Powered by ORACLE Cloud

WHITE PAPER

Oracle Cloud Infrastructure Security Reference Architecture

With Fortinet Security

Executive Summary

Businesses are rapidly deploying a variety of workloads across multiple clouds to modernize applications, innovate and compete in a digital world. Digital transformation (DX) uses innovative technology to enable customers to gain a competitive edge, apply deep learning to business models, and identify potential revenue opportunities. Cloud computing is at the forefront of this transformation and is being adopted at an unprecedented pace. Oracle Cloud Infrastructure (OCI) provides a cloud platform that enables developers, IT professionals, and business leaders to develop, extend, connect, and secure cloud applications, share data, and gain insights across applications and devices. But with business-critical applications and data stored across multiple clouds, there can be serious security challenges. The Fortinet Security Fabric provides advanced security that enables Oracle Cloud Infrastructure to protect workloads and applications from threats to both on-premises and cloud environments.

IDC forecasts that worldwide spending on technologies and services that enable digital transformation will reach US$1.97 trillion in 2022.[1]

Oracle Cloud Infrastructure for Business Transformation

Oracle helps businesses solve their biggest challenges, from processing financial transactions to improving customer experiences and understanding insights from data. A business's most valuable assets—applications and databases—can be managed on Oracle Cloud Infrastructure. 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: Oracle Cloud Infrastructure, 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.

Cloud Security Is Essential to Your Enterprise

As business and technology leaders embark on digital transformation 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. Moreover, understanding and succeeding with a shared security model becomes a critical success factor.

The number of network devices in the cloud has grown. At the same time, cybercriminals 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 a centralized management tool for all network devices. Oracle Cloud Infrastructure provides best-in-class security protection; however, customers have the same responsibility to protect their cloud resources and enforce compliance as they do so for their on-premises applications.

[1] "Worldwide Semiannual Digital Transformation Spending Guide," IDC.

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. Cybercriminals are using machine learning to exploit vulnerabilities as businesses add network devices onto the cloud.

- 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.
- US$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 percent 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.

Prevalence of hybrid clouds

Business transformation demands agility—the ability to adapt quickly and change directions at a moment's notice. According to Technology Business Research (TBR), 51 percent of enterprises have adopted at least one workload that leverages a hybrid cloud or hybrid IT deployment model.[4] Embracing cloud computing may present risks that are not present in a purely on-premises or private cloud environment.

To secure your entire network across hybrid clouds against sophisticated threats, it is critical to have visibility into every network segment, application, device, and appliance, whether virtual, in the cloud, or on-premises. More than 25 percent of enterprise attacks are predicted to target IoT devices by 2020. Siloed apps in multicloud environments make it even harder to respond to threats. Oracle Cloud Infrastructure supports heterogenous architecture and hybrid clouds to provide agility and rapidly scalability. The Fortinet Security Fabric for Oracle Cloud Infrastructure enables businesses to apply policies throughout their hybrid cloud infrastructure in order to promote consistent enforcement and visibility.

VPNs offer an extra layer of security when providing remote access to employees and partners. It's especially important in a multicloud environment to maintain uniform security policies for all corporate employees, applications, and devices regardless of their location. Fortinet VPN technology adds protection in a hybrid cloud with secure communication across Oracle Cloud Infrastructure for both IPsec and secure socket layer (SSL) technologies.

The global hybrid cloud market was pegged at US$36.14 billion in 2017 and is estimated to reach US$171.93 billion by 2025, registering a CAGR of 21.7 percent from 2018 to 2025.[5]

