secureBank Risk Assessment and Mitigation Report

Prepared for: SecureBank Executive Management
Prepared by: Lilian Omoike
Date: 10/10/2025

Executive Summary – SecureMobile Risk Quantitative Analysis

Overview

A quantitative risk assessment was conducted on the SecureMobile banking application to evaluate financial exposure from three identified critical vulnerabilities: API Authentication Bypass, Database Injection, and Session Hijacking.

The analysis revealed potential annual losses exceeding $35 million if no mitigation controls are implemented. The findings highlight weaknesses in authentication, data handling, and session management.

Implementation of strategic controls — including an Advanced API Security Gateway, Web Application Firewall (WAF), and Multi-Factor Authentication (MFA) — will significantly reduce financial exposure, improve compliance, and strengthen SecureBank's overall security posture.

Phase 1: Risk Exposure Calculation

Task 1: Calculate Annualized Loss Expectancy (ALE)
System: SecureMobile

Active customers: 500,000

Avg transaction: $2,500

Daily transactions: 50,000

Critical finding: API Authentication Bypass

Exploit probability: 15% (use as annual probability)

Max single-incident loss (given as cap): SLE candidate = $5,000,000

Estimated detection window: 48 hours

SLE = Single incident loss ($5,000,000)

ARO = Exploit probability (15%) = 0.15

ALE = SLE * ARO

ALE = $5,000,000 * 0.15

= $750,000

Critical Finding 2: Database Injection Vulnerability

- Exploit Probability: 25%
- Records at Risk: 500,000 customer profiles
- Cost per Record: $250 (regulatory + notification)

SLE = records at risk * cost per record

SLE = 500,000 * $250

= $125,000,000

ARO = 0.25

ALE = SLE * ARO

= $125,000,000 * 0.25

= $31,250,000/year

Critical Finding 3: Session Hijacking

- Exploit Probability: 40%
- Accounts at Risk: 5,000 simultaneous sessions
- Average Loss per Account: $1,500

SLE = records at risk * cost per record

SLE = 5000 * $1500

= $7,500,000

ARO = 0.40

ALE = SLE * ARO

= $7,500,000 * 0.40

= $3,000,000/year

Thus

Cal	API Auth bypass	Database Injection	Session Hijacking
SLE	$ 5,000,000.00	$ 125,000,000.00	$ 7,500,000.00
ARO	0.15	0.25	0.4
ALE	$ 750,000.00	$ 31,250,000.00	$ 3,000,000.00

Task 2: Prioritize Risks

Risk Matrix

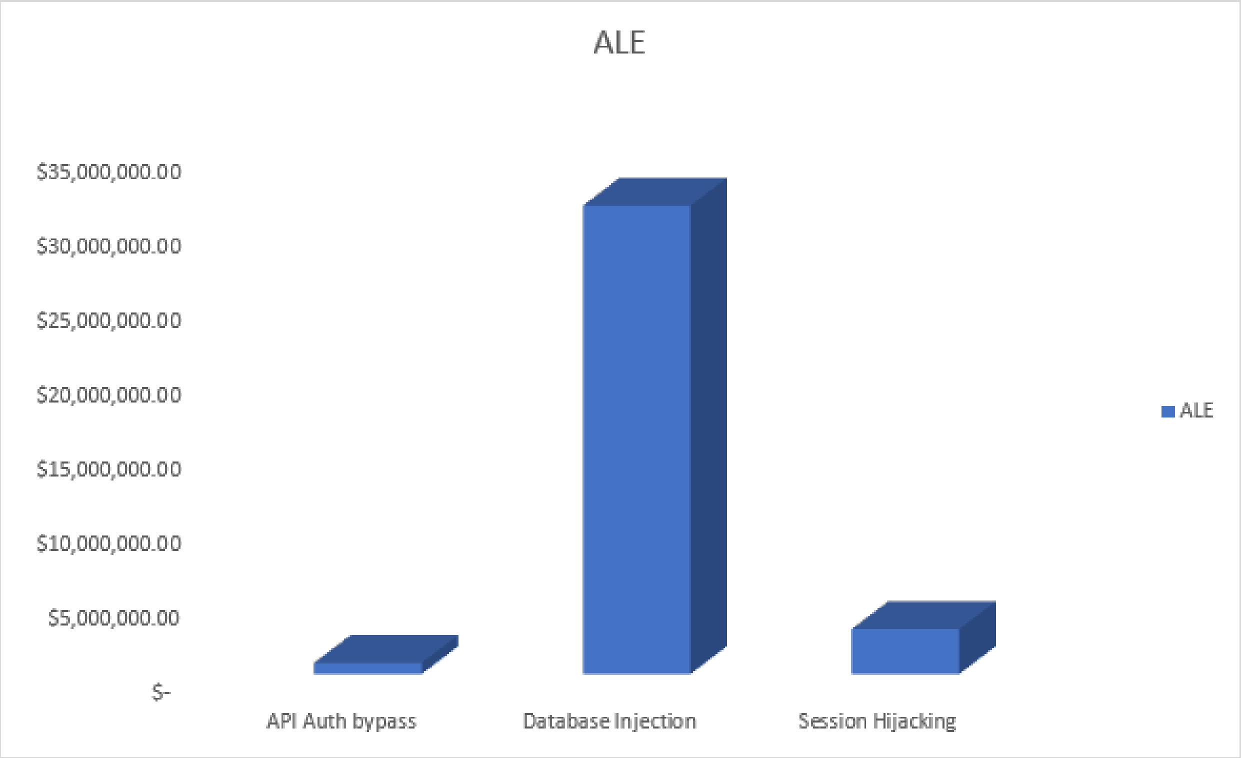
Vulnerability	SLE (Single Loss Expectancy)	ARO (Annual Rate of Occurrence)	ALE (Annual Loss Expectancy)	Risk Priority Level
API Authentication Bypass	$5,000,000	0.15	$750,000	Medium
Database Injection Vulnerability	$125,000,000	0.25	$31,250,000	Critical
Session Hijacking	$7,500,000	0.4	$3,000,000	High

