

Redback Operations

# Deployment Plan for Endpoint Security

SIT374 TEAM PROJECT A

ALESSANDRA DOMINIQUE COLMENARES  
9-17-2024

**Contents**

Introduction .....1

Trimester 1: Preparation and Initial Deployment .....2

Trimester 2 and Beyond: Continuous Improvement.....4

**Introduction**

This General Deployment Plan outlines the key steps for implementing endpoint security measures within the organization. The plan is designed to be carried out over two trimesters, with a structured and phased approach. The first trimester focuses on preparation, execution, and initial review, while the second trimester emphasizes continuous monitoring, feedback integration, and long-term maintenance. The tasks outlined for Trimester 2, such as monitoring, feedback collection, and adjustments, can be repeated in continuity for the following trimesters, ensuring ongoing improvements and alignment with evolving security needs. This iterative process ensures that security measures remain effective and up-to-date over time.

### Trimester 1: Preparation and Initial Deployment

Task	Start date & time	Finish date & time	Owner	Status	Comments/progress
<b>Define the scope, objectives, and specific deliverables.</b>	Week 1	Week 1		Open	
<b>Allocate necessary resources (team, tools, budget).</b>	Week 2	Week 2		Open	
<b>Assign roles and responsibilities to stakeholders.</b>	Week 3	Week 3		Open	
<b>Develop project plan, set milestones, and create risk plan.</b>	Week 4	Week 4		Open	
<b>Begin implementation, focusing on high-priority areas.</b>	Week 5	Week 5		Open	
<b>Roll out essential security measures across endpoint devices.</b>	Week 6	Week 7		Open	
<b>Conduct awareness training on endpoint security practices.</b>	Week 8	Week 8		Open	
<b>Monitor progress and make real-time adjustments as needed.</b>	Week 9	Week 9		Open	
<b>Review user access and</b>	Week 10	Week 10		Open	

<b>implement least privilege principle.</b>					
<b>Conduct evaluation of the security implementation.</b>	Week 11	Week 11		Open	
<b>Gather feedback from stakeholders for improvements.</b>	Week 12	Week 12		Open	

## Trimester 2 and Beyond: Continuous Improvement

<b>Set up monitoring tools to track security metrics.</b>	<b>Week 1</b>	<b>Week 1</b>		<b>Open</b>	
<b>Collect feedback through surveys and regular meetings.</b>	Week 2	Week 2		Open	
<b>Implement minor adjustments based on feedback.</b>	Week 3	Week 3		Open	
<b>Continue refining and updating security protocols as needed.</b>	Week 4	Week 4		Open	
<b>Finalize improvements based on feedback from stakeholders.</b>	Week 5	Week 5		Open	
<b>Maintain ongoing review cycles and introduce new tools.</b>	Week 6-12	Week 12		Open	