The cloud shared responsibility model

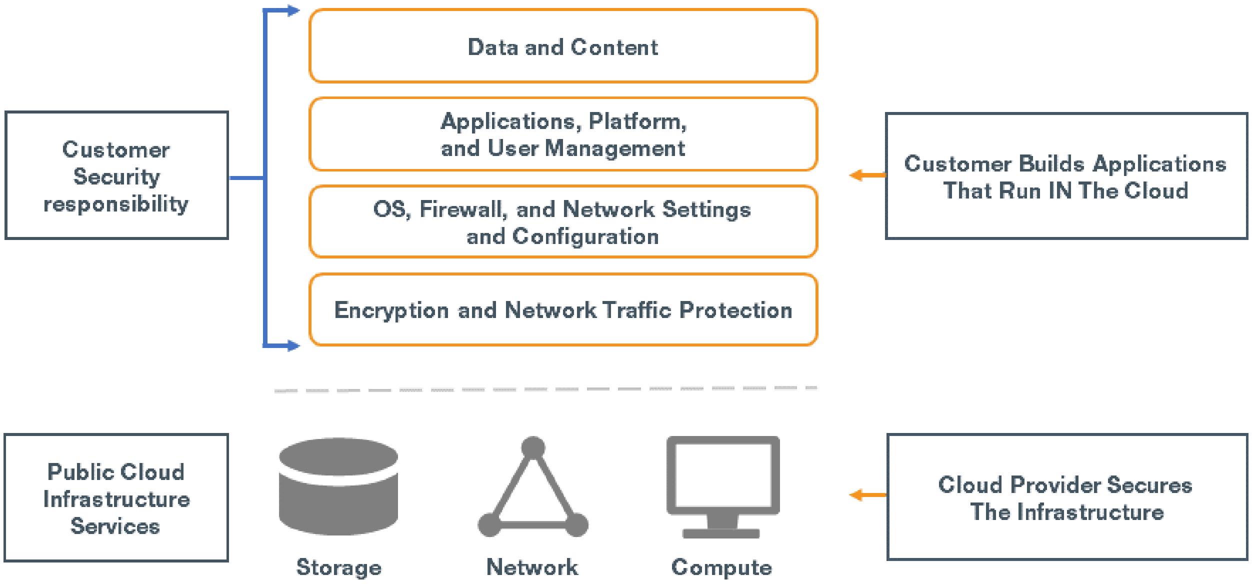
Oracle Cloud Infrastructure offers security technology and operational processes to help secure its enterprise cloud services. Customers must also be aware of their security and compliance responsibilities to securely run workloads on Oracle Cloud Infrastructure. By design, Oracle provides security for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

[2] "Facebook's 50 million account breach is already its biggest ever," USA Today, September 2018.
[3] "South Korean crypto exchange Bithumb says $30 million stolen by hackers," MarketWatch, June 2019.
[4] "Hybrid is driving cloud and overall IT opportunity," Technology Business Research, April 2017.
[5] Allied Market Research, "Hybrid Cloud Market to Reach $171.93 Bn, by 2025 at 21.7% CAGR," October 17. 2018.

In a shared, multi-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data-center facilities, and hardware and software systems) and customers are responsible for securing their workloads and configuring services (such as compute, network, storage, and database).

In a fully isolated, single-tenant, bare metal server with no Oracle software on it, customers responsibility increases as the entire software stack (operating systems and above) where you deploy your applications is brought to the cloud. In this environment, customers are responsible for securing their workloads, configuring their services (compute, network, storage, database), and ensuring that the software components running on the bare metal servers are configured, deployed, and managed securely.

According to a recent Gartner report, "through 2022, at least 95% of cloud security failures will be the customer's fault." The Fortinet Security Fabric Fortinet extends consistent, enterprise security to Oracle Cloud Infrastructure to help protect business workloads across on-premises and cloud environments. Fortinet security creates a unified security posture to apply security policies to your workloads and helps customers better meet their obligations under the shared security model. **According to IDC, Fortinet is the No. 1 most adopted network security solution, having deployed 4.2 million devices.**[6]


Customer Security responsibility
Data and Content
Applications, Platform, and User Management
OS, Firewall, and Network Settings and Configuration
Encryption and Network Traffic Protection
Customer Builds Applications That Run IN The Cloud
Public Cloud Infrastructure Services
Storage
Network
Compute
Cloud Provider Secures The Infrastructure

Oracle Cloud Infrastructure and Fortinet: Enterprise Security for Business Transformation

The Fortinet Security Fabric adds advanced security to Oracle Cloud Infrastructure, 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 apps, are automatically detected and overseen through policy management. Businesses can apply consistent policies throughout their multicloud infrastructures, resulting in reliable enforcement and visibility across all devices and applications. Automatically synchronize your security resources to better enforce policies, coordinate automated responses to threats detected anywhere in your network, and easily manage all your security solutions and products through a single console. Enterprise-class security provides protection for digital transformation of your Oracle workloads, SaaS applications, and web applications.

