Security Audit Report for 1Password

Executive Summary

Prepared by:

Onica

Table of Contents

Introduction ***2***

Purpose ***2***

Security Assessment Methodology ***3***

Conclusion ***3***

Introduction

The reports summarized in this document are taken from AgileBits/Onica security assessment and audit project documentation. This summary outlines the observations, findings, recommendations and remediation effort estimation for security architecture, infrastructure configurations, tools, as well as pointing out where sound practices based on AWS Well-Architected Framework. AgileBits is using AWS services for their information technology assets and moving to the cloud at enterprise scale is a paradigm shift in how an organization deploys and operates. Security on AWS encompasses the ability to protect data, systems, and assets while delivering business value through risk assessments and mitigation strategies. This report will provide detail and best-practice guidance for architecting secure systems on AWS.

Purpose

Onica has been engaged for third-party independent security audit of the existing AWS architecture. This is to ensure that AgileBits is strategically setting themselves up for success and developing a secure enterprise viable cloud. Goals of this effort are to provide validation and review of the currently implemented architecture as an informed outsider and provide feedback of identified security activities or lack thereof as it relates to AWS account access, host setup and security, disk/volume storage management and security, database, S3 and other security related items according to AWS Well-Architected Framework.
Specifically:

- Risk assessment on the current state of security related architecture, implementation and use of tools
- Recommendations around
    - Mitigation and improvement
    - Best practices references
- Efforts estimation on proposed remediation methods

The findings and results of the security assessment performed are a "point in time" assessment and should be used as an input into a larger risk management process and project used to mature AgileBits' overall security posture and provide continual iterative and incremental improvement.

A mature security posture improves return on investment by:

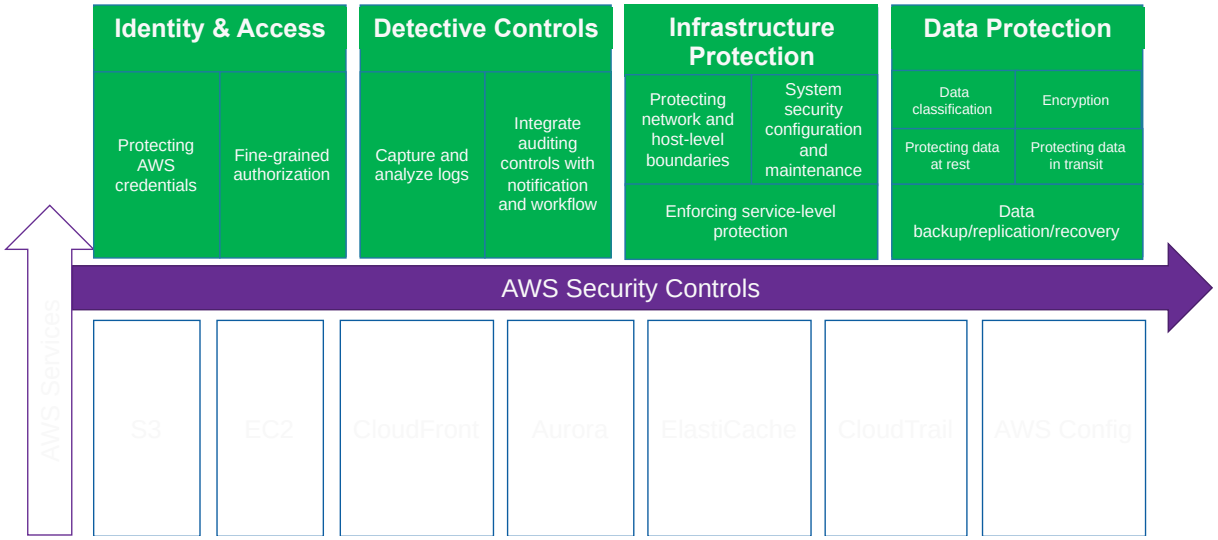
- Increased uptime and high availability by protecting against malicious or accidental service outages
- Adoption of security protocols and solutions to increase data security to prevent unauthorized expose to third parties
- Flexibility and improved incident response activities
- Solid guardrails in place to allow for delivery and innovation while protecting the organization from misconfigurations and exposures by early identification of vulnerabilities
- Greater agility on security for operation teams

Security Assessment Methodology

The AgileBits AWS environments are deployed in nine AWS accounts. This audit assessed and reviewed the existing AWS architectural and services configurations are under use.

Onica conducts this security audit in two demission. Horizontally, we checked the issues for major security controls on AWS, for example, identity and access management, detective controls, infrastructure protection and data protection.

We also checked and audited the major AWS services that AgileBits are actively using. That include AWS S3, AWS AWS EC2, AWS CloudFront, AWS Aurora, AWS ElastiCache, AWS CloudTrail and AWS Config.



The outputs of this effort are mapped to the deliverables in the statement of work:

1. Security Audit Report that includes gaps found, recommendations, and remediation effort.

   This document reflects all considerations in depth of the overall engagement.

2. AWS Well-Architected Review Report

   This document is generated from AgileBits AWS account. It is discussed and reviewed by both AgileBits and Onica.

Onica recommends that AgileBits continue to assess and review their status at appropriate intervals as the adoption increases.

Conclusion

The review of the current AWS environments showed evidence that the AgileBits teams have undertaken significant research and gained a solid understanding of best practices from a platform level. The fundamentals of security best practices are being executed in the implementation. There is no high-risk issue are found during

this security audit. Most of the recommendations from Onica captured in this report are adjustments, extensions, or additional considerations of existing AWS architecture and implement, as opposed to large scale remediations.