MOBILE SECURITY

2017 SPOTLIGHT REPORT

LinkedIn Group Partner

Information Security

ZIMPERIUM®

PRESENTED BY

OVERVIEW

Security and privacy risks are on the rise with the proliferation of mobile devices and their increasing use in the enterprise.

As mobility grows in the workplace, so do challenges from managing bandwidth and device access to handling the most pressing concerns of security.

The 2017 Mobile Security Report focuses on these security challenges and offers fresh insights on the state of mobile threats and solutions.

These days, the computers most vulnerable to cyber threats in the enterprise are mobile phones and tablets. We see that security teams are often blind to the growing risks these devices pose for the enterprise and worse, are unable to deal with threats as they appear.

Many enterprises manage device access to corporate resources, networks and identity, but they can't remediate a threat they can't identify. As more of our computing goes directly from mobile devices to cloud services, network threat detection solutions are ineffective since data often resides outside the corporate data center. You need to adopt a non-signature based mobile threat detection software to protect your organization and its data. It's a serious and growing concern for all CEOs and CIOs.

Shridhar Mittal
CEO, Zimperium

ZIMPERIUM®

MOBILE SECURITY TRENDS REPORT

TABLE OF CONTENTS

INTRODUCTION

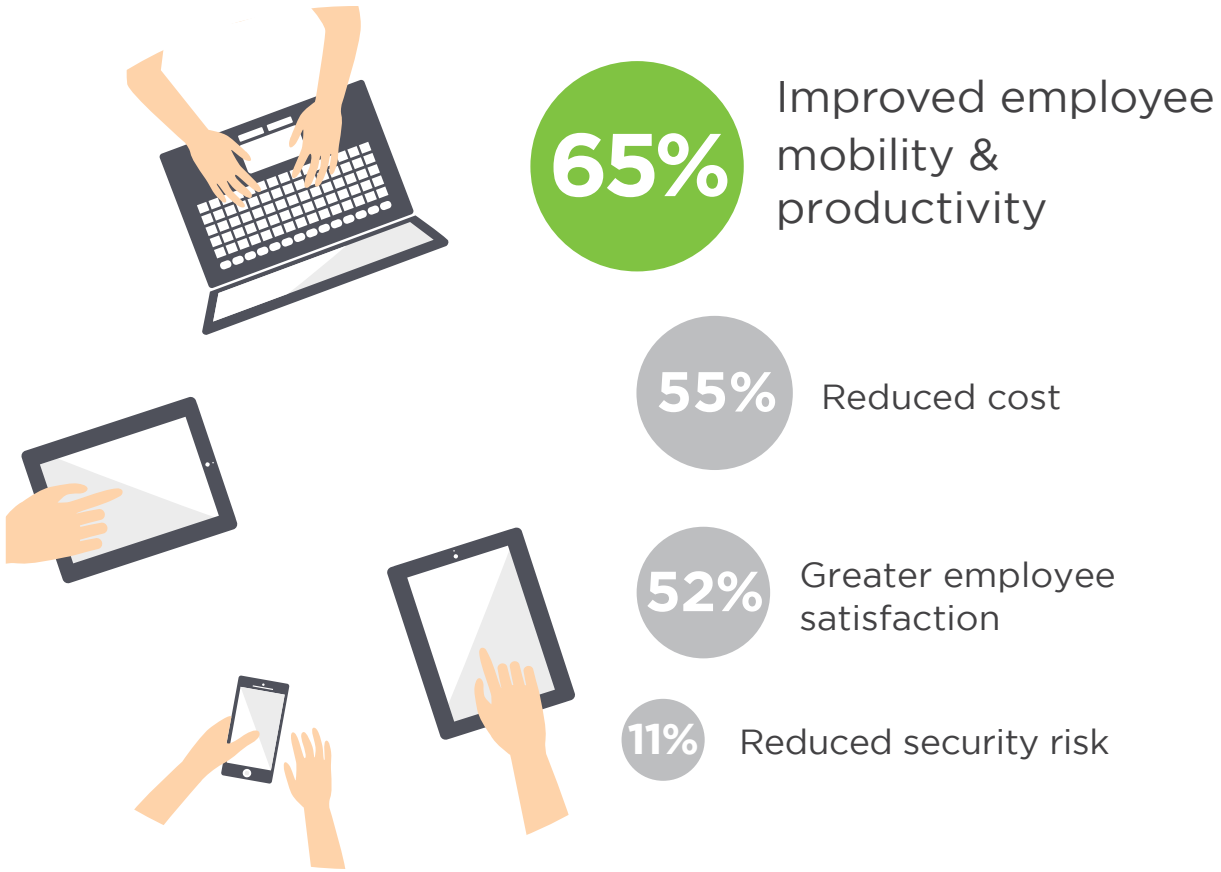
Mobile computing is changing the world. The number of connected devices has grown by 30% year-over-year and is not expected to slow down in 2017. Further driving change is user preference for their smartphones, personal computers, tablets, and other computing technologies.

