Oracle Cloud Infrastructure Security Reference Architecture with Fortinet Security
Executive Summary
Oracle Cloud Infrastructure (OCI) provides a platform that enables developers, IT professionals, and business leaders to develop, extend, connect, and deploy cloud applications, share data, and gain insights across applications and devices. It offers a broad collection of cloud services from a single solution, delivered from the OCI bare metal stack to the OCI Classic public cloud. These services provide basic security controls for customer applications. However, business-critical applications and data stored across multiple clouds introduce new security challenges that require additional protection. The Fortinet Security Fabric provides advanced security that enables OCI to protect workloads and applications from threats to both on-premises and cloud environments.

OCI for Business Transformation
Oracle helps organizations solve their biggest challenges, from processing financial transactions to improving customer experiences and understanding insights from data. An organization’s most valuable assets—applications and databases—can be managed on OCI. To leverage the advantages derived from modern cloud technologies, customers are moving more of their mission-critical workloads and applications to the cloud.

Oracle set an ambitious goal in building its second-generation cloud infrastructure: to create an infrastructure that matches and surpasses the performance, control, and governance of enterprise data centers, while delivering the scale, elasticity, and cost savings of public clouds. The result: OCI, built from the ground up to be an enterprise cloud, equally capable of running traditional multitiered enterprise applications, high-performance workloads, and modern serverless and container-based architectures.

Fortinet Delivers Enterprise-class Security for OCI
Fortinet provides industry-leading security for wherever an organization’s data resides, from on-premises to the public and private cloud. Fortinet purpose-built cloud security solutions integrate directly into the OCI environment, abstracting cloud-specific intricacies and leveraging cloud automation services, delivering the broadest set of security use cases available for OCI.

Fortinet provides enterprise-class security to enable digital transformation (DX) and safely deploy Oracle workloads. In addition, Fortinet security solutions are backed by our industry-leading security research team, FortiGuard Labs, and supported with leading-edge artificial intelligence (AI) and machine learning (ML) technologies.

Cloud Security Is Essential to the Enterprise
As business and technology leaders embark on DX initiatives, they know the threat landscape is changing daily, hybrid solutions are becoming an essential part of their reality, and cloud security is developing into an even higher priority.

The number of cloud workloads is growing at a near exponential rate, expanding the attack surface and creating new challenges for security professionals seeking to ensure the security and compliance of their applications and digital infrastructure. At the same time, cyber criminals are smarter and more dangerous, using scripted attacks that improve their speed and scale. Plus, the increase of heterogeneous cloud environments has expanded the threat landscape. Rapid enterprise adoption of the hybrid cloud model is driving the evolution of cloud security, making agile cloud security a necessity.
Cloud security now requires the ability to automatically detect devices across clouds, apply segmentation within and across cloud environments, and provide centralized security analytics and management across computing platforms. OCI provides best-in-class security for its own infrastructure. However, no cloud platform provider can ensure that organizations apply strong and consistent security policies across clouds, nor can they ensure the security of an organization’s unique applications.

**Expanded threat landscape**

The threat landscape is growing with the proliferation of network devices, Internet-of-Things (IoT) devices, mobile devices, ecommerce, web applications, and vendor portals. Meanwhile, cybersecurity threats involving malware, cryptocurrency, and botnet activity are extremely sophisticated and continue to evolve. Cyber criminals are using ML to exploit vulnerabilities as businesses add network devices onto the cloud.

**The cloud shared responsibility model**

OCI offers security technology and operational processes to help secure its enterprise cloud services. Customers must also be aware of their security and compliance responsibilities to securely run workloads on OCI. By design, Oracle provides security for a cloud’s infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), while tenants are responsible for securely configuring their cloud resources and data in motion. Security in the cloud is thus a shared responsibility between the customer and Oracle.

In a traditional, customer owned and run data center, the tenant is responsible for securing everything—the infrastructure, the applications, and all communications. While this may seem like a challenge, on-premises computing makes it relatively easy to set and enforce security policies to monitor security events and centrally manage security enforcement.

However, security in cloud-based environments is different. Like any cloud provider, Oracle is responsible for the security of the underlying cloud infrastructure, such as data centers, hardware, and software systems, while customers are responsible for securing communication in and out of the cloud, protecting applications, and configuring services such as compute, network, storage, and database. This shared security model poses challenges in terms of added complexity and creates security gaps that grow as more clouds and data centers are added.

