2018

Cybersecurity
INSIDERS

MOBILE SECURITY & BYOD REPORT

ZIMPERIUM

INTRODUCTION

Our professional and personal lives continue to become more digitized as we interact with mobile and IOT devices. These devices enhance countless data-based interactions but also open our lives and enterprises to data and privacy risks.

As mobility grows in the workplace, so do challenges from managing bandwidth and device access to handling the most pressing concerns of security. The 2018 Mobile Security Report focuses on these security challenges and provides insights on the state of enterprise mobile threats and solutions.

The computers most vulnerable to cyber threats in the enterprise are mobile phones and tablets. Security teams are often blind to the actual risks these devices and apps pose for the enterprise and worse, are unable to deal with threats as they appear.

Many enterprises manage mobile device access to corporate systems, networks, and identity, but they lack the ability to remediate a threat they can't identify. As more of our computing initiates directly from mobile devices to cloud services, network threat detection solutions are ineffective. Transactions and data often reside outside the corporate data center and perimeter. Therefore, you need to adopt non-signature based mobile threat defense to provide your teams with threat intelligence to remediate threats to your most used endpoints — mobile devices.

Shridhar Mittal
CEO, Zimperium

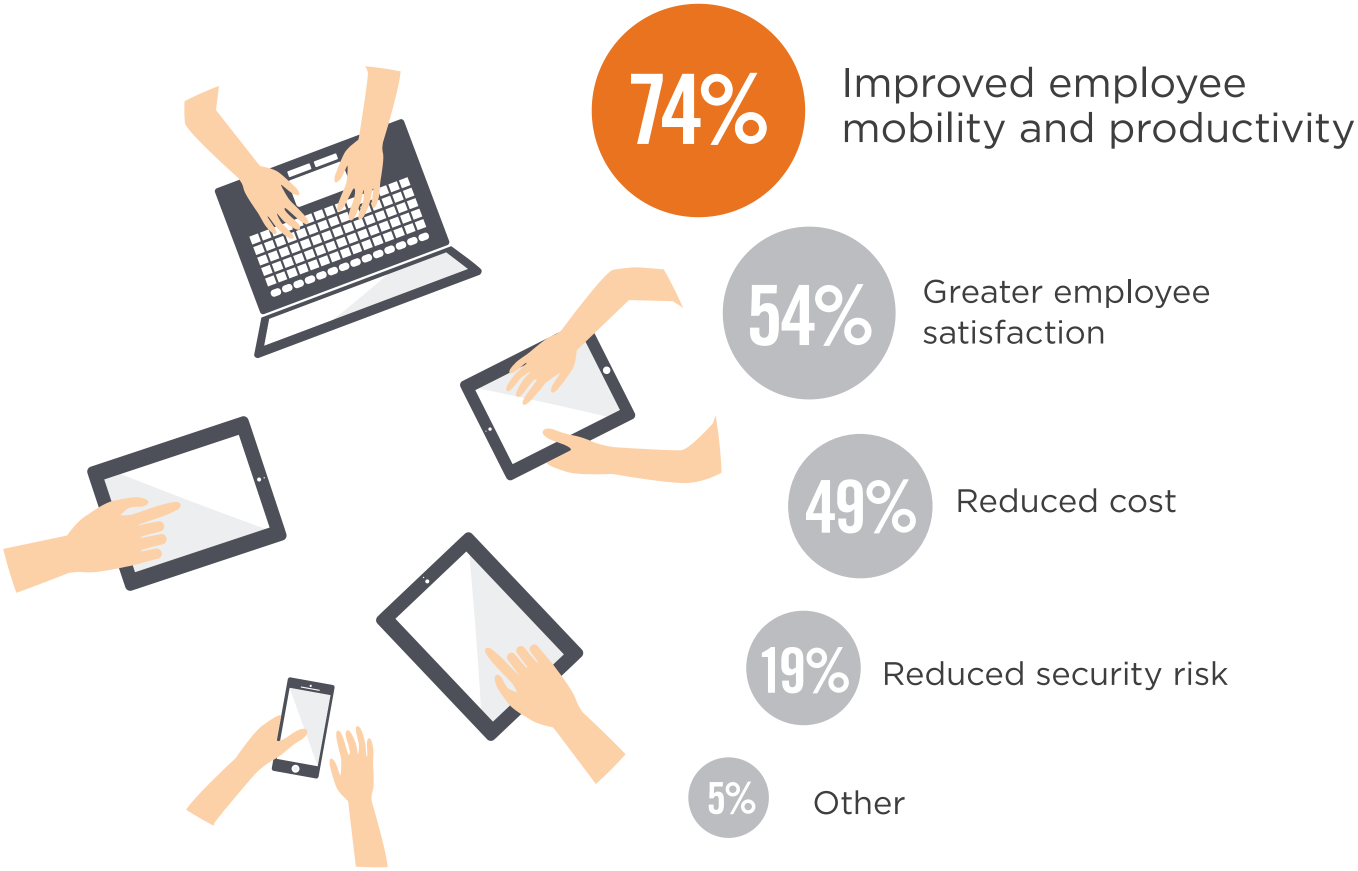
ZIMPERIUM®

BYOD

BENEFITS OF BYOD

We live in a world where mobility is truly ubiquitous and enterprises are benefiting from it. Organizations see a number of significant benefits from adopting BYOD programs. By far, the most common benefit mentioned in our survey is improved employee mobility and productivity (74%), a nine-percentage point jump from last year's survey. Following that is greater employee satisfaction (54%) and reduced cost (49%), a five-percentage point drop compared to last year. It's interesting, considering that BYOD is often considered a security concern, that 19% of the respondents said a benefit of BYOD is reduced security risk (up from 11% last year).

What are the main benefits of BYOD for your company?



