Identity Security Health Assessment

Sample Report for Acme Corp

Executive Summary

Assumptions

Account takeover is a security risk for many businesses – Acme is no exception. In light of increased security threats, preventing unauthorized access to customer data and accounts is critical.

Requirements

Acme engaged with Oort to better understand the security posture of their identity population landscape, understand administrative access (including for Google Workspace), and understand if bypass codes are in use within Duo.

Results

The assessment discovered use of MFA bypass codes, lack of MFA, various inconsistencies, unused licenses, and unusual account activity. This document outlines some of the key findings and provides recommendations for the Acme team.

Overview

Platforms in scope: Okta, Azure AD, Duo, Slack, Google

Identity Snapshot

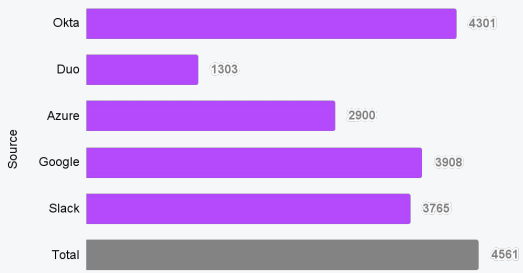
4,561
Total Identities

45 Created
12 Deprovisioned
Last 30 Days (Duo)

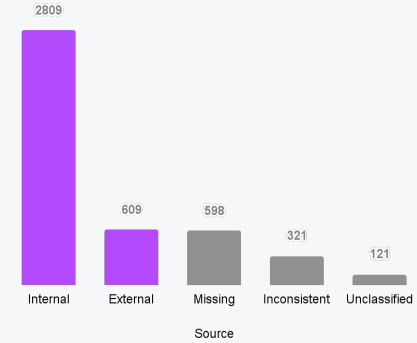
156
Administrators

12 Google Admins
65 Delegated Google Admins

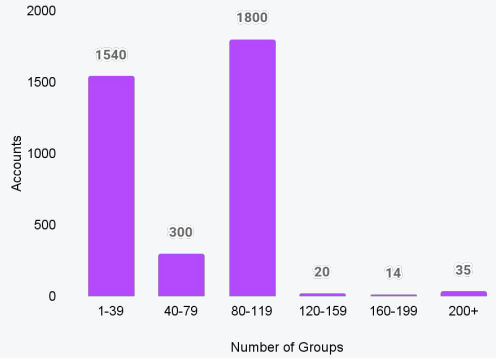
Sources



Types



Groups



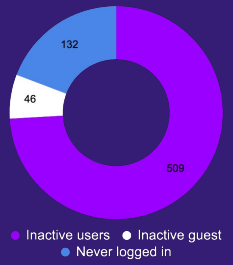
IAM Hygiene

Highlights

- Various **inconsistencies** were identified across identity platforms, indicating possible IAM hygiene issues
- Several hundred **inactive accounts** were discovered, which can present opportunities for cleaning up
- A large number of **applications are unused**, which can provide opportunities to reduce license spend

734

Inactive users and guests or Never Logged In accounts



135

Account Inconsistencies

135

Accounts with user type Missing (Okta)

147 accounts no activity in more than 180 days

170 inactive external Azure guest users

59 Slack User Inconsistencies

99 service accounts with inconsistent user type

3,797 users with unused applications (last 30 days)

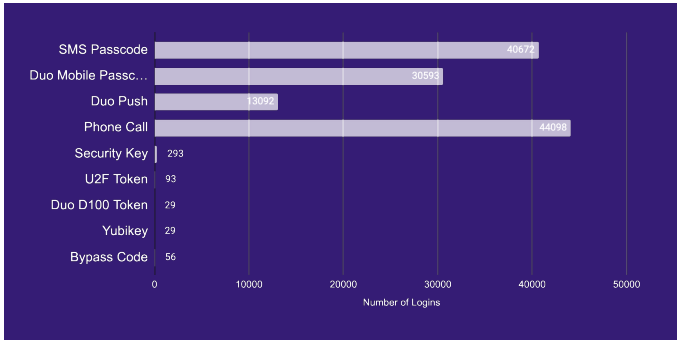
MFA Analysis

Highlights

- **Weak MFA** was used to sign in 209 times (including the CEO)
- **SMS MFA** used heavily
- In two instances, a **Duo bypass code** was used for several days
- 3 accounts appear to use the **same device** (cell number) for authentication