To secure a cloud environment, especially multi-cloud and hybrid cloud environments, a Security Fabric that uses native integrations into each cloud is essential. The Fortinet Security Fabric spans multiple clouds, providing a consistent, easily managed system to protect critical data, applications, and the networks binding them together.

It provides market-leading security solutions for each of these virtualization and cloud environments. Using a cloud-based management tool (FortiManager), a common operating system (FortiOS), an advanced threat-intelligence source to stay ahead of attacks (FortiGuard Labs), and a powerful security information and event management system (FortiSIEM), Fortinet has woven together a single, integrated Security Fabric for complete visibility and control across the entire distributed network environment.
OCI and Fortinet: Enterprise Security for Business Transformation

The Fortinet Security Fabric brings advanced security to OCI, going beyond the infrastructure and protecting the entire network, from hybrid cloud to IoT devices, to provide superior protection against sophisticated threats. All devices, from hosts to workloads to web applications, are automatically detected and overseen through policy management. Businesses can apply consistent policies throughout their multi-cloud infrastructures, resulting in reliable enforcement and visibility across all devices and applications.

Security teams can automatically synchronize security resources to better enforce policies, coordinate automated responses to threats detected anywhere in the network, and easily manage all security solutions and products through a single console. Enterprise-class security provides protection for Oracle workloads, Software-as-a-Service (SaaS) applications, and web applications. The Fortinet Security Fabric can help transform an organization’s security infrastructure from a series of point solutions to a multi-cloud security system able to support hybrid deployments, workloads in motion, and cloud environments with a centralized interface for management and automation.

Three-pillar support

**Broad protection.** Gain visibility and protection for Oracle workloads and web applications across the entire digital attack surface.

**Native integration.** Integrate with OCI and security systems using open standards for real-time threat intelligence and coordinated detection of advanced threats through sophisticated, centralized analytics across hybrid clouds.

**Management and automation.** Achieve unified operations and analytics via a single console to coordinate automated responses and remediation to threats detected across the extended network—from on-premises to OCI to hybrid cloud.

Figure 2: The Fortinet Security Fabric.
Powered by leading security research

The Fortinet Security Fabric is powered by security services from FortiGuard Labs—Fortinet's leading research team that leverages a global network of security sensors and advanced ML technologies. FortiGuard threat intelligence encompasses research performed by FortiGuard analysts in cooperation with the extended security industry and law enforcement organizations.

A unique combination of in-house research, information from industry sources, ML, and AI technologies is why Fortinet security solutions consistently earn high scores in real-world security effectiveness tests at third-party vendors such as NSS Labs, Virus Bulletin, ICSA Labs, AV-Comparatives, and more. FortiGuard Labs uses data collected from sensors positioned around the globe to protect hundreds of thousands of customers every day.

Fortinet-OCI Suggested Architectures

Next-generation firewall for public and hybrid clouds

Fortinet delivers both physical and virtualized security appliances to secure the entire network from on-premises to cloud. FortiGate next-generation firewall (NGFW) virtual appliances allow organizations to mitigate blind spots by implementing critical security controls within the virtual infrastructure. They rapidly provision security infrastructure whenever and wherever it is needed, and feature all of the security and networking services common to traditional hardware-based FortiGate appliances. FortiGate virtual appliances enable organizations to deploy a mix of hardware and virtual appliances, operating together and managed from a centralized management platform.

FortiGate automatically discovers enterprise network items including Oracle enterprise applications, cloud applications, IoT devices, performance workloads, and mobile devices. Reduce complexity and automate visibility into applications, users, and network devices, and protect them from known and unknown threats with advanced threat intelligence.

How it works

- Intelligence from FortiGuard Labs provides automated visibility to help stop attacks. FortiGate delivers scalable performance of advanced security services like threat protection, SSL inspection, and ultralow latency for protecting internal segments and mission-critical environments. Software-defined security allows customers to adopt more robust security best practices and compliance.
- FortiAnalyzer provides data-driven enterprise security insights with centralized network logging, analytics, and reporting.
- FortiManager delivers single-pane-of-glass management across the network and provides real-time and historical views into network activity.

Other considerations

Mitigate the risk of network downtime by adding high availability (HA) to provide failover protection in the event of any number of software or hardware problems.