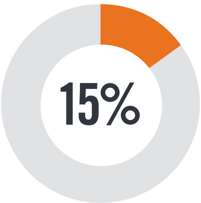
BYOD ADOPTION INHIBITORS

What's keeping organizations from adopting BYOD? There are lots of inhibiting factors. But easily the most common is a concern about information security, cited by 30% of the respondents. Also mentioned as inhibitors are employee privacy concerns (14%), and support cost concerns (11% - up from 4% in last year's survey). Fifteen percent of the respondents said their organization doesn't experience any resistance to BYOD adoption.

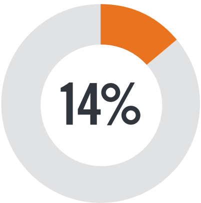
What do you believe is the number one inhibitor to BYOD adoption in your organization?

30%

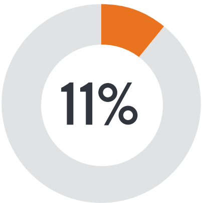
Information security concerns



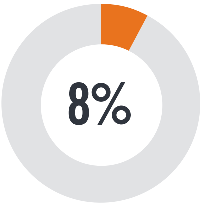
We don't experience any resistance to BYOD adoption



Employee privacy concerns (e.g., over EMM software)



Support cost concerns



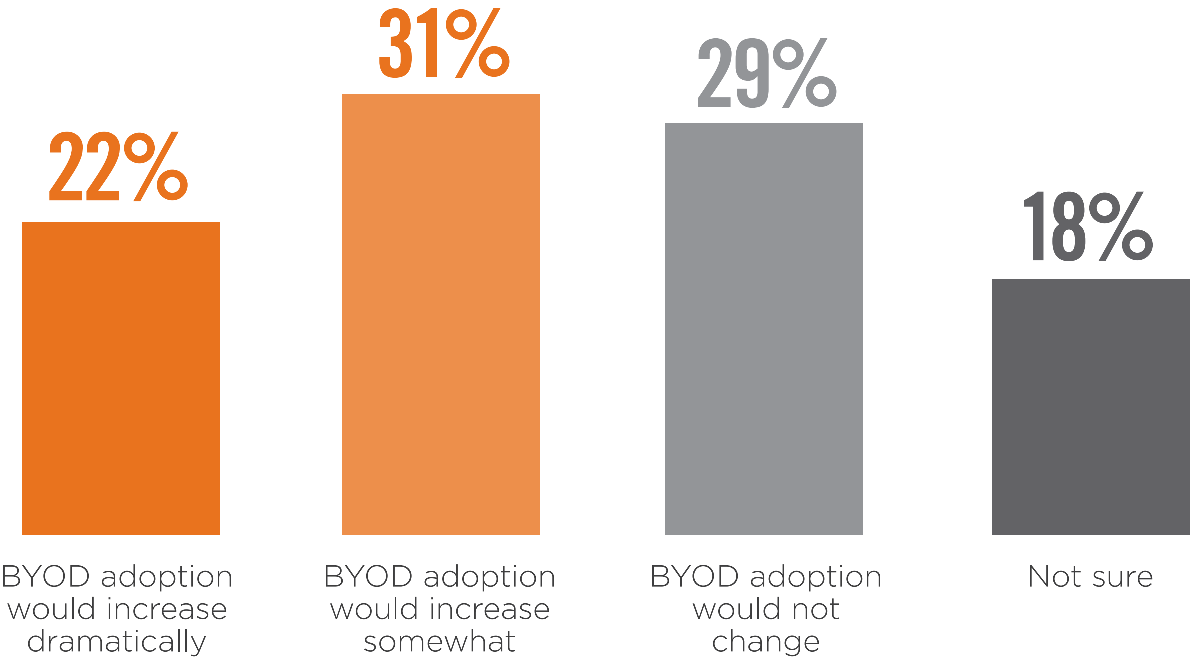
Employees don't want or need access through personal devices

We offer managed/company owned devices as alternatives 8% | Employees don't want to take on the additional expense 5% | User experience concerns (battery life, don't like app choices, etc.) 3% | Management opposition 3% | Other 3%

PERSONAL APPS AND DATA

Respondents were asked how BYOD adoption would change if IT could not view or alter personal data and apps in their organization – one key barrier to BYOD acceptance by employees. Over half of respondents agree that adoption would increase. The largest percentage (31%) said BYOD adoption would increase somewhat, and 22% said it would increase dramatically. Another 29% said BYOD adoption would not change, and 18% were not sure what the impact would be.

How would BYOD adoption change if IT couldn't view or alter personal data and apps in your organization?


22%
31%
29%
18%
BYOD adoption would increase dramatically
BYOD adoption would increase somewhat
BYOD adoption would not change
Not sure

BYOD SECURITY CONCERNS

Organizations have many security concerns about BYOD. At the top of the list is data leakage or loss, including corporate data removal at the time of employee separation or device disposal (61%). Other critical concerns include unauthorized access to company data and systems (53%), users downloading unsafe apps or content (53%), lost or stolen devices 52%), malware (51%), vulnerability exploits (49%), inability to control endpoint security (41%), device management (39%), compliance with regulations (35%), and ensuring that security software is up-to-date (34%). Only 4% of the respondent said there were no concerns about BYOD.

What are your main security concerns related to BYOD?

