Precursor

Security Assessment Report

9fin LTD

AWS Security Review

Version:
2026-11-12 16:42:41

CREST

www.precursorsecurity.com

1. Management Summary

Precursor Security performed an AWS Security Review against the 9fin LTD assets, defined within the Scope of Engagement. The purpose of the assessment was to identify security vulnerabilities which could impact the security of the 9fin LTD assets resulting in the compromise of information, accounts and the system itself.

Vulnerability Summary

A total of 14 findings were identified. The following table details the severity categories for each identified finding:

CRITICAL	HIGH	MEDIUM	LOW	INFO
No findings	No findings	1 finding	1 finding	4 findings

Table 1.1: Finding counts by severity.

Business Risk

The findings of the assessment present a security threat to the 9fin LTD assets.

CloudTrail alerting is not configured for a number of security-relevant events, including root account usage, IAM and security group changes, console sign-ins without MFA, and changes to core networking and account configuration. As a result, security-relevant changes or activity in these areas would not generate an alert, reducing the ability to detect issues in a timely manner.

In addition to the alerting configuration, several identity and access management weaknesses were identified. Hardware MFA is not enabled on the root user account, meaning that a compromise of the root credentials alone would be sufficient for an attacker to gain full administrative control over the AWS account, bypassing what should be a critical secondary layer of protection. Compounding this, IAM access keys were found not to be rotated within a 90-day cycle. Long-lived access keys increase the window of opportunity for credential misuse should a key be leaked, committed to source control, or otherwise compromised, and stale keys are also harder to audit for legitimate versus unauthorised use over time.

The overall security posture of the AWS estate was found to be left with room for improvement. Implementing the recommendations found throughout the body of this report will significantly increase the secure posture of 9fin LTD AWS environment.

2. Summary of Findings

#	Title	Status	Severity
002	Ensure hardware MFA is enabled for the 'root' user account	✔ Resolved	MEDIUM (6.8)
003	Ensure access keys are rotated every 90 days or less	✔ Resolved	MEDIUM (6.5)
013	Ensure IAM password policy requires minimum length of 14 or greater	✔ Resolved	MEDIUM (6.5)
014	Ensure IAM password policy prevents password reuse	✔ Resolved	MEDIUM (5.4)
007	Ensure MFA Delete is enabled on S3 buckets	✘ Unresolved	MEDIUM (4.9)
010	Ensure AWS Config is enabled in all regions	✔ Resolved	MEDIUM (4.3)
005	Ensure a support role has been created to manage incidents with AWS Support	✘ Unresolved	LOW (2.7)
009	Ensure CloudTrail is enabled in all regions	✔ Resolved	LOW (2.7)
012	Ensure AWS Security Hub is enabled	✔ Resolved	LOW (2.7)
001	Ensure security contact information is registered	✔ Resolved	LOW (2.2)
004	Ensure IAM users receive permissions only through groups	✘ Unresolved	INFO (0)
006	Ensure that IAM External Access Analyzer is enabled for all regions	✘ Unresolved	INFO (0)
008	Ensure all data in Amazon S3 has been discovered, classified, and secured when necessary	✘ Unresolved	INFO (0)
011	Monitoring Recommendations	✘ Unresolved	INFO (0)

Table 2.1: Findings ordered by severity.