Frequently Asked Questions
Oracle Supply Chain Security and Assurance Practices

Introduction

Oracle customers worldwide are relying on Oracle products and services to help protect their computing environments and data in the cloud and on-premises. Oracle is a global company that takes great care in the development, engineering, and distribution of its products. The purpose of this document is to provide you with a brief overview of Oracle's supply chain security and assurance practices.

Does Oracle have formal policies that apply to the safety of its supply chain?

Oracle has formal policies that apply to the safety of its supply chain. These policies apply to how Oracle selects third-party hardware and software that may be embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies governing the development, testing, maintenance, and distribution of Oracle software and hardware that aim to address the risks associated with the malicious alteration of these products before purchase and installation by customers.

Oracle is a certified partner in the Customs-Trade Partnership Against Terrorism (C-TPAT) program. By participating in this program, Oracle is helping to secure our borders and to enable the free flow of international trade. Currently, the CTPAT certification is mutually recognized in Canada, New Zealand, Jordan, Japan, South Korea, the European Union and Taiwan.

Does Oracle have formal policies and practices designed to prevent malicious or insecure code from being introduced in the Oracle code base?

Encompassing every phase of the product lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. To develop Oracle products with consistently high security assurance and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards. Oracle Software Security Assurance provides for extensive security testing, including both functional and non-functional activities, for verification of products' features and quality.

The use of third-party and open source software components in Oracle product distributions is also controlled to help prevent the use of components with known and exploitable security weaknesses. External software code used to provide important security functions (e.g., encryption) is submitted to additional scrutiny, and its use requires approval from Oracle's security oversight organizations.

Because the Oracle Cloud largely relies on Oracle products, the Oracle Cloud also benefits from Oracle Software Security Assurance activities. Oracle-developed code used solely in the cloud (i.e., code that is not used in on-premises product distributions) is also subject to Oracle Software Security Assurance.

Oracle also maintains strong controls over its source code to help prevent the introduction of potentially malicious or accidental alteration source code. Oracle's source code protection policies provide for limits on access to source code ("need to know" principle), requirements for independent code review, and periodic auditing of our source code repositories.

ORACLE

Does Oracle have formal policies and practices designed to prevent malicious or insecure code from being introduced in Oracle's hardware products?

Most hardware products have software components embedded into them (e.g., firmware). Oracle Software Security Assurance policies and practices extend to the development of Oracle code used on Oracle hardware systems.

When software updates are performed against hardware used in the Oracle Cloud, the cloud operation teams deliver software images that were previously used and tested in a test environment that closely reflects the production environment and is physically separated from the Oracle cloud production environment. The deployment of these images from test to production is performed through a controlled private network.

Does Oracle have formal policies and practices designed to prevent malicious code from being used in the Oracle Cloud?

The Oracle Cloud benefits from Oracle Software Security Assurance activities because the Oracle Cloud largely relies on Oracle products. Oracle Software Security Assurance policies and standards also apply to Oracle-developed code used solely in the cloud (i.e., code that is not used in on-premises product distributions).

Oracle maintains strong controls over its source code to prevent potentially malicious or accidental corruption of source code. Oracle's source code protection policies provide for limits on access to source code by applying the "need to know" principle, requirements for independent code review, and periodic auditing of our source code repositories.

The use of third-party and open source software components in the Oracle Cloud is also controlled in order to help prevent the use of components with known and exploitable security weaknesses. External software code used to provide important security functions (e.g., encryption) are submitted to additional scrutiny, and their use requires approval from Oracle's security oversight organizations.

Do Oracle supply chain security and assurance policies map to internationally-recognized standards?

Oracle is a certified partner in the Customs-Trade Partnership Against Terrorism (C-TPAT) program. By participating in this program, Oracle is helping to secure our nation's borders and enable the free flow of international trade. As a C-TPAT partner, we continue to maintain security measures, based upon risk analysis consistent with C-TPAT security criteria, in a documented and verifiable format throughout our international supply chains.

Currently, the CTPAT certification is mutually recognized in Canada, New Zealand, Jordan, Japan, South Korea, the European Union and Taiwan.

In addition, Oracle participates in two internationally recognized security evaluation criteria:

1. Common Criteria is an international framework (ISO/IEC 15408) which defines a common approach for evaluating security features and capabilities of Information Technology security products, and
2. The FIPS 140-2 program is jointly administered by the US and Canada.

Security evaluation is a process by which independent but accredited organizations provide assurance in the security of IT products and systems to commercial, government, and military institutions. Such evaluations, and the criteria upon which they are based, help to establish an acceptable level of confidence for IT purchasers and vendors alike.

Can Oracle attest that its software is solely developed in the United States?

Oracle is a global company and as such has employees all over the world serving in various capacities, including development and support. Oracle's ability to attract and retain talent all over the world directly benefits its customers. For example, Oracle World Wide Support uses a "follow the sun" model to enable high priority Service Requests (SRs) be worked on continuously, rather than "9 to 5, in one country only." Access to global talent, including global development resources, enables quicker resolutions to customer issues at a lower price.

