ORACLE

Accelerating Zero Trust adoption with Oracle Linux

Technical Brief

January 2024, Version 1.0

Purpose statement

This document presents how the Oracle Linux operating environment can help expedite the adoption of Zero Trust security. In particular, this document describes Oracle Linux features that organizations can use to align with the pillars of the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model (ZTMM), a path for organizations to devise and implement Zero Trust strategies.

As advised by the CISA, even though the ZTMM is intended for federal agencies as required by the US President's Executive Order 14028 on Improving the Nation's Cybersecurity, every organization should review and consider the adoption of the approaches that it outlines.[1]

Disclaimer

[1] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

ORACLE

Table of contents

Introduction

What is Zero Trust?

Today's highly interconnected infrastructure can give malicious actors a larger attack surface, which can make enterprises more susceptible than ever before to the growing sophistication and frequency of cyberattacks. As a result, the traditional perimeter security model is simply no longer recommended as the only approach to defense.

Zero Trust is a strategic IT security approach focused on preventing threats not only from outside an organization but also from within. It emphasizes that every user, device, or workload connected to an organization's network, irrespective of its location, should never be trusted, always be regularly verified, and be granted least-privilege access to perform its job.

To support the transition to Zero Trust, the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model (ZTMM) presents five distinct foundational pillars—*Identity, Devices, Networks, Applications and Workloads, and Data*—where each ought to be integrated with *Visibility and Analytics, Automation and Orchestration, and Governance* capabilities.[2]

Why Oracle Linux? Because it's more than just an operating system

Oracle Linux is a highly secure and optimized operating environment for developing and deploying applications across distributed and multicloud environments. In addition to shipping an operating system (OS) with secure defaults, Oracle Linux provides virtualization, management, automation, and cloud native computing tools, all of which have been developed with a security-first approach. Oracle's own business operations, product development, and public cloud, Oracle Cloud Infrastructure (OCI), all run on Oracle Linux. Oracle offers the same Linux to its customers, including exhaustive testing, performance improvements, and reliability tunings carried out across a large footprint. This is a key reason why thousands of customers confidently deploy Oracle Linux in their business-critical environments.

Zero Trust security is a complete paradigm shift; therefore, it requires continuous effort and significant time investment to implement and mature. Oracle Linux delivers best-in-class solutions that can help businesses expedite their transition toward Zero Trust.

In the following subsections, Oracle Linux solutions have been detailed under a specific pillar of the ZTMM, however, they can be used to align with other pillars and integration capabilities of the model as per business needs. Note, it is the customer's responsibility to evaluate and implement a solution that meets its regulatory and compliance needs.

[2] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Pillar 1 – Identity

In pursuit of long-term growth, many government agencies and companies are digitizing processes in every aspect, from customer service to supply chain, and looking to run their workloads on-premises and in the cloud. In such borderless environments, over-ambitious granting of roles and responsibilities can lead to systems abuse. Therefore, it is important to help ensure and continuously verify that the proper entities access the correct resources for the right time and only for their intended purpose.

Authentication

Zero Trust enforces risk-based access, necessitating that strong authentication be implemented companywide. When it comes to system security, authentication is a method of identifying an entity attempting to connect to a system. Once a registered user provides their login credentials, the OS will only grant access after it has validated that an active account exists and the provided information matches data stored on the system.

Authentication is profile-based in Oracle Linux. A profile is a collection of predefined features that govern which service or mechanisms are to be used to authenticate system access. In Oracle Linux, multiple profiles are available and can be configured, each of which has been summarized with its service in Table 1.

AUTHENTICATION PROFILE	AUTHENTICATION SERVICE	DESCRIPTION
`sssd`	**System Security Services Daemon (SSSD)**	Using SSSD, a client system can access remote identity and authentication providers. There are many benefits of configuring and using this service, such as: • Single sign-on access; • Offline authentication; • Reduced system load. The `sssd` profile includes most authentication cases like Pluggable Authentication Modules (PAM) and Kerberos. It is used by default by Oracle Linux, therefore the SSSD service is automatically installed and enabled on a newly installed Oracle Linux system.
`winbind`	**Winbind**	Winbind is a client-side service that resolves user and group information on a Windows server. The `winbind` profile is to be used to enable Oracle Linux to understand and work with Windows users and groups.
`minimal`	**System files**	The `minimal` profile does not use a particular service, instead, it directly uses system files to perform system authentication for local users.

