

# Cloud Scanner of Death

Version 1.5

## Professional Cloud Security Assessment Tool

# USER MANUAL

Death's Head Software

Copyright © 2025

Generated: 2025-11-14

---

## Table of Contents

1. <a href="#">Introduction</a> .....	3
2. <a href="#">System Requirements</a> .....	4
3. <a href="#">Installation</a> .....	5
4. <a href="#">Getting Started</a> .....	6
5. <a href="#">User Interface Overview</a> .....	7
6. <a href="#">Cloud Configuration</a> .....	9
7. <a href="#">Running Scans</a> .....	11
8. <a href="#">Understanding Results</a> .....	13
9. <a href="#">Compliance &amp; Reporting</a> .....	15
10. <a href="#">Advanced Features</a> .....	17
11. <a href="#">Troubleshooting</a> .....	19
12. <a href="#">Best Practices</a> .....	20
13. <a href="#">Legal &amp; Compliance</a> .....	21

---

## 1. Introduction

### 1.1 About Cloud Scanner of Death

Cloud Scanner of Death is a professional-grade cloud security assessment tool designed to identify vulnerabilities, misconfigurations, and compliance issues across AWS, Azure, and Google Cloud Platform (GCP) environments. The tool provides comprehensive security scanning with detailed reporting and remediation guidance.

## 1.2 Key Features

- Multi-cloud support (AWS, Azure, GCP)
- Comprehensive vulnerability database with 100+ checks across 10 categories
  - Region-specific scanning across all major cloud regions
  - Real-time API scanning of live cloud infrastructure
  - Historical scan tracking and comparison
- Compliance framework mapping (PCI-DSS, HIPAA, SOC2)
  - Multiple export formats (JSON, HTML, TXT)
- Professional reporting with detailed remediation steps
  - Dark mode UI support
- Customizable scan categories (IAM, Encryption, Network, Storage, Logging, Secrets, Container, Serverless, OWASP, API)

## 1.3 Important Notice

**WARNING:** This tool is designed for authorized security testing only. Always obtain proper authorization before scanning cloud infrastructure. Unauthorized scanning may violate laws and cloud provider terms of service.

---

# 2. System Requirements

## 2.1 Minimum Requirements

Component	Requirement
Operating System	Windows 10 or Windows 11 (64-bit)
RAM	4 GB minimum (8 GB recommended)
Disk Space	500 MB for application and database
Display	1280x720 minimum resolution
Network	Internet connection for cloud API access

## 2.2 Required Dependencies

**No additional installation required!** The standalone executable includes all necessary dependencies bundled within the application.

The following libraries are pre-installed in the executable:

- PyQt6 - User interface framework
- SQLite3 - Database for scan history
- Core Python libraries - For all functionality

**Cloud SDK Support:** The executable includes boto3 (AWS), Azure SDK, and Google Cloud SDK. No additional installation is needed for live API scanning.

**Note:** For developers who want to run from source code, see the Advanced section for Python requirements.

---

## 3. Installation

### 3.1 Installing Cloud Scanner of Death

Cloud Scanner of Death is distributed as a Windows installer package that handles all installation tasks automatically. The installer:

- Installs the application to your chosen location (default: C:\Program Files\Cloud Scanner of Death)
  - Creates Start Menu shortcuts for easy access
  - Optionally creates a Desktop shortcut
- Includes all required dependencies (no additional software needed)
- Registers the application with Windows for proper uninstallation

### 3.2 Installation Steps

1. Download the CloudScannerOfDeath\_Setup.exe installer
2. Double-click the installer to begin
3. If prompted by Windows SmartScreen, click 'More info' then 'Run anyway'
4. Review and accept the license agreement
5. Choose installation location (default recommended: C:\Program Files\Cloud Scanner of Death)
6. Select additional tasks: Desktop shortcut (recommended), Start Menu folder
7. Click 'Install' to begin installation
8. Wait for the installer to complete (typically 30-60 seconds)
9. Optionally launch the application when the installer finishes

**Note:** Administrator privileges are required to install to the default Program Files location. If you don't have admin rights, choose a location in your user folder during installation.

