Quokka Mobile App Risk Intelligence

Q-scout for Corporate-Owned Business-Only

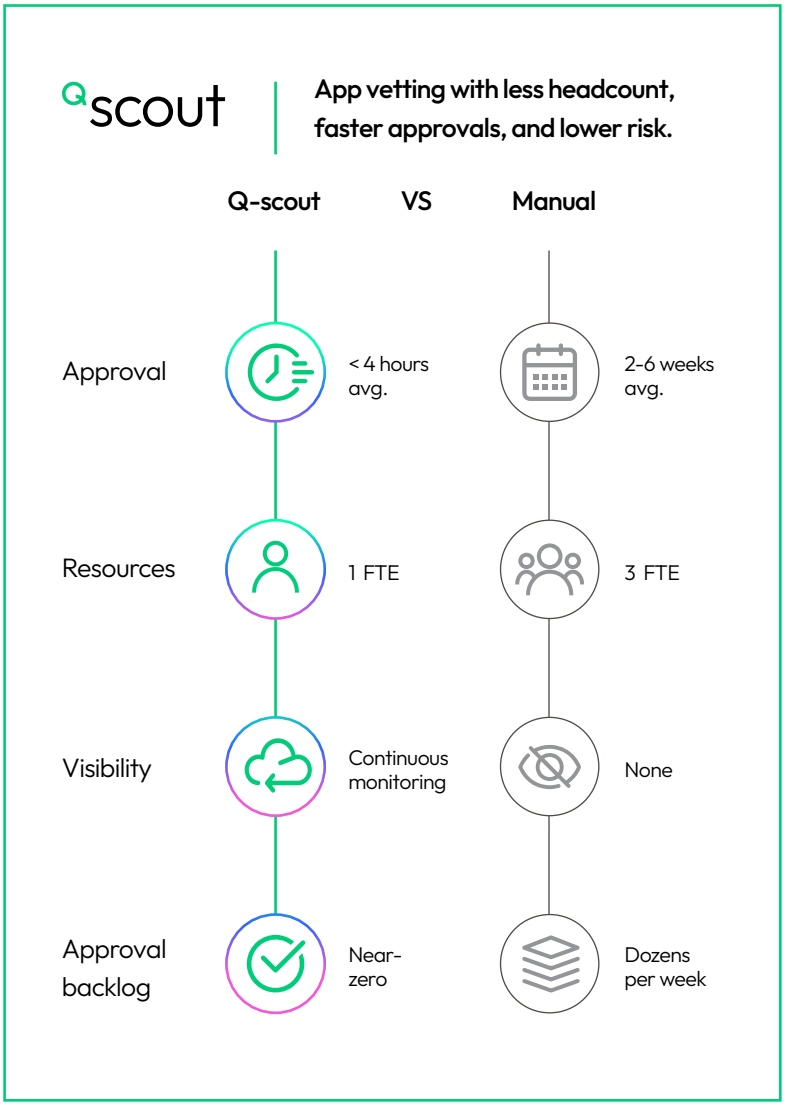
Q-scout accelerates secure app approvals in COBO environments—flagging hidden threats while maintaining security, reducing manual work, and improving productivity across the organization.

COBO (Corporate-Owned, Business-Only) strategies reduce mobile risk through predictability: known devices, managed apps, and defined workflows. But when policies become too rigid, app access slows, and users turn to workarounds—personal devices, unapproved apps, or manual exceptions—reducing productivity.

That's where risk enters the organization.