134
Users successfully signed in using weak MFA

6
Users successfully signed in accounts without MFA at all



504
Inactive accounts have no MFA set up

184
Inactive accounts with no MFA under possible password attacks

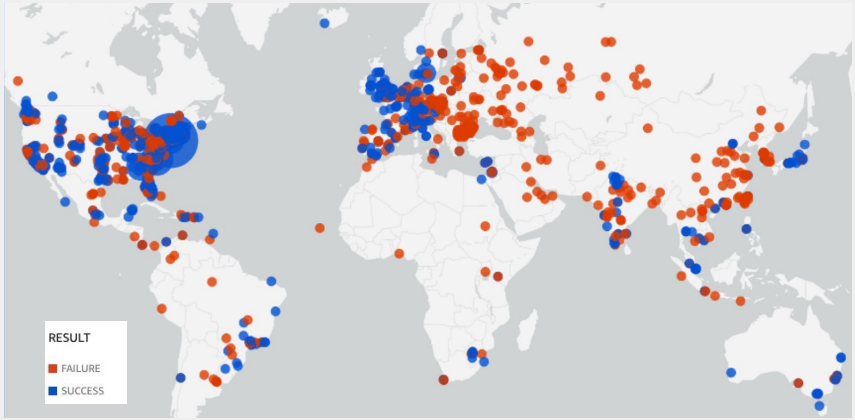
- Weak MFA used to log in to **2** Admin Accounts
- 56 Duo bypass codes used
- CFO used a weak MFA form to sign in
- 18 inactive accounts with no MNFA
- Azure admin service account with no MFA
- 3 accounts use the same device for authentication
- Azure admin service account with no MFA

Threat Insight

Highlights

- Oort detected a range of anomalous behaviour related to Acme accounts
- Failed and success login attempts by executives and admins are displayed on the map, visualizing where probing attempts originate
- It's worth verifying SMAR locations, as some related IPs were flagged as phishing

Account Authentication Result Location: Execs and Admins Only



45 IP Threats Detected

36 Risky Parallel Sessions

24 Okta Admin Anomalies

4 New Email Forwarding Rules

Recommendations

01

Inactive account cleanup

Identify inactive accounts, starting with inactive guest accounts in Azure AD, and suspend any that have not logged in for 90+ days.

02

100% MFA compliance

Measure compliance every day and execute messaging campaigns to drive 100% adoption with strong MFA policies across entire user population.

03

Identity threat monitoring

Monitor for common identity threats and push event information downstream into tools like Slack and ServiceNow.

Oort Benefits

Oort helps customers adopt an identity-first approach to enterprise security. We integrate with your existing IAM tools to give you single pane of glass visibility and control over your identity attack surface.

Customers quickly achieve return on investment (ROI) through:

1. **Reduced risk of security breach from account takeovers** Usernames and passwords are cited to be responsible for over 80% of hacking related breaches. Oort provides continuous monitoring of suspicious activity and threats to your users, helping you to reduce the risk of a breach. Oort provides detection capabilities that are not feasible to build internally, such as identifying risky parallel users and detecting risky users.
2. **Maintain MFA compliance.** Maintain compliance with various frameworks by ensuring users are configuring MFA, and choosing strong factors.
3. **Reduce time investigating incidents.** All Oort customers cite improvements in the time it takes to respond to incidents. Sifting through logs is time-consuming and often do not even have the right context. With Oort, all the information is instantly accessible.
4. **Reclaim unused licenses.** Oort discovered a large number users not using their licenses. Removing these access will free up licenses and have a direct cost saving.

> The simplicity of the tool and its integrations means we need fewer security analysts to get the job done
>
> **Dmitry Sokolovskiy, CISO, Avid**

> Anyone who can use a spreadsheet can use Oort!
>
> **Harry Hoffman, CISO, Northeastern University**