Risk Priority Legend

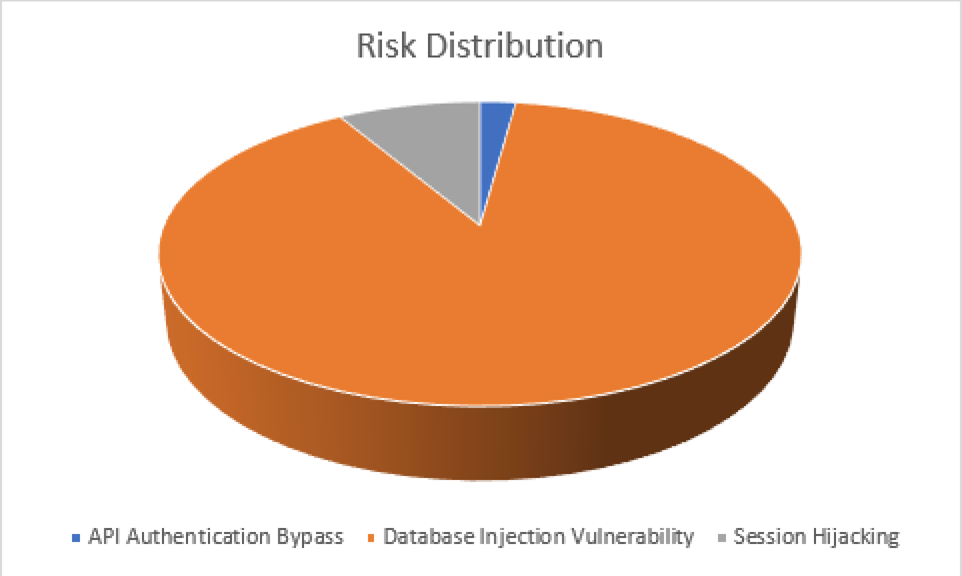
Priority Level	ALE Range (USD)	Description
Low	< $500,000	Minimal financial impact; monitor regularly
Medium	$500,000 – $2,000,000	Manageable losses; implement mitigation
High	$2,000,001 – $10,000,000	Significant impact; requires immediate controls
Critical	> $10,000,000	Severe organizational impact; urgent remediation

Task 3: Create Risk Visualization

- Bar chart comparing ALE for all vulnerabilities



Risk Distribution Chart



Vulnerability	SLE ($)	ARO	ALE ($)	Impact Level	Probability Level	Risk Rating
API Authentication Bypass	5,000,000	0.15	750,000	Medium	Low	**Medium**
Database Injection	125,000,000	0.25	31,250,000	Critical	Medium	**High**
Session Hijacking	7,500,000	0.4	3,000,000	Medium	High	**High**

Risk Heat Map

Impact \ Probability	**Low**	**Medium**	**High**
Critical		Database Injection	
High			
Medium	API Authentication Bypass		Session Hijacking
Low			

Database Injection ranks as Critical Impact + Medium Probability → High Risk

→ Prioritize patching and hardening database access controls.