Table 1. Authentication profiles available in Oracle Linux.

System authentication in Oracle Linux is flexible and not confined just to the available profiles. Profiles can be reconfigured by revising their active features. This flexibility allows organizations to develop customized profiles and implement authentication that complies with their own requirements.

Multifactor authentication

While password-level authentication has been a standard authentication procedure for decades due to convenience, short and common passwords are easily susceptible to phishing and hacking. Integrating more restrictive password-less mechanisms such as key, certificate, or token-based authentication which are a subset of multifactor authentication (MFA), can further help secure an environment. MFA is a core tenet of Zero Trust, as it provides an extra layer of security by using more than one factor to verify a user's identity and ability to access a system.

In Oracle Linux, features associated with each authentication profile can be enabled to have the profile's service perform a specific method of authentication, such as fingerprint and smart card authentication. In fact, system administrators can eliminate password authentication. For instance, the `sssd` profile includes a feature that, when enabled, enforces that a system only employs smart card authentication for all users and disables any other forms, including a password. Furthermore, by shipping OpenSC, Oracle Linux supports PIV and CAC cards that are widely used by the US federal government and its contractors.

User and group administration

Individual management of user accounts and credentials can be a complicated, time-consuming, and repetitive task. Under a Zero Trust architecture, businesses should consolidate and manage accounts from a central location when delivering enterprise identity and access management services.

For complex environments with several hundred servers and thousands of active users, Oracle Linux is able to store and retrieve user and group information from a central server. This can be easily achieved by configuring authentication profiles to use a variety of alternate back-end directory services, such as LDAP, FreeIPA, and Active Directory, simplifying account management.

SELinux

For greater control over users, applications, files, and processes, in the Linux OS, Security-Enhanced Linux (SELinux) can be administered on Oracle Linux. SELinux is a set of kernel mods and user-space tools that supply finer granularity to access control and system-wide admin-defined policies. Unlike conventional Linux security, which is typically based on a Discretionary Access Control policy and provides limited defense from malware, SELinux implements the Mandatory Access Control (MAC) policy for increased mitigation of privilege escalation attacks. For example, during a security-relevant access operation, when a process attempts to open a file, SELinux will intercept it at the kernel level and barricade it if a MAC policy rule does not permit it to continue.

Pillar 2 – Devices

Linux systems are foundational to many large federal agencies and enterprises, as they power cloud infrastructure environments, application servers, and embedded systems, to name a few. Systems that have the latest OS protection and security compliance can avert government and citizen information from being compromised, increasing organizational resiliency to cybersecurity threats.

ZTMM's Devices pillar emphasizes that organizations should not only mitigate risk by tracking and managing systems and their associated vulnerabilities but also aim to do so through automated means. In addition, when migrating to a Zero Trust architecture, organizations should make use of cloud services to help keep systems compliant and strengthen security posture.

Management and monitoring of OS updates

The National Institute of Standards and Technology (NIST) remarks that although "business/mission owners may believe that patching negatively affects productivity, since it requires scheduled downtime for maintenance and introduces the risk of additional downtime if something goes wrong and disrupts operations […], patching should be considered a standard cost of doing business and should be rigorously followed and tracked."[3] With Oracle Linux, government agencies and businesses get the best of both worlds—patching with no downtime.

Oracle Ksplice zero-downtime patching

Oracle Linux offers an automated zero-downtime solution, Oracle Ksplice[4], which can apply non-disruptive security patches within seconds to the supported Linux kernels in Oracle Linux and Ubuntu systems running on-premises or in the cloud. This means that without rebooting systems or, more importantly, the business applications running on them, they can be kept up to date, increasing availability and reliability. Ksplice has already successfully deployed millions of patches to public and private organizations.

Ksplice for Oracle Linux provides zero-downtime patching for key user space libraries (`glibc` and `openssl`) and known exploit detection. When new Common Vulnerabilities and Exposures (CVEs) are discovered and patched with Ksplice, known exploit detection lays down tripwires for select patched vulnerabilities. If an attacker attempts to exploit them, Ksplice will log the breach and automatically send an alert to administrators, allowing businesses to stay ahead of potential security threats.

