information, data, and business operations to the cloud, the operating environment on which their critical applications run must be secured. These mission-critical systems and deployments depend fundamentally on the built-in security and reliability features of the Oracle Linux operating system.

When using Oracle Linux, Oracle recommends that you follow the fundamental security principles such as minimize and secure the software footprint, keep software up to date, restrict network access to critical services, control authentication mechanisms and enforce password restrictions, follow the principal of least privilege, monitor system activity, and keep up to date on the latest security information. These principles are guidelines that should inform your approach to handling security policies. Read the documentation Enhancing System Security to plan and manage your Oracle Linux system security.

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 safeguard the three pillars of protection and stay ahead of cyberattacks.

Get more information about Oracle Linux Security or contact an Oracle Linux representative to discuss Oracle Linux consulting services and see how Oracle Linux can help you protect your people, platforms, and data.

Resources

- oracle.com/linux
- oracle.com/virtualization
- Download Oracle Linux
- Try Oracle Cloud Free Tier
- Oracle Linux documentation
- Oracle Linux Support
- IDC paper: Enabling Modern Infrastructure Across On-Premises and Cloud

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle