

DATASHEET

OCI Security Assurance

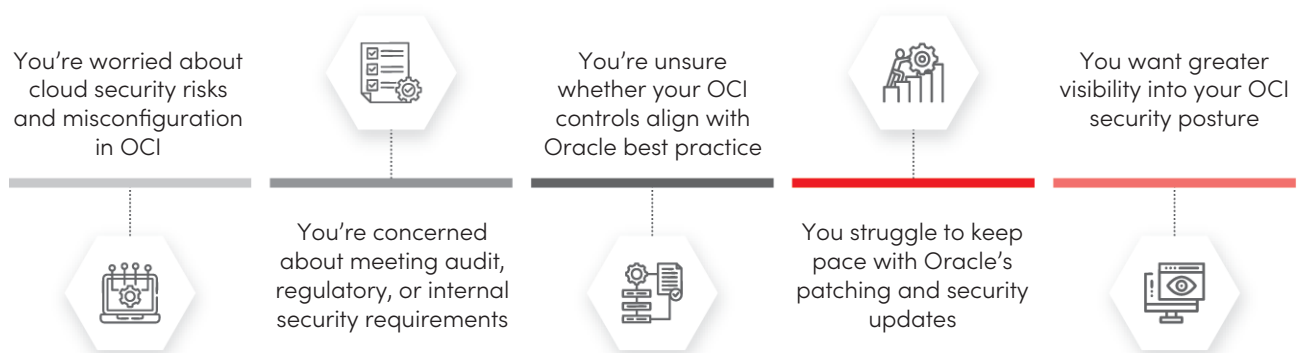
Protect your Oracle Cloud Infrastructure environment from security threats

Cloud security threats are evolving, with AI-identified vulnerability discovery and increasingly capable LLMs accelerating the pace of exploitation.

Misconfiguration remains a leading cause of security breaches. In OCI, weaknesses in identity, network design, logging or patching increase exposure to risk—leading to data loss, service disruption, regulatory penalties and extortion-related threats.

Inoapps' OCI Security Assurance is a fixed-price subscription-based service designed to assess, harden and protect your OCI tenancy. Built on Oracle cloud security best practices and Center for Internet Security (CIS) benchmarks, it delivers point-in-time assurance and ongoing security oversight—giving you confidence in your security posture and audit readiness.

If any of the following sounds familiar, then it's time to talk to Inoapps



What's included in the OCI Security Assurance service

Our service combines proactive cloud security checks, patching oversight and rapid vulnerability response to keep your OCI environment secure, compliant and resilient.

1 Annual OCI security health check

A clear, structured view of your OCI security posture. Our AI-powered security health check benchmarks your OCI tenancy against Oracle security best practices and CIS foundations, covering:

- › Identity & Access Management (IAM)
- › Compartments and tenancy structure
- › Networking and network security (VCNs, security lists, NSGs)
- › Compute, storage and database security
- › Logging, monitoring and auditing
- › Backup, recovery and high availability configuration

You receive a clear, easy-to-read report outlining:

- | | | |
|-----------------------|--|--|
| › What was reviewed | › Pass, fail or advisory status for each control | › Practical, prioritized remediation recommendations |
| › How it was assessed | | |

2 Rapid response to critical OCI security vulnerabilities

When critical vulnerabilities emerge, a timely response is essential. Inoapps will:

- Monitor relevant OCI security advisories and CVEs
- Notify you of critical issues impacting your OCI services
- Provide remediation guidance and implementation support
- Reduce exposure between scheduled reviews or patch cycles

3 CrowdStrike Falcon for enterprise-grade endpoint protection

When urgent vulnerabilities arise, speed matters. We will deploy CrowdStrike Falcon to monitor for Common Vulnerabilities and Exposures (CVEs), advise you when they are released, and apply critical patches promptly and safely, reducing your exposure to risk between scheduled updates.

4 Optional Support Packs

For flexibility when you need it, Inoapps Support Packs are available for:

- Remediation of findings from the OCI security health check
- Secure architecture reviews for new OCI workloads
- Validation of security controls prior to audits
- Configuration of logging, monitoring, and alerting

Why work with Inoapps?

Inoapps provides end-to-end OCI expertise, from secure cloud foundations to ongoing operational assurance. With deep Oracle Cloud experience, proven delivery and AI-driven automation, we help you:



Reduce cloud security risk



Demonstrate audit-ready OCI controls



Protect critical workloads and data



Operate OCI securely and confidently

Ready to strengthen your OCI security posture?

Talk to our experts today and take the first step toward a more secure Oracle Cloud Infrastructure environment.

ORACLE

2025 Oracle Partner Awards

WINNER

Global Certified Managed Services Provider Award



CONNECT WITH US

Email askinoapps@inoapps.com, or find your local office at inoapps.com/contact

 inoapps.com/insights/tag/blogs

 linkedin.com/inoapps

ORACLE | Partner

www.inoapps.com