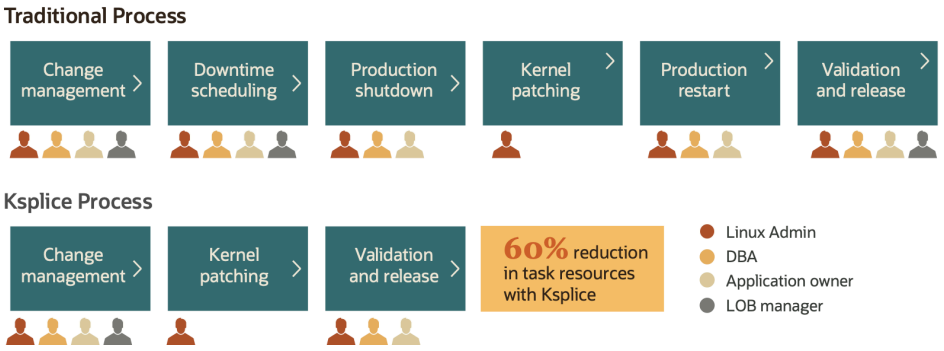

Figure 2. Linux patching process—before and after Ksplice.

"We were able to seamlessly switch from CentOS to Oracle Linux and improve our security by using Ksplice to patch our systems without needing to reboot. This has significantly reduced our time and cost for patching."

Tomasz Fryc
CTO
Alior Bank

[3] NIST Special Publication NIST SP 800-40r4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
[4] Available with an Oracle Linux Premier Support or OCI subscription. For further details, visit: https://www.oracle.com/linux/support/

Oracle Autonomous Linux

Based on Oracle Linux, Oracle Autonomous Linux is a service available in OCI that can perform automatic patch updates without human intervention, helping improve security without management complexity. With its self-patching capabilities, Autonomous Linux systems have Ksplice built in for zero-downtime patching of the kernel and key user spaces. Autonomous Linux also features monitoring and capturing of logs for critical events, such as kernel oops or kernel crashes, allowing root cause analysis to be performed on them. With the help of Oracle Autonomous Linux, organizations can reduce the pressure on overburdened IT staff while adhering to their Zero Trust strategy.

Oracle OS Management Hub

Regardless of where a baremetal server or virtual machine (VM) resides, ensuring that systems remain current with the latest security errata and consistent patch levels is crucial for cybersecurity protection.

Oracle OS Management Hub[5] is a managed service, hosted in OCI, that helps simplify the management and monitoring of updates and patches for Oracle Linux systems located in private data centers—all through a centralized management console or "hub."

Using OS Management Hub, organizations can immediately run update and patch jobs or automate patching policies and schedule them based on their best practices. If critical issues arise across systems, the service includes tools to track and quickly help resolve them. By providing a summary dashboard and real-time security compliance reports, OS Management Hub makes monitoring compliance patching status and the number of updates available for managed environments even easier. Additionally, for businesses looking to further increase application availability and uptime, OS Management Hub allows integration with powerful Oracle Linux features, such as Ksplice.