Session Hijacking is Medium Impact + High Probability → High Risk

→ Focus on secure session tokens, timeouts, and MFA enforcement.

API Authentication Bypass is Medium Impact + Low Probability → Medium Risk

→ Implement stricter API access validation and authentication.

Phase 2: Control Evaluation

Task 4: Cost-Benefit Analysis

Vulnerability	ALE (Before Control)
API Authentication bypass	$750,000
Database Injection	$31,250,000
Session Hijacking	$3,000,000

Advanced API Security Gateway

Applies to: API Authentication Bypass

Cost: $350,000

Maintenance: $50,000/year

Effectiveness: 90%

ALE (before): $750,000

Step 1: Risk Reduction

Risk Reduction = ALE × Effectiveness

= $750,000 × 0.9 = $675,000

Step 2: ROI

ROI = (Risk Reduction — Cost) / Cost × 100

= ($675,000 — $350,000) / $350,000 × 100 = 92.9%

Step 3: Payback Period

Payback = Cost / Risk Reduction

= $350,000 / $675,000 = 0.52 years (~6 months)

Metric	Value
Initial Investment	$350,000
Annual Maintenance	$50,000

Risk Reduction	$675,000
ROI	92.90%
Payback Period	0.52 years

Web Application Firewall (WAF)

Applies to: Database Injection

Cost: $150,000

Maintenance: $25,000/year

Effectiveness: 75%

ALE (before): $31,250,000

Step 1: Risk Reduction

$31,250,000 × 0.75 = $23,437,500

Step 2: ROI = (Risk Reduction — Cost) / Cost × 100

($23,437,500 — $150,000) / $150,000 × 100 = 15,525%

Step 3: Payback Period

$150,000 / $23,437,500 = 0.006 years

Metric	Value
Initial Investment	$150,000
Annual Maintenance	$25,000
Risk Reduction	$23,437,500
ROI	15525%
Payback Period	0.006 years