Leverage multiple availability domains or fault domains to help ensure HA and to protect against resource failure when configuring clusters on OCI. An availability domain is one or more data centers located within a region, completely isolated from each other, fault tolerant, and configured such that a failure that impacts one availability domain is

Global Cybersecurity Breaches

- Facebook’s security breach compromised over 50 million user accounts.²
- Marriott suffered a massive data breach affecting 500 million guests of various Starwood properties. It is the largest data breach reported by a hotel and the second largest ever.
- $31 million in cryptocurrency was stolen from South Korean crypto exchange Bithumb.³
- Iceland was hit with what officials claim is the country’s largest cyberattack ever, a very elaborate phishing campaign mimicking the police service and targeting citizens.
- Italian oil and gas company Saipem was hit by a new version of the Shamoon malware that wiped data from roughly 10% of its systems.
- IBM and HPE were both named targets of a Chinese espionage campaign, Cloud Hopper. U.S. and British officials report the aim was to infect the systems of these and other large service providers to access hosted client data.

² Facebook’s security breach compromised over 50 million user accounts.
³ Marriott suffered a massive data breach affecting 500 million guests of various Starwood properties. It is the largest data breach reported by a hotel and the second largest ever.

³ $31 million in cryptocurrency was stolen from South Korean crypto exchange Bithumb.

Global Cybersecurity Breaches

- Facebook’s security breach compromised over 50 million user accounts.²
- Marriott suffered a massive data breach affecting 500 million guests of various Starwood properties. It is the largest data breach reported by a hotel and the second largest ever.
- $31 million in cryptocurrency was stolen from South Korean crypto exchange Bithumb.³
- Iceland was hit with what officials claim is the country’s largest cyberattack ever, a very elaborate phishing campaign mimicking the police service and targeting citizens.
- Italian oil and gas company Saipem was hit by a new version of the Shamoon malware that wiped data from roughly 10% of its systems.
- IBM and HPE were both named targets of a Chinese espionage campaign, Cloud Hopper. U.S. and British officials report the aim was to infect the systems of these and other large service providers to access hosted client data.

² Facebook’s security breach compromised over 50 million user accounts.
³ Marriott suffered a massive data breach affecting 500 million guests of various Starwood properties. It is the largest data breach reported by a hotel and the second largest ever.

³ $31 million in cryptocurrency was stolen from South Korean crypto exchange Bithumb.
unlikely to impact the availability of others. A fault domain is a grouping of hardware and infrastructure within an availability domain. Fault domains allow organizations to distribute instances so that they are not on the same physical hardware within a single availability domain. As a result, an unexpected hardware failure or maintenance that affects one fault domain does not necessarily affect instances in other fault domains.

High-availability firewalls and scalable application delivery

Business transformation applications and workloads require HA to provide failover protection. A standalone network security gateway is a single point of failure that is vulnerable to any number of software or hardware problems that could compromise the device and bring all traffic on the network to a halt. Customers can add failover protection by adding an additional two or more FortiGate NGFWs to their network to help eliminate downtime. The HA cluster appears to function as a single FortiGate, processing network traffic and providing normal security services such as firewalling, security profile services, and VPN services.

If a failure should occur, another FortiGate device will automatically take over to prevent downtime. Scalable application delivery intelligence provides load balancing across locations, servers, and applications to improve performance and delivery of applications over the cloud. Load balancing keeps network traffic flowing efficiently to support lift-and-shift applications to the cloud, accelerate migration to cloud computing, and support application interoperability between on-premises and cloud applications.

How it works

FortiGate HA is implemented by configuring two or more FortiGate devices to operate as an HA cluster. The HA cluster is installed between an internal network (private subnets) and the internet (public subnet), typically deployed on different availability domains or fault domains on OCI. To the network, the HA cluster appears to function as a single FortiGate, processing network traffic and providing normal security services such as firewalling, security profile services, and VPN services.

FortiGate Benefits

FortiGate virtual appliances offer protection from a broad array of threats, with support for all the security and networking services offered by the FortiOS operating system. In addition, the appliances offer:

- Increased visibility
- Native integration into OCI and other public clouds
- Rapid deployment
- Ability to manage virtual and physical appliances from a single platform
- Simple licensing with no per-user fees
- Support for multiple virtualization platforms
- Full support for FortiHypervisor deployments enabling line-speed security in vCPE deployments
- Wide array of licensing choices to fit any infrastructure
- VDOM-enabled models for multi-tenant environments

Figure 3: HA for failover protection via FortiGate.
The active-active HA model consists of two FortiGate devices deployed and registered within a load balancer such that the traffic is balanced between the two. If system failure occurs on either one of the FortiGate devices, the other one handles all the traffic.

