PulseReport
GATEPOINT RESEARCH

Mobile Threat Defense Strategies

Lookout

Summary Results • April 2016

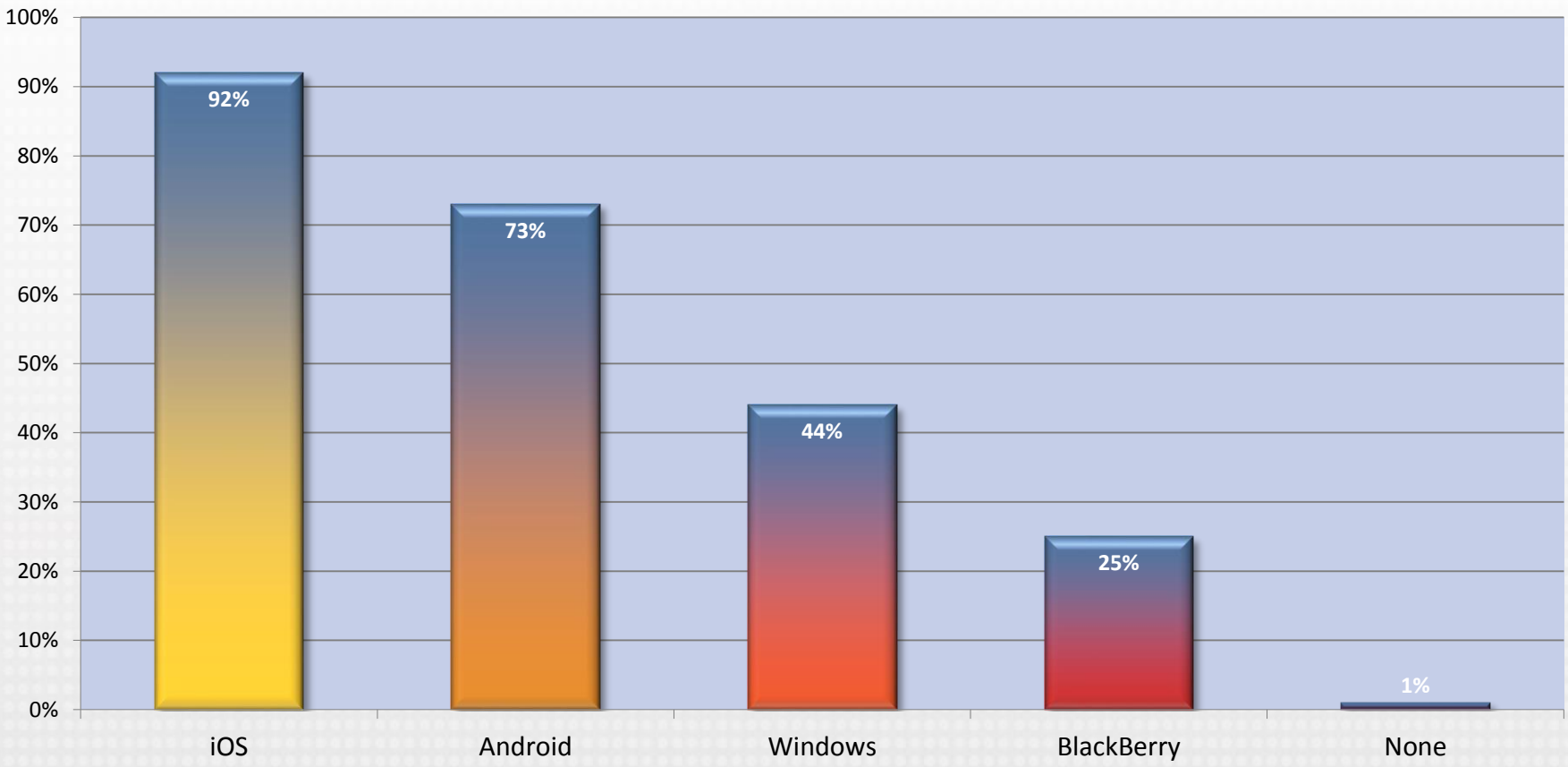
Program Overview

- Between February and April 2016, Gatepoint Research invited selected IT and IT security executives to participate in a survey themed ***Mobile Threat Defense Strategies.***
- Candidates were invited via email and 100 executives have participated to date.
- Management levels represented are predominantly senior decision makers: 10% hold the title CxO, 4% are VPs, 33% are Directors, and 46% are Managers.
- Survey participants represent firms from a wide variety of industries: high tech, general and primary manufacturing; financial services, wholesale trade, transportation, business services, healthcare, utilities, retail trade, and consumer services.
- 88% of survey responders work in Fortune 1000 companies with revenues over $1.5 billion.
- 100% of responders participated voluntarily; none were engaged using telemarketing.