Allowing employees to use their own devices can certainly improve satisfaction, but it also puts the organization at risk for additional security threats. Whether these devices are sanctioned or not through a corporate BYOD program, IT departments need to grapple with setting unified policies especially when it comes to securing mobile devices and the information they access.

BENEFITS OF BYOD ADOPTION

With over 4 billion mobile subscribers, we live in a world where mobility is ubiquitous and enterprises have begun to benefit from it. The top three drivers of BYOD among employees are improved mobility (65%), reduced cost (55%), and greater employee satistaction (52%).

Q: What are the main benefits of BYOD for your company?



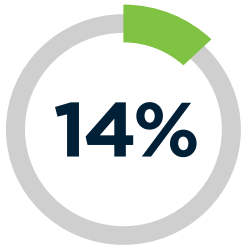
BARRIERS OF BYOD ADOPTION

Security is by far the number one barrier to stronger BYOD adoption. For the IT and security teams inside organizations, this points to potential security gaps or weaknesses that may need to be addressed.

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

31%
Security Concerns

We don't experience any resistance to BYOD adoption



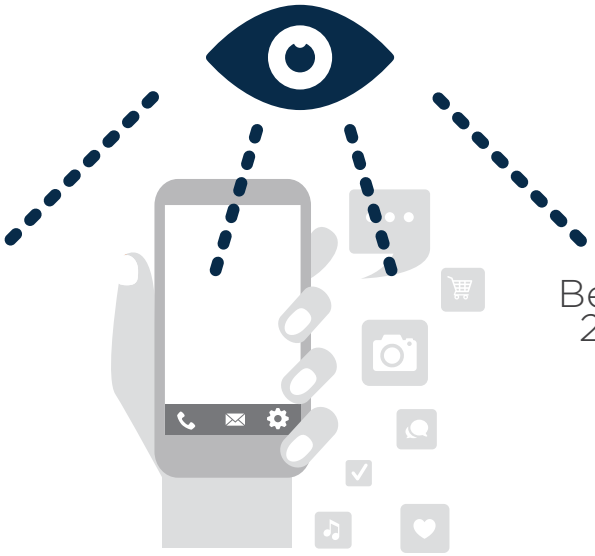
Employee privacy concerns (e.g., over EMM software)

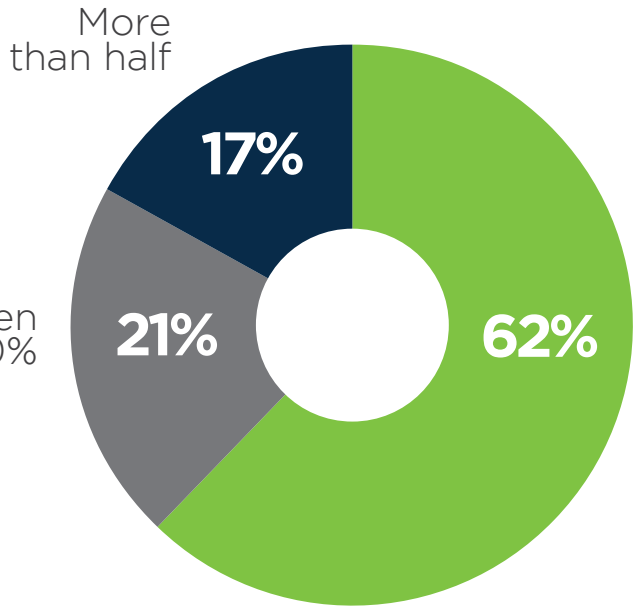
We offer managed / company owned devices as alternatives 12% | Employees don't want to take on the additional expense 6% | User experience concerns (battery life, don't like app choices, etc.) 5% | Employees don't want or need access through personal devices 4% | Support cost concerns 4% | Management opposition 4%

EMPLOYEE PRIVACY CONCERNS

Employee privacy is not a significant barrier to adoption of BYOD. A majority of 62% say that less than 25% of users in their organizations refuse BYOD due to privacy related concerns.

Q: What percent of employees refuse to adopt BYOD due to privacy concerns?