The active-passive HA cluster provides hot standby failover protection. An active-passive cluster consists of a primary unit that processes communication sessions, and one or more subordinate units. The subordinate units are connected to the network and to the primary unit but do not process communication sessions. Instead, the subordinate units run in a standby state. In this standby state, the configuration of the subordinate units is synchronized with the configuration of the primary unit, and the subordinate units monitor the status of the primary unit.

Another option is using floating IP addresses of compute instances. Either the secondary private IP address or the reserved public IP address (attached to a private IP) plays a key role in HA architectures in OCI. In the event of a failover, these IP addresses are automatically unassigned from the primary FortiGate instance and then reassigned to the standby instance.

**Application security with FortiWeb**

Advances in cloud technology are driving the demand for web-based applications. New approaches to application development include containerization, serverless architecture, cloud-native applications, and incorporating ML and AI into business models. Once web applications are on the internet, they become vulnerable to potential threats, and data must be protected to meet and adhere to compliance and regulatory requirements.

FortiWeb is a robust web application firewall (WAF) with an ML approach to anomaly and threat detection to provide enhanced performance. Protect web applications from known and unknown threats automatically, including the OWASP top 10 security risks, to help eliminate the need for manual investigation of potential threats. The Fortinet signature detection engine blocks known attacks, drawing from FortiGuard Labs’ threat-intelligence service and other devices in the Fortinet Security Fabric.

Figure 4: FortiWeb WAF security in an OCI environment.
How it works

The FortiWeb signature detection engine is updated frequently and automatically with data on the latest threats from FortiGuard Labs. All traffic is scanned for any threat that might infect servers or other network devices using FortiGuard Labs’ award-winning antivirus engine. FortiWeb confirms that all web application traffic conforms to HTTP RFC standards, stopping attacks on potential protocol vulnerabilities. Device fingerprinting, packet comparison, and updates from other Fortinet devices help to dynamically monitor traffic sources.

Security Factors While Implementing Applications in the Cloud

- **Deploy and manage workloads in the cloud.** Gain the confidence to safely deploy applications in OCI, and apply the same level of security features in the cloud that are on-premises.
- **Centralized security management.** Fortinet centralized, fully integrated security helps ensure that Oracle applications, workloads, SaaS applications, and other enterprise applications are managed from a single console.
- **Develop cloud-native applications with security.** Building Fortinet security into applications at inception will better ensure that new cloud-native applications arrive securely.
- **Secure hybrid clouds and VPNs.** Maintaining a uniform security policy for all corporate users, applications, and network devices regardless of their location is essential to providing secure access within a hybrid cloud solution and corporate access over VPNs.
- **Ensure compliance with regulatory requirements.** Organizations have compliance and security requirements that are both common and custom to industry. Take control and ownership of those concerns with Fortinet solutions for automated reporting.
- **Enable a shared security model.** Employing a shared security model ensures organizations have robust coverage and real-time protection for critical applications and cloud infrastructure.

Conclusion

Oracle and Fortinet together deliver innovative and secure cloud services that allow users and developers to build, deploy, and manage workloads seamlessly—in the cloud or on-premises. OCI redefines how businesses modernize, innovate, and compete in a digital world and run Oracle enterprise applications, performance-intensive workloads, custom applications, IoT devices, and mobile applications.

While OCI provides secure infrastructure and services to run cloud applications and workloads, the shared responsibility model indicates that customers are responsible for protecting their data and applications hosted or deployed in the cloud. The Fortinet Security Fabric enhances OCI to ensure business-critical applications and network devices are better protected from the ever-expanding threat landscape. With Fortinet, OCI users can better apply consistent security policies throughout their multi-cloud infrastructures. The Security Fabric provides multilayered security protection and operational benefits for running applications over OCI.

With the Fortinet Security Fabric, OCI supports high availability, fault tolerance, and load balancing to help ensure network speed is optimized to deliver redundancy and reliable performance to all network devices. The Security Fabric provides visibility into every network segment, device, and appliance for real-time intrusion detection and prevention. A machine learning-based approach to security offers unsurpassed threat protection for everything in the cloud—applications, workloads, and data. The security architecture of OCI is a scalable platform that enables businesses to fully embrace digital transformation.
1 “Worldwide Digital Transformation Spending Guide,” IDC.

2 Jessica Guynn, “Facebook’s 50 million account breach is already its biggest ever-and may get even worse,” USA Today, October 1, 2018.

3 Mike Murphy, “South Korean crypto exchange Bithumb says $30 million stolen by hackers,” MarketWatch, June 19, 2018.