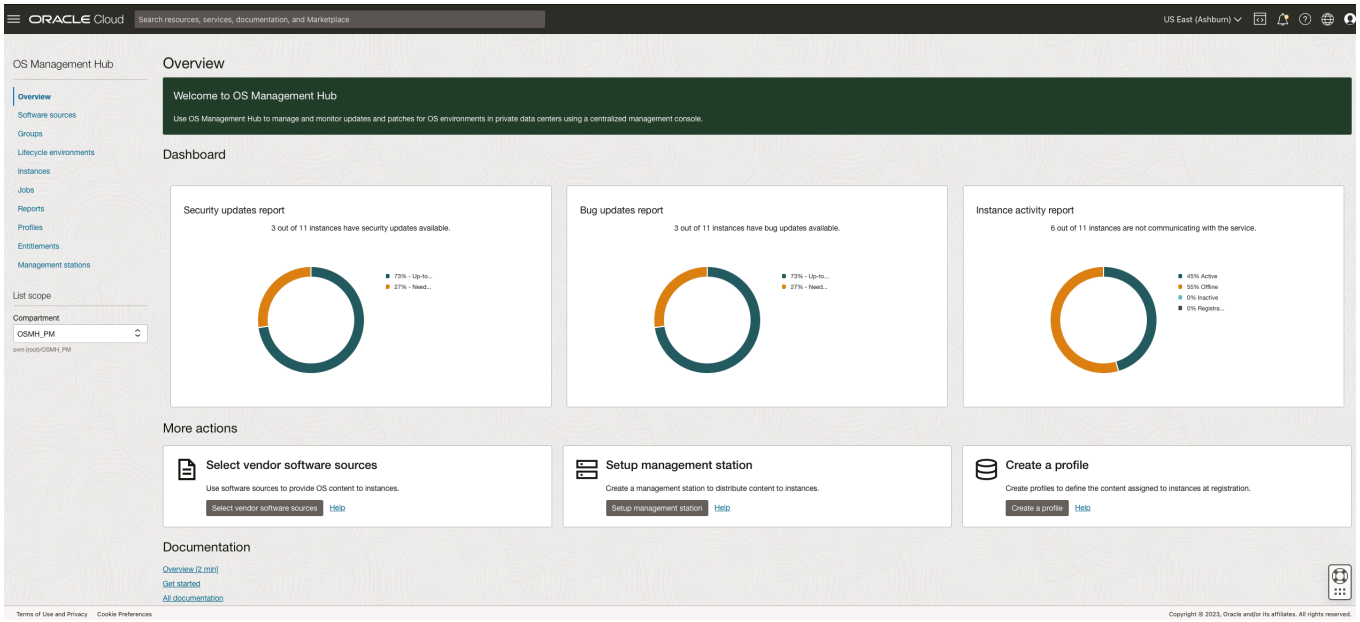

Figure 3. OS Management Hub Overview page.

A part of progressing to a Zero Trust model includes nearly eliminating manual changes or processes. In the case of OS patching throughout lifecycle environments, doing so can help avoid different versions of patches running across production systems and reduce the potential for human error. With OS Management Hub, organizations can maintain the consistency and integrity of patch lifecycle environments by grouping and managing systems together for standard tasks.

[5] Available with an Oracle Linux Support or OCI subscription. For further details, visit: https://www.oracle.com/linux/support/

Infrastructure management

As data centers grow in scale and complexity, deploying, provisioning, and maintaining a greater number of physical servers and virtual machines can become arduous and costly. The journey to Zero Trust can also give rise to additional costs, which means organizations should look to use cost-effective, yet highly performant solutions across their IT infrastructure, including systems management.

Oracle Linux Automation Manager/Engine

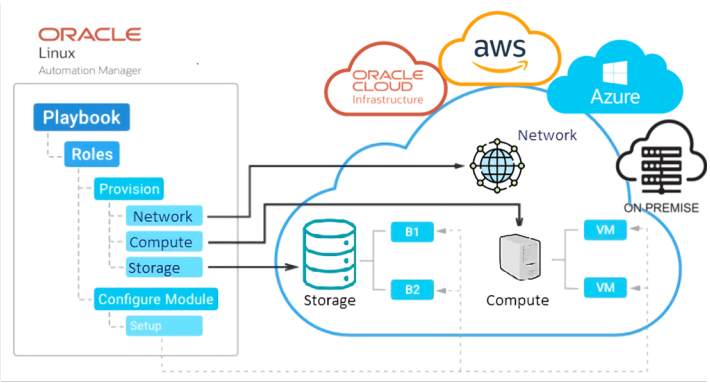

Figure 4. Infrastructure management with Oracle Linux Automation Manager.

With Oracle Linux Automation Manager/Engine, an infrastructure automation solution based on the open source AWX and Ansible projects and designed to be scalable and secure, organizations can configure and control their IT infrastructure on-premises and in the cloud, helping increase operational efficiency.

Oracle Linux Automation Manager delivers a task engine and centralized web-based UI for scheduling jobs and running Ansible playbook tasks, such as user and firewall management and SELinux configuration, on inventories the playbooks interact with. Several capabilities of Oracle Linux Automation Manager can help work toward Zero Trust goals, to name a few:

- ***Limited user access***—Through graphical inventory management, role-based access control (RBAC), and attribute-based access control (ABAC), the right devices and users are given the right access to resources across distributed and multicloud domains. Examples include preventing developers from accessing a production environment or restricting administrator credentials.
- ***Continuous remediation***—Identify and rapidly respond to configuration changes and manage configuration drift by accessing and reviewing generated log files. Execution of all activities can be evaluated by analyzing infrastructure events, monitoring for anomalies, and correlating them from one service to another.