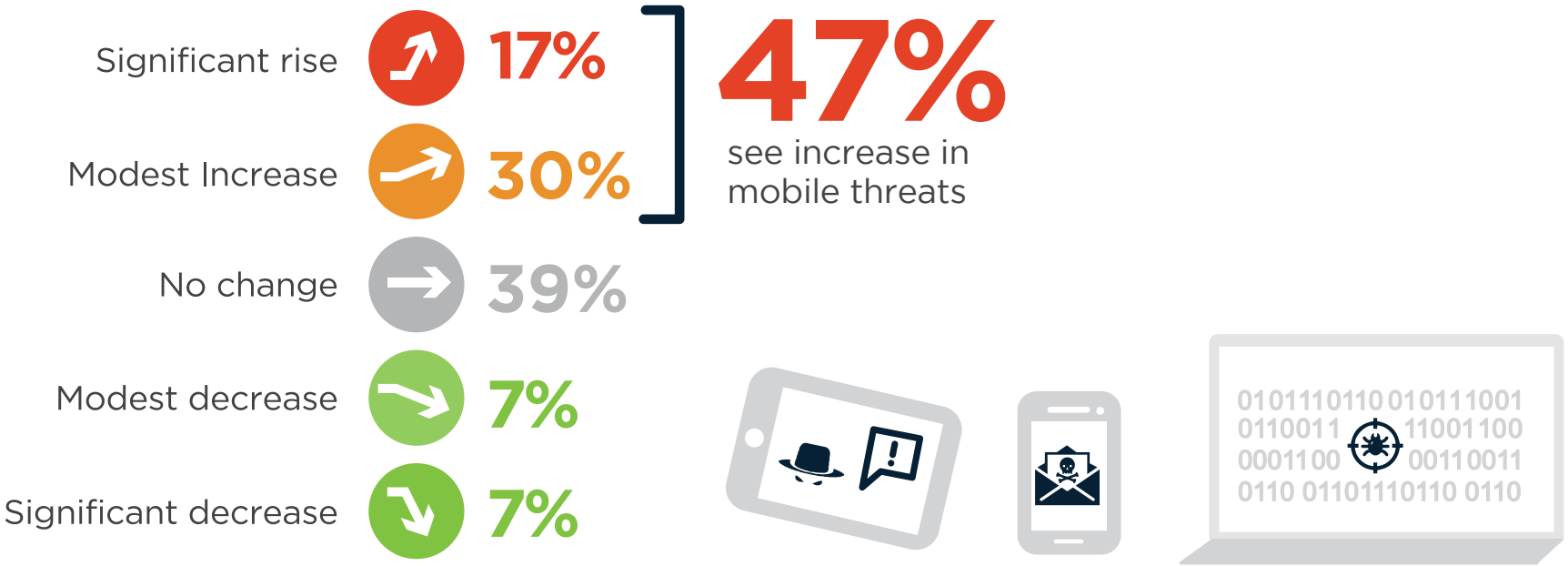


Less than 25% of employees refuse to adopt BYOD due to privacy concerns

MOBILE SECURITY THREATS

The dramatic growth of mobile devices is driving an increase in cybercrime, from stolen identities to major data breaches. Forty-seven percent of respondents observe either a moderate rise (30%) or significant rise (17%) in mobile device threats. Very few respondents (14%) see modest or significant decreases in mobile threats.

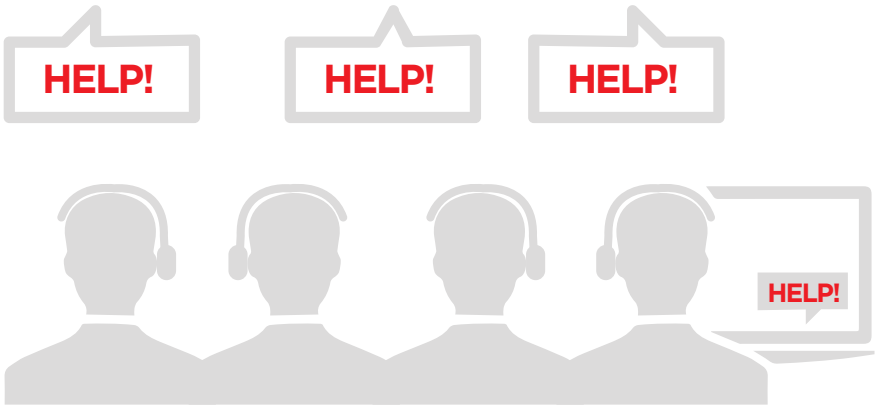
Q: How has the volume of mobile device threats targeting your users' smartphones and tablets changed in the past 12 months?



MOBILE THREATS IMPACT

The impact of mobile threats is being felt in terms of added helpdesk workload and associated cost (26%), need for additional IT resources to manage mobile security (21%), and reduced employee productivity (12%).

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



26% Increased helpdesk workload

21% Additional IT resources needed to manage mobile security

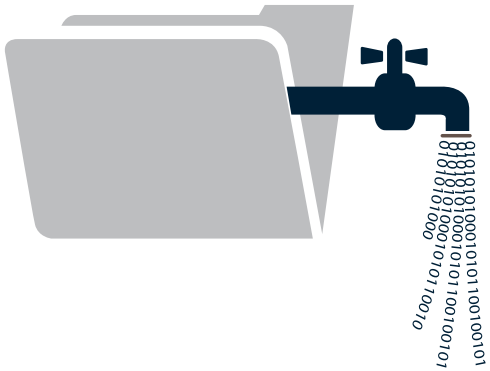
12% Reduced employee productivity

Unauthorized access to corporate data and systems 12% | Malware infections and related cost 11% | Data loss or leakage occurred 11% | Disrupted business activities 7% | The company had to pay regulatory fines 1% | Not sure/Other 27%

BYOD SECURITY CONCERNS

As mobility and BYOD initiatives grow in the workplace, so do security concerns. Of biggest concern related to BYOD is data leakage or loss (69%), download of unsafe applications or content (64%), and the introduction of malware into the organization's IT environment (63%).

