SpyCloud

DATASHEET

IDENTITY THREAT PROTECTION

SpyCloud Identity Guardians

Automatically remediate exposed passwords and active sessions to secure corporate access

01 THE CHALLENGE

Every identity has two doors. Attackers only need one.

Workforce identities get exposed every day, through infostealer malware, successful phishing attacks, third-party breaches, and combolists. Attackers now steal more than passwords. They take sessions, cookies, refresh tokens, and other authentication artifacts — bypassing MFA or taking over authenticated access without logging in.

Passwords and sessions aren't separate identity security problems. They're different paths to the same outcome, both tied to a user's identity. Remediating a password while leaving session data intact still leaves attackers with a way in.

SpyCloud Identity Guardians remediate the full identity exposure tied to access, not just the password. By automatically resetting exposed credentials, revoking active sessions, and removing the access attackers rely on, Identity Guardians close every path into an account across the identity providers you use.

BENEFITS AT A GLANCE

Secure all access points

Automatically remediate exposed passwords and active sessions so stolen cookies or refresh tokens don't outlive a password reset.

Built for every identity environment

Whether you run one or a combination of Active Directory, Microsoft Entra ID, or Okta Workforce Identity, Identity Guardians safeguard access to your corporate environments.

Respond in minutes, not months

Malware-exposed identities trigger automated remediation in as little as five minutes after discovery.

Find identity exposures your directory can't see

Holistic identity correlation uncovers exposures tied to employees' personal accounts, not just corporate identities.

Remediate your way

Configure password resets, session revocation, account actions, and notifications based on exposure source, severity, and policy.

02 PRODUCT OVERVIEW

One automated remediation solution for your identity provider

Identity Guardians continuously monitor your workforce identities against our extensive collection of recaptured identity data from the criminal underground, surfacing exposed passwords and session data and remediating them instantly — all without compromising security or user experience.

Whether your environment is on-premises, cloud, or hybrid, there's an Identity Guardian built for your stack.

Active Directory
ON-PREMISES & HYBRID
Active Directory Guardian

Microsoft Entra ID
CLOUD
Entra ID Guardian

okta
CLOUD
Okta Workforce Guardian

5MIN
FROM DISCOVERY TO REMEDIATION FOR MALWARE-EXPOSED PASSWORDS FOR ACTIVE DIRECTORY

14x
MORE EXPOSED PASSWORDS FOUND WITH HOLISTIC IDENTITY MATCHING

1,000
PASSWORD VARIATIONS TESTED PER EXPOSED CREDENTIAL THROUGH FUZZY MATCHING

03 COVERAGE

Built to secure your identity environment

Identity Guardians keep access secure across your workforce, no matter your identity architecture or the threat.

YOUR ENVIRONMENT	IDENTITY GUARDIAN(S)
On-premises: Active Directory	Active Directory Guardian
Cloud: Microsoft-centric	Entra ID Guardian
Cloud: Okta-centric	Okta Workforce Guardian
Hybrid: Active Directory + Entra ID or Okta	Active Directory Guardian plus Entra ID Guardian and/or Okta Workforce Guardian
Multiple cloud identity providers	Entra ID Guardian and Okta Workforce Guardian

Check back often. Support for more IdPs coming soon.

04 HOW IT WORKS

Turn exposed data into closed access, automatically

SpyCloud continuously recaptures exposed identity data from the criminal underground, matches it against your monitored workforce identities, and hands off confirmed exposures to the right Identity Guardian for automated remediation — no analyst intervention required.

1

RECAPTURE

SpyCloud continuously recaptures credentials, cookies, sessions, and authentication data from malware, successful phishing attacks, third-party breaches, and combolists.

2

MATCH

SpyCloud continuously monitors workforce identities against recaptured identity data to uncover exposed credentials and stolen sessions.

3

REMEDIATE

When SpyCloud confirms an exposure, the appropriate Identity Guardian automatically resets passwords, revokes sessions, or both according to policy.

4

REPORT

SpyCloud logs every remediation action for auditing and operational visibility.

05 IMPLEMENTATION

Deployed to fit your stack

Each Identity Guardian is delivered to match how your identity provider runs, from a local application for Active Directory to cloud-native integrations for Entra ID and Okta.

PRODUCT	DELIVERY
Active Directory Guardian	Local browser-based application plus AD Password Filter.
Entra ID Guardian	Azure application installed via an ARM template. Cloud-native, no infrastructure to deploy for session capabilities.
Okta Workforce Guardian	Okta Workflows integration for credential remediation. Cloud-native, no infrastructure to deploy for session capabilities.

06 CAPABILITIES

Detect and remediate across every identity provider

Identity Guardians catch and remediate exposures two ways: through continuous monitoring, and the moment a user tries to authenticate. One policy governs remediation across Active Directory, Entra ID, and Okta.

CAPABILITY	Active Directory Guardian	Entra ID Guardian	Okta Guardian
CONTINUOUS MONITORING	**ACTIVE DIRECTORY**	**ENTRA ID**	**OKTA**
Malware, phishing, third-party breach, and combolist detection	✓	✓	✓
Exposed credential detection	✓	✓	✓
Exposed session data detection	—	✓	✓
Fuzzy matching (1,000 variations of each exposed password)	✓	—	—
Holistic identity matching (up to 14x more passwords)	✓	—	—
Shared Credential detection	✓	—	—
Configurable scan timing	✓	—	✓
AUTOMATED REMEDIATION	**ACTIVE DIRECTORY**	**ENTRA ID**	**OKTA**
Password reset	✓	✓	✓
Session revocation	✓ *	✓	✓
Block exposed passwords at creation	✓ **	—	—
Disable or suspend accounts	✓	✓	✓
Custom user notifications	✓	✓	✓
Configurable remediation policy (by exposure type, source, and severity)	✓	✓	✓
Logging and telemetry	✓	✓	✓

- *Via downstream Okta workflows (on credential matching)
- **Requires AD Password Filter installed on your domain controller

Running multiple identity providers? Identity Guardians work together under a single remediation policy to protect identities across your entire environment.

07 PRICING & REQUIREMENTS

What you need to get started

PRICING

Identity Guardians pricing depends on the number of IdPs in use, cloud IdP instances, AD domains (if applicable), plus workforce account tier.

REQUIREMENT	DETAILS
SpyCloud License	SpyCloud Workforce Threat Protection with API key.
Active Directory Guardian	Windows 10 or Windows Server 2012+, 8 GB RAM, 20 GB storage, 2 GHz processor.
AD Password Filter	Windows Server 2012+, 200 MB free disk space, installed on every domain controller.
Entra ID Guardian	Active Entra ID tenant and licensing.
Okta Workforce Guardian	Active Okta Workforce Identity license with Okta Workflows enabled.

08 THE OUTCOME

Automatically stop identity-based attacks before attackers can act

SpyCloud Identity Guardians protect the full identity, not just the password, by automatically remediating exposed credentials and stolen sessions across every identity provider you use.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions use advanced analytics and AI to accelerate investigations and protect workforce, consumer, and supplier identities from the threats that matter most: authentication bypass, session hijacking, malicious insiders, account takeover, ransomware, and fraud. Its data from malware-infected devices, successful phishes, combolists, and third-party breaches also powers many popular dark web monitoring and identity theft protection offerings. Customers include 7 of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 250 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

Remediate the full identity, not just the password

Reset exposed credentials, revoke stolen sessions, and close every path in — automatically.

SPYCLOUD.COM ›