Request for Proposal: Enterprise Mobility Management (EMM) Software Solution

Table of Contents

1. Introduction

[Company Name] is seeking proposals for a comprehensive Enterprise Mobility Management (EMM) software solution to secure and manage our organization's mobile devices, applications, and data. This RFP outlines our requirements for a robust system that will protect corporate assets, ensure compliance, and enable employee productivity across various mobile platforms.

1.1 Key Components

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Identity and Access Management (IAM)

2. Project Objectives

The primary objectives for implementing an EMM solution are:

1. Establish comprehensive mobile device security across all platforms
2. Ensure protection of corporate data on both company-owned and BYOD devices
3. Streamline mobile application deployment and management
4. Enable secure access to corporate resources
5. Maintain compliance with industry regulations
6. Improve IT operational efficiency

3. Technical Requirements

3.1 Multi-Platform Device Support

- Support for iOS, Android, Windows, and other relevant operating systems
- Management of smartphones, tablets, laptops, and IoT endpoints
- Comprehensive device lifecycle management

3.2 Security Requirements

- Data encryption for devices and communications
- Multi-factor authentication support
- Secure container solutions
- Advanced threat protection
- Policy-based access control

3.3 Integration Requirements

- Active Directory/LDAP integration
- Email system integration
- Certificate management
- API availability
- SSO capabilities

3.4 Infrastructure Requirements

- Cloud-based deployment options
- On-premises deployment support
- Hybrid deployment capabilities
- High availability architecture
- Disaster recovery support

4. Functional Requirements

4.1 Device Control

Tip: Device control is fundamental to EMM security - focus on granular permissions, monitoring capabilities, and integration with existing security infrastructure to ensure comprehensive endpoint protection while maintaining user productivity.

Requirement	Sub-Requirement	Y/N	Notes
Device Type Control	Granular control over USB drives		
	External hard drive management		
	Smartphone access control		
	Tablet device management		
	IoT device control		
Policy Management	Device usage policy creation		
	Policy enforcement automation		
	Custom policy definition		
Access Control	Device whitelist/blacklist		
	Read/write permission management		
	Temporary access provisioning		
Data Protection	Removable device encryption		

	Data transfer monitoring		
	DLP integration		
Monitoring	Real-time connection monitoring		
	Usage auditing and logging		
	Alert system configuration		

4.2 Web Control

Tip: Web control mechanisms should balance security with usability - implement granular filtering, real-time threat detection, and flexible policy management while maintaining acceptable performance and user experience.

Requirement	Sub-Requirement	Y/N	Notes
URL Filtering	Predefined category filtering		
	Custom category creation		
	HTTPS inspection		
Access Control	Time-based restrictions		
	User/group-based policies		
	Social media controls		
Security Features	Real-time malware scanning		
	Safe search enforcement		
	Proxy prevention		
Management	Bandwidth control		
	Custom block pages		
	Browser-independent filtering		

4.3 Application Control

Tip: Application control must balance security with business needs - implement granular controls for execution, monitoring, and policy enforcement while ensuring critical business applications remain accessible and performant.

Requirement	Sub-Requirement	Y/N	Notes
Inventory Management	Application discovery		
	Version tracking		
	License monitoring		
Execution Control	Granular execution policies		
	Whitelist/blacklist management		
	Vendor-based controls		
Security	File hash verification		
	Application sandboxing		
	Vulnerability scanning		
Monitoring	Real-time usage tracking		
	Policy violation alerts		
	Performance impact analysis		

4.4 Asset Management

Tip: Effective asset management requires comprehensive visibility and control - focus on automated discovery, detailed tracking, and lifecycle management while maintaining accurate inventory and compliance status.

Requirement	Sub-Requirement	Y/N	Notes
Discovery	Automated asset detection		

	Hardware specification tracking		
	Software inventory		
Lifecycle Management	Asset check-in/check-out		
	Retirement tracking		
	Ownership management		
Integration	ITSM tool integration		
	Active Directory sync		
	Inventory systems connection		
Reporting	Asset status tracking		
	Compliance reporting		
	Usage analytics		

4.5 System Isolation

Tip: System isolation capabilities must provide rapid response to threats while maintaining business continuity - implement granular controls for network access and application availability with clear restoration procedures.

