ORACLE

Putting Data Security and Protection First

Automated, always-on, architected-in security

Cloud Security's Current State

Data is the most valuable currency in modern business and, as the **7.9 billion records exposed through data breaches in 2019** suggest, cybercrime's greatest prize. It's unsurprising, then, that some organizations still have reservations about passing data responsibilities to a public-cloud provider. But that's not to say there aren't inherent risks to an organization operating their own on-premises data center. Privilege abuse, configuration mistakes, and ignorance of policy are common IT challenges—all of which can be mitigated through the use of a public-cloud provider that puts security first. In fact, we're seeing a rapid shift in attitudes, with the "Oracle and KPMG Cloud Threat Report 2020" showing that **75% of organizations now see public clouds as more secure than on-premises systems**—an increase over the previous year. At Oracle, we want every organization to take advantage of the cloud's agility, flexibility, and scalability without compromising their own data, or their customers' data. That's why we bake security into all our cloud solutions at the architectural level, ensuring full-stack protection and a platform that's secure by design.

75%

of organizations now see public clouds **as more secure than on-premises systems**

We recognize there's no silver bullet against cybercrime, which is why Oracle Security protects against major points of vulnerability, including:

- Privilege escalation
- Misconfigurations
- Weak cloud-security posture
- Unpatched systems
- Unencrypted data
- Human error
- Vulnerable web applications
- Malicious insider abuse

Full-stack Protection

Oracle takes a layered approach to provide powerful data protection against a wide array of risks and threats. At the center lies your data, which is secure by design through our zero-trust architecture. This helps you decide how infrastructure, users, devices, and applications interact with that data.

With a continuous assessment of risk and trust, Oracle provides comprehensive security. And because our security solutions cover your infrastructure with full-stack protection, you can grow your business with confidence that whatever happens next, your Oracle security solutions will detect threats, remediate errors and anomalies, and always protect your data from attacks.

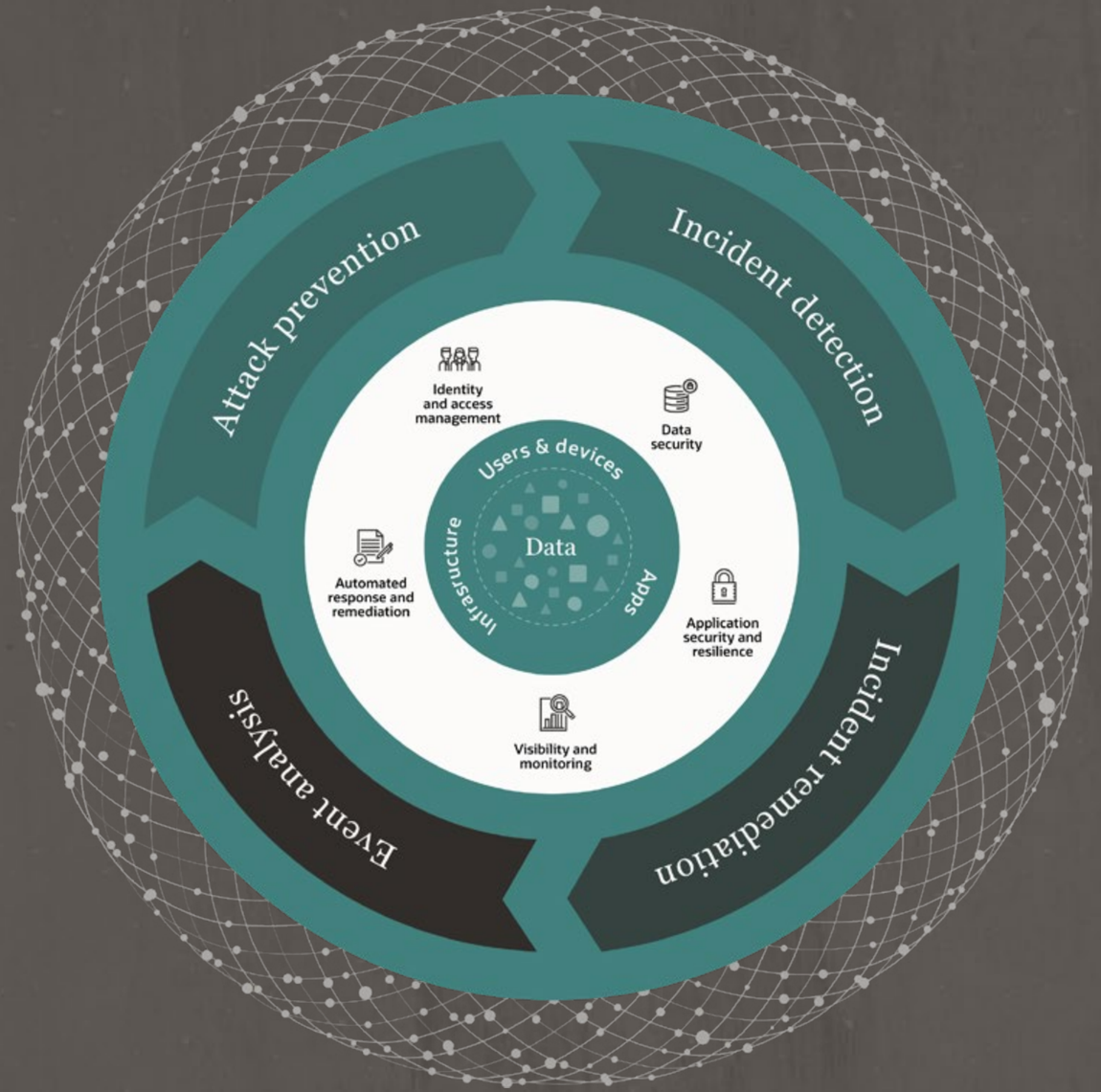
IT professionals are more worried about corporate security than safety at home

