ORACLE

Oracle Utilities Cloud and Cybersecurity

Utilities have always held security and safety of their information and assets to the utmost priority. Concerns continue to grow surrounding cybersecurity due to the growing digitalization and automation of critical infrastructure and information storage, while at the same time threats continue to escalate both in volume and sophistication. Security breaches and successful attacks can't be tolerated in the utility industry as this can disrupt essential services and cause significant security, economic, safety, and social impacts.

Increasing attacks on utility infrastructure emphasizes the ever-present threat to utilities core operations. Security is embedded in every layer of Oracle Cloud, including infrastructure and applications, to offer continuous and seamless protection. Oracle security services are simple, prescriptive, and integrated. This helps reduce complexity and enables you to focus more on your business. These securities and protections include:

- Defense in depth strategy and controls across all digital assets
- Engineered security into every layer of the stack from application to hardware
- All data is encrypted by default at rest and in motion
- Automated patching with Oracle Autonomous Linux and Oracle Autonomous Database reducing surface attack area
- Implementing on-premises cloud-based subscription models behind customer firewalls.

Oracle understands the importance of Utility Data

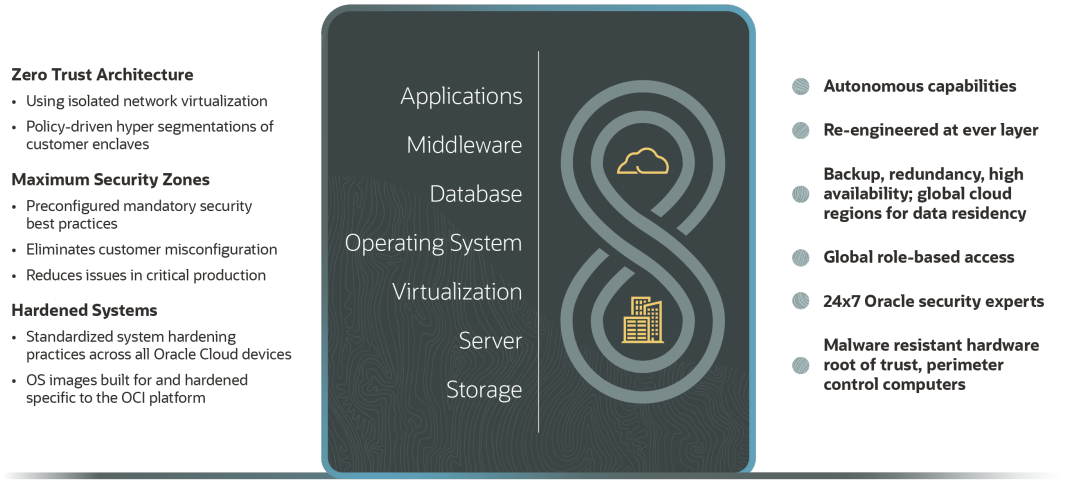
Oracle Cloud Infrastructure (OCI) is designed with data handling and management practices that help customers configure their data and provide the tools to help them protect their data and applications from outside threats. OCI's built-in security also helps drive the efficiency of security teams, with customers reporting a 35% efficiency improvement across security teams.

- **Data Encryption** – OCI has a "ubiquitous encryption" program that requires teams to encrypt all data at rest and in transit, including customer tenant data. Oracle encrypts all data at rest and in transit, by default.
- **API Security** – In modern cloud environments, APIs are critical to application function. However, they also can create broader attack surfaces. Oracle recognizes the importance of API security for applications in cloud environments and has developed the API Gateway service to provide that security. API Gateway is a fully managed regional service that integrates with customers' networks on OCI. API gateways enable customers to publish public or private APIs, process incoming requests from a client, and help to apply policies for security, availability, and validation. Connections from clients to API gateways always use Transport Layer Security (TLS) to help preserving the confidentiality and integrity of data. Customers can also configure the connections from API gateways to backend services to use TLS.

- **Data Destruction** – Oracle uses physical destruction and logical data erasure processes so that data doesn't persist in decommissioned hardware.
  - Storage Media Destruction – Oracle Asset Management requirements explicitly prohibit the removal of storage media that contains customer data from the data hall in which it's stored. Each data hall in a data center contains a secure media disposal bin. When a hard disk or other storage media is faulty or removed from production for disposal, it's placed in this secure bin for storage until it's degaussed and shredded.
  - Data Erasure – OCI Data Erasure enables secure and permanent deletion of data when it's no longer needed, to support data privacy and compliance with regulations. OCI offers various methods for data erasure, including secure host wipe, media destruction, and key deletion for storage volumes.

Built on the secure Oracle Cloud Platform with 24X7 monitoring

Vertical integration – Maximum performance and security



Oracle's utility applications being backed by OCI security creates a safer and reliable platform across our customers utility business. This means Oracle customers don't have extra cost and risk of paying other cloud platforms to store vital information and data. 24/7 monitoring provides constant data security and alerts customers if anything is irregular.

Development practices built into every phase of the lifecycle

Oracle's Software Security Assurance (OSSA) model incorporates resiliency into the design, build, test & maintenance of products.

- Reduces occurrences of security weaknesses in Oracle products
- Deploying and maintaining Cloud Services in a fully secure configuration
- Identification of weaknesses and security risks through pro-active analysis and testing
- Expedited remediation of weaknesses with transparent disclosure and documentation policies

Connect with us

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