Observations and Conclusions

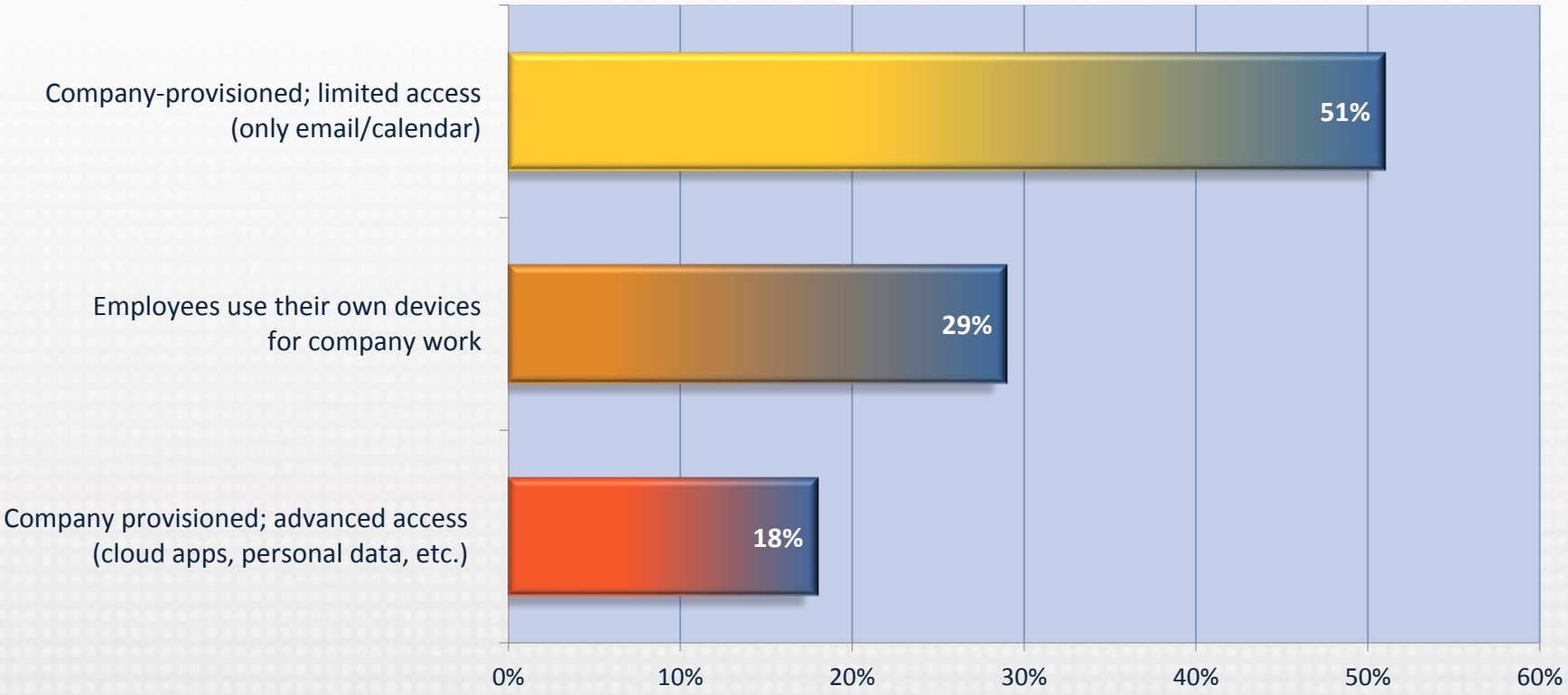
- **Companies formally support the leading mobile OS's**. Asked which mobile operating systems their organization formally supports, 92% of respondents list iOS , but high levels of support are also cited for Android, Windows, and BlackBerry. Only 1% answered "none."
- **Limited, company-provisioned device support is still most prevalent.** 51% of respondents report their company supports only limited-access, company-supplied email/calendar apps. 29% require employees to use their own devices.
- **information accessed through mobile is not secure.** 22% of respondents don't trust the security of enterprise information when it is accessed on employee devices or through mobile applications. Another 19% are not sure.
- **Mobile security measures: MDM, Identity management, remote lock**. Respondents' top solutions to thwart mobile environment threats include using mobile device management (86%), ID management (84%), and remote lock/wipe capability (75%).
- **The big challenge? Balancing user vs. enterprise needs.** Asked about the security challenges associated with a mobile workforce, respondents' top challenge is providing user satisfaction while still serving enterprise needs (57%).
- T**his year's model: secure and satisfying.** Respondents report their top goals in mobile security over the nest 12-24 months include deploying secure apps (49%), increasing user satisfaction (41%), and more secure customer-facing apps (40%).
- **Protecting phones and tablets is key.** Respondents rated six key aspects of mobile security solutions. Highest priority: securing smartphones and tablets from all threats (70%).

What mobile operating systems does your organization formally support?