Oracle Linux Manager

Another solution that helps automate the management of Oracle Linux systems is Oracle Linux Manager. With the tools that Oracle Linux Manager provides, the Oracle Linux software life cycle can be managed from initial installation, through software configuration, maintenance, upgrades, auditing, and eventual decommissioning. Oracle Linux Manager helps keep Oracle Linux systems up to date with stable software configurations and consistent patch levels, all of which are vital for user productivity.

Pillar 3 – Networks

As businesses move away from perimeter-based security approaches, hardening software, such as applications and databases, higher up in a technology stack is vital, however, doing so at a lower level is no less important. In addition to built-in facilities for network firewall control and access control security policies, Oracle Linux comprises solutions designed with a security-first architecture to help mitigate threats from the underlying infrastructure and enhance network security.

Oracle Linux virtualization solutions

Oracle Linux KVM

Kernel-based Virtual Machine (KVM) delivers a set of modules that permit the Oracle Linux kernel to be used as a hypervisor and therefore VMs, which facilitate strong isolation, to be run. By default, Oracle Linux KVM is built into Oracle's own Linux kernel developed for mission-critical performance and security optimizations, the Unbreakable Enterprise Kernel (UEK). Oracle Linux KVM includes support for Intel VT-x and VT-d hardware extensions along with the Secure Encrypted Virtualization for AMD-V enabled processors.

Patching of a hypervisor is non-trivial; through traditional approaches, it can be laborious to do since VMs and applications running on top must be interrupted for updates to be applied. For increased security and uptime, Oracle Linux KVM integrates with Ksplice for zero-downtime patching—on-premises or in the cloud.

For federal agencies and businesses planning to incorporate the benefits of the cloud in their Zero Trust strategy, Oracle Linux KVM delivers superior performance and security for cloud deployments. In fact, OCI uses Oracle Linux KVM by default. Workloads can move between different deployment models, for example, from on-premises to OCI, with the transition being virtually effortless. But that's not all. Oracle offers an Oracle Linux KVM image in OCI with two versions, one based on Oracle Linux and the other configured to run Oracle Autonomous Linux. Through such options, hosting of an Oracle Linux KVM-based environment is simplified with OCI services, like Block Volumes and VNICs, and features of Autonomous Linux can be extended to KVM deployments in OCI.

Oracle Linux Virtualization Manager

To configure, monitor, and manage an Oracle Linux KVM environment, including hosts, VMs, storage, networks, and users, data center administrators can deploy Oracle Linux Virtualization Manager, a server virtualization management platform built from the open source oVirt project. Oracle Linux Virtualization Manager offers an easy-to-use web interface for centralized management and a REST API to manage Oracle Linux KVM infrastructure. Moreover, it includes several automation options and management interfaces for monitoring virtualized system health status and comprehensive event tracking.

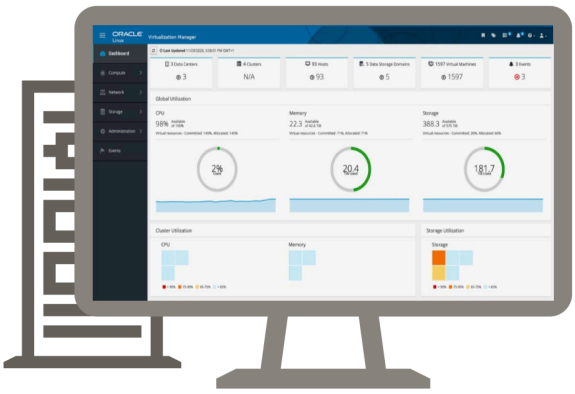

Figure 5. Oracle Linux Virtualization Manager Dashboard.

For enhanced security, Oracle Linux Virtualization Manager can be integrated with an external LDAP or Active Directory authentication system (also discussed earlier in the *Pillar 1-Identity* subsection).

