

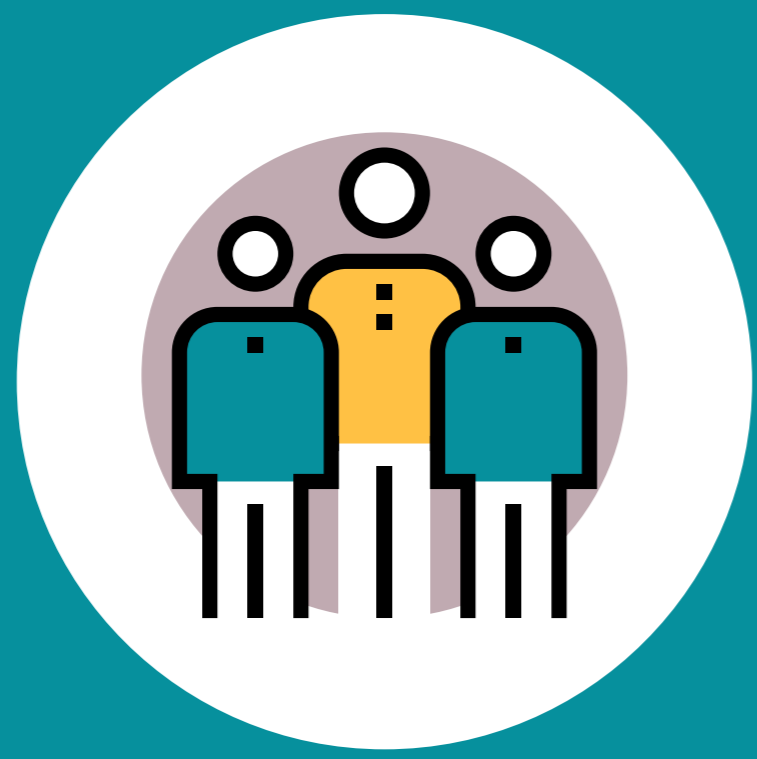
SECURITY CHALLENGES OF BYOD

EMPLOYER MOBILE SECURITY MANAGEMENT



86%

preferred to manage mobile security in a common end-point management environment



74%

agreed involving employees is a good way to improve security measures



72%

agreed allowing employees to use different security solutions is too time consuming



69%

agreed they try to include employees in mobile security decisions



66%

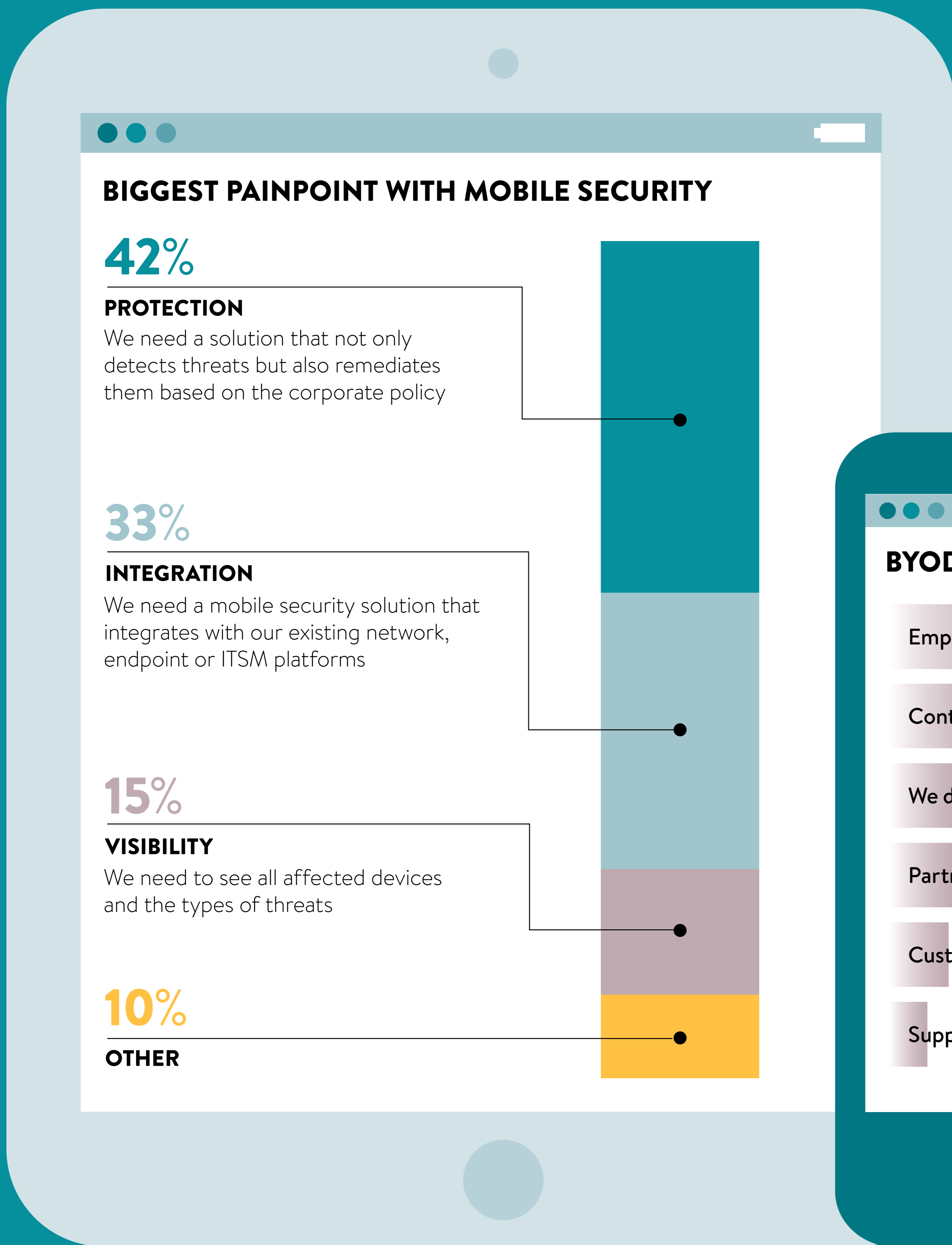
agreed potential productivity increases from personal devices outweighed risks



