HALOCK®

CLOUD SECURITY ASSESSMENT

Touch the sky.

The cloud is an invaluable asset, but it has underlying risks.

Majority of cloud breaches are from access-related vulnerabilities.

Most public cloud environments store some sensitive data.

Many organizations do not check the risk of their cloud service.

How Do You

Understand and prioritize risks?

Maintain business continuity?

Enable security business growth?

Cloud Covered

HALOCK's Cloud Security Assessment gives you insight on your risks. The assessment provides a review of Azure, AWS, and Google (GCP) cloud environments to identify risk and recommends how to remediate them. HALOCK combines manual analysis of these cloud platforms using the applicable CIS benchmarks combined with the Tenable Cloud Security solution. Clients receive a comprehensive look at cloud environments, allowing them to better enhance their security. HALOCK will provide analysis for the following security areas:

Identification of:

- Assets related to all user, computer, network, data, management and security resources.
- Potential toxic combinations of access privileges, non-secure configurations, and vulnerabilities.
- Accounts that are over-privileged, unused, and may pose higher risk.
- Anomalous events based on the behaviors of account usage and access.

Analysis of:

- Security events
- Logging and monitoring configuration
- Configured policies
- Deployed subscriptions and applicable configurations
- Authentication methods
- Network architecture as deployed
- Configured security center capabilities

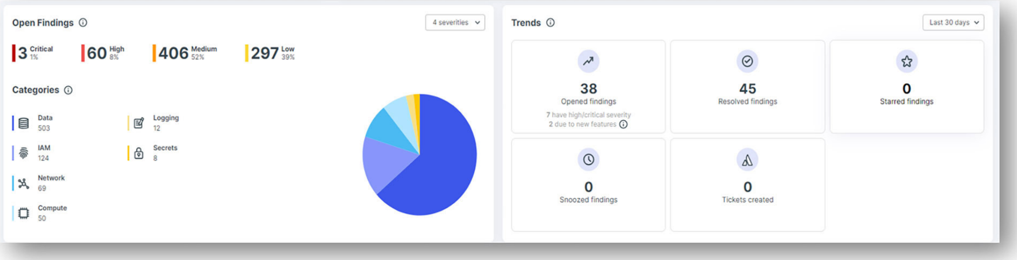
Why Choose HALOCK?

As authors of the **Duty of Care Risk Analysis (DoCRA)** Standard and developers of **CIS RAM**, HALOCK has specialized insight to guide you through a risk method to establish **reasonable** and appropriate security. ***Risk expertise like no other.***

The Methodology and Deliverables

- **Manual review** using the appropriate security benchmarks from CIS for Azure, AWS, and GCP.
- **Automated review** using Tenable Cloud Security.
- **A detailed report** with prioritized findings and recommendations to address findings.

Findings Dashboard



Open Findings ⓘ

4 severities

3 Critical 1%	60 High 8%	406 Medium 52%	297 Low 39%

Categories ⓘ

Category	Count
Data	503
IAM	124
Network	69
Compute	50
Logging	12
Secrets	8

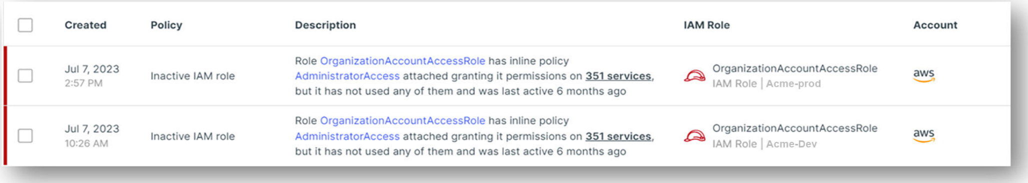
Trends ⓘ

Last 30 days

- 38 Opened findings — 7 have high/critical severity, 2 due to new features ⓘ
- 45 Resolved findings
- 0 Starred findings
- 0 Snoozed findings
- 0 Tickets created

Recommendation: Review the critical findings and remediate asap. High findings should be reviewed and assessed for applicability to the instance as a next step. Medium and lower findings should be reviewed and addressed as available.

Critical Findings

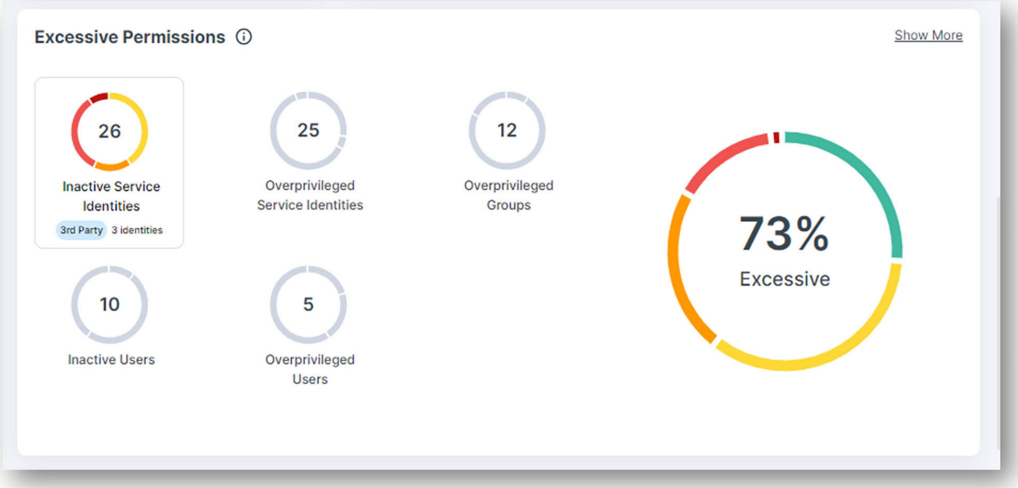


□	Created	Policy	Description	IAM Role	Account
□	Jul 7, 2023 2:57 PM	Inactive IAM role	Role OrganizationAccountAccessRole has inline policy AdministratorAccess attached granting it permissions on 351 services, but it has not used any of them and was last active 6 months ago	OrganizationAccountAccessRole IAM Role | Acme-prod	aws
□	Jul 7, 2023 10:26 AM	Inactive IAM role	Role OrganizationAccountAccessRole has inline policy AdministratorAccess attached granting it permissions on 351 services, but it has not used any of them and was last active 6 months ago	OrganizationAccountAccessRole IAM Role | Acme-Dev	aws

Recommendation: Review role CLIENT Access Role and delete if not required.

Excessive Permissions

This is a breakdown of potentially excessive permissions. The goal is to enforce the principle of least privilege in your environment. The percentage includes permissions with any severity level, and excludes used permissions (green), or permissions that are excluded from policies (gray).



Excessive Permissions ⓘ

Show More

- 26 Inactive Service Identities — 3rd Party 3 identities
- 25 Overprivileged Service Identities
- 12 Overprivileged Groups
- 10 Inactive Users
- 5 Overprivileged Users
- 73% Excessive

The details of the identities with excessive permissions are located in the "Detailed Findings" section.

Recommendation: It is a security best practice to regularly audit the accounts and applicable usage across all cloud environments.

- User accounts that are over privileged should be "right" sized.
- Accounts that are inactive should be reviewed and removed if possible.
- Groups that are over privileged should be "right" sized.
- Service accounts that are overprivileged should be "right" sized.

FINDING: Excessive Permissions

Cloud Security Assessment identifies

- Critical configuration flaws
- Inventory of cloud assets and identities
- Unused and over-privileged accounts
- Toxic combinations
- Non-secure ports and protocols in use
- Permissions on assets and services that are too permissive
- Exposed secret keys

tenable
Cloud Security