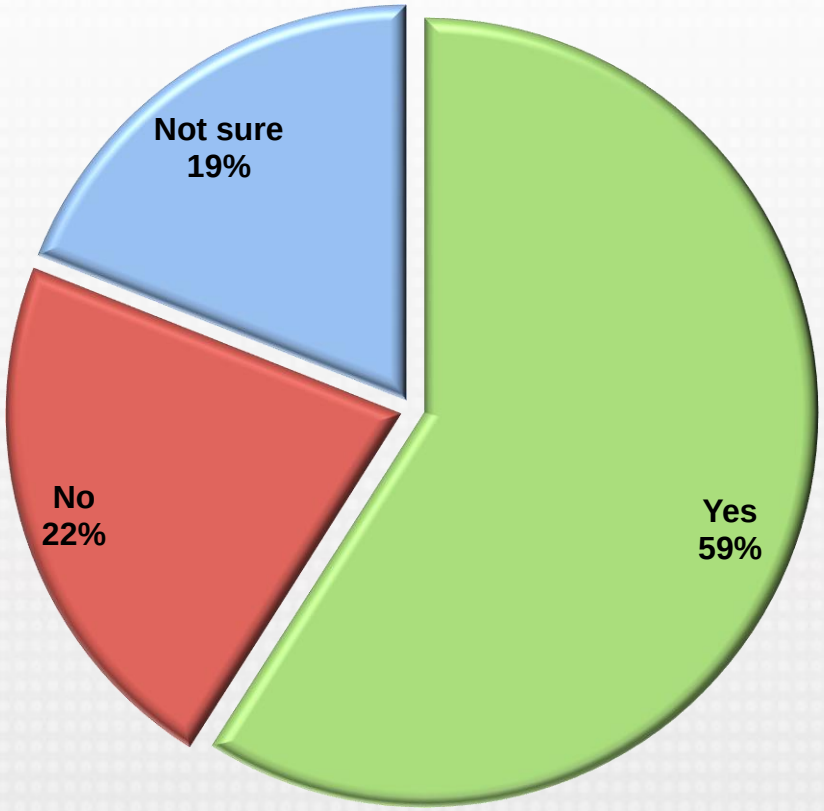
Companies formally support the leading mobile OS's. *Asked which mobile operating systems their organization formally supports, 92% of respondents list iOS , but high levels of support are also cited for Android, Windows, and BlackBerry. Only 1% answered "none."*

What is the most common form of device ownership that your organization supports?



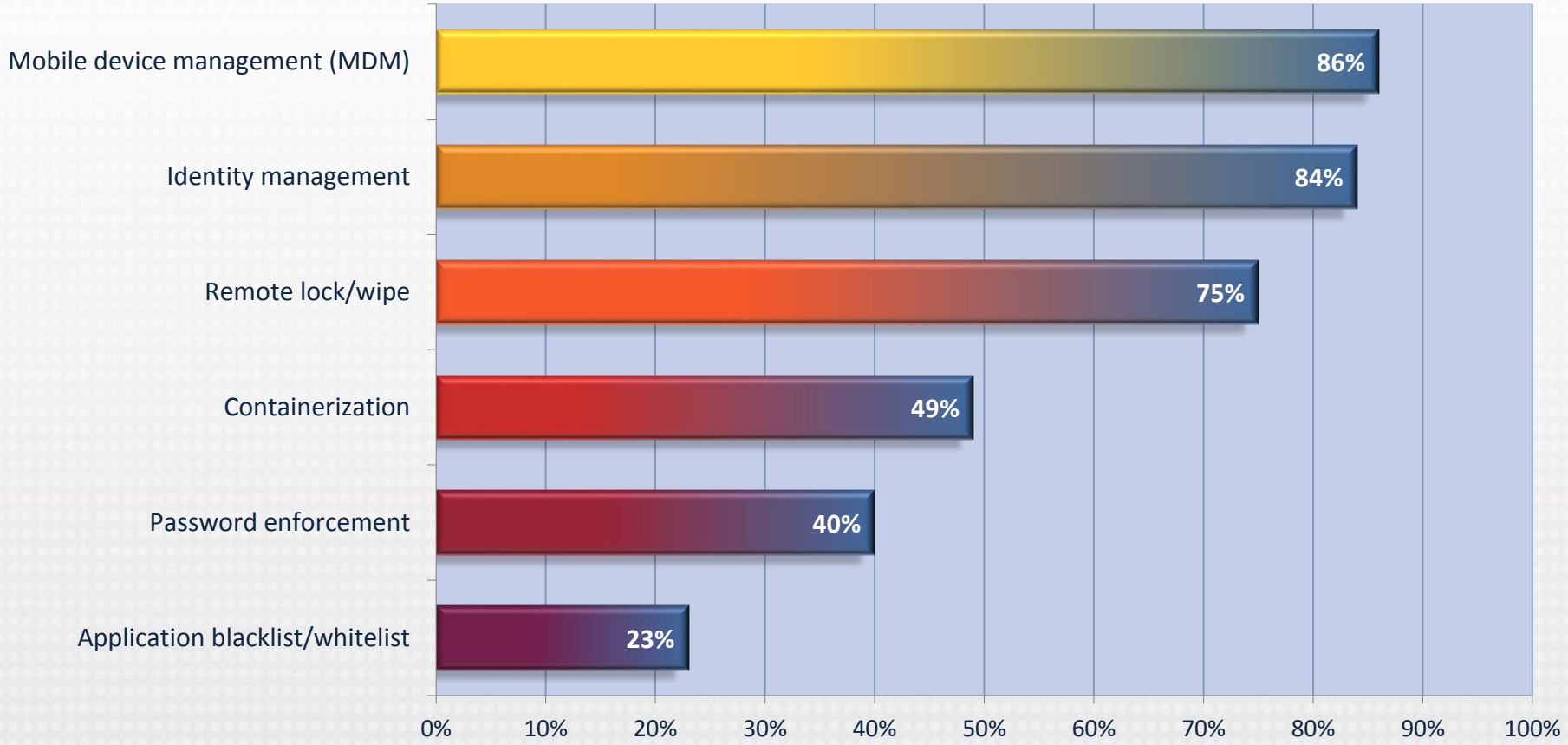
Limited, company-provisioned device support is still most prevalent. *51% of respondents report their company supports only limited-access, company-supplied email/calendar apps. 29% require employees to use their own devices.*

