CLOUDGUARD

# Microsoft Sentinel Health Check

Maximise security performance and optimise costs with comprehensive analysis and expert recommendations

Microsoft Solutions Partner
Security

## Service Overview

Microsoft Sentinel is essential for securing your business, people, customers, and data. However, like any service, it demands regular maintenance and optimisation for peak performance. While it offers insights through Health and Audit tables, expert analysis is crucial as they only reveal part of the picture. Customised elements like analytical rules, playbooks, and connectors often go unassessed, highlighting the need for a comprehensive review.

## Capabilities

The CloudGuard Microsoft Sentinel Health Check provides in-depth evaluation of your Microsoft Sentinel environment, including Entra/Active Directory integration, connector health, analytical rules, and Microsoft Defender settings. We offer detailed reports and expert recommendations to optimise performance and security, ensuring your Sentinel instance operates at its best to protect your business and data.

## Benefits

Regularly reviewing Microsoft Sentinel performance is crucial for maintaining strong cybersecurity measures. By analysing performance metrics and identifying areas for improvement, businesses can mitigate risks effectively and protect critical assets against evolving threats. This service offers:

- Improved security posture with thorough analysis
- Advanced performance with optimisation strategies
- Comprehensive insights into your Sentinel ecosystem
- Tailored recommendations for optimal setup and operation
- Operational cost savings through fine tuning and best practice

**CloudGuard ®**
www.cloudguard.ai | hello@cloudguard.ai | +44 (0) 161 504 3313


Classification: Unrestricted
Version: cg_mshc/a/en/r1

CLOUDGUARD

## Sentinel Health Check

CloudGuard will complete a full analysis of security elements that are connected to your Microsoft Sentinel instance. The Health Check objectives are:

- Summarise the connected Entra/Active Directory connected services and their identified health
- Identify the Microsoft licenses present and reported in Entra/AD
- Identify Entra/AD users
- Identify key User Settings, Conditional Access Policies
- Identify Group Settings
- Identify App Registrations
- Identify External Identities and Federations
- Identify Configured Identity Providers
- Review configuration of Sentinel Connectors and associated Health status
- Review Log Analytics configuration and consumption attributes
- Review Log Analytics workspaces
- Review Microsoft Defender connector and settings
- Sentinel Use Cases and Audit performance

## Microsoft Defender Health

If your business deploys Microsoft Defender solutions, our Health Check offers in-depth analysis of optimal configuration settings. We prioritise integrated Defender services to ensure comprehensive protection across all business security domains. Our assessment aims to identify essential settings and alerts that contribute to Microsoft Sentinel's effectiveness.

- Microsoft Defender for Endpoint vulnerability management
- Microsoft Defender 365 Email and Collaboration
- Microsoft Defender for Cloud (last 30 days)
- Microsoft Defender XDR
- Microsoft Defender for Cloud Apps (last 30 days)

## Microsoft Entra/Active Directory Health

Microsoft Sentinel heavily relies on the health of Microsoft Entra (formerly Active Directory), which is a critical dependency. Despite assumptions of seamless functionality, issues often lurk beneath the surface. For instance, conflicting conditional access policies or overridden Multi-Factor Authentication settings may leave your users vulnerable. Our Health Check aims to identify inactive or suboptimal security policies, ensuring adherence to best practices and improving overall defence.

CLOUDGUARD

ASSESS

## Cost Optimisation

Microsoft Sentinel uses the Fusion AI database for Log Analytics. There are 3 types of log storage providing different capabilities and cost levels.

| Sentinel Logs | Features | Retention Default | Analytics Enabled | Cost |
|---|---|---|---|---|
| Basic | Only basic logs | 5 days | None | Low |
| Analytical | All logs | 90 days | All configured | High |
| Archive | All logs | By policy | By policy/query | Lowest |

CloudGuard will work with you to understand key factors that accelerate Log Analytics cost optimisation:

- Custom table ingestion strategies for non-critical log sources
- Base retention period for Log Analytics data
- Log Analytics archive strategy
- Workspace ingestion configuration
- Analytical query and reporting requirements
- Logic Apps connected and executed

## CloudGuard Health Check Health Report

The CloudGuard report details the output from our comprehensive health checks, presenting it as a structured report with expert recommendations. We will guide you through this report in a feedback session, ensuring clarity and understanding in all areas. Optional follow-on services are available to implement these recommendations if you need support in those areas. This is separate from the Health Check service.

## About CloudGuard®

CloudGuard is a leading Managed Security Services Provider (MSSP), offering a range of services to protect organisations against evolving cyber threats. With a focus on proactive threat detection, automated response, and responsive support, CloudGuard helps businesses to navigate the complexities of the digital landscape securely.

Contact Us