Q: What are your main security concerns related to BYOD?



69%
Data leakage /loss

64%
Users download unsafe apps or content

63%
Malware

Lost or stolen devices 61% | Unauthorized access to company data and systems 58% | Vulnerability exploits 49% | Inability to control endpoint security 45% | Device management 41% | Network attacks via WiFi 38% | Ensuring security software is up-to-date 38% | Compliance with regulations 32%

KEY MOBILE SECURITY REQUIREMENTS

As our previous findings have indicated, BYOD in the workplace comes with several challenges and risks. Protection capabilities (44%, up from 42%), visibility into mobile threats (20%, up from 15%), and integration with existing platforms (22%, down from 33%) are the most critical requirements for mobile security.

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

44%

PROTECTION

We need a solution that not only detects threats but also remediates them based on the corporate policy

22%

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

20%

VISIBILITY

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

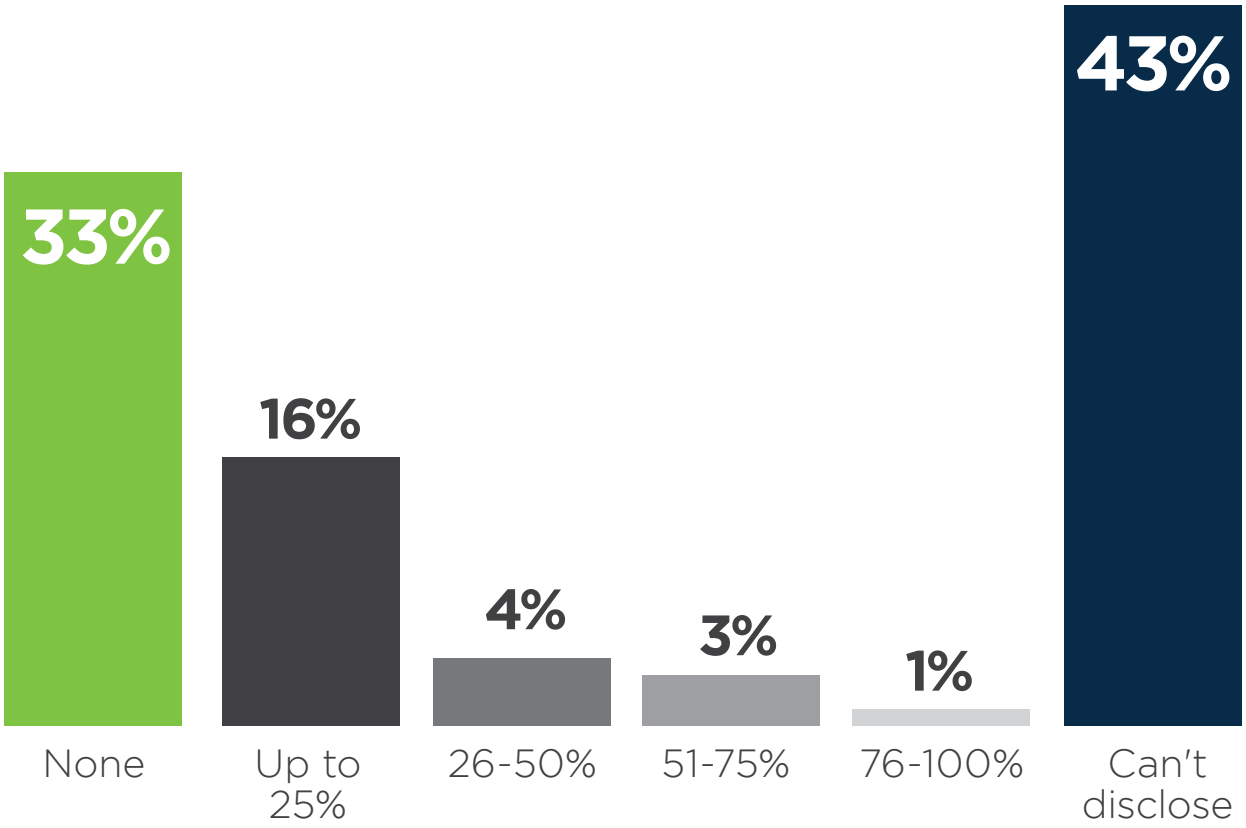
14%

NONE

MOBILE SECURITY BREACHES

About a quarter of respondents confirmed they experienced mobile device hacks or data leaks. The shadow number is likely much higher considering 43% decided to not disclose their attacks statistics.