Oracle KPMG Cloud Threat Report 2020

Three foundational principles of Oracle Security

To help every organization move forward with confidence, we underpin each of our core solution areas with three strategic security pillars:

Automated, always-on, and architected-in.



Oracle Cloud Infrastructure Security

Oracle Cloud Infrastructure is built from the ground up to meet the needs of mission-critical applications while delivering modern development controls.

Oracle Cloud Infrastructure is the only cloud platform built to run Oracle Autonomous Database, the industry's first and only self-driving database. But how does Oracle keep customers, their data, and their cloud-based workloads and innovation secure?

Automated Patching

With Oracle Autonomous Linux and OS Management in Oracle Cloud Infrastructure, OS security patches are automatically applied. This helps reduce complexity and human error, while delivering increased cost savings, security, and availability.

No human interaction is needed, helping improve IT staff productivity, security, and availability. Automate provisioning, scaling, and monitoring and deliver 30 to 50% TCO savings over five years compared to other on-premises and cloud platforms.

Always-on Encryption

Oracle Cloud Infrastructure uses a ubiquitous encryption program toencrypt all data, in all places, at all times. For customer tenant data, it uses encryption both at rest and in transit.

In fact, our Block Volumes and Object Storage services enable at-rest data encryption by default using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit data is kept secure using Transport Layer Security (TLS) 1.2 or later.

Customers also benefit from a tiered defense strategy and highly secure operations that extend from the physical hardware layer in Oracle data centers to the web layer. Many of the protections and controls available in Oracle Cloud also work with third-party clouds and on-premises solutions to help keep modern enterprise workloads and data secure—wherever they're hosted.

Architected-in Customer isolation

Oracle Cloud Infrastructure is built around our security-first principles. Its architecture helps reduce risk from advanced threats and isolates tenant data to ensure data privacy and security.

This means customers benefit from:

- *Isolated network virtualization that reduces the risk of hypervisor-based attacks*
- *Customer tenancy isolation that limits the risk of threat proliferation*
- *Hardware-based root of trust that ensures each server is provisioned with clean firmware*
- *Network segmentation that isolates services to ensure access is controlled, monitored, and driven by strict policies*

Oracle Cloud Infrastructure in financial services

Security-first Oracle Cloud Infrastructure is ideal for financial services firms that are tired of managing and updating traditional infrastructure. Updating legacy platforms can be slow and see rising upgrade costs over time—tying up valuable resources that could be better used to deliver new innovations and compete against challenger banks and other digitally-savvy competitors like financial technology (fintech) startups.

By migrating infrastructure to the public cloud, firms can reduce infrastructure complexity and improve security while allowing IT staff to refocus their talent on higher-value tasks such as responding to verified security risks or innovating around the customer.

Because Oracle Cloud Infrastructure can run security-sensitive workloads with automated security monitoring, firms can remain compliant with strict industry regulations while improving data visibility and application security, and getting ahead of digitally-savvy competitors.

Oracle Autonomous Database Security

Oracle Autonomous Database helps organizations transform IT database operations by automatically patching, updating, securing, and managing itself—reducing the risk of human error and unexpected downtime, and accelerating the pace of innovation while using fewer resources.

Here's how Oracle Autonomous Database delivers.

Automated Patching

Oracle Autonomous Database automates formerly manual security tasks, helping reduce security administration costs by up to 55%.

Proactive security automation, including automated patching, can also reduce the risk of data breaches occurring after common vulnerability and exposure alerts have been issued.

Patches are deployed with zero downtime, enabling organizations to stay safe and productive while removing the risks of human error and administrative neglect.

Always-on Encryption

As in Oracle Cloud Infrastructure, data in Oracle Autonomous Database is always encrypted—whether at rest or in motion.

