Mobile security buyer's guide

Ensure all your endpoints are protected

A mobile workforce faces evolving threats.

Successful mobile deployments require sharp visibility and decisive action.

Employees are increasingly working away from their desks or corporate offices, and they're working on mobile devices. Defending these scattered modern endpoints can be a challenge, especially as users face new threat vectors.

Cyber threats aren't unique to our computers. The risk to mobile devices is real.

- **40%** of mobile devices used for work operate with a known vulnerability.
- Workers are **50%** more likely to fall victim to a phishing attack on a mobile device than a laptop.
- **1%** of mobile workers are impacted by malware, but the advanced persistent threats (APTs) allow attackers to target users with great precision

That's why **Mobile Security** is critical to protect your mobile workers, devices, and data. A robust mobile security program includes:

- Preventing security misconfigurations
- Blocking attacks
- Detecting compromise with robust forensics and incident response

Key features

So what security capabilities should you consider implementing for some or all of your mobile fleet?

Secure Configuration Management

Mobile device hardening

- Establish good security hygiene
- Perform compliance audits
- Monitor for configuration vulnerabilities

Patch management

- Prioritize patching with detailed vulnerability reports
- Mitigate OS and app vulnerabilities

Data Loss Prevention

- Control the flow of business data between apps
- Restrict application access based on user or device state

Acceptable Use Policy

- Restrict web usage with dynamic category-based policies
- Enforce AUP by user, group, region, or global configuration

Attack Prevention

Malware & other app risks

- Block malware
- Identify vulnerable and risky apps
- Prevent sensitive data leaks in apps
- Monitor alternative app marketplace usage

Adversary-in-the-Middle

- Identify rogue hotspots and protocol attacks
- Mitigate Adversary-in-the-Middle with encrypted tunnels

Web Threats

- Prevent phishing, including zero-day attacks
- Block malicious network traffic, including C2 and data exfiltration
- Neutralize cryptojacking, spam, and other web-based threats

Secure Access

Protect Data in Transit

- Establish encrypted tunnels to key business applications and data

Audit Critical Application Usage

- Report on all applications being accessed by mobile workers

Enforce Real-time Access Policies

- Establish access policies that incorporate user details and device posture checks

Threat Detection & Response

Collect Rich Telemetry

- Gather detailed logs for offline analysis

Detect Anomalies

- Enable threat hunting and search for anomalies that indicate malicious activity
- Incorporate indicators of compromise and new learnings into threat intelligence to improve future detections

Remediate Threats

- Deny access to critical applications and workloads when compromise detected
- Remove malware and return user to productive state

Achieve Trusted Access Outcomes with Jamf

Jamf helps organizations protect their most prized assets by ensuring that only authorized users, on enrolled devices, that meet the organization's security requirements, are able to access sensitive business applications.

Choose your mobile security capabilities wisely

The threat landscape and our methods of work are constantly evolving. Adequate protections from yesterday don't guarantee security today. Here are some considerations when choosing your mobile security solutions.

Investigate solution capabilities.

It's important to examine what your solution is actually capable of — it's not enough that it claims a "mobile security" feature. Your solution should account for the unique threats to mobile devices, not just apply computer security concepts to a mobile device.'

Security requires device management.

A single security solution may not meet all your requirements, nor is security software alone enough. Device management is critical for security; after all, you can't secure what you can't see. Your management software helps you keep devices in compliance and remediate potential issues.

The user experience is important.

Employees use mobile devices because their mobility helps them stay productive. Security policies that hinder device functionality too much aren't helpful to users, who may find unapproved workarounds to avoid them.

Mobile devices have developed into essential work tools that users rely on to be productive. When devices are experiencing a policy action, it is imperative that workflows be established to return the user to work as quickly as possible.

Not all devices require the same security tooling. Consider the deployment scenario and use case before applying tools and policy configurations. For example:

- Consider how your employees are using their devices. Their roles affect their risks. For example:
  A standard employee with access to some sensitive data and the web needs protection from common threats. Their devices should be kept in compliance and be protected from phishing and malware. Content filtering, threat defense and Zero Trust Network Access help secure them further.
- A deskless worker, like in retail, benefits from content filtering and app security. If their device doesn't have access to a browser, phishing is less of a risk.
- Executives and roles with access to more critical data are often targeted. They require additional protections and often need to meet regulatory requirements.