



Disrupt your identity debt

Gathid is a lightweight identity security and access governance solution that is able to offer immediate in depth contextual visibility and control over your identities and their access rights across all on premise and cloud systems.

This allows you to take control of Identity Debt, effectively solve Access Creep and ensure business continuity through better organizational identity security.



Continuous Identity Security Posture Management

Identity is now arguably the largest attack surface for an enterprise to secure and traditional identity providers are struggling. It is becoming increasingly difficult to effectively process data from the large and disparate mix of on premise and cloud systems that organizations use today. Coupled with this traditional identity providers are expensive as well as difficult, intrusive and time intensive to deploy with limitations around role matrix implementation and mining as well as integration into legacy business application systems and platforms. The end result is that a CISO and CIO cannot be sure they have full and continuous visibility into the identity security across their entire organization.

Inspired by the power of **gathered identities** (pronounced "gathered", spelled the way an Aussie would say it), Gathid disrupts your existing identity debt, by demolishing silos, spotting identity security and access outliers, and helping you make smarter Identity security and Access decisions every day.

Gathid helps to identify and rationalize access chaos in a simple way, a must have for any Identity Governance and Administration (IGA) program. Our lightweight, cloud-based, SaaS solution maps, measures and monitors identities to systems and their access permissions, and shows where access is out of compliance, everyday.

Utilizing low risk, read-only extracts from source systems, and utilizing Gathid's patented 'relationship technology', this system creates virtual connections, linking identity and access metadata, delivering rapid cross-system context and a daily view of the access footprints of your identities from day one.

Gathid takes a new, entirely unique and super simple approach to understanding and gaining control over complex identity and access issues.

At the start of the journey

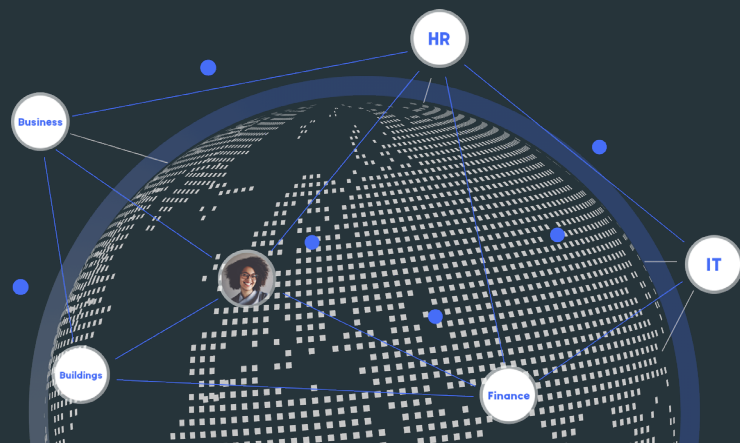
Model current identity and access posture from key systems, such as HR, AD, Azure AD / Entra and Okta etc as well as non SSO custom applications to establish 'true' identity reality.

In the middle of the journey

Review initial result, map in additional business critical systems and commence remediation to get aligned with Executive acceptable identity security risk posture baseline.

When full automation is achieved

Continuous visibility to detect deviation from Executive acceptable identity security risk posture baseline and rapidly course correct, either automatically or manually, as required to ensure ongoing compliance.



Fill gaps in traditional IAM and PAM while gaining unique identity security risk insights.

Identity access changes happen every day, companies struggle to know 'who' has 'what' levels of access across all their on premise and cloud assets opening dangerous attack pathways. Gain visibility and get in control with Gathid.

Optimize Traditional IAM and PAM

Existing IAM / PAM Validation

Continuously check that automated onboarding and offboarding via existing traditional IAM / PAM is being completed correctly.

Advanced Role Mining

Automate and amplify process of analyzing user-to-resource mapping data to determine or modify user permissions for role-based access control in an enterprise.

Advanced Role Matrix

Create, monitor & enforce role matrix scenarios for each on premise and cloud systems including those highly specialized and secure systems that do not connect to traditional IAM / PAM.

Full Coverage

Cover all on premise systems whether on premise or in the cloud including those that currently are not covered via existing traditional IAM / PAM.

Unlock Unique Cyber Insights

Correct Access

Who has been terminated in HR systems but still has access to AD and other key on prem and cloud business systems?

Full Estate Attack Pathway Visibility

Set alerts to continuously notify when advanced identity security attack paths appear which provide access to your key on prem and cloud systems.

Incident Response

Historical data is stored to allow Incident Responders to review identity security changes prior, during and after an incident.

Continuous Risk Posture Visibility & Enforcement

Executive

CISOs / CIOs can have a continuous view of identity risk posture across entire organization.

SOC & IR

Red, Blue & IR Teams can prepare to detect, defend and investigate advanced identity security risk vulnerabilities.

Risk / Governance

Simplify, expediate and expand with continuous user access reviews across all on-premise and cloud systems.

Integrate & Automate

Simple ticketing systems integration allows for identity risk to be remediated as part of normal business processes.