Do you trust that the information accessed on employee devices and mobile applications is adequately secured in your enterprise?



information accessed through mobile is not secure. *22% of respondents don't trust the security of enterprise information when it is accessed on employee devices or through mobile applications. Another 19% are not sure.*

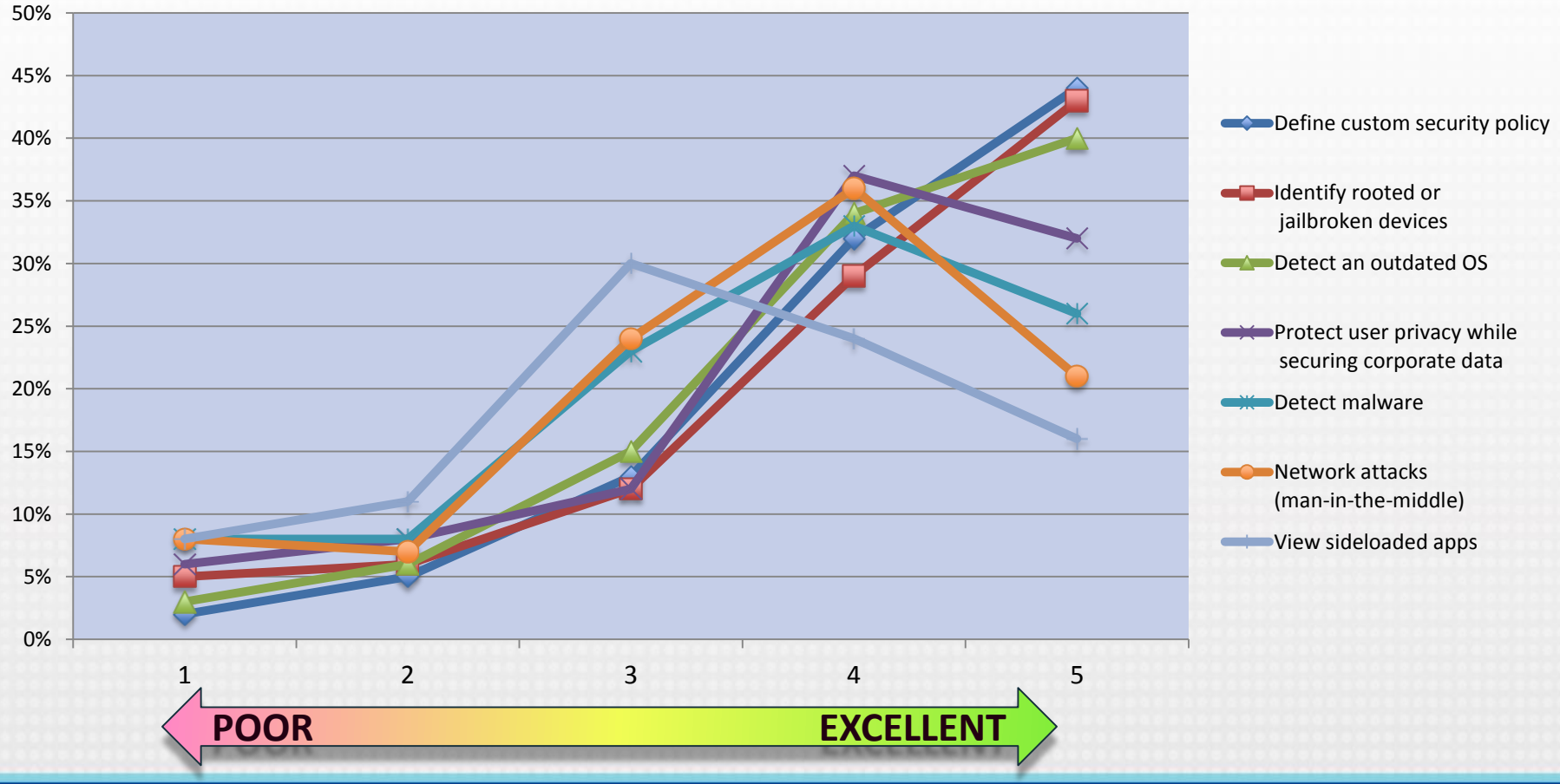
What solutions do you rely on to protect the enterprise from threats in the mobile environment?