Requirement	Sub-Requirement	Y/N	Notes
Network Control	Connection termination		
	Selective access restriction		
	VPN management		
Application Control	Selective deactivation		
	Service management		
	Process control		

Recovery	Restoration procedures		
	Self-service options		
	Validation checks		
Monitoring	Isolation event logging		
	Status tracking		
	Compliance verification		

4.6 Endpoint Intelligence

Tip: Endpoint intelligence must provide actionable insights about device security status - implement comprehensive threat data collection, correlation with global intelligence, and automated analysis while maintaining performance.

Requirement	Sub-Requirement	Y/N	Notes
Threat Intelligence	Real-time feed integration		
	Global threat data correlation		
	Local telemetry collection		
Analysis	Threat pattern recognition		
	Behavioral correlation		
	Risk assessment		
Visualization	Customizable dashboards		
	Threat landscape mapping		
	Impact visualization		
Hunting	Automated threat hunting		
	Retrospective analysis		

	IOC identification		

4.7 Firewall

Tip: Endpoint firewall protection requires sophisticated traffic control - focus on application awareness, location-based policies, and integration with other security tools while maintaining network performance.

Requirement	Sub-Requirement	Y/N	Notes
Traffic Control	Inbound traffic filtering		
	Outbound traffic control		
	Protocol filtering		
Application Control	App-aware filtering		
	Custom rule creation		
	Port control		
Location Awareness	Policy adaptation		
	Network type detection		
	VPN integration		
Management	Centralized administration		
	Policy distribution		
	Rule conflict detection		

4.8 Malware Detection

Tip: Malware detection requires multi-layered analysis capabilities - implement real-time scanning, behavioral analysis, and machine learning while maintaining system performance and minimizing false positives.

Requirement	Sub-Requirement	Y/N	Notes

Real-time Scanning	File system monitoring		
	Process analysis		
	Memory scanning		
Behavioral Analysis	Activity monitoring		
	Pattern recognition		
	Anomaly detection		
Advanced Detection	Machine learning analysis		
	Rootkit detection		
	Fileless malware detection		
Response	Quarantine management		
	Automated remediation		
	Incident reporting		

4.9 Incident Reports

Tip: Incident reporting must provide clear, actionable information - implement customizable templates, trend analysis, and automated distribution while ensuring compliance with reporting requirements.

Requirement	Sub-Requirement	Y/N	Notes
Report Generation	Template customization		
	Automated generation		
	Scheduling options		
Analysis	Trend identification		
	Impact assessment		

	Root cause analysis		
Visualization	Interactive dashboards		
	Custom charts		
	Data filtering		
Distribution	Automated delivery		
	Format options		
	Access control		

4.10 Security Validation

Tip: Security validation must verify control effectiveness - implement automated testing, simulated attacks, and continuous monitoring while maintaining system stability and minimizing business impact.

Requirement	Sub-Requirement	Y/N	Notes
Testing	Automated assessments		
	Control validation		
	Configuration checks		
Simulation	Attack scenario testing		
	Response validation		
	Recovery testing		
Monitoring	Continuous validation		
	Performance impact		
	Compliance checking		
Integration	Change management		

	Third-party testing		
	Reporting systems		

4.11 Self-Service Portal

Tip: Self-service capabilities must balance user empowerment with security - implement intuitive interfaces, automated workflows, and clear documentation while maintaining policy compliance.

Requirement	Sub-Requirement	Y/N	Notes
User Interface	Intuitive design		
	Mobile responsiveness		
	Accessibility compliance		
Device Management	Registration workflow		
	Configuration options		
	Status monitoring		
Security	Password management		
	Policy acknowledgment		
	Compliance checking		
Support	Knowledge base access		
	Ticket management		
	Chat support		

5. AI-Enhanced Features

5.1 Predictive Analytics for Security

Tip: Predictive analytics should leverage machine learning to identify patterns and anomalies in security data, enabling proactive threat prevention while minimizing false positives.