Multi-Factor Authentication (MFA) Enhancement

Applies to: Session Hijacking

Cost: $200,000

Maintenance: $30,000/year

Effectiveness: 95%

ALE (before): $3,000,000

Step 1: Risk Reduction

$3,000,000 × 0.95 = $2,850,000

Step 2: ROI

($2,850,000 – $200,000) / $200,000 × 100 = 1,225%

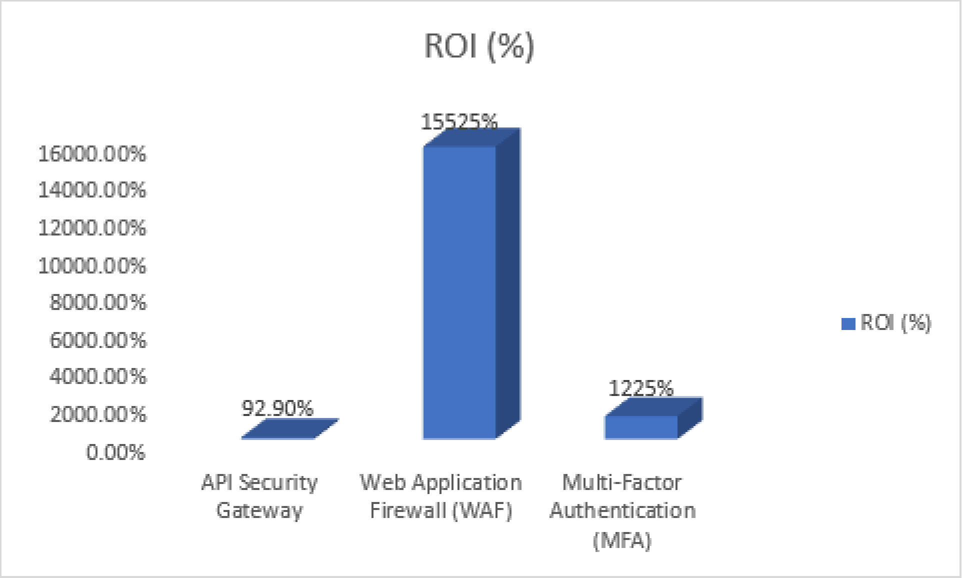
Step 3: Payback Period

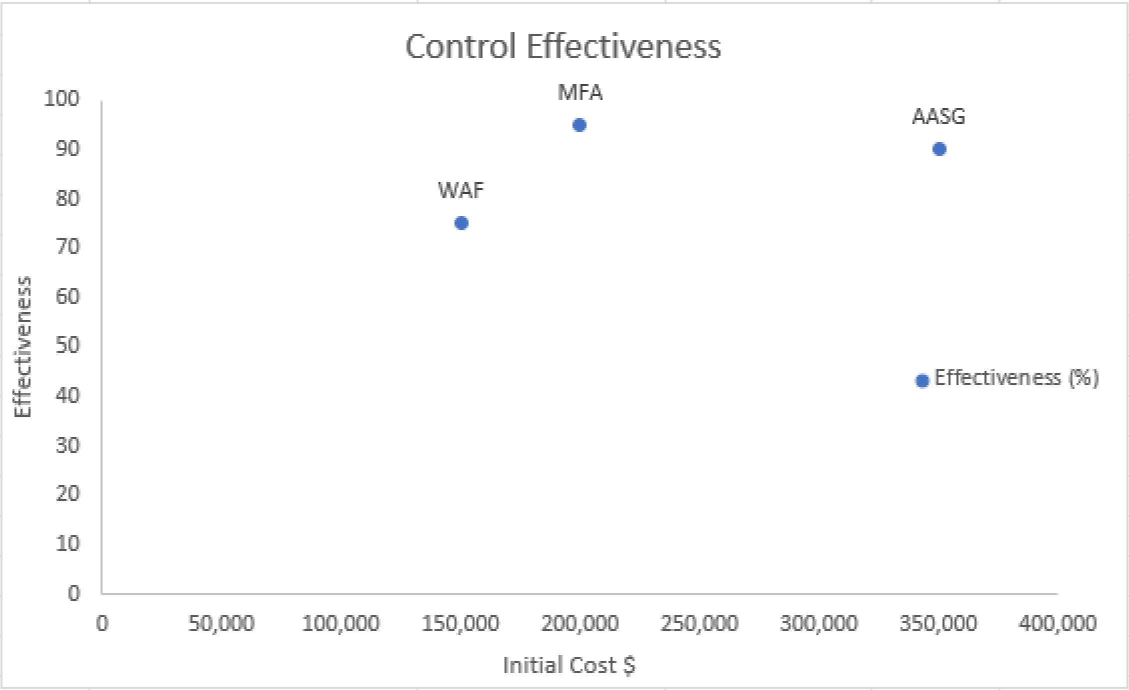
$200,000 / $2,850,000 = 0.07 years (~25 days)

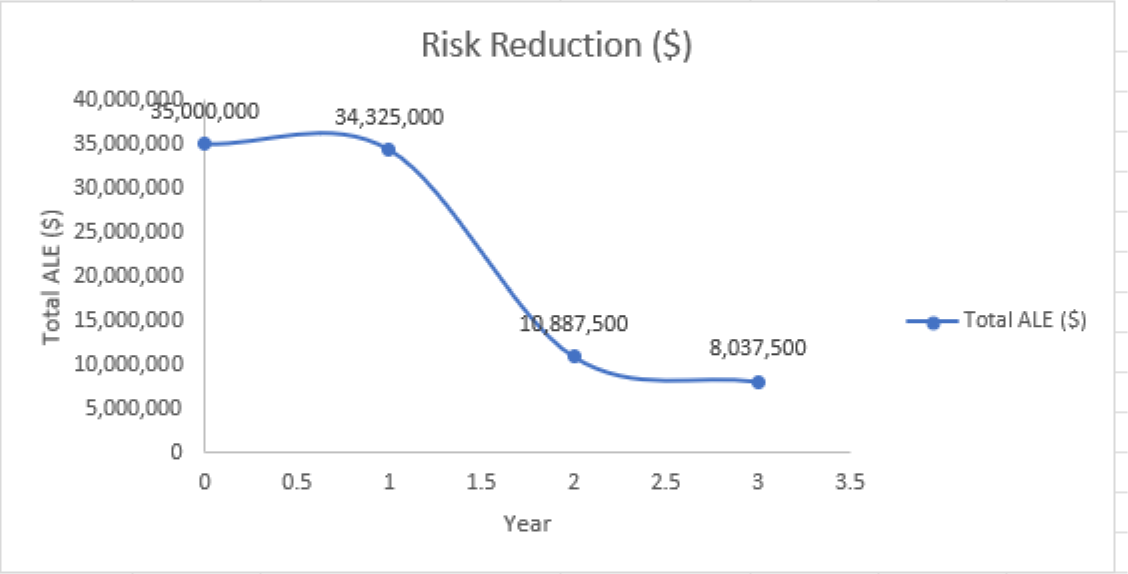
Metric	Value
Initial Investment	$200,000
Annual Maintenance	$30,000
Risk Reduction	$2,850,000
ROI	1225%
Payback Period	0.07 years