### 3.3 Windows Security and Antivirus

**IMPORTANT:** Windows Defender and other antivirus software may flag the installer or application as potentially unwanted due to its security scanning capabilities. This is a false positive.

### **If Windows SmartScreen blocks the installer:**

1. Click 'More info' in the Windows SmartScreen popup
2. Click 'Run anyway' to proceed with installation

### **If your antivirus quarantines the installer or application:**

1. Restore the file from quarantine
2. Add an exclusion for the installation folder (usually C:\Program Files\Cloud Scanner of Death)
3. Re-run the installer if needed

**To add a Windows Defender exclusion:** • Open Windows Security → Virus & threat protection → Manage settings

- Scroll to Exclusions → Add or remove exclusions
  - Click 'Add an exclusion' → Choose 'Folder'
- Select C:\Program Files\Cloud Scanner of Death

## 3.4 First Launch

After installation completes, launch the application from:

- Desktop shortcut (if you selected this option during installation)
  - Start Menu → Cloud Scanner of Death
  - Or directly from the installation folder

Upon first launch, the application will:

- Display a splash screen with the Death's Head Software branding
  - Initialize the scan history database
- Verify cloud SDK availability (all bundled in the installation)
  - Display the main application window ready for use

## 3.5 Application Data Location

The installer creates the following structure:

Location	Contents
C:\Program Files\Cloud Scanner of Death	Application executable and program files
Same folder as executable	scan_history.db (SQLite database with all scan results)
AppData\Roaming\DeathsHeadSoftware	User settings and preferences (auto-created)
Start Menu	Application shortcuts
Desktop (optional)	Application shortcut

**Note:** The scan\_history.db database is created in the installation folder on first run. This database grows over time as you save scans. Settings and window preferences are stored separately in your Windows user profile.

## 3.6 Uninstalling

To uninstall Cloud Scanner of Death:

- **Windows 10:** Settings → Apps → Apps & features → Cloud Scanner of Death → Uninstall
- **Windows 11:** Settings → Apps → Installed apps → Cloud Scanner of Death → Uninstall
- **Or use:** Control Panel → Programs → Uninstall a program

**Note:** Uninstalling removes the application but preserves your scan\_history.db database file. If you want to completely remove all data, manually delete the C:\Program Files\Cloud Scanner of Death folder after uninstalling.

---

# 4. Getting Started

## 4.1 Launching the Application

After installation, launch Cloud Scanner of Death from:

- Start Menu → Cloud Scanner of Death (recommended)
  - Desktop shortcut (if created during installation)
- Installation folder: C:\Program Files\Cloud Scanner of Death\cloud\_scanner\_of\_death.exe

## 4.2 First Launch

When you first launch Cloud Scanner of Death, you'll see a splash screen followed by the main application window. The interface is divided into several key areas:

- Menu bar with File, Edit, View, Tools, and Help menus
- Cloud Scan Configuration panel for selecting providers and categories
- Tabbed interface for Findings, History, Compliance, Configuration, and Reports
  - Console output panel for verbose logging
  - Status bar showing current operation status

## 4.3 Quick Start Guide

To perform your first scan:

1. Select a cloud provider from the dropdown (AWS, Azure, GCP, or Multi-Cloud)
2. Choose a region or select 'All Regions' for comprehensive scanning
3. Select the categories to scan (IAM, Encryption, Network, Storage, Logging, Secrets, Container, Serverless, OWASP, API)
4. Click 'Start Cloud Scan'

- 5. Monitor progress in the console output panel
  - 6. Review findings in the Security Findings tab when complete
- 

# 5. User Interface Overview

## 5.1 Menu Bar

### File Menu:

Menu Item	Shortcut	Description
New Scan	Ctrl+N	Clear results and prepare for a new scan
Export	Ctrl+E	Export results to JSON, HTML, or TXT
Exit	Ctrl+Q	Close the application

### Edit Menu:

Standard editing operations (Undo, Redo, Cut, Copy, Paste, Select All) for text fields and console output.