61%

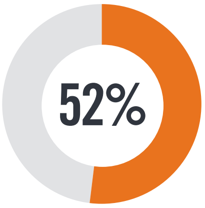
Data leakage/loss
(incl. corporate data removal at the employee separation or device disposal)

53%

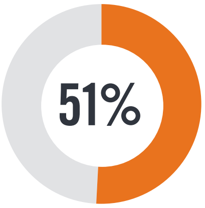
Unauthorized access to company data and systems

53%

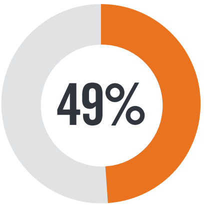
Users download unsafe apps or content



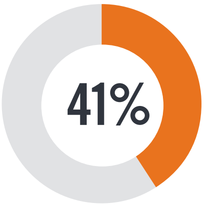
Lost or stolen devices



Malware



Vulnerability exploits



Inability to control endpoint security

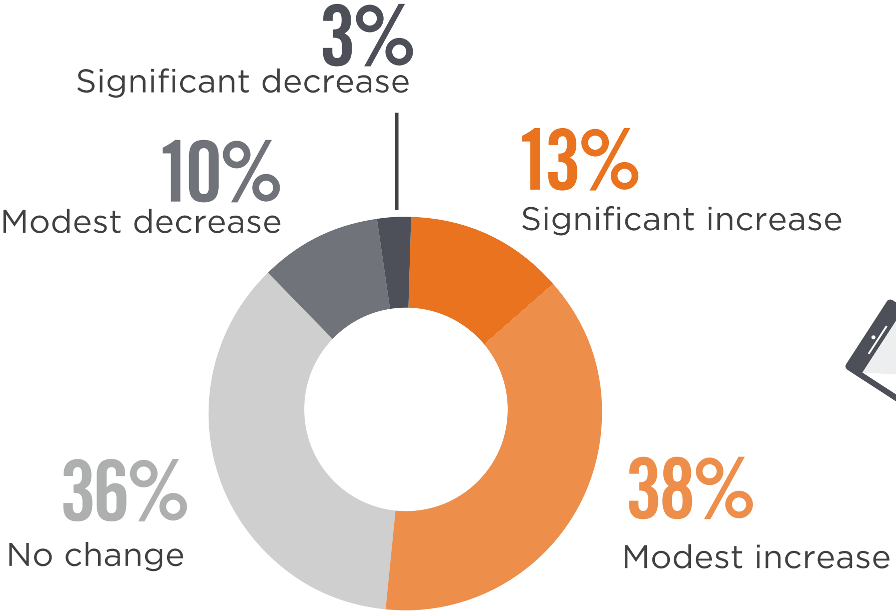
Device management 39% | Compliance with regulations 35% | Ensuring that security software is up-to-date 34% | None/other 5%

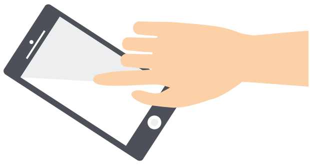
THREATS AND ATTACKS

RISING MOBILE THREATS

The dramatic growth of mobile devices continues to drive an increase in cybercrime, from stolen identities to major data breaches. Fifty-one percent of respondents observe either a moderate increase (38%) or significant increase (13%) in mobile device threats in the past 12 months. Only very few respondents (14%) see modest or significant decreases in mobile threats.

How has the volume of mobile device threats targeting your users' smartphones and tablets changed in the past 12 months?

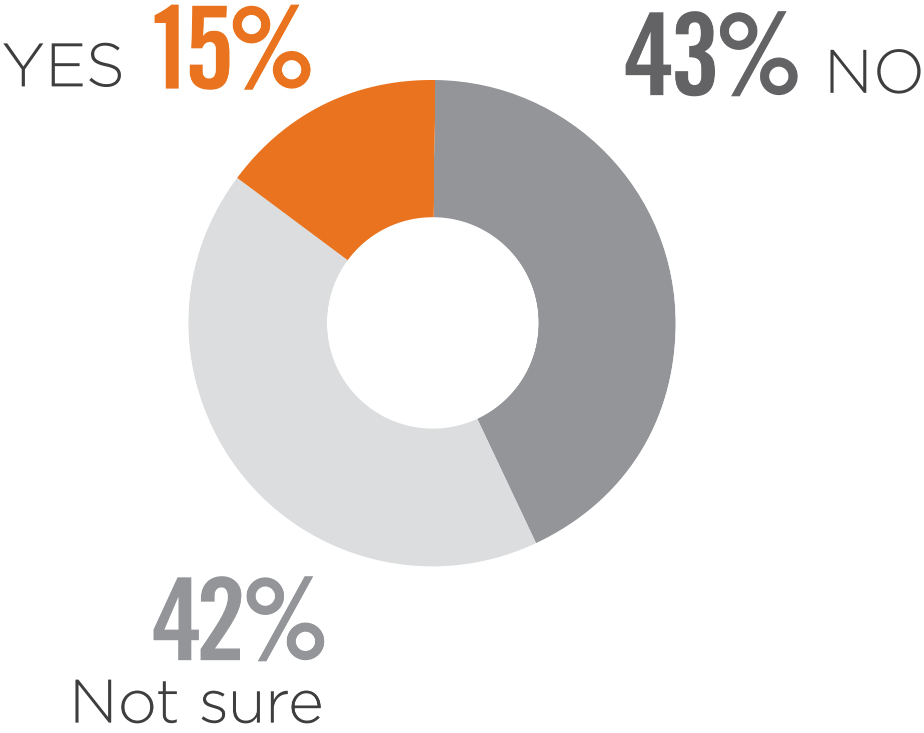




PAST SECURITY BREACHES

An alarming four of ten cybersecurity professionals can’t tell whether mobile devices have been involved in security breaches in their organization.

Have mobile devices been involved in security breaches in your organization in the past?



NEGATIVE IMPACT

Mobile security threats impact organizations in many significant ways, mostly related to the cost and effort to mitigate malware infections (22%) and deployment of additional IT security staff to manage mobile security (21%).

