

Solution Datasheet

Sharelock

for  ONE IDENTITY™

"Oh, if only we had noticed that strange change of employee activity behaviour three months ago. This was one early signal of the attack, but nobody noticed it."

Get a little help from your Identity friends !

Infuse [Sharelock Behavioral Risk Insights](#) into [One Identity Manager](#), and [enable Line of Business managers](#) to be part of your extended security team, evaluating [selected anomalous behaviors early](#) on rather than late on. [Inside the One Identity Manager UI](#) they use every day.

The Challenge

How often do you hear such a 'too late' comment after a data breach, fraud or ransomware attack?

And you'll keep hearing it [unless you start involving business people](#) and asking them to evaluate those very anomalous behaviours performed by their employees/contractors are either a business-justifiable exception [or the early signal of a downstream security situation](#).

The solution at a glance

Sharelock detects anomalous user behaviors against the individual behavioral baselines, correlate such set of anomalies against its insider threat models, and then [signals](#) to One Identity Manager [Security situations](#) (e.g. suspected account compromise, suspected data sabotage) and [Recommendations](#) for suggesting «*keep/review/revoke*» actions on specific applications.

All these risk insights are then made available inside One Identity Manager with pre-configured rules and workflows, [enabling Line Managers to act within the One Identity UI and provide](#) their valuable business contributions on such 'application related' security situations.

Solution Datasheet

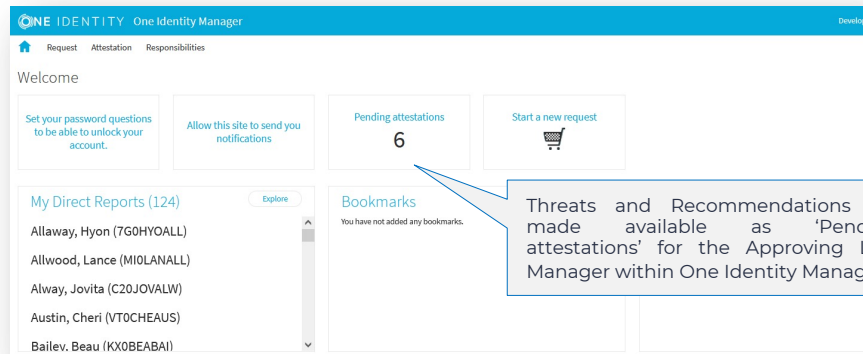
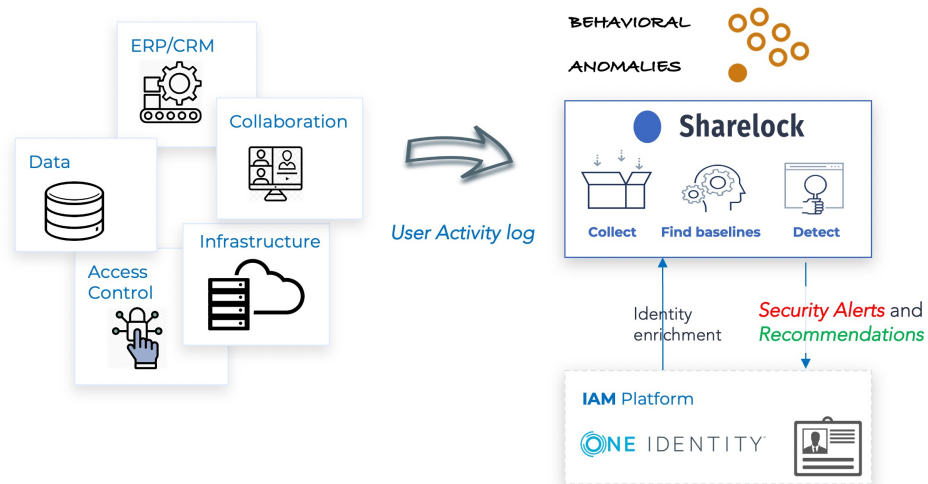
Sharelock

for **ONE IDENTITY™**

Capability overview

Sharelock delivers two types of 'signals' to One Identity Manager:

- **(Potential) Threats/Security alerts:** According to the Sharelock correlation engine, the given user has 'many' behavioral anomalies triggering a specific threat (e.g. data exfiltration attempt).
- **(Access) recommendations:** Sharelock suggests recommendations to close the gap between 'should be' vs 'as is'. Recommendations are either 'remove', 'consider revocation' or keep.



Solution Datasheet

Sharelock

for **ONE IDENTITY™**

Security Alerts

Sharelock detects **anomalous behaviors** against the predefined IoBs (Indicators of Behavior) and then **correlates multiple anomalous behaviors** for preventing threats such as compromised accounts, data exfiltration activities or other risky situations resulting from several anomalies.

Such security alerts are sent to One Identity Manager so that the Line Manager can **review** them and **investigate accordingly** in the One Identity Manager UI.