---

[6] IDC Worldwide Security Appliances Tracker, April 2018 (based on annual unit shipments).

FortiGuard Labs finds and mitigates IT threats

Fortinet provides additional security solutions beyond the native security groups that are supported by FortiGuard Labs — Fortinet's in-house team of 200+ global researchers that help detect and protect against known and unknown threats. Sophisticated machine learning based on true artificial intelligence is used to achieve enhanced threat detection accuracy while minimizing false positives.

Our latest quarterly Threat Landscape Report highlights:

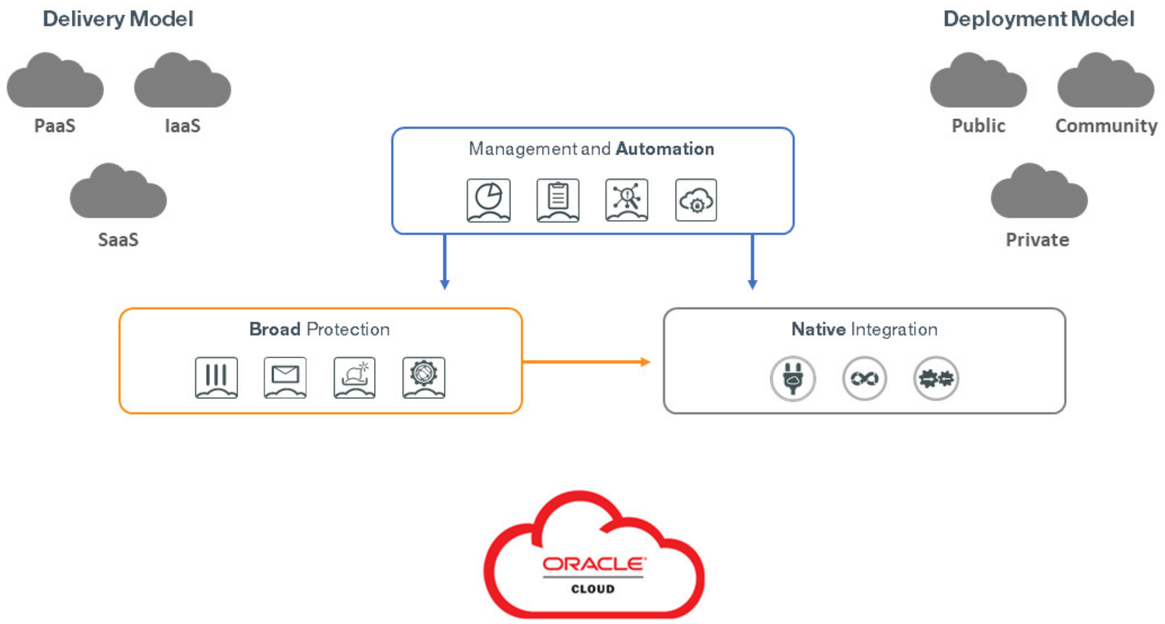
- Growth in new malware variants rose 129 percent over this time last year.
- Mobile devices, particularly Android, continue to be a main target of attackers.
- IoT devices are a popular crypto jacking platform.
- Ransomware attacks continue to be a problem.

Fortinet customers are protected against these vulnerabilities, between discovery and the patch, by our IPS signatures.
FortiGuard Zero-day Program.