▶ **What actual negative impact did mobile threats have on your company in the past 12 months?**

22%

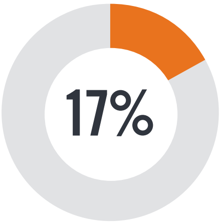
Malware infections and related cost

21%

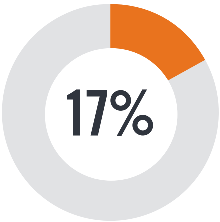
Additional IT resources needed to manage mobile security

20%

Unauthorized access to corporate data and systems



Disrupted business activities



Reduced employee productivity

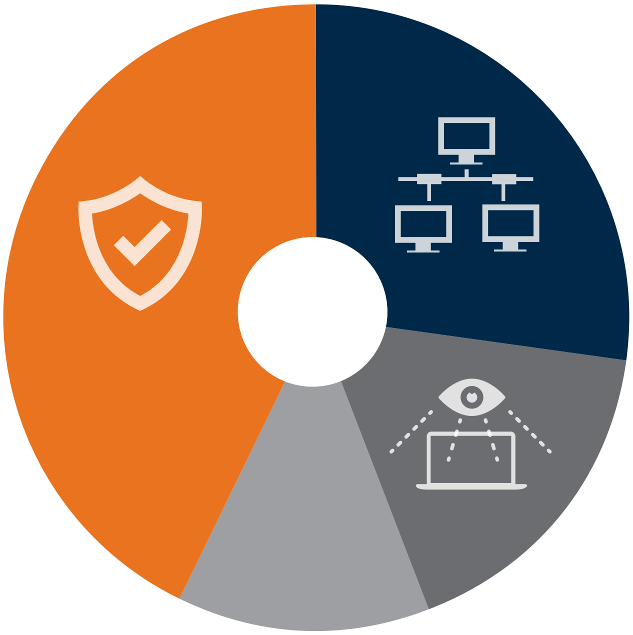
Data loss or leakage occurred

None 31% | The company had to pay regulatory fines 5% | Other 4%

MOBILE SECURITY REQUIREMENTS

When it comes to the biggest pain point associated with mobile security solutions, respondents are most concerend about protection capabilities (43%) over ease of integration into existing IT infrastructure (27%) and visibility into attacks and affected devices (17%).

What is your biggest pain point when it comes to mobile security?



43%
PROTECTION
We need a solution that detects threats and remediates them based on the corporate policy

27%
INTEGRATION
We need a mobile security solution that integrates with our existing network (e.g., SIEM), Endpoint (e.g., MDM or EMM), or ITSM (e.g., System Center) platforms

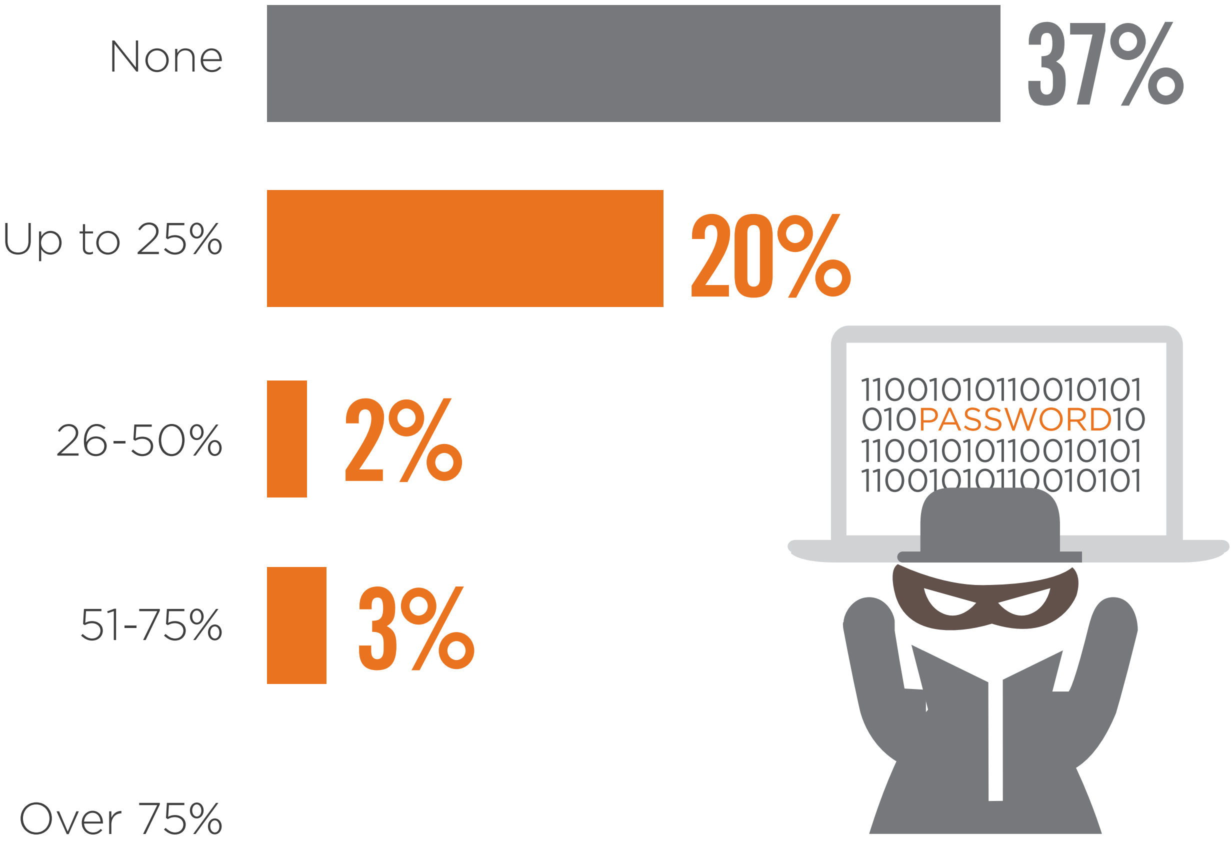
17%
VISIBILITY
We need to see all affected devices and the types of threats

13%
NONE/OTHER

HACKED DEVICES

Six of ten organizations confirm their mobile devices have been hacked or implicated in data leaks.