Oracle Linux Virtualization Manager and Oracle Linux KVM are certified under the Common Criteria.

The Common Criteria (CC) is the international framework (ISO/IEC 15408) that defines a common approach for evaluating the security features and capabilities of IT products.

Together, Oracle Linux Virtualization Manager and Oracle Linux KVM include many security functions (which have been evaluated under the CC) that can pertain to network security. Some of these are listed in Table 2 below.[6]

SECURITY FUNCTION	DESCRIPTION
VM Hardware-based Isolation	There are isolation mechanisms present that constrain a Guest VM's direct access to physical devices.
VM Networking & Separation	Mechanisms that are used to transfer data between Guest VMs, including control of virtual networking components, can be controlled.
Virtual System Self Protection	Self-protection mechanisms have been implemented including execution environment mitigations, hardware-assists, hypercall controls, isolation from VMs, and controls for removable media.
Protected Communications	Integrity and confidentiality of communications are protected.
Secure Administration	Secure management of the security functions the solutions provide is available, including: • Administrator authentication with passwords • Configurable password policies • RBAC • Access banners • Management of critical security functions and data
Cryptographic Operations	A cryptographic module is implemented.

Table 2. Select security functions of Oracle Linux Virtualization Manager and Oracle Linux KVM.

For additional information on the CC certification of Oracle Linux Virtualization Manager and Oracle Linux KVM, see Oracle Linux KVM Common Criteria Certification.

The Oracle Linux STIG image

A Security Technical Implementation Guide (STIG) is written by the Defense Information Systems Agency (DISA) to provide guidance on configuring a system to meet cybersecurity requirements for deployment within the Defense Department's (DOD) IT network systems. DOD agencies or organizations that are a part of the DOD information networks (DODIN) are required to comply with STIGs.

Oracle offers an Oracle Linux STIG image, hardened to follow STIG guidelines and help automate compliance. An Oracle Linux STIG image instance can be deployed in OCI. The Oracle Linux STIG image's compliance is assessed with a scan against the target DISA STIG Security Content Automation Protocol (SCAP) Benchmark profile. If changes are made to an instance running an Oracle Linux STIG image, such as adding new configuration settings, its compliance can be affected. Using the OpenSCAP tool included with Oracle Linux and certified by the NIST, an instance can be rescanned for compliance and automated compliance testing can be configured.

[6] https://www.oracle.com/a/ocom/docs/kvm-security-target.pdf

Pillar 4 – Applications and Workloads

It is imperative that applications are delivered and managed in a secure manner. In a Zero Trust environment, organizations should strive to deploy infrastructure to a cloud environment with minimal manual intervention and implement best practices for DevSecOps and continuous integration/continuous deployment processes.

With the modernization of applications comes simpler application maintenance, faster time to market, and greater business velocity. Nonetheless, achieving such benefits does not come easily when faced with the complexity of selecting and integrating software to assemble a cloud native environment.

Oracle Cloud Native Environment

To embrace cloud native DevSecOps, businesses using Oracle Linux can take advantage of Oracle Cloud Native Environment to configure, deploy, update, and upgrade infrastructure for the rapid development and deployment of cloud native applications. Oracle Cloud Native Environment is based on open standards, specifications, and APIs defined by the Open Container Initiative and Cloud Native Computing Foundation (CNCF).

Oracle Cloud Native Environment delivers an integrated set of components—including CNCF-certified Kubernetes module, container runtimes, storage, networking, observability, and diagnostics—to help shift workloads to a cloud native architecture and exploit the economic advantages of open source and the cloud. Organizations can flatten the learning curve while adopting cloud native application development, decrease deployment errors and time, and most importantly, fuel rapid innovation.

The following exemplifies one of the many powerful features of Oracle Cloud Native Environment.

Managing the interaction and operation of services in a microservices architecture

Microservices are the core of cloud native application architecture. Though various components of microservices can affect the overall performance of every application, one of the more prominent ones is how they communicate with one another.

Oracle Cloud Native Environment supplies the open source Istio service mesh for simplified service-to-service communication and network operations between microservices in Kubernetes clusters, including service discovery, load balancing, security, recovery, telemetry, and policy enforcement capabilities. In addition, it can handle various aspects of microservice management, from identity and authentication to transport security. Oracle Cloud Native Environment tools like these enable teams to focus on value-added projects instead of programming such capabilities into application code, helping drive continuous, secure software delivery.

