Static, rule-based identity governance practices are a poor fit for hybrid IT environments. With static rule-based governance, users are often granted access they don’t need because the cost of lost productivity outweighs increased risk from the bigger security perimeter. Or, users may be denied access to accounts they do need, leading to access delays, frustration, and suboptimal workarounds. Enterprise users have accounts in a large number of applications and cloud environments, and privileges assigned to them tend to increase over time. Poor identity hygiene rivals hackers with malicious intent in threatening the security of hybrid environments.

Obsidian is a security solution built around protecting identity and access. Obsidian enables organizations to secure users by providing consolidated visibility and monitoring of accounts, privileges and activity for on-premises and cloud solutions. Using Obsidian, organizations can prune dormant accounts thereby reducing identity risk without impacting productivity. With a lower risk profile, organizations not only reduce the chance of a costly breach, they lower the indirect costs of ongoing security efforts. For applications that carry operational costs on a per account basis, smaller account footprints also result in direct cuts to operational budgets.

Service usage - Jul 31, 2019

<table>
<thead>
<tr>
<th>Active accounts</th>
<th>Inactive accounts</th>
<th>Total accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of accounts with some activity in the last 90 days</td>
<td>Number of accounts with no activity in the last 90 days</td>
<td>All accounts</td>
</tr>
<tr>
<td>3490</td>
<td>2370</td>
<td>5860</td>
</tr>
</tbody>
</table>

Key Features

- Visibility into active and inactive accounts across monitored services
- Support for “use it or lose it” access enforcement
- Customizable timeframe for activity analysis
- Ability to filter by services and administrative accounts
- Exportable reports for identity operations follow-up
- Automatic retrieval, storage and analysis of data from cloud services
New sales manager “Joe” joins the team and is assigned accounts on a number of applications based on organizational policy.

Joe has used Salesforce, Slack and GSuite, but has been inactive on Dropbox.

Obsidian surfaces inactive accounts in each monitored service.

Administrators can export user details and start pruning access.