***Mobile security measures: MDM, Identity management, remote lock**. Respondents' top solutions to thwart mobile environment threats include using mobile device management (86%), ID management (84%), and remote lock/wipe capability (75%).*

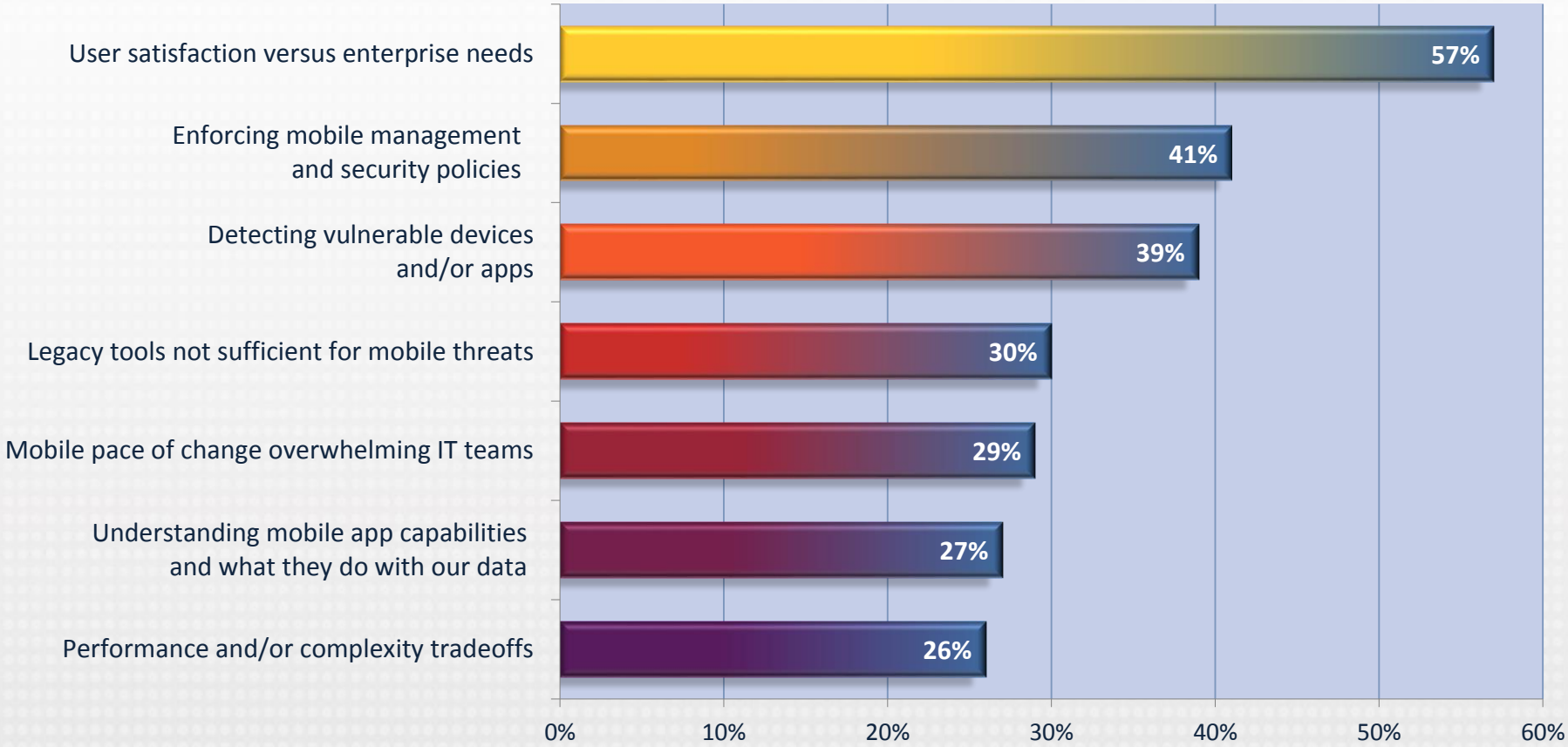
How would you rate your current capabilities to address the following?

(rate 1-5, 1=poor, 5=excellent)