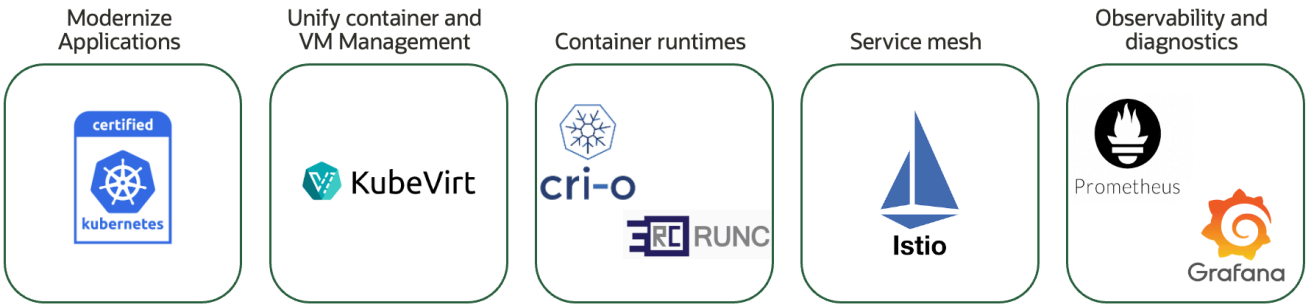

Figure 6. Select tools supplied by Oracle Cloud Native Environment.

Pillar 5 – Data

Selecting the right Linux distribution is an indispensable step to bolstering security in the face of hacktivism and ransomware attacks. Oracle Linux ships an enterprise-class OS engineered to provide data integrity and high performance for business-critical production environments. To help organizations proactively improve the security of the OS and safeguard data with security controls, Oracle Linux includes a comprehensive security stack comprising tools for certificate management, public key cryptography, and data encryption.

Certificate management and data encryption

Public key cryptography is an asymmetric encryption technique that secures data involved in communications across an unsecure public network. By using a private key and its public counterpart, it verifies the identity of an entity on the other end of a network connection. OpenSSL is a full-featured cryptographic software library that provides an open source implementation of the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) communication protocols and allows for core cryptographic functions.

Oracle Linux contains tools for OpenSSL that can be used to create Certificate Signing Requests, self-signed certificates, and personalized CA certificates. Because the `openssl` package is shipped with Oracle Linux, organizations can perform a wide variety of cryptography functions belonging to the OpenSSL library, such as encryption/decryption of files and testing of client-side and server-side TLS/SSL with HTTP and SMTP servers.

Data is vulnerable anywhere it resides; it can be intercepted during transmission over networks or stolen from storage devices and media. Consequently, corporate security policies and governmental regulations like HIPAA, GLBA, SOX, and PCI DSS, are progressively making data encryption mandatory. Oracle Linux includes cryptographic libraries that can be used by applications to deliver data encryption facilities and are designed to help prevent data sprawl and shield confidential data. In addition to using a robust password hashing algorithm (`SHA-512`), Oracle Linux provides several data protection strategies, including full disk, network traffic, and hardware-accelerated encryption.

To learn more about certificate management, data encryption, and additional Oracle Linux features to manage and implement best practices for system security, visit Managing Certificates and Public Key Infrastructure and Enhancing System Security.

Common Criteria Certified and FIPS 140-2 Compliant

Oracle Linux 8 and Oracle Linux 7 are CC certified; the certification was performed against the General Purpose Operating System Protection Profile.

Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that must be satisfied by a cryptographic module that is used within a security system to protect sensitive, but unclassified information. According to the NIST, products sold to US and Canadian government agencies are required to undergo the FIPS 140-2 validation to safeguard sensitive or designated information.[7]

Oracle Linux cryptographic modules are FIPS 140-2 validated for x86_64 and aarch64 platforms on Oracle Linux 8 and Oracle Linux 7.

Such rigorous independent third-party evaluations can help provide confidence in the design and security of Oracle Linux, as a variety of commercial, government, and military institutions all deploy Oracle Linux systems while constructing Zero Trust environments.

