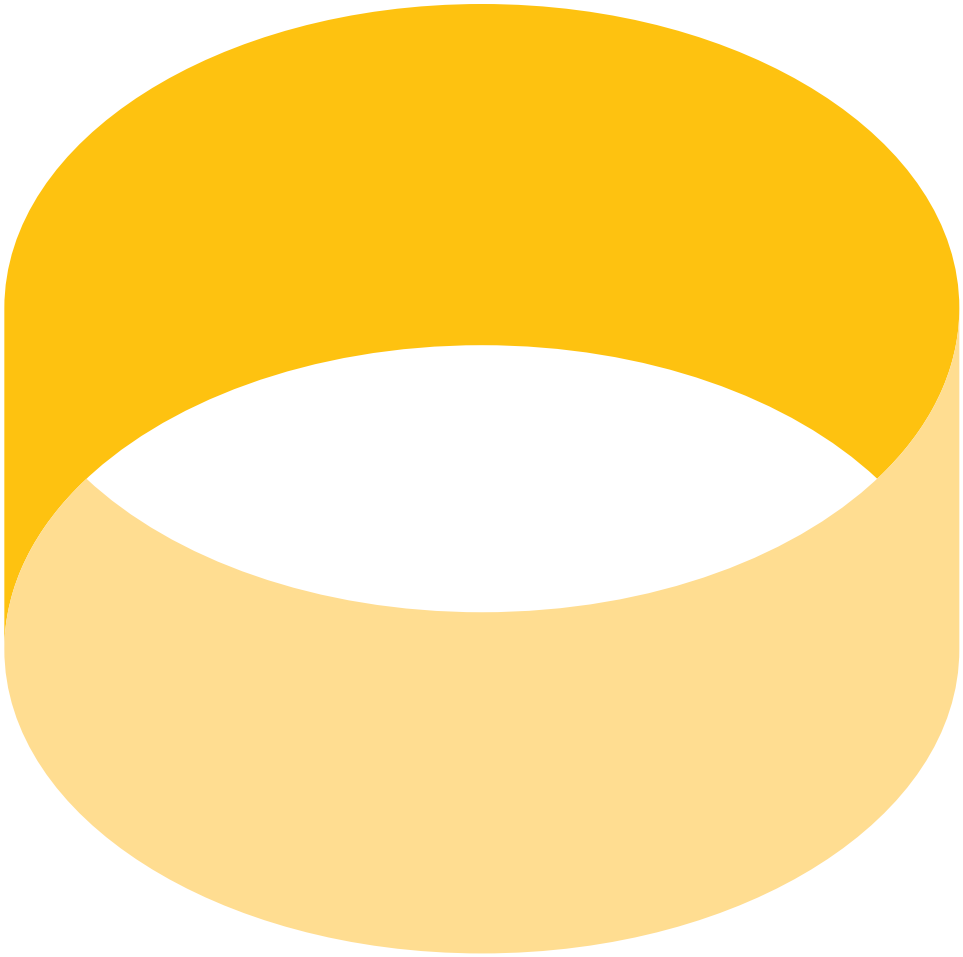

Symantec Enables Security in the Oracle Cloud

Security and compliance for your Oracle Cloud Infrastructure as a Service environments

WHITE PAPER

Symantec

Overview

This document surveys the Symantec™ products that enforce and manage security and compliance for the applications and data in your Oracle Cloud Compute and Bare Metal instances.

Oracle Cloud Infrastructure as a Service customers share security responsibility with Oracle. Per the Oracle Cloud Shared Responsibility Model, Oracle manages cloud infrastructure security; that is, Oracle protects the global infrastructure and its platform services. But Oracle Cloud Infrastructure as a Service customers are responsible for the security around, and the applications they've deployed in, the Oracle Cloud.

Specifically, Oracle Cloud customers must provide the following to secure their Oracle Compute and Bare Metal instances:

- Identity and access management
- Antimalware protection
- Threat protection
- Endpoint protection
- Patching and hardening
- Vulnerability scanning
- Security configuration management
- Compliance assessments
- Security monitoring
- Log analysis

Reference Architecture for Security Deployment

Oracle Cloud Infrastructure as a Service capabilities—addressing computing, network, storage, and other areas—can run any workload in the cloud. Oracle Bare Metal Cloud Services combine the elasticity and utility of a public cloud with the granular control, security, and predictability of on-premises infrastructure. The result: high performance, high availability, and cost-effective infrastructure services.

Oracle provides several options for connecting your corporate network to the Oracle Cloud network, and for securing your Oracle Cloud Compute and Bare Metal instances. Symantec supports the two most common security deployment models:

A. Management Server and Console Deployed On-Premises
B. Management Server and Console Deployed in the Oracle Cloud Infrastructure

A. Management Server and Console Deployed On-Premises

In this model, you deploy the Symantec security management console on-premises and deploy the agents in the Oracle Cloud. Use the console to manage your Oracle Cloud assets alone or in combination with on-premises physical and virtual assets plus your Oracle Cloud instances.

