Google Worskpace Assessment Report

Company

Prepared by:

Report Period:

Executive Summary

This report presents the findings from a Google Workspace security configuration assessment. The report identifies key strengths, highlights areas for improvement, and provides actionable recommendations. By addressing these findings, the organization can enhance its security posture, protect critical assets, and mitigate potential risks.

Google Workspace Security Configuration Assessment

Strengths in Security and Operations	
Strong SPF and DMARC Records	The organization has implemented robust SPF and DMARC records for email security. These measures are essential in protecting against phishing and spoofing attacks, ensuring that only legitimate emails are delivered and reducing the risk of domain-based threats.
Improvements Made During Assessment	The organization made several adjustments to their Google Workspace configuration during the assessment in order to enahance overall security posture.

Identificaiton of Additional Considerations	Several additional security and privacy capabilities of the Google Workspace platorm were discovered and are being considered for implementation. The team will weigh the implications of the controls against the organization's operational and strategic needs.

Opportunities for Security Improvement	
Decision on Central Directory for SSO	The organization is planning to implement SSO and must decide on a central identity provider. Google Workspace offers a simpler, cost-effective solution, while Okta provides greater flexibility, including customer identity management. Choosing the right central directory is foundational for identity and access management, as it impacts scalability, usability, and integration with other tools and services.
DKIM Record Implementation	The organization has not yet created a DKIM record to compliment its SPF and DMARC configurations. Without DKIM, email security is incomplete, leaving messages more vulnerable to tampering during transit. Adding a DKIM record would enhance email authentication and integrity, providing an additional layer of protection against spoofing and phishing.

Log Aggregation and Monitoring	Google Workspace generates a large volume of authentication and activity logs that are not currently aggregated with other organizational log sources, such as firewall, endpoint, and infrastructure logs. These logs are reviewed manually only occasionally, making it impractical to analyze millions of logs monthly and increasing the risk of missing critical security events. Implementing a SIEM would centralize log data, enabling real-time threat detection and response while allowing a security team to manage logs efficiently and respond promptly to incidents.