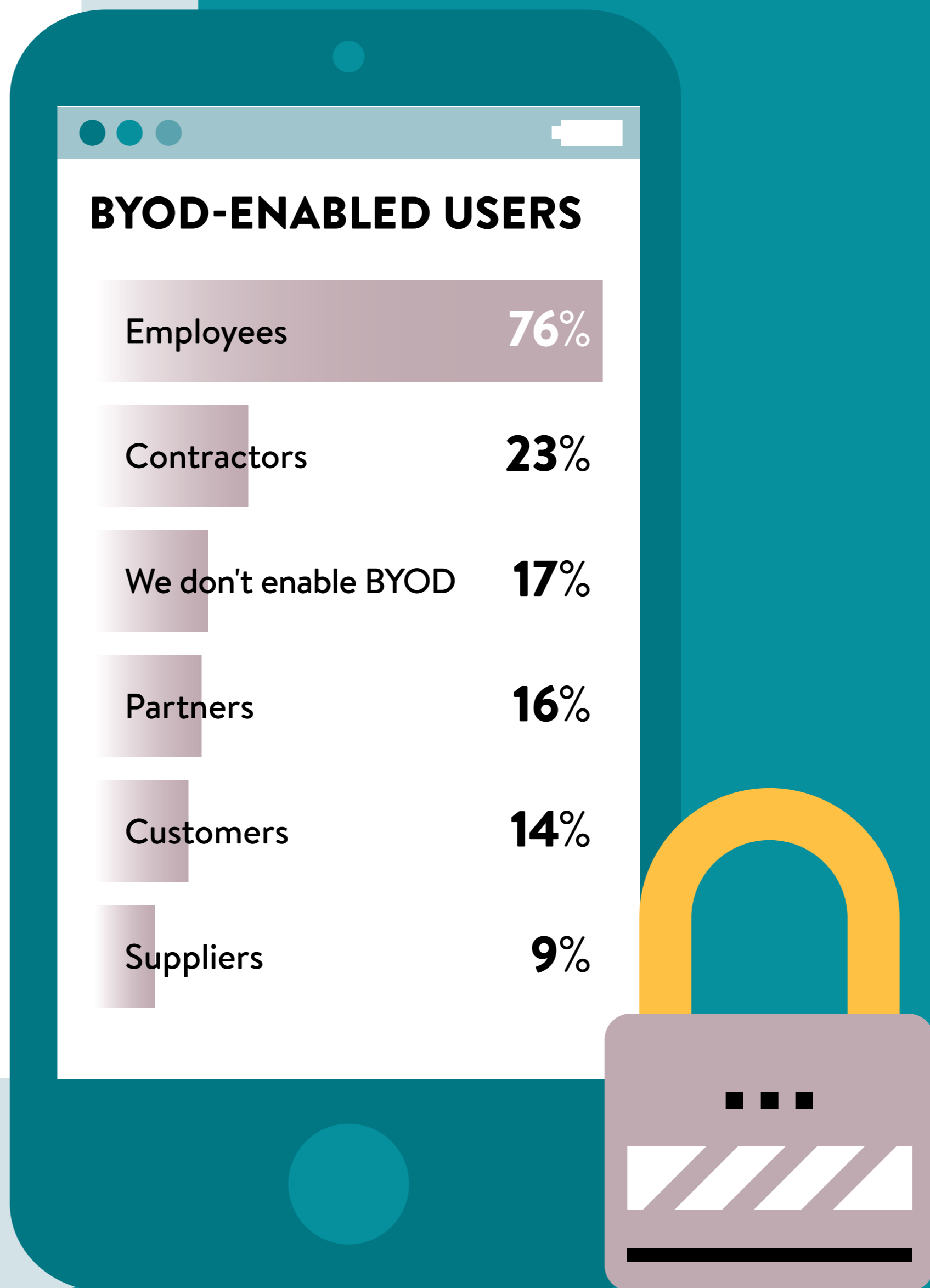
57%

agreed employees have enough knowledge of security apps to make the right decision