Each Oracle Autonomous Database service is automatically configured to use industry-standard Transport Layer Security (TLS) 1.2 to encrypt data in transit, while data at rest is encrypted using Oracle Transparent Data Encryption.

Oracle Transparent Data Encryption not only helps simplify compliance with data-privacy regulations like GDPR, CCPA, and PCI, but prevents OS users from abusing their privileges to access sensitive data. It also helps to prevent data theft, data loss, and improper storage and backup decommissioning.

Architected-in Separation of duties

Oracle Autonomous Database eliminates direct access to the database node and local file system, while isolation between service administrators and service consumers is delivered through Oracle Database Vault.

This separation of duties reduces the risk of administrator wrongdoing and eliminates Oracle service administrators' ability to view or modify enterprise data stored in Oracle Autonomous Database. Security controls within Oracle Database Vault can also help you stay compliant with data privacy laws and standards—such as GDPR—and prevent user-privilege abuse.

Separation of duties also makes it more difficult for cybercriminals to disable security controls, create false users, and access sensitive data.

Oracle Autonomous Database in telecommunications

A popular telecommunications provider has a legally binding obligation to its many global customers that the data with which it is entrusted will not be disclosed.

Unfortunately, a breach does one day occur, and it's quickly discovered that it could have been prevented had the provider's database been updated with the latest security requirements. The cause? Human error, resulting in an unpatched system, allowed cybercriminals to take advantage of a short window of vulnerability and access sensitive customer data.

By moving to a self-securing database that automates encryption and patching, the provider not only eliminates chances of future human error, but improves its security hygiene and rebuilds trust among its customer base.

Oracle Software as a Service Security

All Oracle SaaS solutions offer the benefits of a modern cloud suite. They provide complete, agile, secure, and open solutions for the entire organization without the caveats that come with updating and managing a costly, physical on-premises solution.

And with Oracle's security-first approach, these solutions also offer complete peace of mind.

Automated
Response and remediation

Oracle Identity Cloud Service (IDCS) delivers automated behavioral monitoring across the full stack, and offers secondary authentication like multifactor authentication (MFA).

Oracle Cloud Access Security Broker Service (CASB) can also analyze behaviors and act according to the risk level assigned to a user or application. In cases where suspicious behavior is identified, Oracle CASB can block user access to high-risk services, automatically alert approved users, and take action based on pre-defined policies—for example, automatically notifying auditors about suspicious transactions.

Always-on
Monitoring

Oracle delivers complete SaaS security controls to application owners, auditors, and security operations teams through three strategic technologies:

- *Oracle Identity Cloud Service (IDCS)*
- *Oracle Cloud Access Security Broker (CASB)*
- *Oracle Risk Management Cloud (RMC)*

Together, they enable enterprise users to analyze how user credentials and entitlements are being used to better identify suspicious behavior and rapidly respond to it. This includes looking at user behavior, and cross-referencing it with historical data to create an advanced, automated monitoring and response model.

Architected-in
Integrated cloud-security services

Every Oracle Fusion SaaS application includes Oracle Identity Cloud Service (IDCS) built in by default. This ensures consistent, identity-based security is woven into all parts of the enterprise security fabric.

Oracle Cloud Access Security Broker (CASB) also acts as part of the security foundation for all Oracle SaaS applications, enabling greater visibility into the entire cloud stack—while giving IT the tools they need for automated threat detection, predictive analytics, and security configuration management.

For enhanced risk-mitigation controls and the enablement of application compliance standards, Oracle SaaS users can use Oracle Risk Management Cloud (RMC).

Oracle SaaS in retail

A global ecommerce retailer develops and delivers customer-facing apps to users around the world as part of its core business. While it has to deal with the complexities of launching apps and services at a global scale, it also needs systems in place to deal with fraudulent purchases.

Oracle Identity Cloud Service (IDCS) helps ease the pressure by automatically identifying suspicious transactions. Using geolocation data, Oracle IDCS can flag when transactions come from unexpected locations (such as when a user's IP address doesn't match where their account is registered). It can then apply two-factor authentication via SMS to determine whether the transaction is valid.

By automatically flagging suspicious transactions and applying additional user verification, the retailer can protect its bottom line and brand image without having to dedicate significant IT resources.

Why Oracle Security?

With Oracle, security is built in from the ground up to deliver full-stack protection, automate threat responses, and ensure seamless, always-on protection.

This way, customers enjoy peace of mind knowing that their data and operations are secure. And because security is automated, organizations can get back to what matters most: growing the business.

Oracle Autonomous Database is the industry's first self-securing database

Learn more

Oracle Cloud Infrastructure leverages a security-first approach in its architecture

Explore

Oracle protects mission-critical SaaS applications in the cloud

Learn how

ORACLE