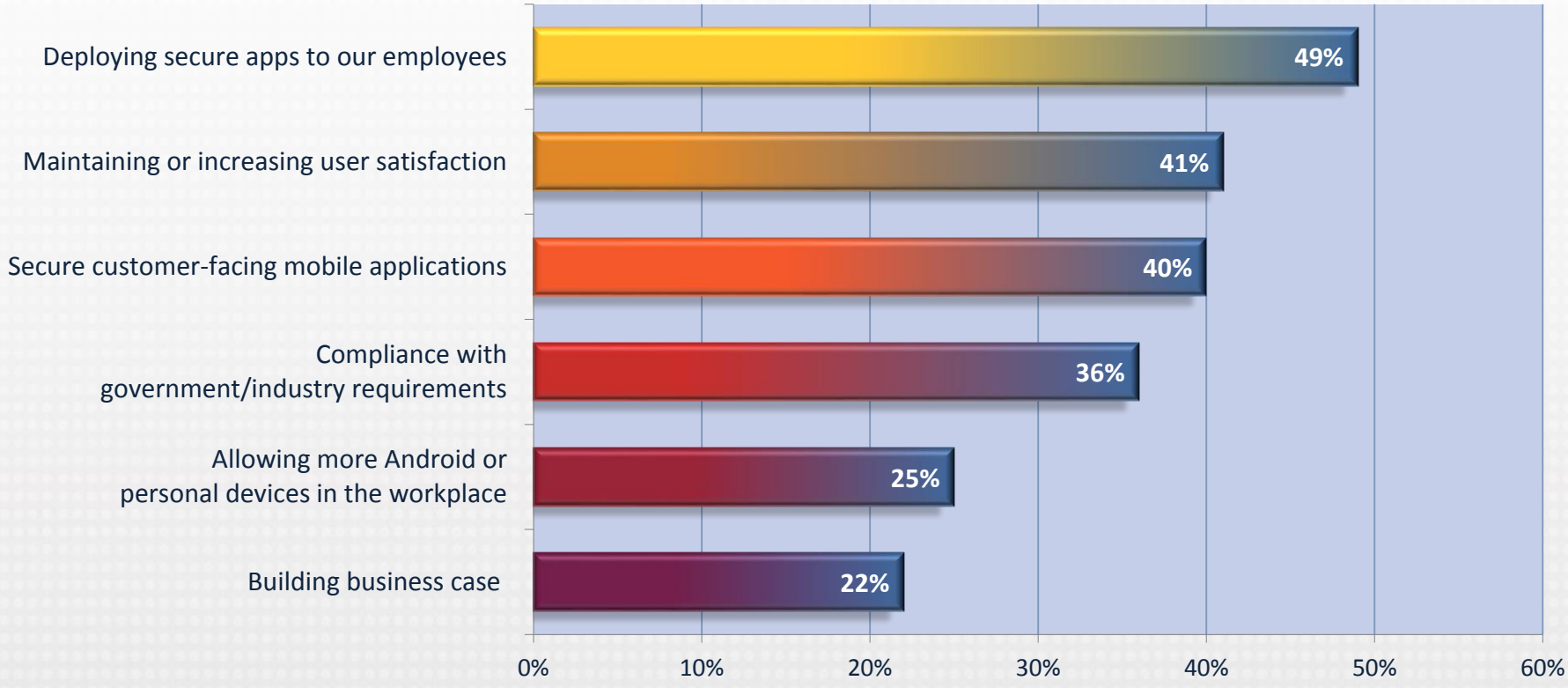
Good at security policy, poor at thwarting network attacks. *Asked about current capabilities, respondents give themselves high marks for defining custom security policy, but are less confident that they can handle network attacks.*

What security challenges are you struggling with to enable a mobile workforce?



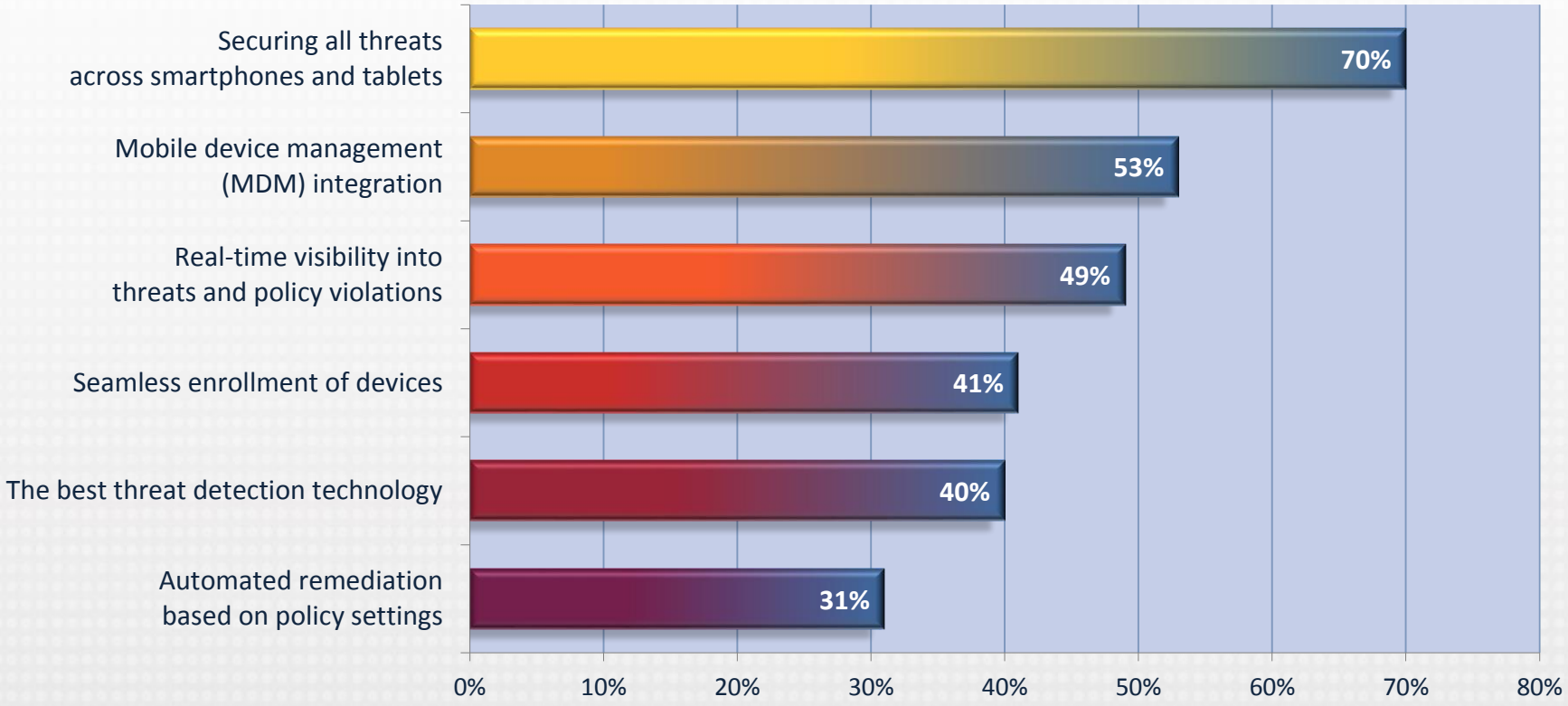
The big challenge is balancing user vs. enterprise needs. *Asked about the security challenges associated with a mobile workforce, respondents' top challenge is providing user satisfaction while still serving enterprise needs (57%).*