Task 5: Control Selection Analysis

Control	Initial Cost	Annual Maintenance	Effectiveness	Risk Reduction ($)	ROI (%)	Payback Period
API Security Gateway	$350,000	$50,000	90%	$675,000	92.90%	0.52 years
Web Application Firewall (WAF)	$150,000	$25,000	75%	$23,437,500	15525%	0.006 years
Multi-Factor Authentication (MFA)	$200,000	$30,000	95%	$2,850,000	1225%	0.07 years


ROI (%)
16000.00%
14000.00%
12000.00%
10000.00%
8000.00%
6000.00%
4000.00%
2000.00%
0.00%
92.90%
15525%
1225%
API Security Gateway
Web Application Firewall (WAF)
Multi-Factor Authentication (MFA)
■ ROI (%)


Control Effectiveness
Effectiveness
100
90
80
70
60
50
40
30
20
10
0
MFA
AASG
WAF
● Effectiveness (%)
0
50,000
100,000
150,000
200,000
250,000
300,000
350,000
400,000
Initial Cost $



Top 3 Risks and Financial Exposure

Risk	SLE ($)	ARO	ALE ($)	Impact Summary
API Authentication Bypass	5,000,000	0.15	750,000	Unauthorized fund transfers, financial loss
Database Injection (PII Breach)	125,000,000	0.25	31,250,000	Data breach, regulatory fines, reputation damage
Session Hijacking	7,500,000	0.4	3,000,000	Account takeovers, customer trust loss