How many of your mobile devices were hacked or had data leaks?

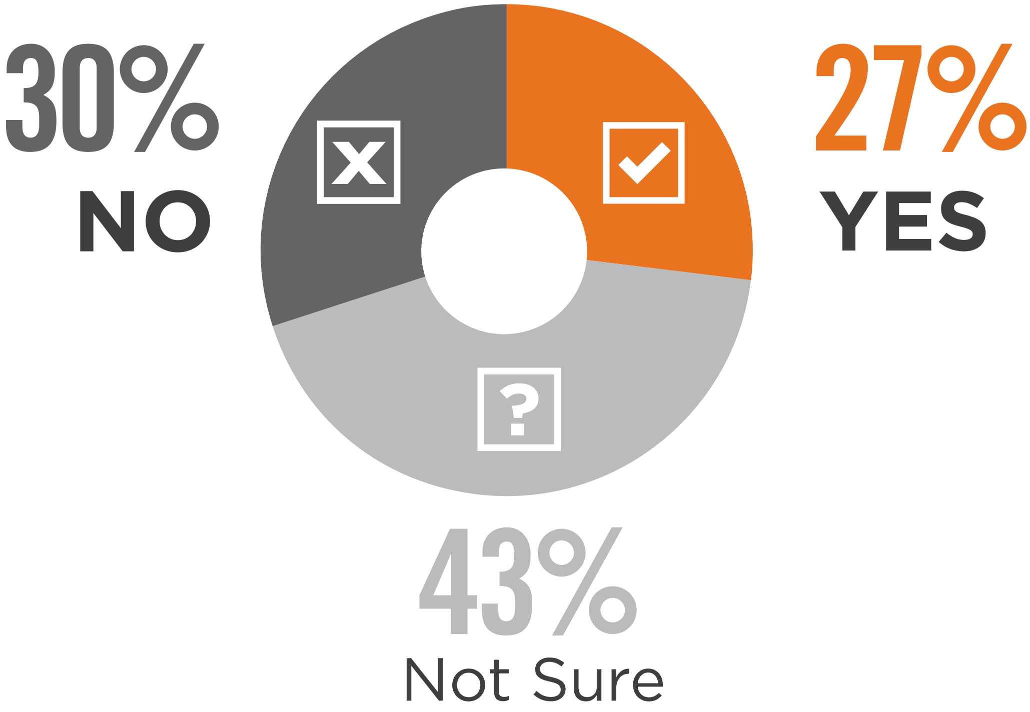


Don’t know/can’t disclose 38%

MALWARE ATTACKS

About one quarter of the organizations surveyed (27%) have had malware downloaded by BYOD or corporate-owned devices. Slightly more (30%) claim they have not had malware downloaded by devices. The largest, and perhaps most alarming share of organizations (43%) are not sure or can’t disclose whether they’ve had a malware download on any devices.

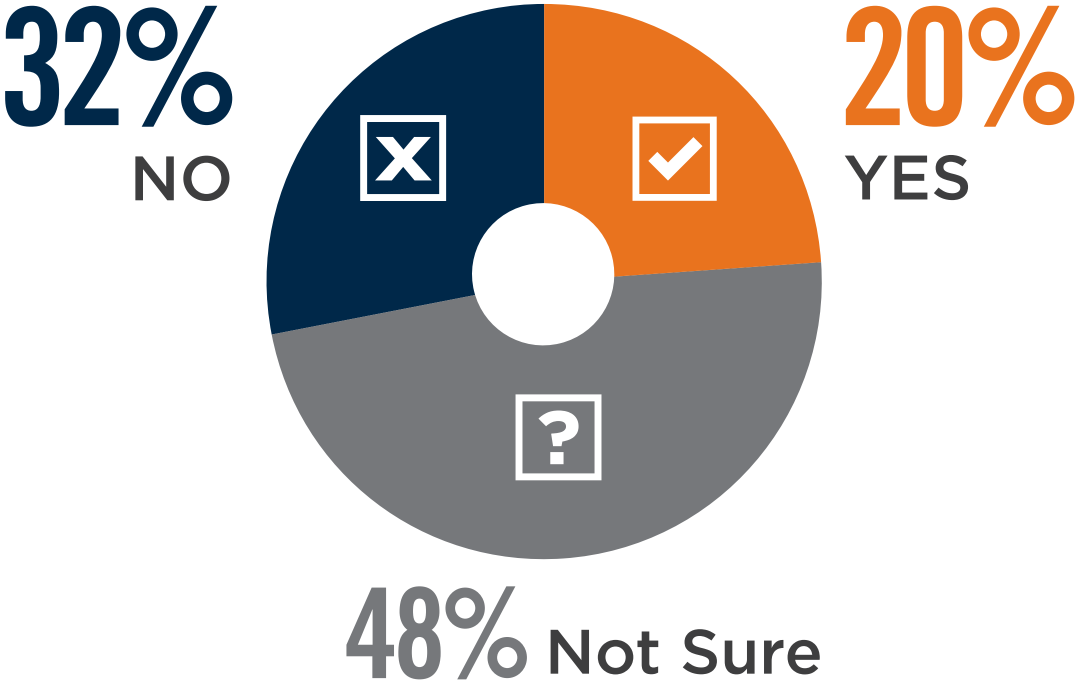
▶ **Have any of your BYO or corporate-owned devices downloaded malware in the past?**



MALICIOUS WIFI

Twenty percent of organizations confirm their mobile devices have connected to malicious WiFi networks in the past. Equally alarming is that about half of organizations has no way of knowing their vulnerability to malicious WiFi.

Have any of your BYO or corporate-owned devices connected to a malicious WiFi in the past?