What are your priorities for securing mobility over the next 12-24 months?



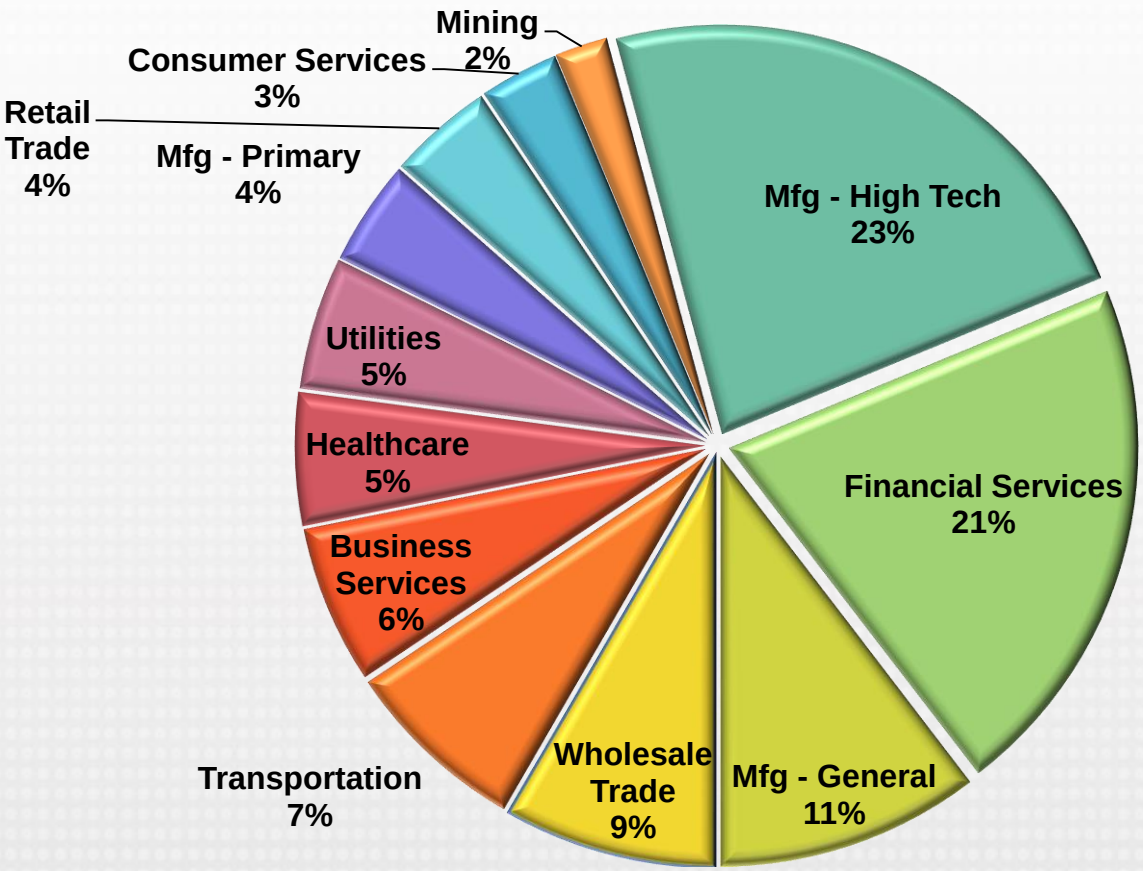
This year's model: secure and satisfying. *Respondents report their top goals in mobile security over the nest 12-24 months include deploying secure apps (49%), increasing user satisfaction (41%), and more secure customer-facing apps (40%).*

What key aspects most matter to you in mobile security solutions?