How it works

Fortinet fabric cloud security includes three pillars

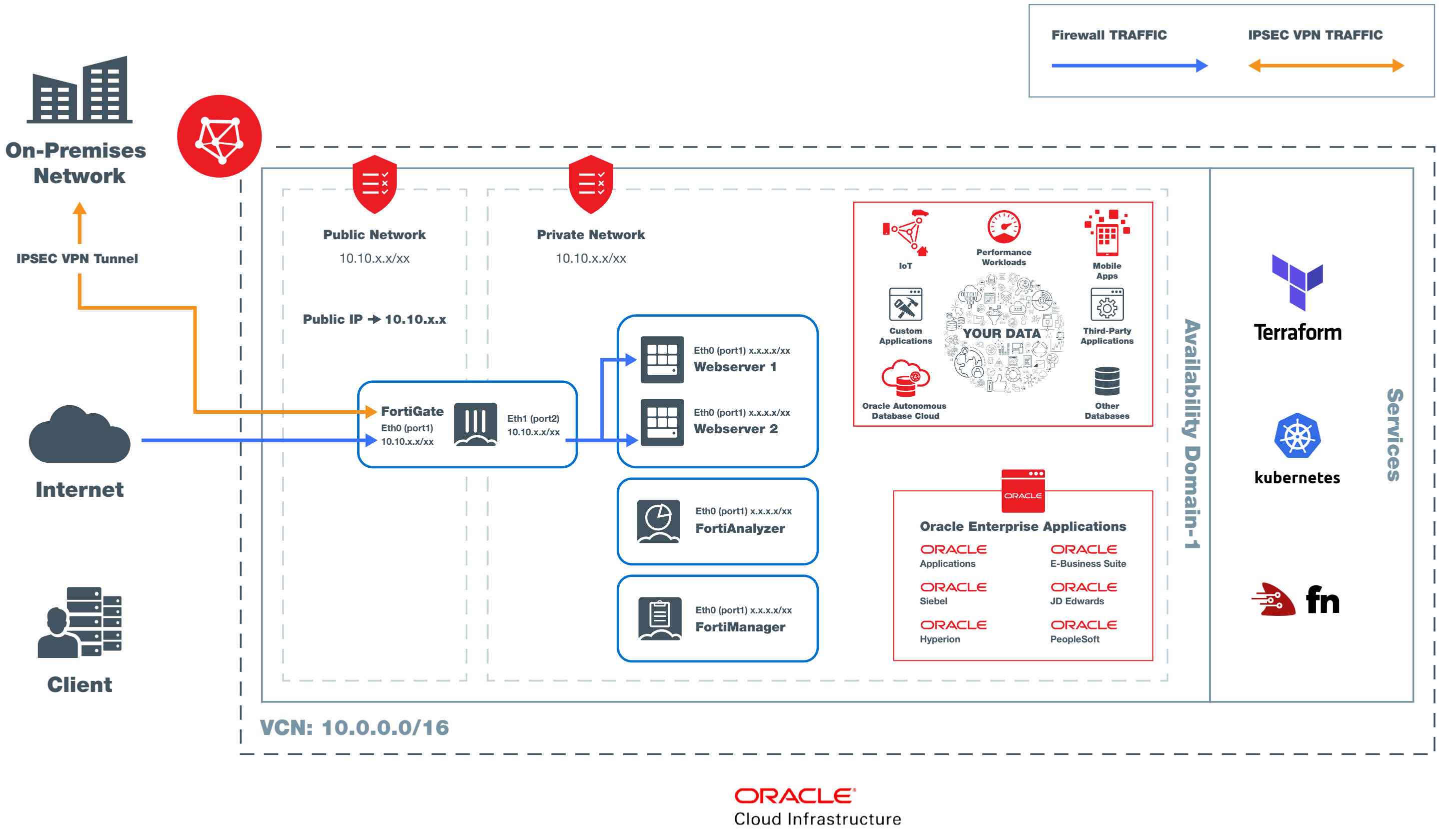
1. Broad Protection
   Visibility and protection for Oracle workloads and web applications are provided across the entire digital attack surface.
2. Native Integration
   Integration with Oracle Cloud Infrastructure and security systems using open standards to provide real-time threat intelligence and coordinated detection of advanced threats through sophisticated, centralized analytics across hybrid clouds.
3. Management and Automation
   Operations and analytics are done via a single console to coordinate automated responses and remediation to threats detected across your extended network, from an on-premises network, to Oracle Cloud Infrastructure to your hybrid cloud.



Fortinet Oracle Cloud Infrastructure Security Reference Architecture

Next-generation firewall for public and hybrid clouds

FortiGate enterprise firewalls utilize security processors and threat intelligence services from FortiGuard Labs to help protect business-critical applications and deliver strong threat protection against the most advanced known and unknown threats to stop attacks in real-team. Flexible security deployments support public cloud, hybrid cloud, or on-premises environments. FortiGate automatically discovers enterprise network items including Oracle enterprise applications, cloud applications, IoT devices, performance workloads, and mobile apps devices to reduce complexity and automate visibility into applications, users, and network devices. FortiGate's enterprise security protection automatically protects applications and network devices using advanced threat intelligence, enables a unified security posture across on-premises and cloud environments, and centralizes security for all enterprise network devices and applications.



