Cloud Locksmith

Microsoft 365 Identity Security Platform

Product Overview

What Cloud Locksmith Does

Cloud Locksmith is a continuous identity security platform for Microsoft 365 tenants. It connects through Microsoft Entra ID using OAuth 2.0, reads tenant configuration through Microsoft Graph in read-only mode, and surfaces identity risks that are otherwise invisible between periodic manual reviews.

Problems Solved

- MFA gaps that leave accounts protected by a password alone.
- Dormant accounts, including former employees or unused service accounts still holding active access.
- Privileged role sprawl, including excess Global Admin assignments.
- Conditional Access coverage gaps that let users or apps bypass policy.
- Configuration drift that accumulates silently between manual security reviews.

Target Customers

- SMBs on Microsoft 365 (roughly 50-300 employees) without a dedicated security function.
- Managed Service Providers managing identity posture across multiple client tenants.
- Organizations preparing for compliance reviews or cyber insurance renewals.
- Teams that need identity risk coverage before they can justify a full security hire.

Continuous Monitoring

Ongoing scans surface new identity risks as they appear, rather than only at the time of a one-off audit.

Verified Remediation

Fixes are applied only after explicit admin approval. Every remediation captures a snapshot beforehand, so changes can be rolled back in seconds if needed.

Historical Reporting

Findings and remediation history are retained so posture improvements can be tracked over time, not just viewed as a single snapshot.

License Optimization

Identifies unused or underutilized Microsoft 365 licenses to help reduce unnecessary subscription spend.

Audit Trails

Every remediation action, rollback, and privileged access event is logged for accountability and compliance review.

How Access and Data Are Protected

- OAuth 2.0 authentication via Microsoft Entra ID. Cloud Locksmith never collects or stores your Microsoft password.
- All tenant data is read through the Microsoft Graph API using delegated permissions scoped to admin consent.
- OAuth access and refresh tokens are encrypted and are never exposed to the browser.
- Tenant data is logically isolated per customer; no query spans more than one tenant.
- All remediation actions, rollbacks, and privileged access events are logged.
- Cloud Locksmith does not access email bodies, document contents, Teams messages, or calendar data. If a Microsoft Graph permission isn't documented on our Security page, we don't have it.

Full detail on data handling, infrastructure security, and our compliance roadmap is available at cloudlocksmith.co/security.

- Continuous protection: identity risk is monitored on an ongoing basis, not just at a point-in-time audit.
- Deterministic remediation: every fix is explicit, reviewable, and reversible; nothing changes in your tenant without approval.
- Insurance-ready reporting: severity-ranked findings and audit trails suitable for compliance and cyber insurance review.

Website: cloudlocksmith.co
Support: support.cloudlocksmith@gmail.com