MOBILE SECURITY TECHNOLOGIES

Organizations are using a host of mobile security technologies and policies to protect data, systems and users. Among the most common technologies are password protection (68%), endpoint security tools (62% - up from 43% in last year's survey), and mobile device management (56%).

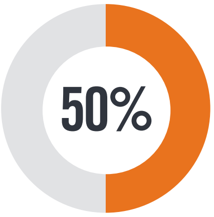
Which of the following mobile security technologies are in place or planned?

68%
Password protection

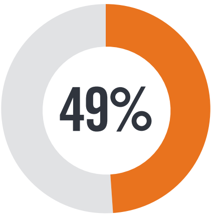
62%
Endpoint security tools

56%
Remote wipe

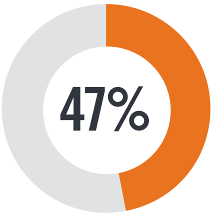
56%
Mobile device management (MDM)



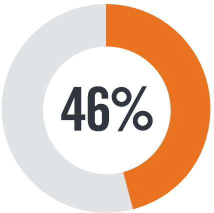
Device encryption



Data removal at employee separation or device disposal



VPN to on-premises security gateway



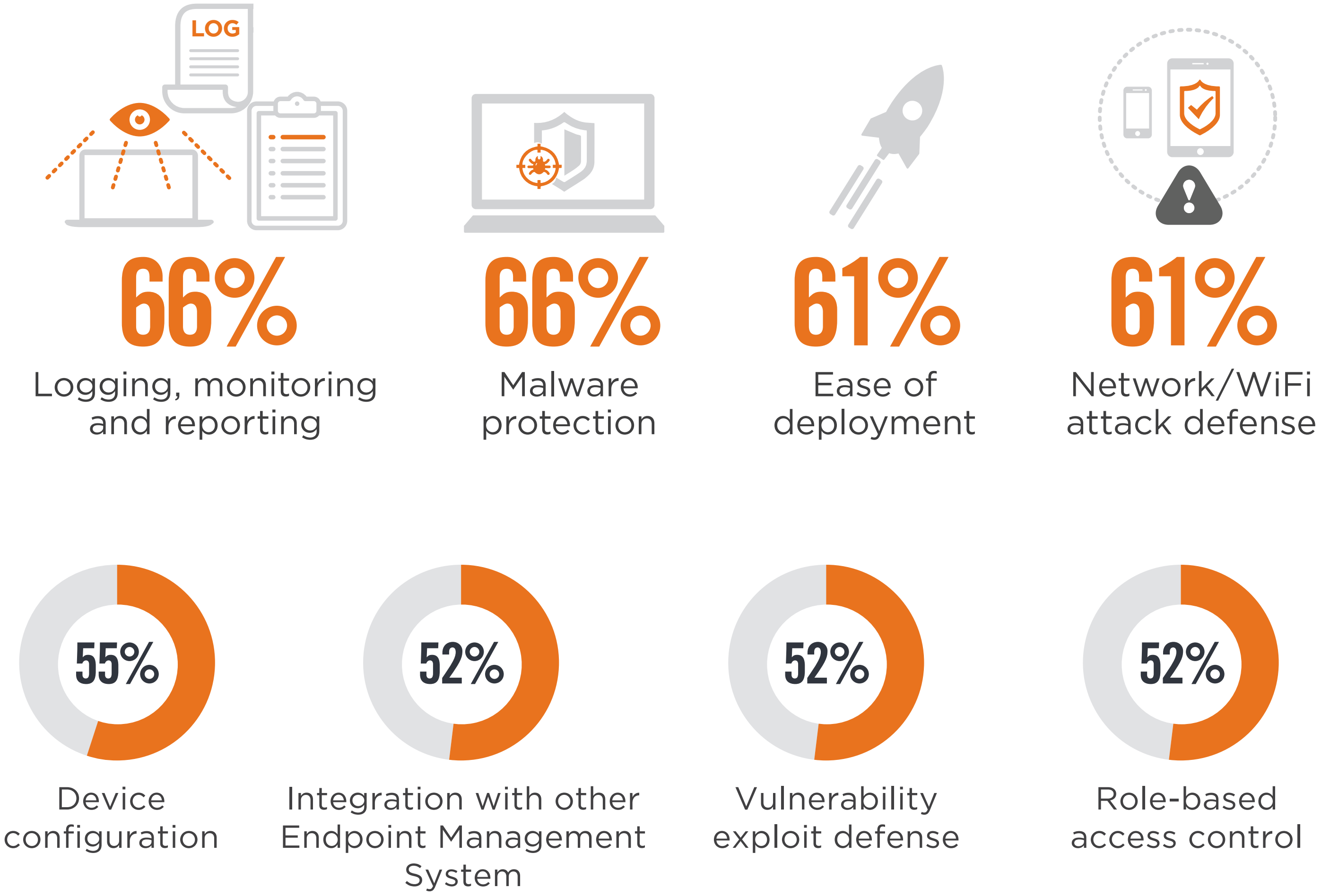
Network access control (NAC)

Mobile device file/data encryption 47% | Mobile device antivirus/anti-malware 46% | VPN to cloud-based security gateway 44% | DLP/Access Control 42% | Mobile application management (MAM) 36% | Auditing of mobile devices 34% | Attack and penetration testing of mobile applications 34% | Mobile Threat Detection & Management (MTM) 33% | Automated remediation using other security systems 30% | Virtual desktop infrastructure (VDI) 27% | Containerization / micro-virtualization 21% | Not sure 7% | None 2%

KEY REQUIREMENTS FOR MTM

Cybersecurity professionals confirm that their organizations prioritize logging, monitoring and reporting capabilities (66%) as part of their mobile security posture together with malware protection (66%). This is closely followed by ease of deployment (61%).

In your opinion, what key capabilities are required for Mobile Threat Management solutions?