How it works

FortiGate next-generation firewall threat 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 ultra-low latency for protecting internal segments and mission critical environments. Software-defined security allows customers to adopt more robust security best practices and compliance.

FortiAnalyzer: Data-driven enterprise security insight delivers centralized network logging, analytics, and reporting.

FortiManager: "Single pane of glass" management across the network provides real-time and historical views into network activity.

Customer business outcomes

1. Highly secure computing between on-premises and cloud environments
2. Support enhanced security requirements for hybrid cloud and VPNs
3. Accelerate migration to the cloud with enterprise security
4. More secure connection of network perimeter to encompass cloud computing
5. Provide disaster recovery and backup

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 high availability and to protect against resource failure when you configure your cluster on Oracle Cloud Infrastructure. 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 unlikely to impact the availability of others. A fault domain is a grouping of hardware and infrastructure within an availability domain. Fault domains let you distribute your 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.

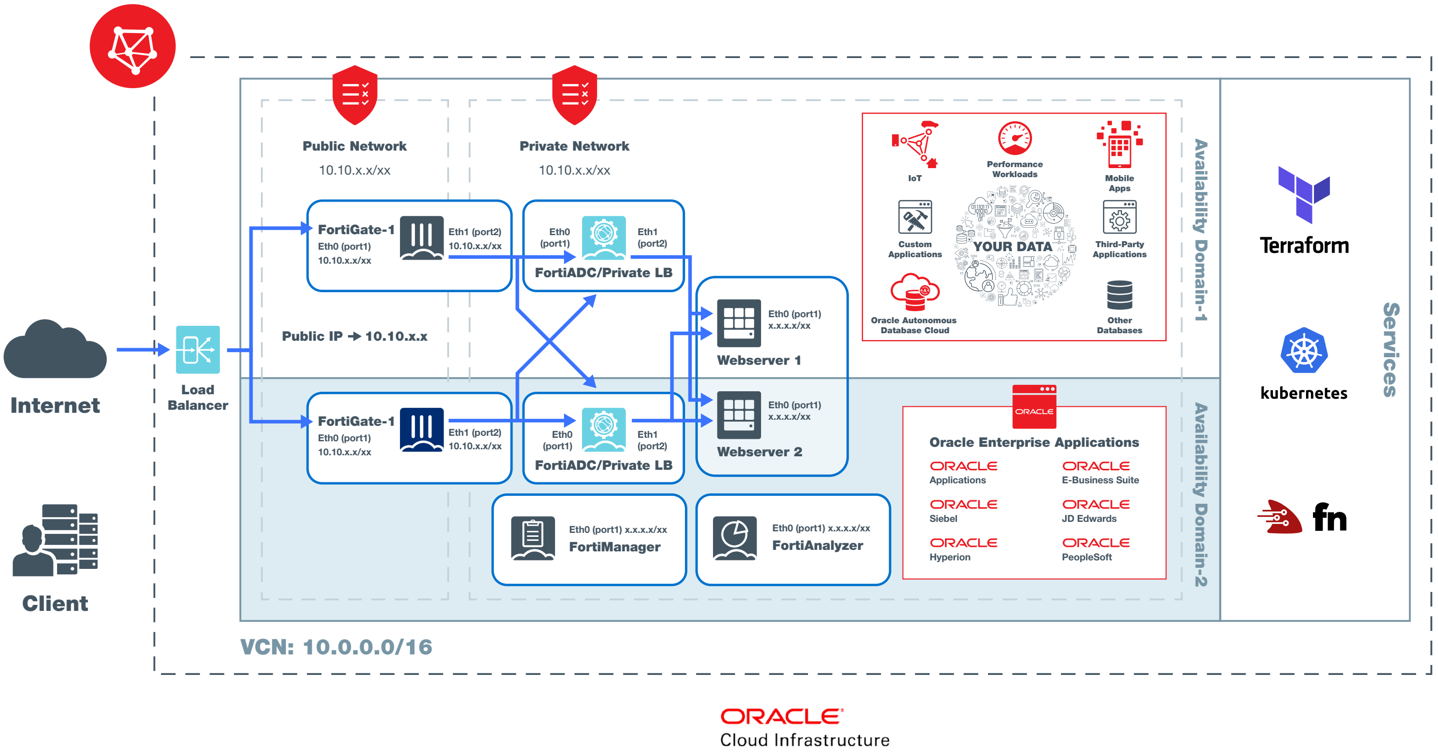
Improve the speed of your enterprise applications across the network by optimizing performance with scalability to enhance user experience.