Threat Severity



ONE IDENTITY One Identity Manager

Request Attestation Responsibilities

Pending Attestations - Sharelock potential security situations

Display name	Employee	Threat Name	Threat Detected on...	Status	New	Due date	Risk index	Decision
YHRebman - Insider Threat - GDPR Compliance (10461)	Munro, Rebecca (YHREBMAN)	Insider Threat - GDPR Compliance (10461)	4/16/2021 6:03:20 PM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input type="checkbox"/>
YHRebman - Insider Threat - SOX Compliance (10021)	Munro, Rebecca (YHREBMAN)	Insider Threat - SOX Compliance (10021)	4/16/2021 5:42:33 PM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input type="checkbox"/>
YHIsayin - Insider Threat - Data Sabotage (10562)	Lynn, Tuan (YHISAYIN)	Insider Threat - Data Sabotage (10562)	4/16/2021 5:37:27 PM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input type="checkbox"/>
YSBobbell - Compromised Account (10761)	Ellingham, Bobbie (YSBOBELL)	Compromised Account (10761)	4/16/2021 5:14:22 PM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input type="checkbox"/>
YSBobbell - Compromised Account (10761)	Ellingham, Bobbie (YSBOBELL)	Compromised Account (10761)	7/26/2021 2:00:00 AM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
YSBobbell - Insider Threat - Data Sabotage (10561)	Ellingham, Bobbie (YSBOBELL)	Insider Threat - Data Sabotage (10561)	4/16/2021 5:37:25 PM	pending	Yes	No date set	1,00	<input checked="" type="checkbox"/> <input type="checkbox"/>

6 result(s)

Display name: **YSBobbell - Compromised Account (10761)** Status: **pending**

Information Workflow Attestation policy History

Threat Detected on: 7/26/2021 2:00:00 AM

Threat Description: A compromised account is an account for which someone other than the owner/delegate of the account has access to the username and password (credentials). Often, the compromised credentials are used to gain access to an email account for sending spam or phishing messages from a legitimate-looking source.

Anomalous Behaviors: DESCRIPTION: Access/VPN/Anomalous failed logins

Due date: YSBobbell - Compromised Account (10761)

Display name: YSBobbell - Compromised Account (10761)

Risk index: 1,00

Approval: pending

Attestation run: Sharelock potential security situations - 26/07/2021 15:07:43

Attestation policy: Sharelock potential security situations

[Show Details](#) [Actions](#)

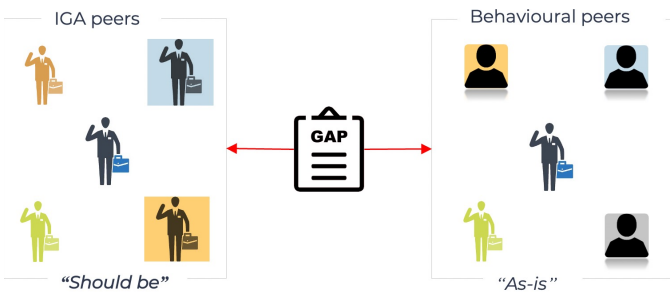
Solution Datasheet

Sharelock

for **ONE IDENTITY™**

(Access) Recommendations

Sharelock features a powerful peer-grouping analytics capability and leverages it to **provide recommendations** ('keep', 'remove', etc.) in the One Identity Manager UI. Such recommendations aim to **close the gap** between the '*should be*' state - described in One Identity Manager - and the '*as is*' state derived from actual behaviors.



Recommendations

TIMESTAMP: Apr 9 2021 09:26 PM	LAST USED (DAYS AGO) Never		
ATTRIBUTE BizApps/Homegrown app #1	AUTHORIZED Yes	USED No	AUTHORIZED IAM PEERS 100%
RECOMMENDATION Revoke	REASON Not used, nor by 68% of the IAM peers		

ONE IDENTITY One Identity Manager

Request Attestation Responsibilities

Pending Attestations - Sharelock User Account Recommendations

View Settings Search

Display name	User account	Employee	Application name...	Status	New	Due date	Risk Index	Decision
D37regou	D37regou	Gourlay, Rosario (W48R05GOU)	Data_Sharepoint	pending	Yes	No date set	0,00	☑ ☒
HK2regou	HK2regou	Gourlay, Rosario (W48R05GOU)	Collab_Cisco_Call_Min	pending	Yes	No date set	0,00	☑ ☒
rosario.gourlay@icmc.org	rosario.gourlay@icmc.org	Gourlay, Rosario (W48R05GOU)	Collab_Exchange	pending	Yes	No date set	0,00	☑ ☒

Display name: D37regou Status: pending

Information Workflow Attestation policy History

Not approved before: Yes

User account: D37regou

Employee: Gourlay, Rosario (W48R05GOU)

Application name: Data_Sharepoint

Canonical Name: D37regou

Recommendation: Consider Revocation

Reason: Not used, but used by 66% of the IAM peers

Due date: []

Display name: D37regou

Risk index: [] 0,00

Approval: pending

Attestation run: Sharelock User Account Recommendations - 17/06/2021 15:24:24

Attestation policy: Sharelock User Account Recommendations

Solution Datasheet



for  **ONE IDENTITY™**

Benefits

Zero trust risk management posture

- Achieve an 'early on' rather than 'oh too late' Zero trust security posture
- Infuse behavioral insights into One Identity Manager with the out-of-the-box integration with Sharelock.
- Enable Business users to easily provide their contributions on risky situations and recommendations

Protection of the investment

- Protect and enrich your investment with One Identity Manager.
- No change management impact, Line Managers use their everyday One Identity Manager UI and processes.
- No additional skills: the Sharelock integration package with One Identity Manager is built using standard One Identity configuration features (UI, workflows and data model extensions).

Sharelock

About us

Sharelock.ai is a leading provider of AI-powered [Identity Behavioral Insights](#) for the Zero Trust Identity architecture.

Founded by CrossIdeas Identity veterans, Sharelock bridges the gap between Identity Management and Security Intelligence, enabling [business users to prevent security risks](#) connected to anomalous user behaviors, [early on rather than 'oh, too late.'](#)

Our whereabouts

- Sharelock S.r.l.
- Via Gustavo Giovannoni 76, 00128 Rome (Italy)
- www.sharelock.ai
- info@sharelock.ai