

Putting data security and protection first

AUTOMATED, ALWAYS-ON, ARCHITECTED-IN

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. Privilege abuse, configuration mistakes, and ignorance of policy are common IT challenges—all of which can be mitigated using a public-cloud provider that puts security first. 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.

The challenges

No silver bullet exists 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

↑ 141%
YoY increase in records exposed through data breaches¹

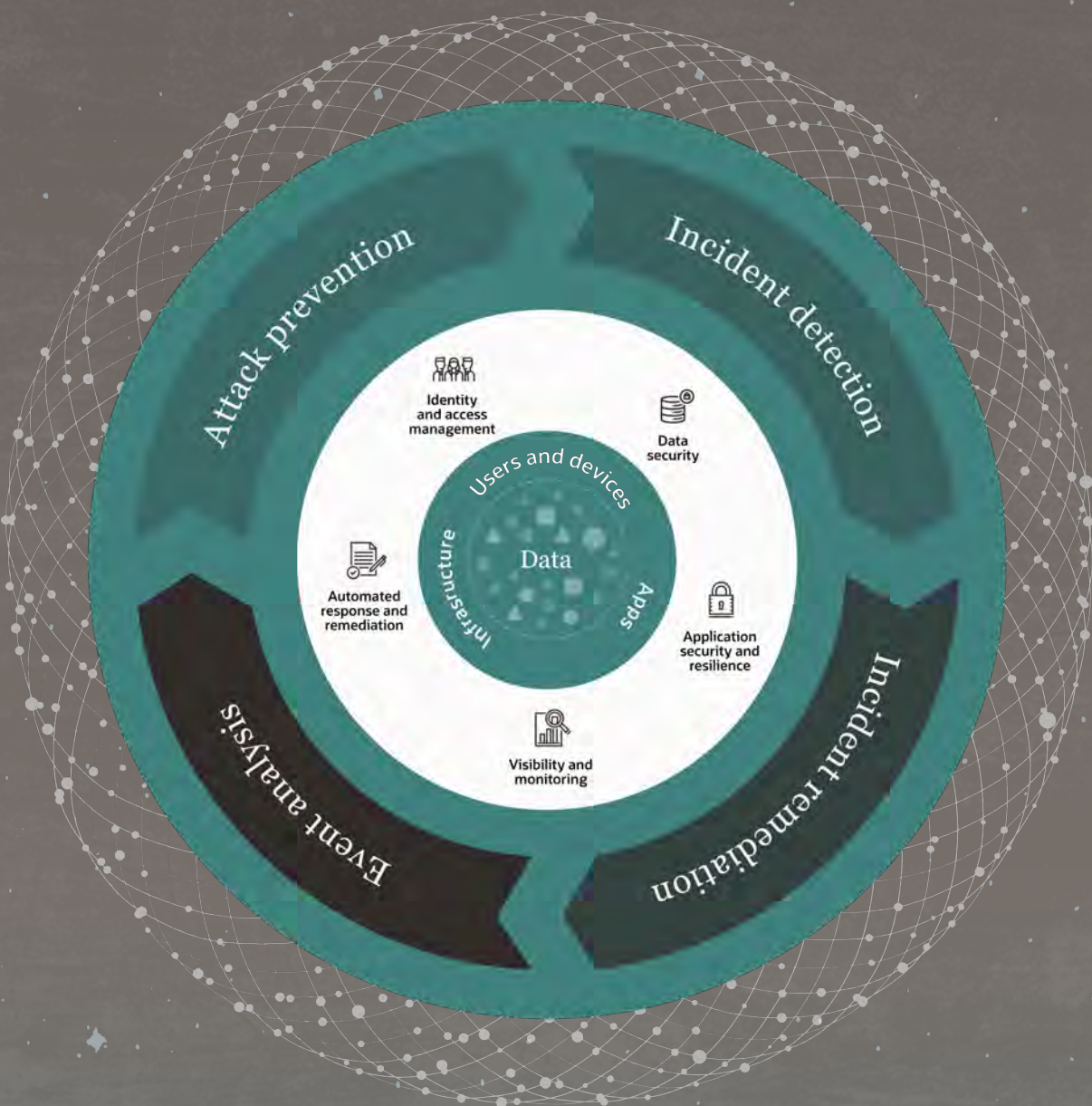
75%
Of organizations now see public clouds as more secure than on-premises systems²

€182 Million
The cumulative total of EU GDPR fines in 2020³

Full-stack protection

Oracle's layered approach provides powerful data protection solutions that defend 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 that covers your infrastructure with full-stack protection. With always-on solutions to detect threats, remediate errors and anomalies, and help protect your data from attacks, you can grow your business with confidence.



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, architected-in.



Automated

Oracle provides automated response and remediation across the full stack for effective behavioral monitoring that detects and alerts upon suspicious activity, while reducing the risk of human error.



Always-on

Oracle's security first approach includes always-on encryption, both at rest and in-motion, in Oracle Cloud and Oracle Autonomous Database. Organizations can be confident in seamless protection with continuous security posture management and vulnerability scanning.



Architected-in

Oracle Cloud security solutions are fully integrated and often offered free of charge. Security-first design principles mean security and performance are both maximized, without the need for complex installations or deployments.

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.

To learn more about Oracle Security, read our eBook **Putting Data Security and Protection First**

[Learn more](#)

¹ <https://www.riskbasedsecurity.com/2021/01/21/new-research-no-of-records-exposed-increased-141-in-2020/#download>

² <https://www.oracle.com/cte>

³ <https://www.itgovernance.co.uk/gdpr-fines-quarterly-report>