Traditional COBO App Workflows

- Approval bottlenecks delay field teams and frontline workers
- Users find workarounds—installing unapproved apps or using personal devices
- IT teams are forced to choose between speed and confidence, sacrificing accuracy or productivity
- Apps evolve silently—adding risky SDKs or behaviors post-approval



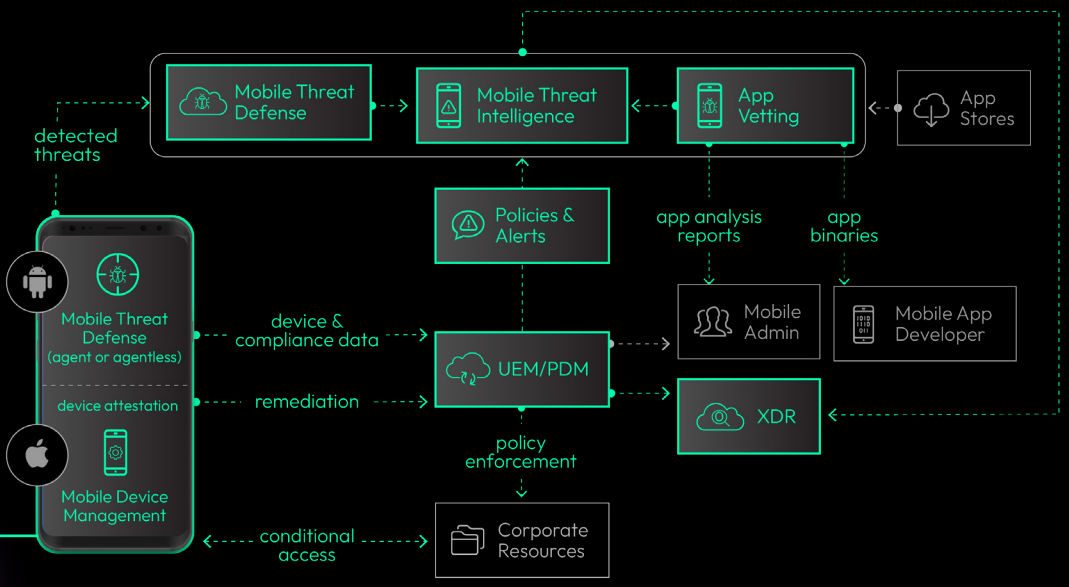
Organizations don't need to choose between accuracy and productivity.

Q-scout analyzes app behavior before and after deployment, flags hidden risks like data exfiltration and malicious SDKs, and integrates seamlessly with existing workflows for policy-based enforcement.

It delivers a complete app vetting and approval solution—no additional tools, working with the tools already in place. Simply select the app, and Q-scout handles the rest—analyzing even the latest OS versions and protected or obfuscated apps to deliver fast, confident decisions.

Works with Your Existing Stack

- ✓ Connects to your existing MDM platforms
- ✓ Sends app risk telemetry to your MDM for automated enforcement
- ✓ Enhances Conditional Access
- ✓ No new apps, agents, or changes for users



Threat detection that goes beyond the surface

Data Exfiltration
Flags apps sending sensitive data to unauthorized or foreign servers.

Risky or Malicious SDKs
Detects embedded code that leaks data or violates compliance. Includes SBOMs and CVE alerts.

Supply Chain Vulnerabilities
Provides full SBOMs for all apps on demand. Alerts on known CVEs in third-party libraries.

Post-Install Behavior Changes
Flags apps that activate hidden or risky features after install.

App Collusion
Detects apps working together to bypass OS restrictions or share data.

C2 Infrastructure Communication
Alerts on traffic to malicious domains or IPs.

Malicious Updates
Flags apps that become risky after updates, SDK changes, or silent payloads.

Case Study

A large global government department replaced manual app reviews with Q-scout

25K+ iOS devices protected

97% reduction in FTEs for app vetting

200+ hours saved in manual review time

+ faster app deployment to field teams

Why Q-scout for COBO environments

Accelerates app approvals
Cuts review time from weeks to hours

Increase employee productivity
More approved apps means less friction and faster work

Detects hidden threats
Flags behaviors missed by app stores and EMMs

Integrates seamlessly
No agents, MDM changes, or user disruption

Supports compliance readiness
Audit-ready reports for GDPR, NIAP, OWASP

Monitors app risk continuously
Detects new risks after approval

Reduces policy exceptions
Enables confident decisions and secure access without delays

Supports all apps natively
Covers obfuscated, RASP-protected, and latest iOS apps without extra tooling

Quokka

Discover how Q-scout helps you maintain security without increasing manual work or slowing down access to apps. **Schedule a demo.**