### View Menu:

**Toggle Dark Mode** - Switch between light and dark themes for comfortable viewing in different lighting conditions.

### Tools Menu:

- **Cloud Credentials** - Configure API credentials for live scanning
- **Compare Scans** - Compare two historical scans to track changes

### Help Menu:

- **User Guide** - Quick reference guide
- **About** - Application version and copyright information

## 5.2 Main Tabs

Tab	Description
Security Findings	Displays all discovered vulnerabilities with severity, provider, location, and compliance information
Scan History	Shows historical scans with comparison capabilities
Compliance	Breakdown of findings by compliance framework (PCI-DSS, HIPAA, SOC2)
Configuration	Cloud provider credential management
Reports	Detailed text-based security report with all findings and remediation steps

---

# 6. Cloud Configuration

## 6.1 Cloud API Scanning

Cloud Scanner of Death connects directly to cloud provider APIs to perform real-time security assessments of your infrastructure. The application includes all necessary cloud SDKs (boto3 for AWS, Azure SDK, and Google Cloud SDK) bundled within the executable.

To perform scans, you'll need to configure credentials for the cloud providers you want to assess. The scanner requires read-only permissions to examine resources without making any changes to your cloud environment.

## 6.2 Configuring AWS Credentials

To scan AWS resources, navigate to the Configuration tab and enter:

- **Access Key ID** - Your AWS access key (e.g., AKIAIOSFODNN7EXAMPLE)
- **Secret Access Key** - Your AWS secret key
- **Default Region** - The primary AWS region to scan (e.g., us-east-1)

**Note:** The IAM user or role associated with these credentials must have read-only permissions for the services being scanned (EC2, S3, RDS, IAM, CloudTrail, etc.).

## 6.3 Configuring Azure Credentials

Azure authentication uses DefaultAzureCredential, which supports multiple authentication methods. Enter your Subscription ID in the Configuration tab. The tool will use your Azure CLI credentials or environment variables for authentication.

**Subscription ID:** Your Azure subscription GUID

## Azure AD/Entra ID Service Principal Authentication

For programmatic access and automated scanning, Cloud Scanner of Death supports Azure AD (now called Microsoft Entra ID) service principal authentication. This method provides more granular control over permissions and is recommended for production scanning environments.

To use service principal authentication, you'll need to create an App Registration in Azure AD/Entra ID and configure the following credentials in the Configuration tab:

- **Client ID (Application ID)** - The unique identifier for your Azure AD application registration (e.g., 12345678-1234-1234-1234-123456789012)
- **Client Secret** - The secret key generated for your application (also called Application Secret)

- **Tenant ID** - Your Azure AD tenant identifier (Directory ID)

These credentials enable the scanner to authenticate against Azure Graph API and Azure Resource Manager APIs to enumerate and assess resources across your Azure subscriptions. The service principal must be assigned appropriate read-only roles (such as Reader or Security Reader) at the subscription or resource group level.

**Required Permissions:**

- Reader role for resource enumeration
- Security Reader role for security-specific assessments
- Microsoft Graph API permissions for Azure AD user and policy checks

**Note:** When using service principal authentication, set the `AZURE_CLIENT_ID`, `AZURE_CLIENT_SECRET`, and `AZURE_TENANT_ID` environment variables, or enter them in the Configuration tab. The tool will prioritize service principal credentials over `DefaultAzureCredential` when these are provided.

## 6.4 Configuring GCP Credentials

GCP authentication requires a service account with appropriate permissions. Enter your Project ID in the Configuration tab. Ensure the `GOOGLE_APPLICATION_CREDENTIALS` environment variable points to your service account key JSON file.

