Quest Identity Defense Assurance

Overview

The **Quest Identity Defense Assurance** Service Offering is designed to guide you through the steps necessary to start effectively using the Quest Identity Defense subscription. Regular reviews will ensure configuration and usage remain aligned with current functionality as well as best practices.

Approach and Activities

Quest will schedule three (3) sessions up to two (2) hours each, over the course of two (2) weeks to guide you through onboarding. Subsequently, Quest will schedule regular (generally monthly) assurance sessions. The activities below will be completed, though the specific session agenda may vary based on pace of progress.

Planning and Onboarding

Quest will host one (1) session (up to two (2) hours) with you to verify environment readiness and establish the base configuration, during which Quest and you may discuss:

- Review Project Scope and Activities
- Overview of your Environment, Requirements, and Goals
- Best Practices for Quest Identity Defense
- Verify environment preparedness and prerequisites

During the session, Quest will assist you with configuration of Quest Identity Defense services in accordance with the results of the planning session.

- Set up new Quest Identity Defense Organization
- Add tenants, grant application consent and connect to on premises Active Directory
- Verify Change Auditor; add new agents
- Review processes for collecting Active Directory and Entra/M365 data, performing security assessments, and classifying Tier 0 and Privileged objects
- Review the Quest Identity Defense dashboard for monitoring and managing security

Configuration and Testing

Quest will host a configuration session with you to:

- Configure dashboard widgets

- Review methods and best practices for ongoing management of Quest Identity Defense
- Configure alerts and SIEM integration (as applicable)
- Quest will guide you through testing scenarios to validate Quest Identity Defense behavior and assist you with validating up to two (2) production test scenarios

Knowledge Transfer

Quest will provide guidance to you by performing a knowledge transfer and product overview of the Quest Identity Defense services implemented throughout the course of the engagement. If requested, Quest may conduct an additional knowledge transfer session (up to two (2) hours) which may include:

- Review the items configured during the engagement
- Verify you can run, create and view security reports
- Description of integration with other Quest offerings
- Introduction of Support resources

Assurance

Quest will conduct regular, scheduled sessions once per month during the subscription year with you to ensure your ongoing alignment with best practices, product updates, and lessons learned. Topics addressed may include:

- Upgrade to current version of products
- New and/or updated features and functionality
- Updates to best practices and recommendations
- Additional use cases and new integrations
- Your questions and configuration updates

Prerequisites and Assumptions

You agree to cooperate with Quest in its delivery of the Service. You agree to the following:

- You will ensure that adequate licensing for Secure Management platform and Microsoft platform are in place prior to beginning of engagement.
- You will ensure all prerequisites for onboarding to the Secure Management platform are fulfilled in advance of the Planning and Onboarding session
- You will commit a technical resource for the working sessions with adequate authority to conduct the migration.
- All activities will be performed remotely utilizing Quest provided web and voice conferencing.
- You will collaborate with Quest to schedule sessions within the two (2) weeks following purchase.

SKU	
CAB-QOD-PP	QUEST IDENTITY DEFENSE PREPAID ASSURANCE FIXED FEE