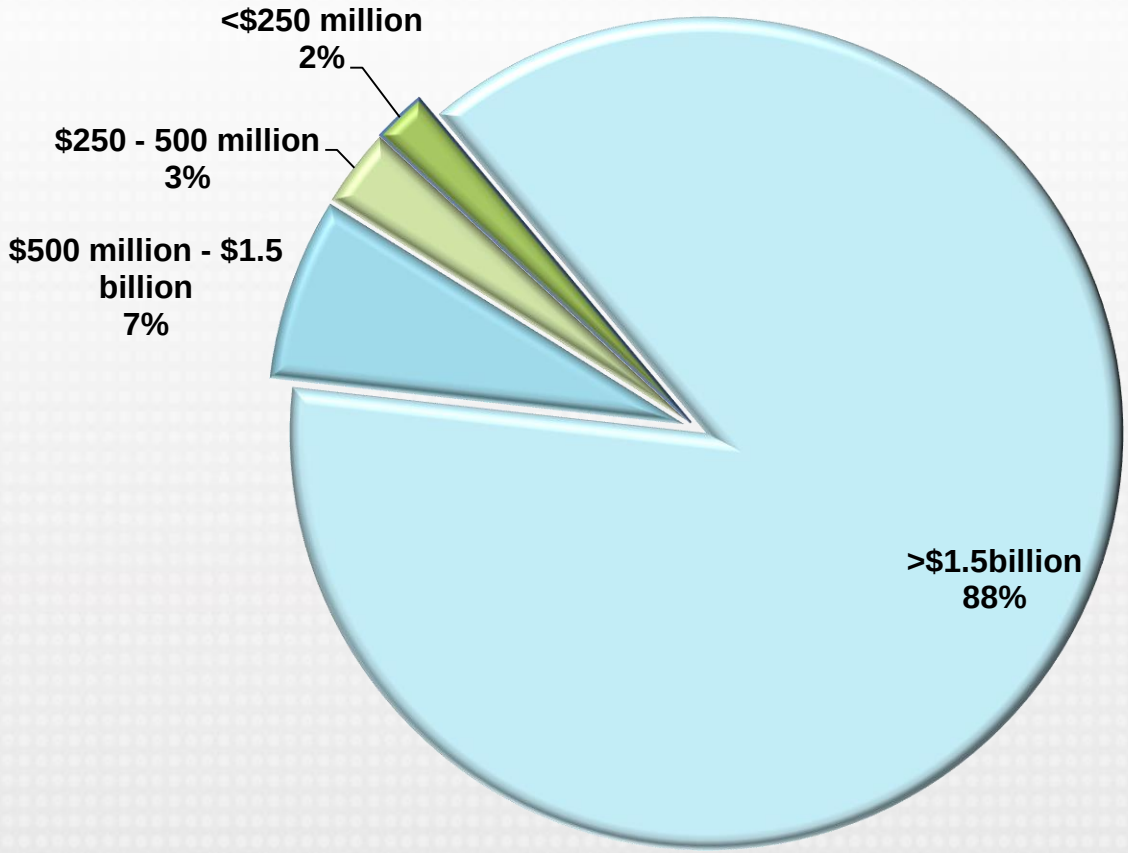
Protecting phones and tablets is key. *Respondents rated six key aspects of mobile security solutions. Highest priority: securing smartphones/tablets from all threats (70%).*

Profile of Responders: Industry Sectors



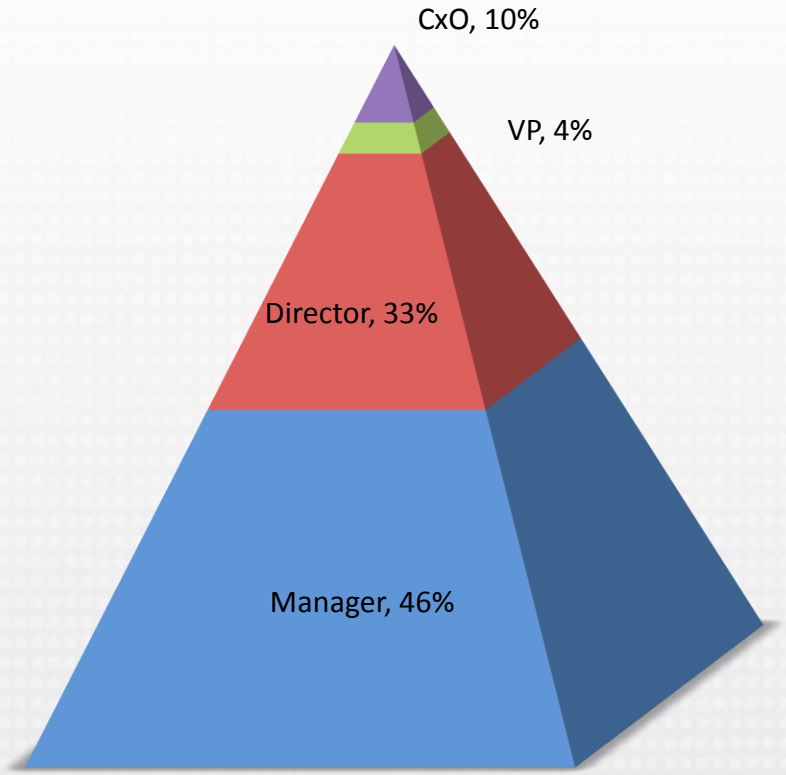
A wide variety of industry sectors were represented in the survey.

Profile of Responders: Revenue



88% of survey responders work in Fortune 1000 organizations with annual revenues of more than $1.5 billion.

Profile of Responders: Job Level



47% of responders hold executive level positions in their organizations.

Lookout Mobile Threat Protection (MTP) is the only enterprise mobile security solution that can anticipate and defeat the next generation of mobile threats. With an easy-to-deploy endpoint agent on your employees' devices, Lookout provides real-time threat data to a centralized admin console, allowing you to enforce security policies and protect against advanced attacks.

To learn more, go here.