**Project ID:** Your GCP project identifier

## 6.5 Credential Security

**IMPORTANT:** Credentials are stored in memory only during the application session. They are NOT saved to disk. You must re-enter credentials each time you launch the application. This design prevents credential exposure through saved configuration files.

---

# 7. Running Scans

## 7.1 Selecting Scan Scope

### Cloud Provider Selection:

- **AWS** - Scan Amazon Web Services only
- **Azure** - Scan Microsoft Azure only
- **GCP** - Scan Google Cloud Platform only
- **Multi-Cloud (All)** - Scan all three providers in a single operation



## Region Selection:

Choose between 'All Regions' for comprehensive coverage or select a specific region. The tool supports all commercial AWS regions (33+), Azure regions (75+), and GCP regions (40+).

**Note:** Scanning all regions increases scan time proportionally to the number of regions and categories selected.

## Category Selection:

Category	Description	Typical Checks
IAM	Identity & Access Management	MFA status, credential age, permission policies
Encryption	Data Encryption	Encryption at rest, TDE, encryption keys
Network	Network Configuration	Security groups, firewalls, open ports, VPC settings
Storage	Storage Security	Public access, versioning, logging
Logging	Logging & Monitoring	CloudTrail, activity logs, audit logs
Secrets	Secrets Management	Hardcoded credentials, exposed API keys, secret rotation
Container	Container Security	Image vulnerabilities, registry access, runtime configs
Serverless	Serverless Security	Function permissions, execution roles, environment variables
OWASP	OWASP Top 10	Injection flaws, broken authentication, security misconfigs
API	API Security	Authentication, rate limiting, input validation, endpoints

## 7.2 Starting a Scan

Once you've configured your scan parameters:

1. Click 'Start Cloud Scan' button
2. Monitor progress via the progress bar and status messages
3. Review findings as they appear in real-time in the Security Findings tab
4. Wait for scan completion (indicated by 'Scan complete' message)
5. Review the generated report in the Reports tab

## 7.3 Stopping a Scan

You can stop a running scan at any time by clicking the 'Stop Scan' button. The application will gracefully terminate the scan operation and preserve any findings discovered up to that point. Stopped scans are not automatically saved to history.

## 7.4 Multiple Scans

When starting a new scan with existing results, the application will prompt you to:

- Clear previous results, or
- Append new findings to existing results

Appending results allows you to combine findings from multiple scans into a single report.

---

## 8. Understanding Results

### 8.1 Severity Levels

Severity	Color	Description	Action Required
CRITICAL	Red	Immediate security risk requiring urgent attention	Fix within 24 hours
HIGH	Orange	Significant security risk that should be addressed promptly	Fix within 1 week
MEDIUM	Yellow	Moderate security concern requiring attention	Fix within 1 month
LOW	Green	Minor security issue or best practice violation	Fix as resources permit

### 8.2 Finding Details

Each finding includes comprehensive information:

- **Title** - Brief description of the vulnerability
- **Severity** - Risk level (CRITICAL, HIGH, MEDIUM, LOW)
  - **Cloud Provider** - AWS, Azure, or GCP
  - **Location** - Region where the resource was found
  - **IP Address** - Associated IP address (if applicable)
- **Category** - Security domain (IAM, Encryption, Network, etc.)
  - **Resource ID** - Identifier of the affected resource
  - **Resource Type** - Type of cloud resource
  - **Description** - Detailed explanation of the issue
  - **Remediation** - Step-by-step fix instructions
- **Compliance Frameworks** - Relevant standards (PCI-DSS, HIPAA, SOC2)

### 8.3 Viewing Finding Details

Double-click any finding in the Security Findings table to view complete details in a popup dialog. This includes the full description and remediation steps.

### 8.4 Filtering and Sorting

Click on column headers in the Security Findings table to sort by that field. You can sort by severity, provider, location, or any other column to organize findings according to your priorities.