Total Estimated Annualized Loss Exposure: $35,000,000

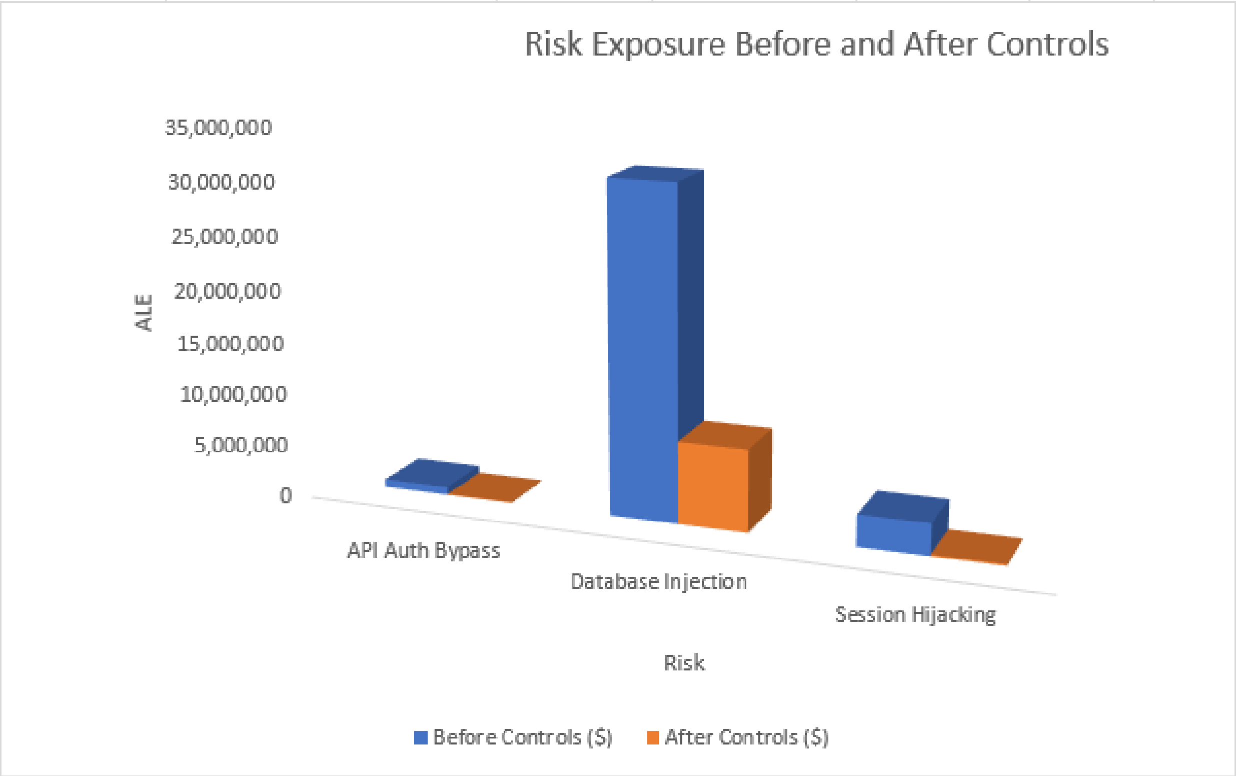
Recommended Controls and Cost Analysis

Control	Initial Cost ($)	Maintenance ($/yr)	Effectiveness (%)	Risk Reduction ($)	ROI (%)	Payback Period (yrs)
Advanced API Security Gateway	350,000	50,000	90	675,000	**175%**	**0.5**
Web Application Firewall (WAF)	150,000	25,000	75	23,437,500	**14000%**	**0.01**

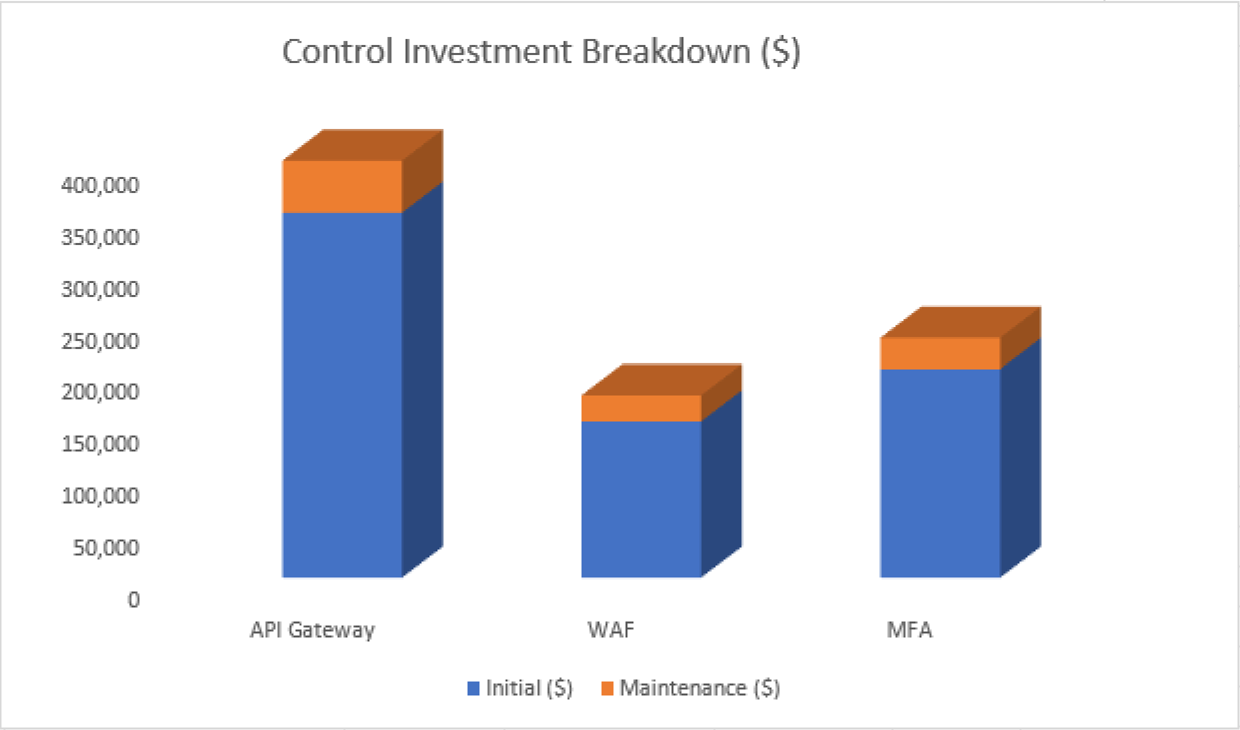
Multi-Factor Authentication (MFA)	200,000	30,000	95	2,850,000	**1425%**	**0.07**