Source: Webroot 2014



67%
of BYOD users have a security app installed
Source: Webroot 2014



Source: Crowd Research Partners 2016

MAIN SECURITY CONCERNS RELATED TO BYOD

72%

Data leakage/loss

56%

Unauthorised access to company data/systems

54%

Users download unsafe apps or content

52%

Malware

50%

Lost/stolen devices

49%

Vulnerability exploits

48%

Inability to control endpoint security

39%

Ensuring security software is up to date

38%

Compliance with regulations

37%

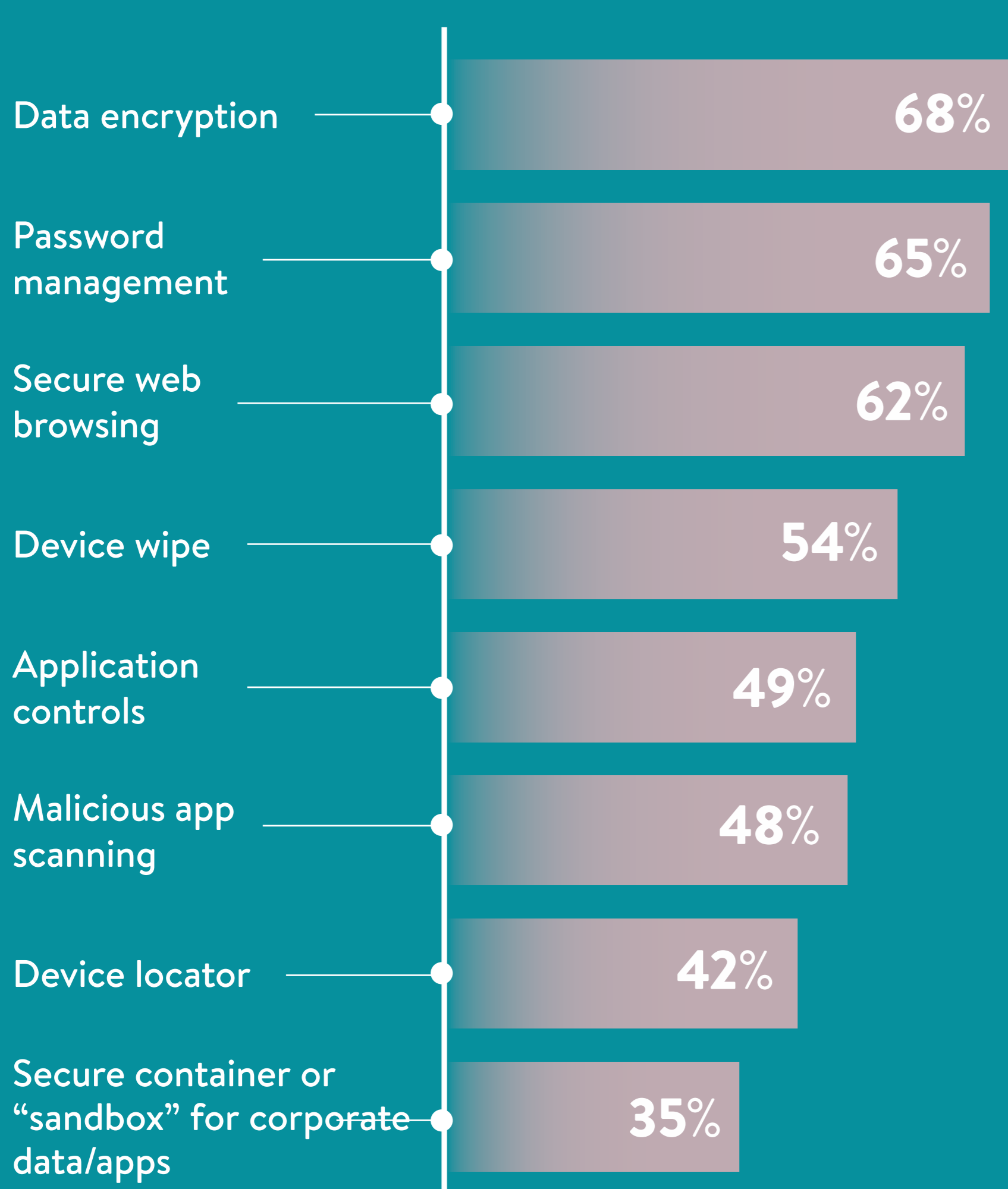
Device management

35%

Network attacks via wi-fi

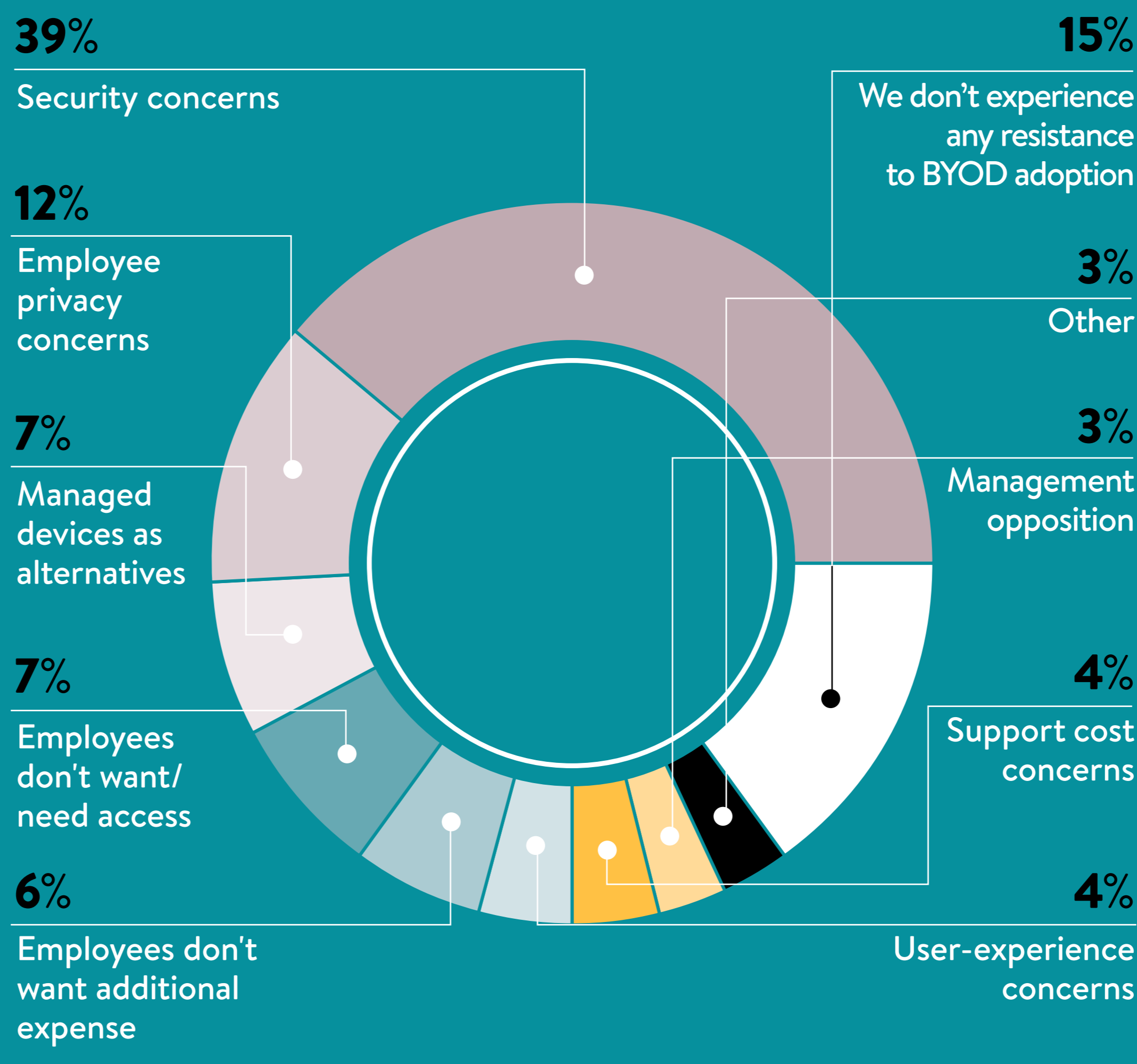
Source: Crowd Research Partners 2016

ESSENTIAL MOBILE SECURITY FEATURES



Source: Webroot 2014

INHIBITORS TO BYOD ADOPTION



Source: Crowd Research Partners 2016

EMPLOYEE CONCERNS OVER MANDATED SECURITY



Source: Webroot 2014