Better protect your web applications from the most advanced threat vectors using detection techniques such as signatures, IP reputation, and behavioral analysis.

High availability and scalable application delivery

Business transformation applications and workloads require high availability 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 next-generation firewalls to their network to help eliminate downtime. The high availability cluster appears to functions as a single FortiGate, processing network traffic and providing normal security services such as firewalling, security profile services, and VPN services.

By adding high availability, 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 Oracle Cloud Infrastructure. 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.

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 that 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), play a key role in high availability architectures in Oracle Cloud Infrastructure. In the event of a failover, these IP addresses are automatically unassigned from the primary FortiGate instance and then reassigned to the standby instance.

FortiGate next-generation firewall threat intelligence from FortiGuard Labs provides automated visibility to help stop attacks with redundant failover. Additional FortiGate next-generation firewall devices can be added for failover protection.

FortiADC application delivery controllers (ADC) distribute traffic across multiple geographic locations for global server load balancing. Policy-based routing dynamically rewrites content so application and server configurations can optimize load balancing. Enable scalable, secure, and fast web application delivery with compression, caching, HTTP 2.0, and HTTP page speedup.

FortiAnalyzer provides data-driven enterprise security insight to ensure centralized network logging, analytics, and reporting.

FortiManager enables “single pane of glass” management across the network and provides real-time and historical views into network activity.