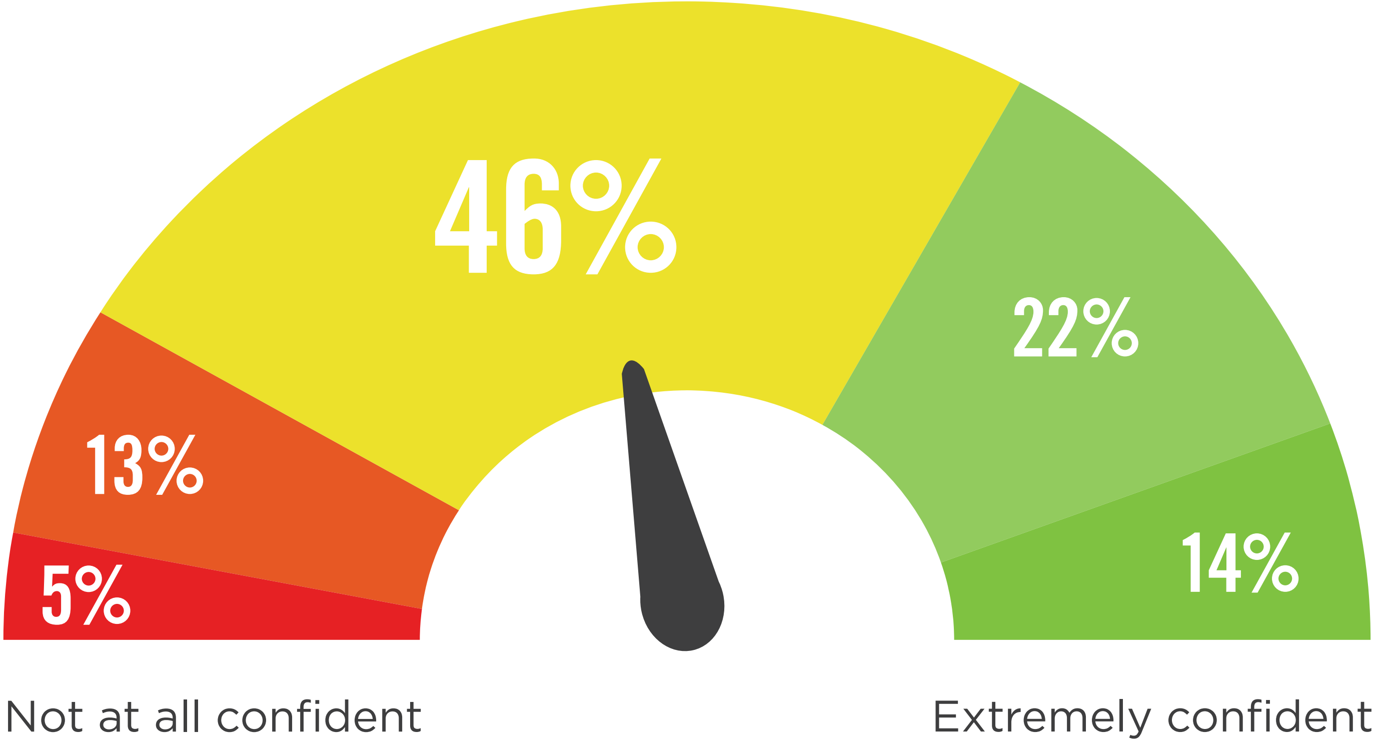
Cross-platform support 52% | App Risk Detection 45% | Other 5%

BUDGET

CONFIDENCE IN SECURITY

An alarming two-thirds of organizations lack confidence in their mobile security posture.

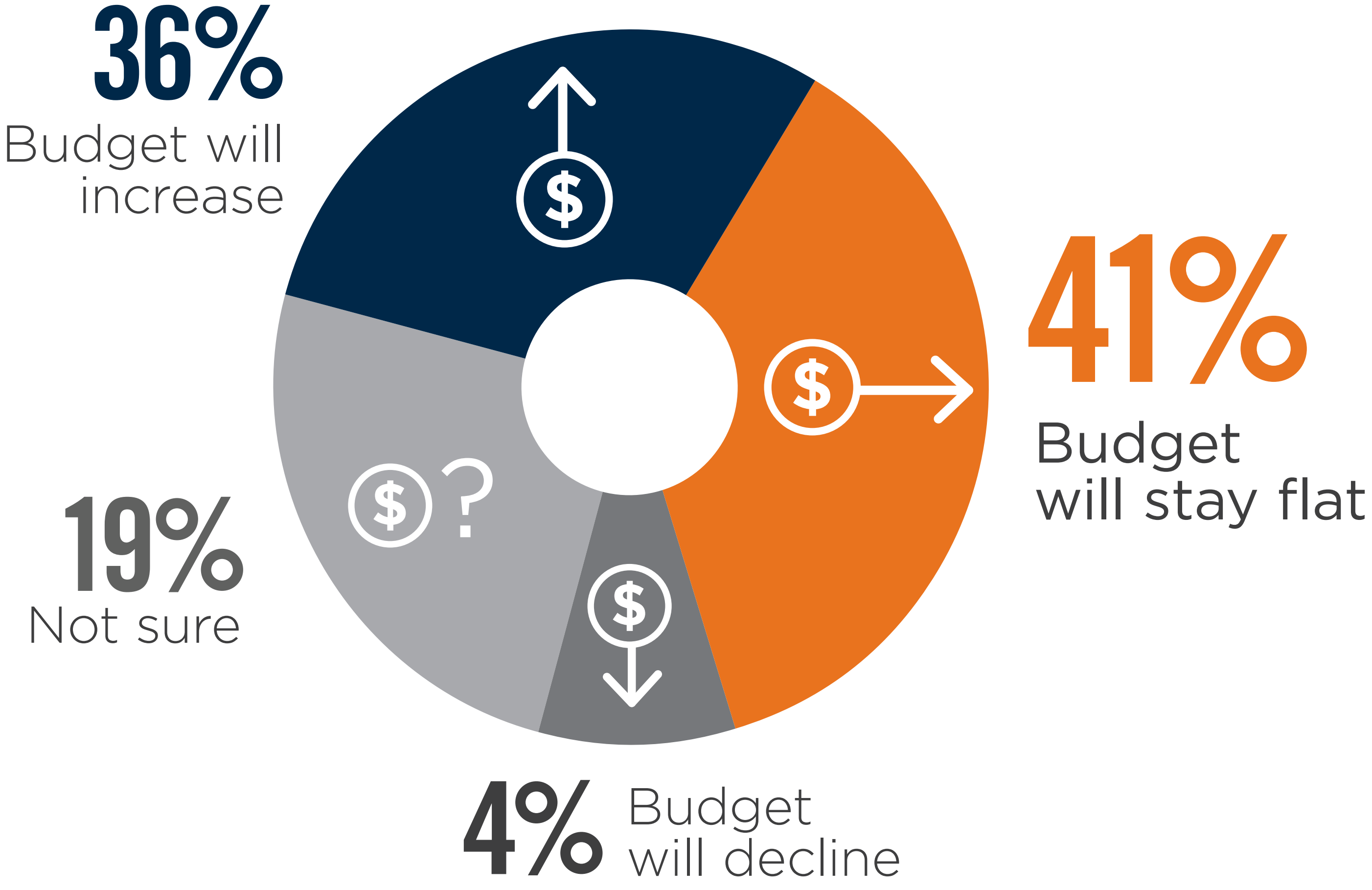
How confident are you in your organization's mobile security posture?