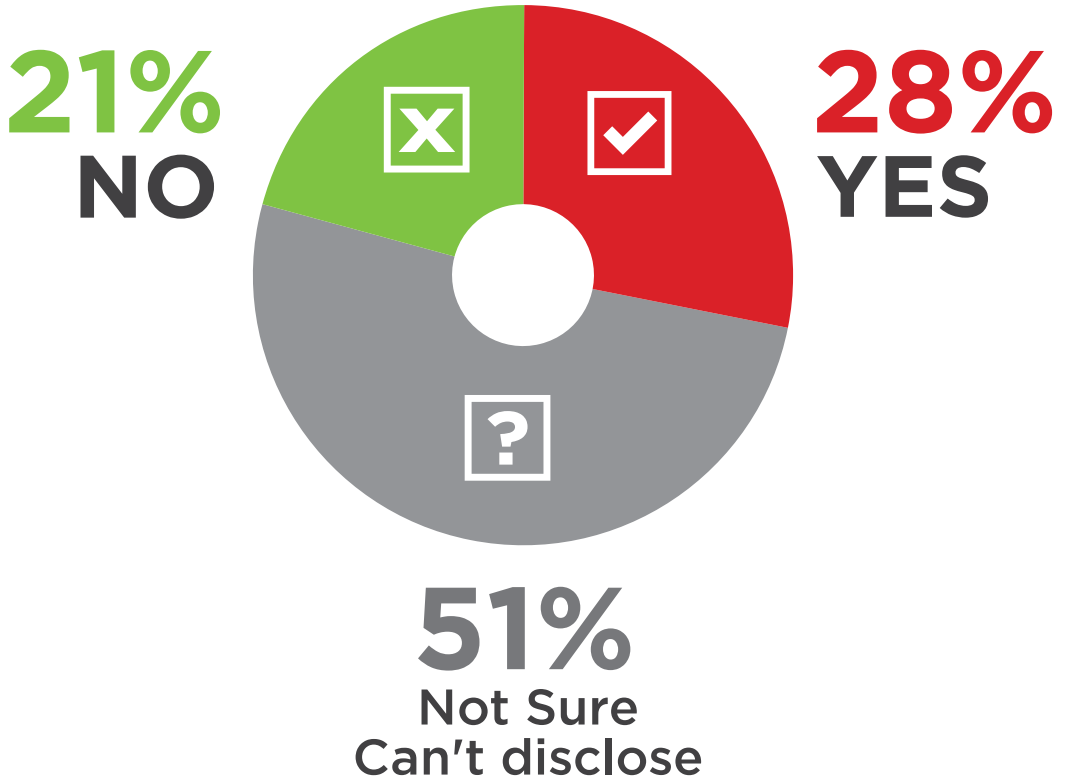
Q: How many of your mobile devices were hacked or had data leaks?



MALWARE THREAT

Twenty-eight percent of the surveyed organizations reported that BYOD or corporate-owned devices have downloaded malware at some point in the past - that is down from 39% in the previous survey. More than half of respondents said they are “not sure” if malware has been downloaded to mobile devices. These findings indicate a lack of effective monitoring of BYOD and corporate-owned devices in the workplace. It is imperative organizations implement BYOD programs in conjunction with the necessary programs to properly monitor device use, implement security technologies to detect and prevent malware penetration, and train employees across all departments and levels to protect all data stored on or accessed through mobile devices.

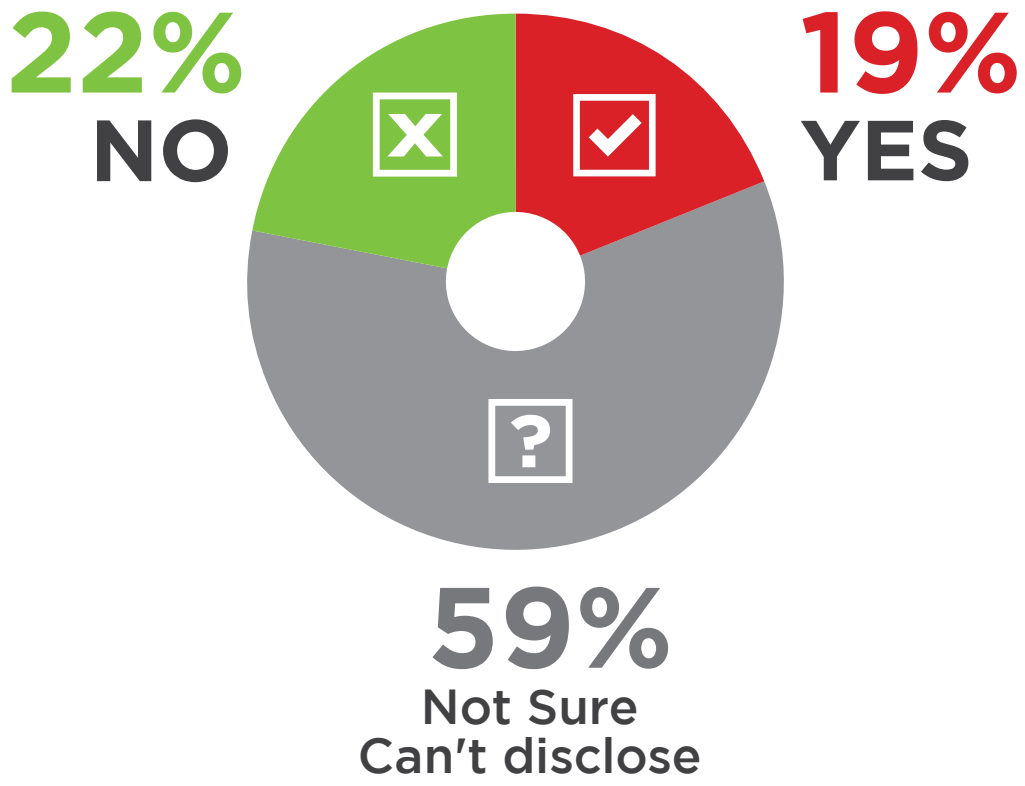
Q: Have any of your BYO or corporate-owned devices downloaded malware in the past?