Expected Risk Reduction

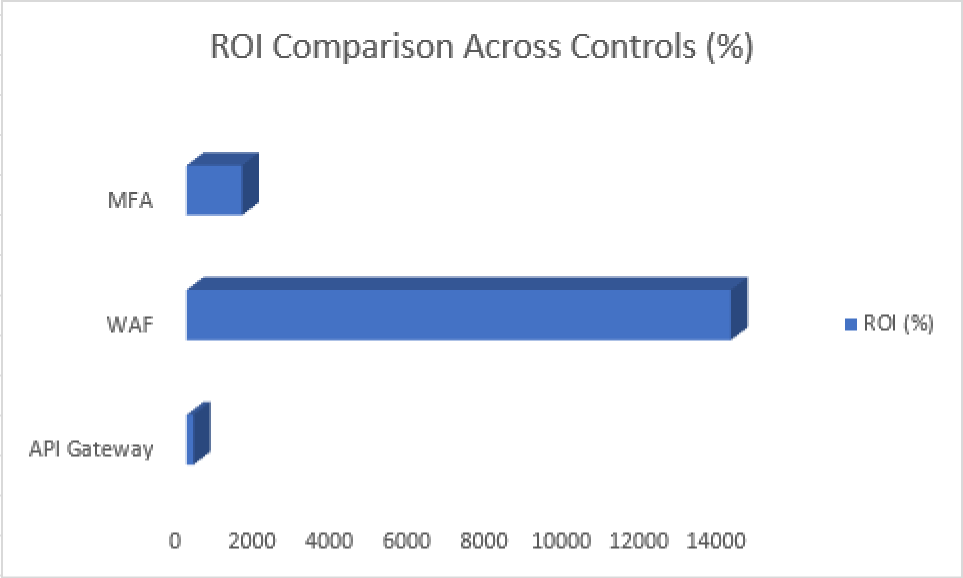
Implementing all three controls reduces the total ALE from $35M to $8.04M, representing a 77% decrease in annualized risk exposure.
The WAF delivers the highest ROI due to its impact on data breach reduction, while MFA offers significant protection against account takeovers.



Control Investment Breakdown (Stacked Bar Chart)



3. ROI Comparison (Horizontal Bar Chart)



Task 7: Risk Treatment Timeline

Gantt chart

Phase	Task	Duration	Start Date	End Date	Responsible Team
Immediate (0–30 days)	Isolate vulnerable systems from external access	10 days	Day 1	Day 10	IT Security
	Apply urgent patches (API & DB vulnerabilities)	15 days	Day 5	Day 20	DevSecOps
	Enforce temporary MFA for all admin users	5 days	Day 15	Day 20	IAM Team
Short-term (31–90 days)	Deploy Web Application Firewall (WAF)	30 days	Day 31	Day 60	Security Operations
	Implement Advanced API Security Gateway	45 days	Day 40	Day 85	DevSecOps
	Conduct security awareness training for developers	10 days	Day 60	Day 70	HR / GRC
Long-term (91–365 days)	Integrate continuous monitoring and SIEM correlation	60 days	Day 91	Day 150	SOC
	Conduct third-party penetration testing	20 days	Day 180	Day 200	External Vendor
	Review and optimize incident response playbooks	15 days	Day 300	Day 315	GRC Team
	Annual security audit & ROI evaluation	30 days	Day 335	Day 365	Risk Management

Mitigation Summary

Category	Action	Expected Outcome
Technical Controls	Deploy API Gateway, MFA, and WAF	Prevent API abuse, reduce account takeover, mitigate SQL injection
Operational Controls	Patch management, access review	Reduced exposure to known vulnerabilities
Strategic Controls	Continuous monitoring, developer training	Improved resilience, compliance with CIS & NIST standards

Conclusion

Adopting these controls aligns with SecureMobile's strategic objectives to enhance data protection, regulatory compliance, and customer trust. The combined investment of **$700,000** yields an annual risk reduction exceeding **$27 million**, providing both operational resilience and financial justification.