Oracle products often include third party software (in some cases, open source software) which may have been developed in whole or part outside of the United States. This enables the company to bring innovative products and services to market swiftly, and to provide broad compatibility across various IT technologies and vendors.

While Oracle has formal processes to "vet" third-party libraries, Oracle cannot ensure that all third-party code is "developed in the USA." However, our secure development requirements apply the same high standards across all development, including on premises products, cloud services, and other programs delivered by World Wide Support, regardless of where these products and services are geographically developed.

Does Oracle manufacture some of its hardware products outside of the United States?

In addition to a manufacturing plant located in the United States, Oracle currently employs hardware manufacturing plants in China, Mexico, Thailand, and Laos.

How is source code and sensitive engineering information secured?

Oracle maintains strong controls over its source code. Oracle's source code protection policies provide for limits on access to source code by applying the "need to know" principle, requirements for independent code review, and periodic auditing of our source code repositories.

Oracle maintains strong controls over the technical description of vulnerabilities in Oracle code. Oracle's Security Vulnerability Information Protection Policy defines the classification and handling of information related to product security vulnerabilities. All security bugs are recorded into a corporate database, and access to this database is tightly controlled.

Are mechanisms in place to control the flow of sensitive development and design information across national boundaries?

As Oracle is a global corporation with employees serving in multiple capacities around the globe, the company protects its information on a "need to know" basis and in compliance with applicable laws rather than based on national boundaries.

Oracle's Information Protection Policy governs data classification and access of sensitive information, including source code, across Oracle and its subsidiaries. Oracle employs restrictions on access to sensitive information, which are based on business needs (e.g., those who do not have a business need to access source code cannot access it, and within source code systems, access is limited so developers do not get access to all code). Oracle has additional information protection requirements based on applicable laws (e.g., limitations on access to encryption technologies due to U.S. export restrictions).

Does Oracle have policies to prevent the use of counterfeit hardware?

All hardware purchases are routed through standard Oracle hardware supply chain processes. These processes are designed to vet Oracle's suppliers and prevent the acquisition of counterfeit products, and source from trusted vendors only.

How does Oracle procure hardware for the Oracle Cloud systems?

The Oracle Cloud largely relies on Oracle engineered systems. In addition, all internal hardware purchases are routed through standard Oracle hardware supply chain processes Hardware products and their related embedded software (such as operating systems) are formally evaluated by Oracle staff prior to their acquisition for fitness of purpose (e.g., scalability) as well as inherent security. The security assurance practices of the vendor are also formally evaluated (e.g., to review the vendor's security fixing policies).

What security testing and vetting is performed against critical non-Oracle components of the Oracle Cloud architecture (e.g., non-Oracle firewalls, network devices, etc.)?

Prior to their selection, non-Oracle components that are intended to be part of the Oracle Cloud architecture are formally evaluated by Oracle for fitness of purpose (e.g., scalability) as well as for security. The security assurance practices of the vendor are also evaluated (e.g., to review the vendor's security fixing policies).

How does Oracle procure hardware for its corporate and development systems?

All internal hardware purchases are routed through standard Oracle hardware supply chain processes. Hardware products and their related embedded software (such as operating systems) are evaluated by Oracle staff prior to their acquisition for fitness of purpose (e.g., scalability) as well as security. The security assurance practices of the vendor are also evaluated (e.g., to review the vendor's policies and process for addressing security issues).

How does Oracle report its use of third-party components in Oracle software and hardware product distributions?

Oracle provides selected information about its use of third party components in the product documentation (e.g., the terms of some third-party licenses requires disclosure of the use of these components). Typically, these disclosures will not include specific versions of the libraries in use because those versions can and likely will change during the life of the product.

Oracle does not currently provide a bill of materials (BoM) for its products. The reasons for this are many, among them the fact that in most cases customers cannot “swap out” a version of an embedded library for a newer version.

What mechanisms are in place to prevent the malicious alteration of Oracle’s hardware systems when they are shipped across national boundaries?

Oracle and its logistics providers maintain custody and control of the hardware from the pickup at the point of origin to the fulfillment of the applicable Incoterm. In most cases, Oracle operates on a delivered model meaning that Oracle has control until customer signature (DDP) or delivery to a designated airport (DAP). Each leg of the delivery process is documented in the provider's system and freight is checked at each transfer point for damage or tampering.

Exceptions are noted on paperwork and/or in the lead logistics provider’s system. Every DDP delivery is required to have a customer signature after inspection for damage or tampering (tape or bands removed). DAP orders are deemed to be completed when the aircraft arrives where Oracle has received a “confirmed on board” (COB) notice from the airline.

What process does Oracle follow to deliver software products for on premises and in the Oracle Cloud?

Oracle’s eDelivery site is used for the distribution of most Oracle software. The eDelivery site supplies a cryptographic hash for software downloadable from eDelivery. Additionally, Oracle cryptographically signs all Oracle operating system software delivered through online repositories so that customers can confirm that this software has not been maliciously tampered with during or after download.

Oracle Corporation, World Headquarters **Worldwide Inquiries**

500 Oracle Parkway Phone: +1.650.506.7000

Redwood Shores, CA 94065, USA Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/blogs

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services