# 9. Compliance & Reporting

## 9.1 Compliance Framework Mapping

Cloud Scanner of Death maps findings to three major compliance frameworks:

Framework	Focus	Key Requirements
PCI-DSS	Payment Card Industry Data Security Standard	Data encryption, access controls, monitoring
HIPAA	Health Insurance Portability and Accountability Act	PHI protection, encryption, audit logs
SOC2	Service Organization Control 2	Security, availability, confidentiality

## 9.2 Compliance Tab

The Compliance tab provides a summary of findings organized by framework. This view helps prioritize remediation efforts based on your organization's compliance obligations.

The table shows the count of CRITICAL, HIGH, and MEDIUM findings for each framework, allowing you to quickly assess compliance gaps.

## 9.3 Exporting Reports

Export findings in multiple formats using File > Export or Ctrl+E:

Format	Use Case	Contents
JSON	API integration, automation, further processing	Complete structured data with all fields
HTML	Executive presentations, web viewing	Professional formatted report with color coding
TXT	Documentation, audit trails	Plain text report with all findings and remediation

## 9.4 Report Sections

All exported reports include:

- **Executive Summary** - Total findings by severity
  - **Target Account Information** - Scanned cloud accounts
    - **Compliance Mapping** - Findings by framework
  - **Detailed Findings** - Complete vulnerability details grouped by severity
  - **Remediation Guidance** - Step-by-step fix instructions
- 

# 10. Advanced Features

## 10.1 Scan History

All completed scans are automatically saved to the scan\_history.db database. The Scan History tab displays previous scans with key metrics:

- **Scan ID** - Unique timestamp-based identifier
- **Scan Date** - When the scan was performed
  - **Providers** - Cloud platforms scanned
- **Total Findings** - Number of vulnerabilities discovered
  - **Critical/High Counts** - Count of severe findings
  - **Risk Score** - Calculated risk metric (0-100)

## 10.2 Loading Historical Scans

Double-click any scan in the history to load its findings into the current view. This allows you to review past results without re-running scans.

## 10.3 Scan Comparison

Compare two historical scans to track security posture changes over time:

1. Navigate to the Scan History tab
2. Select two scans by clicking on their rows (hold Ctrl to select multiple)
3. Click 'Compare Selected' button
4. Review the comparison showing new, resolved, and unchanged findings

Scan comparison helps identify:

- New vulnerabilities introduced since the last scan
  - Successfully remediated issues
- Persistent security problems requiring attention

## 10.4 Multi-Region Scanning

When 'All Regions' is selected, the scanner performs comprehensive coverage across:

- AWS: 33+ commercial regions
- Azure: 75+ regions including sovereign clouds
- GCP: 40+ regions worldwide

**Note:** All Regions scans can take significantly longer but provide complete coverage. Consider limiting to specific regions for routine scans.

## 10.5 Console Output

The Console Output panel provides verbose logging of all operations. Use this for:

- Monitoring scan progress in real-time
- Debugging credential or connection issues
- Tracking which regions and categories are being scanned
- Reviewing application events and status changes

Console output can be copied for troubleshooting or documentation purposes.

---

# 11. Troubleshooting

## 11.1 Common Issues

### Issue: Installer won't run - Windows SmartScreen blocks it

**Symptom:** 'Windows protected your PC' message when trying to run CloudScannerOfDeath\_Setup.exe.

**Solution:** Click 'More info' and then 'Run anyway'. This is a false positive. The installer is digitally packaged and safe to run.

### Issue: Installation requires administrator privileges

**Symptom:** Installer prompts for administrator password or fails to install to Program Files.

**Solution:** Right-click the installer and choose 'Run as administrator'. If you don't have admin rights, choose a custom installation location in your user folder (e.g., C:\Users\YourName\CloudScanner) during installation.

### Issue: Antivirus deletes or quarantines the installer

**Symptom:** The installer file disappears after download or during installation.

**Solution:** This is a false positive. Restore the file from quarantine and add an exception in your antivirus for the C:\Program Files\Cloud Scanner of Death folder before installing.