MALICIOUS WIFI

Wi-Fi offers low-cost, ubiquitous networking, but it can open organizations to new vulnerabilities that arise when mobile devices connect to untrusted, potentially malicious Wi-Fi networks. As our study reveals, 19% of the surveyed organizations confirmed that the BYOD or corporate-owned devices have, in fact, connected to malicious Wi-Fi in the past. Worse yet, over half (59%) are unsure, leaving them vulnerable to the possible loss or theft of corporate data.

Q: Have any of your BYO or corporate-owned devices connected to a malicious Wi-Fi in the past?

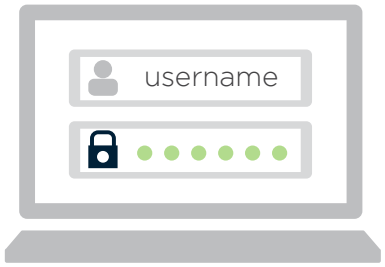


MOBILE SECURITY TECHNOLOGIES

The significant growth and integration of mobile technologies in both the personal and business spheres is driving IT departments to rethink the security technologies they are using to protect sensitive data and devices. The most commonly used mobile security controls include password protection (77%), remote wipe (72%), device encryption (69%), data removal at device disposal (63%), and mobile device management / MDM (58%). It should be noted that 19% of respondents say they have no mobile security technologies in place.

Q: Which of the following mobile security technologies are in place?

Password protection



77%

Remote wipe

72%

Device encryption

69%

Data removal at employee separation or device disposal

63%

None

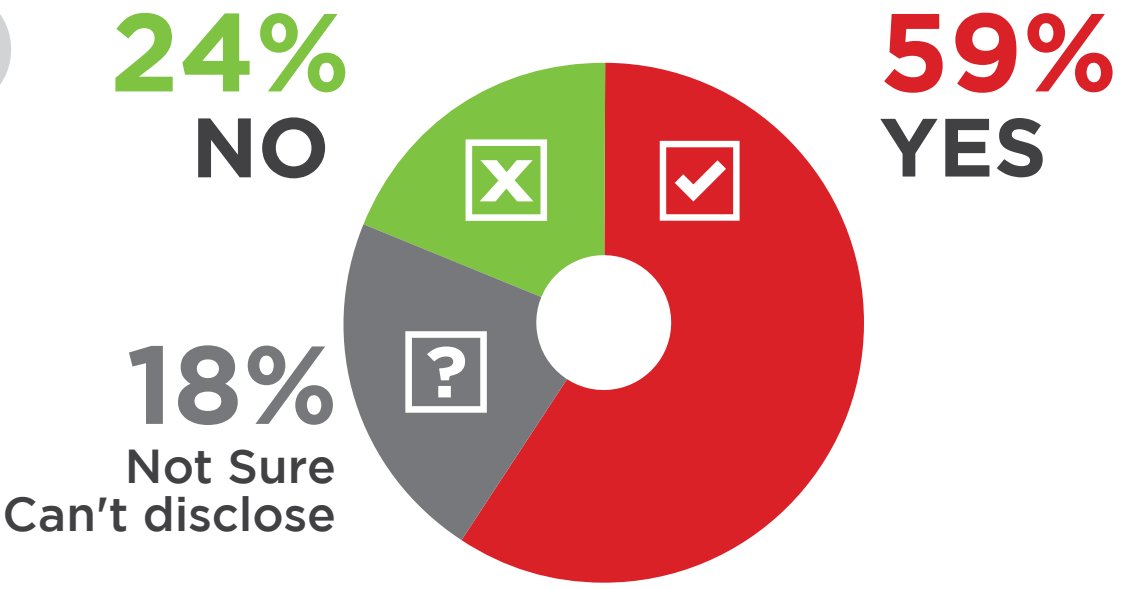
19%

Mobile device management (MDM) 58% | Mobile device file/data encryption 48% | VPN to onpremises security gateway 47% | Endpoint security tools 43% | Device management 41% | Mobile device antivirus/antimalware 39% | Network access control (NAC) 38% | DLP / Access Control 37% | Mobile application management (MAM) 33% | Auditing of mobile devices 30% | Virtual desktop infrastructure (VDI) 30% | VPN to cloudbased security gateway 29% | Containerization/microvirtualization 23% | Automated remediation using other security systems 22% | Mobile Threat Detection & Management (MTM) 22% | Attack and penetration testing of mobile applications 22% | None 19% | Not sure 32%

MOBILE APP SECURITY

A majority of organizations (59%) are concerned about introducing security risks to their customers via their consumer or business apps.