[7] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Conclusion

As architecture modernization escalates, leading to the decentralization of infrastructure, it creates new potential for security gaps. With the increase in cybercrime, guarding business assets behind firewalls, intrusion prevention systems, and network intrusion systems, does not suffice. Cybercriminals continue to learn how to breach the gaps. As a result, one of the greatest defenses to shield an organization's network is not to trust anything or anyone by default—Zero Trust.

Contrary to standard network security posture, with Zero Trust security no one is trusted by default from inside or outside the network. By requiring continual verification from every user attempting to access resources, organizations can regulate access to systems, networks, and data without giving up control. But, it is important to keep in mind that, Zero Trust security is not a single product or service that can be enabled with a push of a button. Rather, it is a security strategy that may demand cultural and philosophical adjustments within organizations.

To better align with Zero Trust principles, specifically, the pillars of the ZTMM discussed within the scope of this paper, organizations need IT solutions that enable greater control over user access and as a result, reduce risks of internal and external breaches.

Security is at the core of Oracle Linux and not bolted on as an afterthought. With security-first design principles deeply integrated into Oracle Linux, such as granular separation of duties, least privilege access, and encryption, organizations can deploy, optimize, and manage applications designed to minimize risks from constant threats. Whether it be zero-downtime patching or isolated network virtualization, Oracle Linux delivers solutions engineered to help foster automated security for threat mitigation and protection. Oracle Linux can assist government agencies and businesses in meeting their stringent compliance and privacy regulations with reduced complexity.

Oracle Linux is not just another Linux distribution—it is tuned for compute-intensive and data-heavy workloads—deployed on-premises, in the cloud, or at the edge. Whatever the scale of operations, Oracle Linux can be the catalyst to help accelerate your path to an effective Zero Trust security model.

For more information

WEB RESOURCES	WEB URL
Oracle Linux	http://www.oracle.com/linux
Download Oracle Linux	https://yum.oracle.com/oracle-linux-downloads.html
Oracle Linux 8: Enhancing System Security	https://docs.oracle.com/en/operating-systems/oracle-linux/8/security/
Linux Security	https://linux.oracle.com/security/
Zero Trust Security Model	https://www.oracle.com/security/what-is-zero-trust/
Oracle Cloud Infrastructure	https://www.oracle.com/cloud/

TECHNICAL PAPERS	WEB URL
How to Raise the Bar for Cybersecurity by Securing the OS	https://www.oracle.com/linux/os-security/

Staying ahead of cyberthreats: Protecting Your Linux systems with Oracle Ksplice	https://www.oracle.com/a/ocom/docs/dc/lpd400081532-whitepaper-ksplice.pdf
Eliminate Trade Offs Between Security and Availability	https://www.oracle.com/a/ocom/docs/oracle-ksplice-flier.pdf
Using Advanced Intrusion Detection Environment with Oracle Linux Automation Manager	https://www.oracle.com/a/ocom/docs/linux/using-advanced-intrusion-detection-environment.pdf
Improving Federal Security with Automated Patching: Market Trends Report	https://www.oracle.com/a/ocom/docs/dc/improving-federal-security-with-automated-patching.pdf
Oracle Linux completes new Common Criteria certifications	https://blogs.oracle.com/linux/post/oracle-linux-completes-new-common-criteria-certifications
Ten Simple Steps to Enabling FIPS 140-2 Mode in Oracle Linux	https://www.oracle.com/a/ocom/docs/linux/ten-simple-steps-to-enabling-fips-140-2-mode-in-oracle-linux.pdf

DATA SHEETS	WEB URL
Oracle Linux	https://www.oracle.com/a/ocom/docs/linux/oracle-linux-ds.pdf
Oracle Linux for Arm	https://www.oracle.com/a/ocom/docs/linux/oracle-linux-for-arm.pdf
Oracle Linux for Oracle Cloud Infrastructure	https://www.oracle.com/a/ocom/docs/linux-for-cloud-infrastructure-4024517.pdf
Protecting your Linux Systems with Oracle Ksplice Zero-Downtime Updates	https://www.oracle.com/a/ocom/docs/ksplice-datasheet-487388.pdf

Connect with us

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

blogs.oracle.com/linux facebook.com/oraclelinux twitter.com/oraclelinux