## Issue: Application won't launch after installation

**Symptom:** Double-clicking the shortcut does nothing or shows an error.

**Solution:** Check if antivirus quarantined the .exe after installation. Add C:\Program Files\Cloud Scanner of Death to your antivirus exclusions, then run the installer's Repair option from Add/Remove Programs.

## Issue: Slow first launch

**Symptom:** Application takes longer than expected to start the first time.

**Solution:** First launch initializes the database and settings, which takes a moment. Subsequent launches will be faster. If consistently slow, check if antivirus is scanning the application on every launch.

## Issue: SDK Not Found

**Symptom:** Dialog on startup indicating missing cloud SDKs (rare with installed version).

**Solution:** All SDKs are bundled in the installation. If this message appears, the installation may be corrupted. Repair or reinstall the application from Add/Remove Programs, or download fresh from the official source.

## Issue: Authentication Errors

**Symptom:** Error messages related to credentials or access denied.

**Solution:** Verify credentials in the Configuration tab. Ensure the IAM user/role has appropriate read permissions. Check that credentials are not expired.

## Issue: Slow Scan Performance

**Symptom:** Scans take excessive time to complete.

**Solution:** Consider scanning specific regions instead of 'All Regions'. Reduce the number of categories being scanned. Scanning all 10 categories across all regions can take significant time. Focus on priority categories for routine scans.

## Issue: Application Crashes During Scan

**Symptom:** Application closes unexpectedly while scanning.

**Solution:** Ensure sufficient system resources (RAM). Check console output for error messages before crash. Try scanning a smaller scope (single provider, specific region).

# 11.2 Getting Support

For additional assistance:

- Review console output for detailed error messages
  - Check the GitHub repository for known issues
    - Ensure you're using the latest version
  - Contact Death's Head Software support
- 

# 12. Best Practices

## 12.1 Scanning Recommendations

1. Schedule regular scans (weekly or monthly) to maintain security posture
2. Test the scanner in a non-production environment before scanning production
3. Use specific regions for routine scans, All Regions for comprehensive audits
4. Always obtain authorization before scanning production environments
5. Create read-only IAM roles/users specifically for scanning purposes
6. Review and act on CRITICAL and HIGH findings immediately
7. Track progress using scan comparison features
8. Export and archive scan results for compliance documentation

## 12.2 Security Considerations

Follow these security practices when using the scanner:

- Never share or commit credentials to version control
- Use least-privilege access for scanning credentials
  - Rotate scanning credentials regularly
- Scan from secure, controlled environments
- Protect exported reports containing sensitive information
  - Review findings before sharing with broader teams
- Maintain audit trails of who performed scans and when

## 12.3 Remediation Workflow

Recommended approach to addressing findings:

1. Export scan results for documentation
2. Prioritize by severity (CRITICAL first)
3. Group findings by responsible team/owner
4. Create tickets/issues for each finding or group
5. Follow provided remediation guidance

6. Verify fixes in development/staging first
  7. Re-scan to confirm issue resolution
  8. Document remediation actions for audit purposes
- 

# 13. Legal & Compliance

## 13.1 Authorized Use Only

### IMPORTANT LEGAL NOTICE:

Cloud Scanner of Death is designed for authorized security testing only. Users must obtain proper authorization before scanning any cloud infrastructure. Unauthorized scanning may:

- Violate computer fraud and abuse laws
- Breach cloud provider terms of service
- Result in account suspension or termination
  - Lead to civil or criminal liability
  - Cause service disruptions

## 13.2 Data Protection

This tool accesses and processes information about your cloud infrastructure. Users are responsible for:

- Protecting credentials and scan results
- Complying with data protection regulations (GDPR, CCPA, etc.)
  - Ensuring proper authorization for data access
- Securing exported reports containing sensitive information
- Following organizational data handling policies

## 13.3 Compliance Standards

While Cloud Scanner of Death identifies compliance-related issues, it does not guarantee compliance with any standard.

