

Cloud Security Assessment

As more organizations migrate to the cloud or adopt fully cloud-native models, their threat landscape evolves accordingly. For these organizations, traditional asset-specific penetration testing provides limited insights, focused on the self-managed infrastructure (IaaS). In contrast, cloud-first SaaS and PaaS models often shift certain security responsibilities and controls to the Cloud Service Provider (CSP) under the shared responsibility model.

Bitdefender offers a comprehensive Cloud Security Assessment, where our specialists analyse the client's cloud environment for misconfigurations that attackers could potentially exploit. This exercise identifies non-compliant or insecure configurations, and strengthens the overall security posture of the cloud environment. Additionally, the assessment highlights any operational gaps in the organization's management processes that may contribute to misconfigurations.

Our team of skilled consultants brings extensive experience in cloud security across a wide range of Cloud Service Providers (CSP). Leveraging Bitdefender's in-house cloud security posture management tool (GravityZone CSPM+), we perform automated scans aligned with industry best practices and leading global compliance frameworks.

Engagement Lifecycle

- ↳ **Scoping:** Bitdefender works with their clients to understand the size of their cloud environment, including but not limited to the CSPs in use, the number of cloud workloads, the number of IAM users/roles and the number of storage buckets.
- ↳ **Deployment:** Depending on the scope of the assessment, Bitdefender may deploy CSPM+ within the in-scope CSPs during this stage, before the assessment phase
- ↳ **Assessment:** Bitdefender will perform a combination of automated and manual security configuration reviews against the in-scope cloud resources in the following domains:
 - ↳ Identity and access management
 - ↳ Logging & monitoring
 - ↳ Data encryption & protection
 - ↳ Infrastructure security

Additionally, Bitdefender consultants will conduct interviews with relevant stakeholders to understand the organizational context for the cloud deployment.

Once the initial report has been generated, Bitdefender consultants will walk the relevant client teams through the findings and the

At-a-Glance

We conduct a thorough analysis of the client's cloud environment to identify misconfigurations that attackers could potentially exploit. The objective is to detect non-compliant or insecure configurations that may expose the organisation to risk.

This comprehensive assessment evaluates both technical and administrative controls, exposing potential gaps and providing a holistic view of the organisation's cloud security posture. Our approach combines both automated scanning with targeted manual techniques to ensure depth, accuracy, and actionable insights.

Key Benefits

- ↳ Boost in overall cloud security posture
- ↳ Results from the assessment are contextualised to the organisation
- ↳ Reduce the likelihood of a system breach or data leak
- ↳ Provide actionable insights and recommendations to increase security posture of the cloud environment
- ↳ Provide holistic insights at an environmental level as opposed to simply listing the security weaknesses for an individual network asset

recommended remediation actions.

- ↳ **Follow-up:** Once the remediation is complete, Bitdefender can perform a follow-up review to verify that the findings have been suitably remediated.

The Bitdefender Difference

- ↳ **Expertise:** Our consultants pair their offensive and cloud security expertise to provide in-depth insights on the broader context of the impact from security misconfigurations
- ↳ **Customer Focus:** Not all environments are the same. For these reasons, Bitdefender's commitment to customer focus means contextualising recommendations according to organizational needs.
- ↳ **Cutting Edge Technology:** Where deployable, Bitdefender is able to use our internal market leading CSPM tool, CSPM+, to perform automated scanning to augment the manual review efforts of the consultants.