MOBILE SECURITY BUDGET

The survey respondents report good news showing that budgets for mobile security are on the rise for 36% of organizations who plan to increase mobile security spend over the next 12 months, compared to 26% in last year's survey.

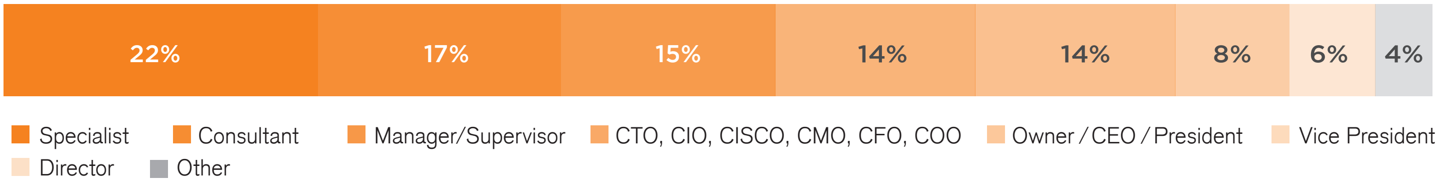
How is your mobile security budget going to change over the next 12 months?



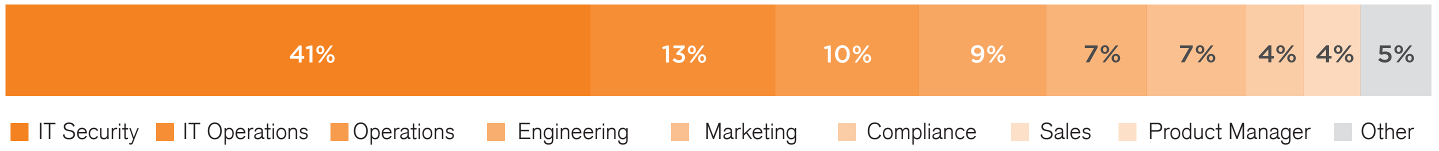
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest mobile & BYOD security threats faced by organizations and the solutions to prevent and remediate them. The respondents range from technical executives to managers and IT security practitioners. They represent organizations of varying sizes across many industries.

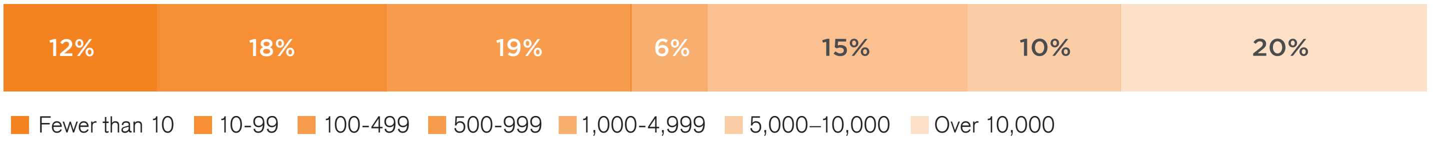
CAREER LEVEL



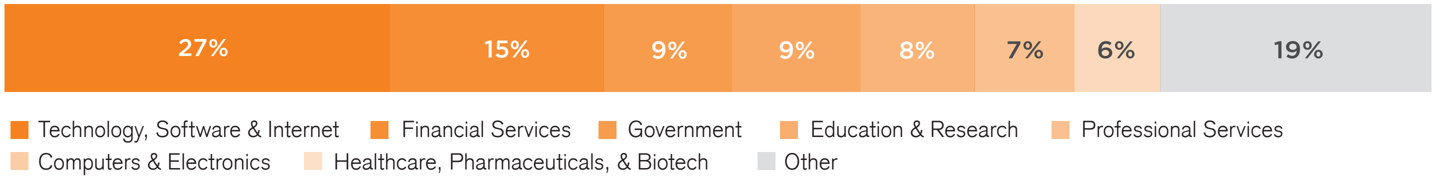
DEPARTMENT



COMPANY SIZE



INDUSTRY


Technology, Software & Internet
Financial Services
Government
Education & Research
Professional Services
Computers & Electronics
Healthcare, Pharmaceuticals, & Biotech
Other