AppOmni

ACME HOLDINGS, INC - SALESFORCE RISK ASSESSMENT

Company Name:

ACME HOLDINGS, INC.

Date of Assessment:

02/01/2026

Contacts

NAME	TITLE	E-MAIL	PHONE NUMBER
Primary Contact of Customer	Matthew Sample	matthewsample@xyz123.com	800-555-1212
AppOmni Primary Point of Contact	Maria Leadership	marialeadership@appomni.com	888-555-1313

Purpose Statement (What Are We Doing):

AppOmni is going to review Acme Holding's Salesforce environment to assess its security posture, identify misconfigurations, and will review identities and its access.This assessment will provide actionable guidance and recommendations to strengthen the security of Acme Holding's Salesforce environment and critical data.

Systems / SaaS Evaluated:

Salesforce

Executive Summary

Acme Holdings maintains 5 communities, 3 Force.com sites, and 30 installed applications. Acme Holdings has 2,684 users (internal and external) with 321 users that have not logged in within the last 90 days. There is 1 critical data SaaS alert and 6 high data SaaS alerts. There are 6 high alert security configuration warnings. There is 1 critical SASE and network alert and 5 high alerts. This environment has 14 inactive Salesforce admin accounts that have not been accessed in 6 months. The critical and high alerts should be addressed immediately.

AppOmni

ACME HOLDINGS, INC - SALESFORCE RISK ASSESSMENT

Present Critical and High Risks and Insights:

- Data records exposed to anonymous world (3 records)
- Profile IP Range Restrictions include IPs outside of configured global trusted networks
- Org Setting 'Require multi-factor authentication (MFA) for all direct UI logins' must be true

Current Recommendations and Priority:

- [ ] Restrict open data access
- [ ] Review and audit IP range restrictions and remove unauthorized IP addresses
- [ ] Activate and require MFA for all direct UI logins

Detailed Summary

Provide a comprehensive analysis of the environment, identifying systemic issues, configuration drift, and specific vulnerabilities found during the assessment period...

Detailed Risk Explanations

RISK 1 CRITICAL	Anonymous exposure of records can result in data theft, misuse, and privacy breaches.
RISK 2 HIGH	Potential data exposure from untrusted IPs
RISK 3 HIGH	Without MFA, user accounts are highly susceptible to credential theft and unauthorized access.
RISK 1 MEDIUM	Longer session times increase exposure to hijacked or unattended sessions.

Detailed Recommendations

REC 1 P1	Audit access to the data records and the systems with access; Remove any external access not approved. Restrict access to specific identities and IP ranges.
REC 2 P2	Audit IP ranges with access to Salesforce. Remove any IP ranges that are no longer useful and accessible. Centralize access to specific IP addresses in office.
REC 3 P3	Require all users with direct UI logins to use MFA by policy. Any identities and users via API will have restricted access.
REC 1 P4	Reduce unattended sessions to <15 minutes by policy to avoid incorrect access or exposure.