Organizations must:

- Conduct comprehensive compliance assessments beyond automated scanning
  - Engage qualified compliance professionals
- Maintain documentation of all compliance activities
  - Regularly review and update security controls
- Implement a complete security program, not just scanning

## 13.4 Disclaimer



Cloud Scanner of Death is provided 'as is' without warranty of any kind. Death's Head Software is not liable for:

- Accuracy or completeness of scan results
- Actions taken based on scan findings
- Damages resulting from use or inability to use the tool
  - Security breaches or incidents
- Compliance failures or audit findings

## 13.5 Copyright & Licensing

Copyright © 2025 Death's Head Software. All rights reserved.

This software and documentation are proprietary. Unauthorized copying, distribution, or modification is prohibited.

---

# Appendix A: For Developers - Running from Source

## A.1 Python Requirements

If you need to run Cloud Scanner of Death from Python source code (for development or modification):

**Required:**

- Python 3.8 or higher
- pip install PyQt6

**Optional (for live API scanning):**

```
pip install boto3 # AWS
pip install azure-identity azure-mgmt-compute # Azure
pip install google-cloud-compute google-cloud-storage # GCP
```

## A.2 Running from Source

```
python cloud_scanner_of_death.py
```

## A.3 Building Your Own Executable

If you modify the source and want to create a new .exe:

```
pip install pyinstaller
pyinstaller --onefile --windowed --name cloud_scanner_of_death cloud_scanner_of_death.py
```

## A.4 Creating an Installer with Inno Setup

The official distribution uses Inno Setup Compiler to create a Windows installer. To build your own:

1. Build the executable using PyInstaller (see A.3 above)
2. Download and install Inno Setup Compiler from [jrsoftware.org](http://jrsoftware.org)
3. Create an Inno Setup script (.iss file) or use the provided one
4. Configure the script with your application details
5. Compile the script to generate CloudScannerOfDeath\_Setup.exe

**Note:** The Inno Setup script should include the executable, any required DLLs, and optionally the skull.png splash screen image. It should create Start Menu shortcuts and offer a desktop shortcut option.

---

# Appendix B: Vulnerability Database

## B.1 Check Coverage

Cloud Scanner of Death includes comprehensive checks across 10 security categories covering 100+ cloud misconfigurations and vulnerabilities:

### AWS Checks:

- Root account MFA status
- IAM policy wildcard permissions
  - Access key rotation
  - RDS encryption
  - EBS encryption
- S3 bucket public access
- Security group open ports
  - CloudTrail logging
- Secrets in environment variables
- Lambda function permissions

- API Gateway authentication
- Container image vulnerabilities
  - And more...

## Azure Checks:

- MFA for admin accounts
  - VM disk encryption
- Network security group rules
- Storage account public access
  - Activity log configuration
- Key Vault secret management
  - Container registry access
- Function app authentication
  - API Management policies
  - And more...

## GCP Checks:

- Primitive role assignments
- Service account key rotation
  - Firewall rule configuration
- Storage bucket public access
  - Audit logging status
- Secret Manager configuration
  - Cloud Run service security
- Cloud Functions permissions
  - API Gateway controls
  - And more...

# B.2 Coverage by Category

Category	AWS	Azure	GCP	Total Checks
IAM	4	2	2	8
Encryption	4	2	2	8
Network	4	2	2	8
Storage	3	2	2	7
Logging	2	1	1	4
Secrets	5+	3+	3+	11+
Container	4+	3+	3+	10+
Serverless	6+	4+	4+	14+
OWASP	10+	8+	8+	26+
API	5+	4+	4+	13+

**Note:** The '+' symbol indicates categories with extensible checks that may include additional vendor-specific or framework-specific validations.

---

# Cloud Scanner of Death

## Version 1.5

**Death's Head Software**

Professional Cloud Security Solutions

For support and updates:

Visit our [GitHub repository](#)

© 2025 Death's Head Software

All rights reserved