The way it works: You establish a secure connection to your Oracle Cloud infrastructure using an Oracle Cloud connectivity option—such as VPN, Virtual Cloud Network, or Network Cloud Service FastConnect—and configure your on-premises Symantec server to deploy and manage the agents that secure your Oracle Cloud environments.

B. Management Server and Console Deployed in the Oracle Cloud Infrastructure

In this model, you deploy the Symantec console in the Oracle Cloud environment, enabling and managing security for Oracle Cloud instances only. This is a common deployment scenario for organizations that separate their Oracle Cloud environments from their on-premises infrastructure.

Security and Compliance for Oracle Cloud Deployments

The following optimized Symantec security products are available to secure your content and applications in Oracle Cloud Compute and Bare Metal instances.

Symantec Threat Protection for Oracle Cloud Infrastructure as a Service

Symantec threat protection for Oracle Cloud instances comprises signature and heuristic-based malware detection, policy-based protection, and more, and can be tailored to specific Oracle Cloud workloads. In addition, you must maintain a sustainable vulnerability management program that satisfies industry and regulatory compliance mandates. For example, PCI-DSS 3.1 Requirement #5 states that covered organizations must: "Protect all Systems against malware and regularly update antivirus software or programs."

Symantec meets Oracle Cloud security objectives and compliance obligations for several use cases, including:

Use Case 1: Antimalware protection for Oracle Cloud instances. Deploy Symantec Endpoint Protection clients in the Oracle Cloud, then manage these clients using the on-premises console. See the "Reference Architecture" section above for additional guidance.

Use Case 2: Security and compliance monitoring and hardening of Linux and Windows cloud workloads on Oracle Cloud. Symantec Data Center Security: Server Advanced

- Locks down configuration settings, file systems, and use of removable media with application and device control.
- Blocks zero-day exploits with application whitelisting, granular intrusion prevention, and real-time file integrity monitoring.
- Secures OpenStack deployments with full hardening of Keystone identity service modules.
- Protects end-of-life Windows Server 2003 systems and other legacy platforms.

Choose on-premises or cloud deployment per your operational needs and security compliance objectives.

Use Case 3: Protection for content in SaaS applications hosted on the Oracle Cloud. Deploy Symantec Protection Engine to scan, detect, and protect data transmitted to/from hosted SaaS applications.

Symantec Threat Protection for Oracle Cloud End Users

Get complete endpoint protection for users accessing the Oracle Cloud platform—for example, as part of a lift-and-shift replatform of on-premises infrastructure—and manage all of this infrastructure with resources deployed in the Oracle Cloud platform.

Symantec Endpoint Protection provides a layered approach to protecting Oracle Cloud endpoints. It offers antivirus capabilities and detects and blocks unknown malware with reputation-based analysis and real-time behavioral monitoring that applies machine-learning heuristics. It also provides policy lockdown features, such as application control, for your Oracle Cloud instances. Drawing on the world's largest civilian threat intelligence network, Symantec Endpoint Protection effectively protects against targeted attacks and advanced threats, and facilitates more accurate detection without slowing down Oracle Cloud performance.

Symantec Information Protection for the Oracle Cloud

Data protection—your ability to discover, identify, and ensure secure access to sensitive data—is a critical component of your organization's security.

Symantec Data Loss Prevention, now integrated with full cloud access security broker (CASB) capabilities from Symantec CloudSOC, enables you to mitigate risk exposure to data breaches when deploying mission-critical workloads on the Oracle Cloud. Use Symantec DLP to discover confidential data on the Oracle Cloud and enforce policy-based usage control.

Symantec DLP gives you deep content inspection and sophisticated DLP policy and incident management for relevant Oracle Cloud workloads. For example: You can prevent emails with confidential data from being sent through Oracle Cloud-hosted instances of Microsoft Exchange Server, and extend existing data loss prevention policies from your on-premises Symantec DLP deployments to your content in the Oracle Cloud.

Symantec DLP for Oracle Cloud enables you to:

- Extend your DLP coverage and get direct visibility of content in more than 60 cloud apps, including Microsoft Office 365, Box, Dropbox, Google Apps, and Salesforce.
- Put to use full CASB capabilities so you can continuously monitor content additions, changes, and access rights in cloud applications.
- Take advantage of existing DLP policies and workflows for cloud applications so you don't have to rewrite your finely-tuned rule sets.

Symantec Security and Compliance Assessment for the Oracle Cloud

Oracle Cloud Infrastructure as a Service customers also share responsibility for compliance with Oracle.

Symantec Control Compliance Suite provides enterprise-grade asset discovery and security configuration assessment capabilities for your Oracle Cloud instances. It delivers asset auto discovery; automates security assessments across procedural, technical, and third-party controls; and calculates and aggregates risk scores according to business-defined thresholds. Use this information for both operational and mandate-based reporting, as well as to prioritize remediation and risk reduction in the data center.