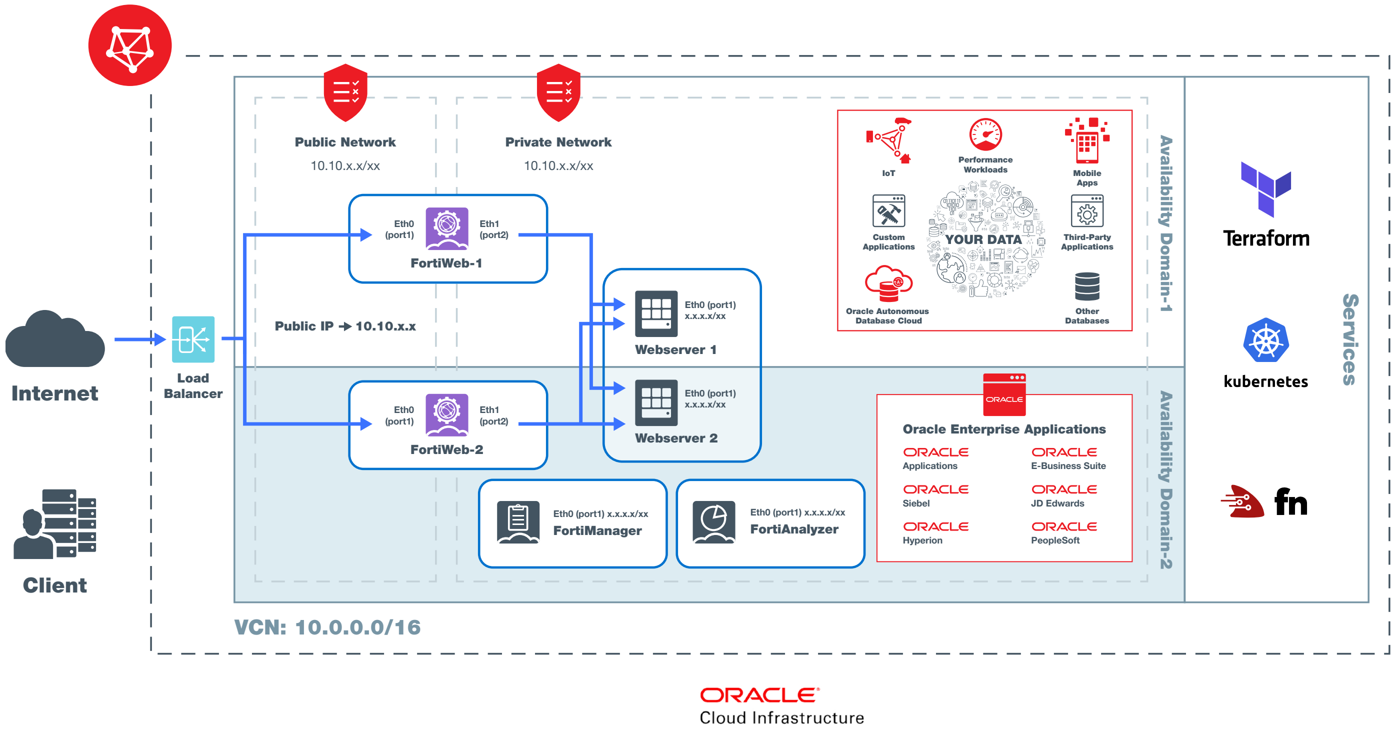
Customer business outcomes

1. Adding failover protection and redundancy to existing infrastructure
2. Setting up new branch offices
3. Incorporate load balancing to improve cloud performance

Application security

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 machine learning 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.

Fortinet’s FortiWeb is a robust web application firewall (WAF) with a machine learning approach to anomaly and threat detection to provide enhanced performance. Protect your 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. Fortinet’s signature detection engine blocks known attacks, drawing from FortiGuard Labs’ threat intelligence service and other devices in the Fortinet Security Fabric. FortiWeb provides complete protection against OWASP top 10 threats with a continuously updated security posture and data protections.



How it works

FortiWeb's 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.

Customer business outcomes

1. Protect applications on Oracle Cloud Infrastructure
2. Lift-and-shift workloads to the cloud
3. Modernize applications with containers
4. Develop cloud-native applications

Security Factors While Implementing Applications in the Cloud

- Deploy and manage workloads in the cloud: Fortinet provides you the confidence to bring your applications to Oracle Cloud Infrastructure securely and apply the same level of security features that you have on-premises to your cloud environment.
- Centralized security management: Fortinet's centralized, fully integrated security, helps ensure that your 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 your applications at inception will better ensure that new cloud native applications arrive securely.
- Secure hybrid clouds and VPNs: Maintaining uniform security policy for all corporate users, applications, and network devices regardless of their location is essential to providing more secure access within a hybrid cloud solution and corporate access over VPNs.
- Ensure compliance with regulatory requirements: Your business will have compliance and security requirements that are both common and custom to your business. Fortinet helps you take control and ownerships of those concerns.
- Enable a shared security model: Oracle Cloud Infrastructure comes with a high level of security functionality. But at the infrastructure level, it's not privy to the real-time security visibility and access control needed by your applications. By employing a shared security model, you have robust coverage for what matters.

Conclusion

Oracle delivers innovative and integrated cloud services that allow users and developers to build, deploy, and manage workloads seamlessly—in the cloud or on-premises. Oracle Cloud redefines how businesses modernize, innovate, and compete in a digital world. Oracle Cloud Infrastructure provides a highly secure cloud environment to run Oracle enterprise applications, performance-intensive workloads, custom applications, and IoT and mobile apps.

While Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure to ensure your mission-critical applications and network devices are better protected from the ever-expanding threat landscape. With Fortinet, Oracle Cloud Infrastructure users can better apply consistent security policies throughout their multi-cloud infrastructures. The Security Fabric provides multilayer security protection and operational benefits for running applications over Oracle Cloud Infrastructure.

With Fortinet Security Fabric, Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure is a scalable platform that enables businesses to embrace digital transformation.

FORTINET
ORACLE
Cloud Infrastructure
www.fortinet.com

April 2019
C:\Users\srockwell\Desktop\Fortinet Oracle Whitepaper\Fortinet and Oracle Whitepaper Folder\Fortinet and Oracle Whitepaper