Q: Are you concerned about introducing security or privacy risks in the mobile apps you develop for your customers?

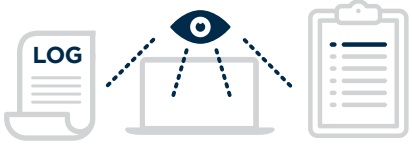


KEY REQUIREMENTS FOR MTM

The most requested capability for mobile threat management solutions is malware protection (68%), followed by logging, monitoring and reporting (64%), indicating the need for better visibility into security threats and their impact on mobile devices across the organizations.

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

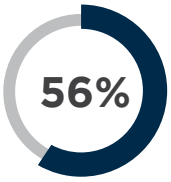
68%
Malware protection



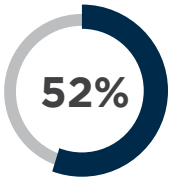
64%
Logging, monitoring and reporting

59%
Ease of deployment

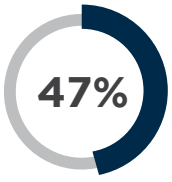
56%
Vulnerability exploit defense



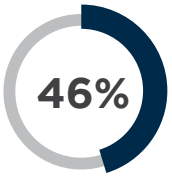
Network / Wi-Fi attack defense



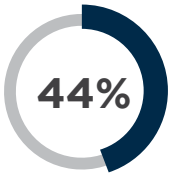
Device configuration



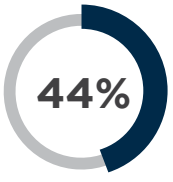
Cross-platform support



Role-based access control



Integration with other endpoint management systems

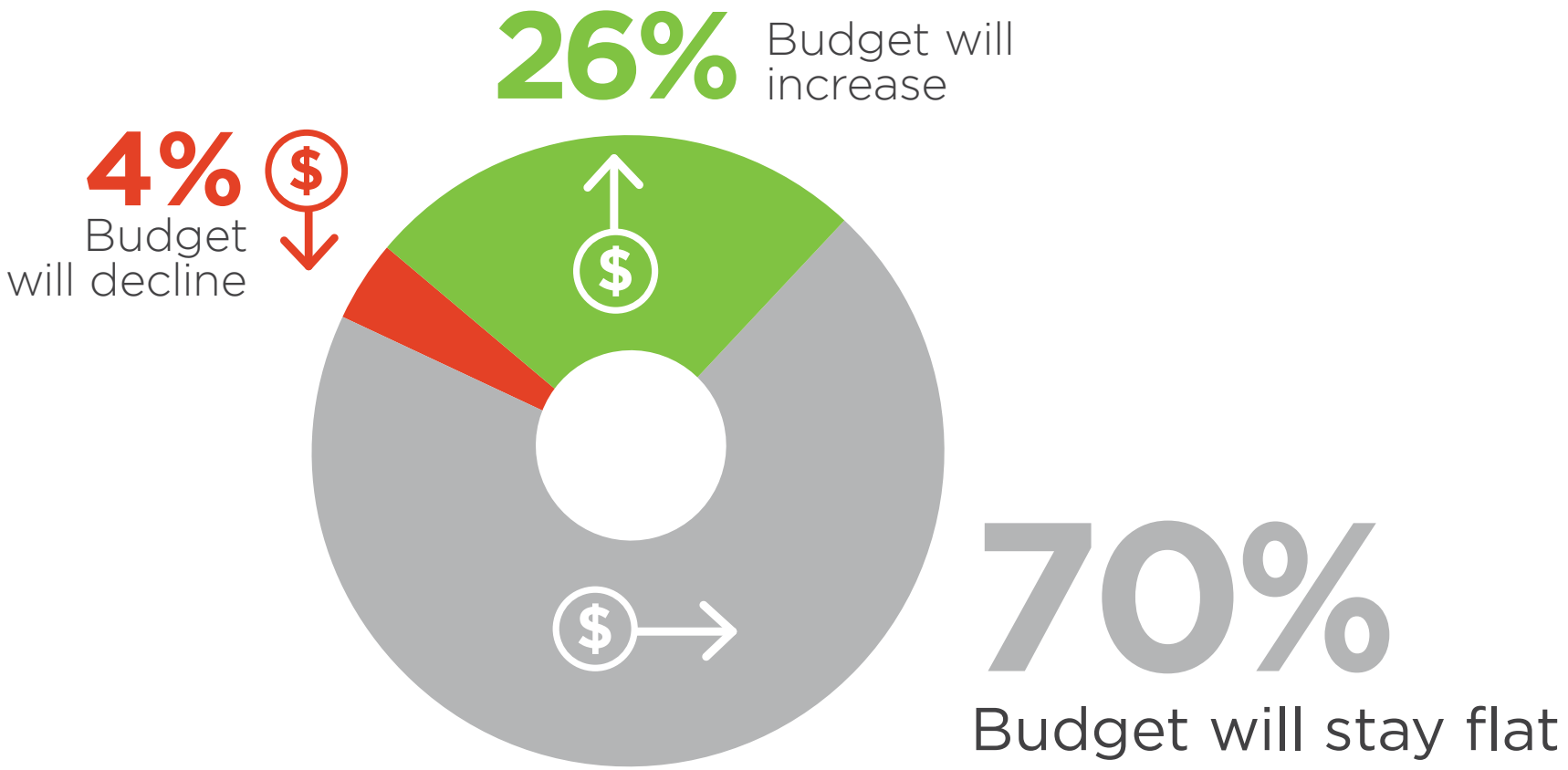


App risk detection

MOBILE SECURITY BUDGET