Symantec Identity and Access Management for the Oracle Cloud

Identity management is the foundation of Oracle Cloud security—whether to enable Single Sign On (SSO) or to provide role-based access to Oracle Cloud Services.

Symantec VIP Access Manager integrates SSO with strong authentication, access control, and user management, giving users and administrators control, convenience, and compliance capabilities for public and private cloud-based applications. It uses identity and/or context-based access control across multiple cloud applications, solving cloud security problems without impacting user productivity. In the cloud, where a traditional enterprise perimeter doesn't exist, this solution fills the gap. Available on-premises or as a hosted service for the Oracle Cloud.

Symantec Delivers Security Products Optimized for the Oracle Cloud

Symantec is the global leader in cyber security. Our Integrated Cyber Defense Platform helps 15,000 enterprises defend against sophisticated attacks, and our digital safety products protect 50 million consumers and their families. Our advanced technology portfolio is powered by the world's largest civilian threat intelligence network, enabling us to see and protect against the most advanced threats.

What does this mean for Oracle Cloud customers?

Cyber Security in Four Key Areas

We are uniquely suited to integrate security products, services, and threat intelligence on the Oracle Cloud across four key areas:

1. Access Governance
2. Advanced Threat Protection
3. Information Security
4. Workload Protection

Access Governance

By authenticating users, enforcing access policy, and providing compliance logging and reporting across the endpoint, network, web and public cloud, we combine access governance with leading information security and threat protection. Oracle Cloud customers benefit from:

- Complete control over access to critical resources
- Assurance that only authorized users can access networks and applications
- Policy enforcement controlling access across all on-premises and cloud environments
- A single sign-on (SSO) for all cloud applications
- A network-based control point for managing access to cloud, web, and Shadow IT applications

Advanced Threat Protection

We detect and block advanced threats targeting customer data and applications, wherever they reside, by combining multilayer inspection and threat detection techniques—including AV signatures, advanced machine learning, artificial intelligence, behavioral analysis, sandboxing, memory protection, and more. Oracle Cloud customers benefit from

- Multiple policy enforcement points, including endpoint, network, and cloud
- The industry's largest set of telemetry data and the greatest number of correlated threat vectors
- Protection for all Symantec-secured devices and infrastructure

Information Security

We enable customers to monitor, protect, and control access to data across managed (corporate devices, network, and email) and unmanaged (cloud apps and mobile devices) environments. Data loss prevention (DLP), encryption (endpoint encryption, tokenization), and identity technologies are integrated to protect information in cloud applications, for mobile users and remote offices, and through email. These protections fuse with a full suite of on-premises security products. Oracle Cloud customers benefit from the ability to

- Implement standards (PCI, GDPR, etc.) compliance programs
- Protect intellectual property
- Apply a single set of policies and controls from on-premises to cloud
- Eliminate blind spots by extending DLP policies to identify sensitive data
- Extend policies and enforcement to cloud applications and services
- Enable role-based access to sensitive data via myriad devices
- Reduce costs for protecting sensitive data

Workload Protection

We provide visibility, protection, and real-time monitoring of critical workloads wherever they are—across public and private clouds, and traditional on-premises data centers. Whether customers are 'all in' with the public cloud, or prefer a hybrid approach, we provide advanced protections and continuous, automated compliance and risk assessment of mission-critical applications and resources. Oracle Cloud customers benefit from:

- Complete workload protection, monitoring, and micro-segmentation across clouds and on-premises data centers
- Protection against OWASP Top 10 threats and advanced threats
- Accelerated application performance
- Discovery and mapping of all assets and networks, along with role-based and operational mandate-based reporting on security configurations

Security Powered by Unparalleled Global Intelligence

Our Global Intelligence Network (GIN), the foundation for our Integrated Cyber Defense Platform, fuels the products and services across the Symantec portfolio. Our GIN enables all our products to share threat intelligence and improve security outcomes for customers across enterprises—from endpoints to servers, and at the network traffic level—and around the globe. We automatically update our intelligence on millions of malicious files and URL threat indicators every day, providing the broadest and deepest threat intelligence in the industry.

This level of visibility across endpoint, email, and web traffic enables us to discover and block targeted attacks that would otherwise be undetectable from any single control point.

More Information

Try It Now for FREE

Try the world's most complete endpoint protection by downloading a free 60-day trial today.

Read third-party reviews and find out why Gartner ranks Symantec as a leader in the Endpoint Protection Platform Magic Quadrant: https://www.symantec.com/products/performance-center

Visit Our Website

Symantec home page: enterprise.symantec.com
Symantec Endpoint Protection: go.symantec.com/sep

Speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745-6054

Speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website: http://www.symantec.com/contact-us

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_WP_Enables_Security_Oracle_Cloud_EN_v1a