While the future of mobile computing is certainly bright, there are many security challenges to address. These concerns are reflected in the budget priorities for 26% of organizations who plan to increase mobile security spend over the next 12 months. Only four percent of respondents are planning on reducing security investments.

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

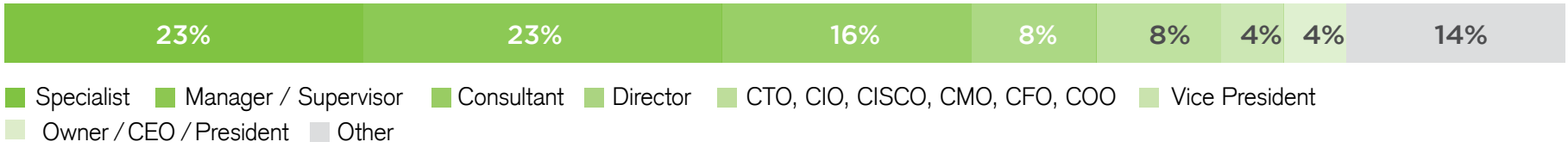


METHODOLOGY AND DEMOGRAPHICS

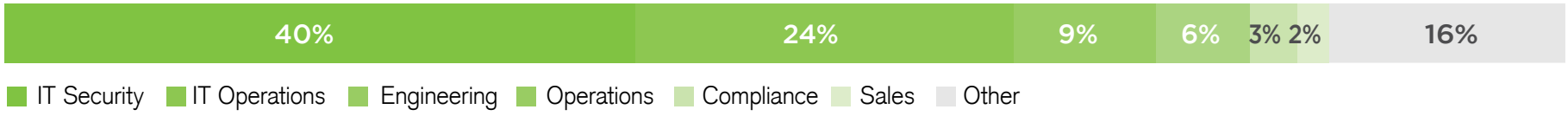
METHODOLOGY & DEMOGRAPHICS

The 2017 Mobile Security Report is based on the results of a comprehensive online survey of over 1,900 cybersecurity professionals to gain more insight into the latest 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. Their answers provide a comprehensive perspective on the state of cybersecurity today.

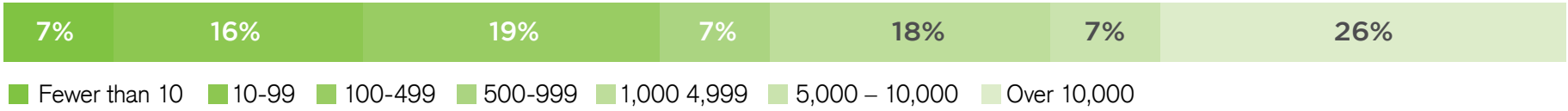
CAREER LEVEL



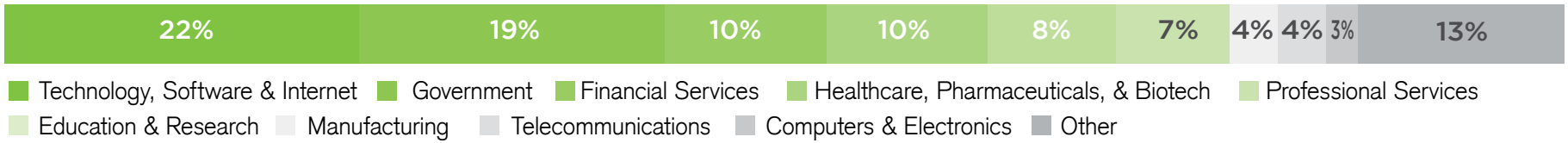
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSOR OVERVIEW

SPONSOR

Zimperium | www.zimperium.com

Zimperium, the global leader in Mobile Threat Defense, offers real-time, on-device protection against both known and unknown mobile device, network and application cyberattacks. Its advanced machine learning-based platform provides visibility, security and management of attacks on all three mobile threat vectors - Device, Network and Applications for iOS, Android and Windows devices.