BYOD & MOBILE SECURITY

SPOTLIGHT REPORT

LinkedIn Group Partner

Information Security

Sponsored by

Lumension® IT Secured. Success Optimized.™

zixcorp®

VECTRA™ Security that thinks.™

IBM

SPONSORS

We would like to thank our sponsors for supporting the
BYOD & Mobile Security Report.

Lumension
IT Secured. Success Optimized.™

Lumension | www.lumension.com

Lumension Security, Inc., a global leader in endpoint management and security, develops security software solutions that help businesses protect vital information and manage critical endpoint risk. Lumension delivers the award-winning Lumension® Endpoint Management and Security Suite with Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance.

zixcorp

ZixCorp | www.zixcorp.com

ZixCorp offers industry-leading email encryption, a unique email DLP solution and an innovative email BYOD solution to meet your company's data protection and compliance needs. ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government for easy to use secure email solutions.

VECTRA™
Security that thinks.™

Vectra Networks | www.vectranetworks.com

Vectra Networks is the leader of real-time detection of cyber attacks in progress. The Vectra X-series breach detection platform continuously monitors network traffic to automatically detect any phase of an ongoing cyber attack. The platform provides visually intuitive reports of hosts under attack and context about what the attacker is doing. Vectra automatically prioritizes attacks that pose the greatest business risk, enabling organizations to quickly make decisions on where to focus their time and resources. Vectra Networks' investors include Khosla Ventures, IA Ventures and AME Cloud Ventures. The company's headquarters are in San Jose, Calif. Visit www.vectranetworks.com for more information.

IBM

IBM | www.ibm.com/security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

INTRODUCTION

Welcome to the 2014 edition of the BYOD & Mobile Security Report.

Our second annual edition of the BYOD & Mobile Security Report explores the state and challenges of securing BYOD and mobility in 2014.

The results are in. We received over 1,100 responses and gained new insights into the state of BYOD and mobile security practices in 2014 - all reviewed in detail on the following pages.

Thanks to everyone who participated in this survey.
We hope you will enjoy this report.

Holger Schulze

Holger Schulze
Group Founder
Information Security
Community on LinkedIn

Email: hhschulze@gmail.com

LinkedIn Group Partner
Information
Security

SURVEY HIGHLIGHTS

The 5 Major Trends in BYOD & Mobile Security

1 The key drivers for BYOD are about keeping employees mobile (57 percent), satisfied (56 percent) and productive (54 percent).

2 The biggest BYOD security concerns are loss of company or client data (67 percent) and unauthorized access to company data and systems (57 percent).

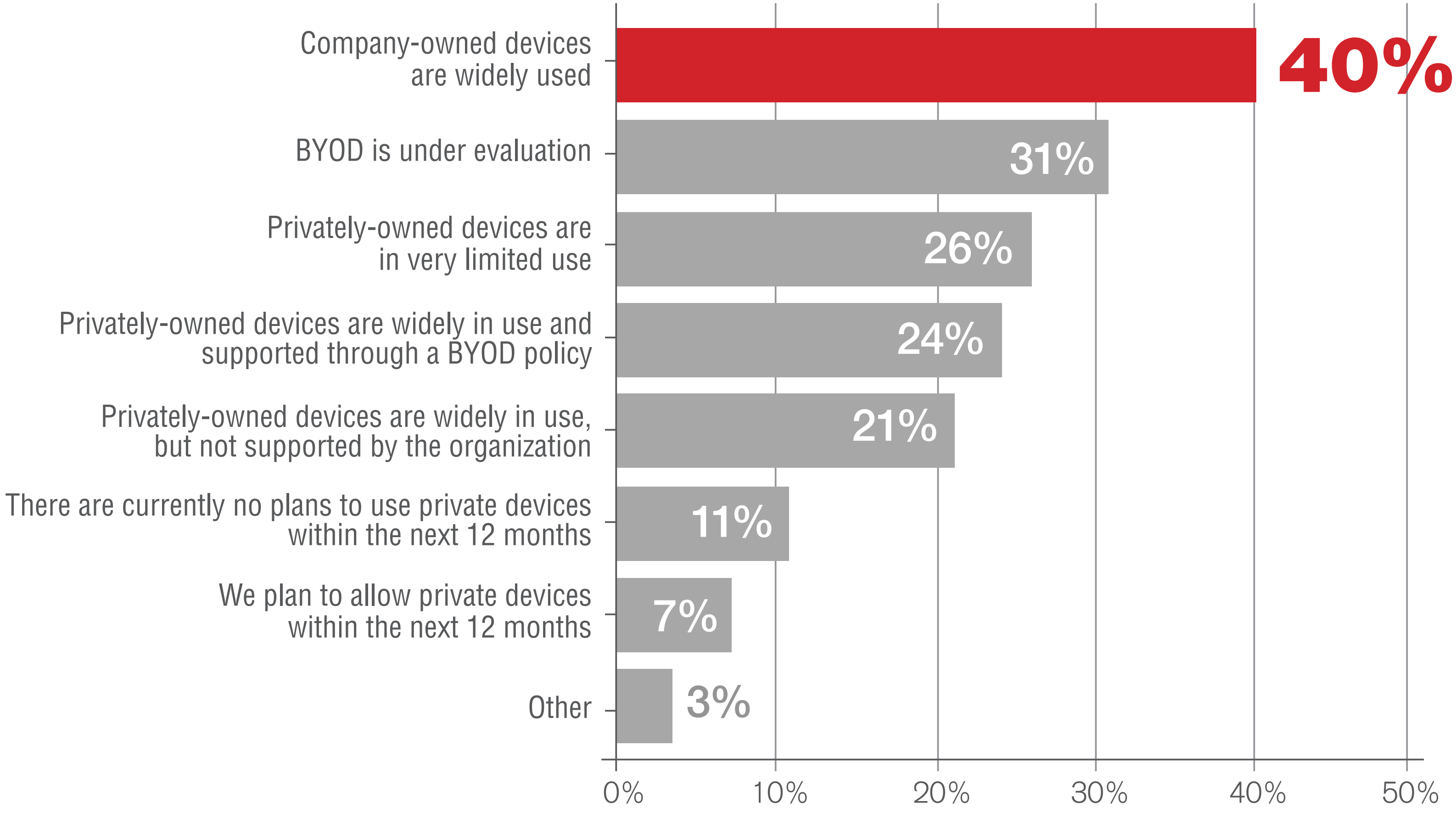
3 Additional IT resources to manage security incidents (30 percent) are by far the biggest negative impact of mobile security threats.

4 Smartphones (87 percent) are the dominant form factor among supported mobile devices, followed by laptops (79 percent) and tablets (68 percent).

5 The most common risk control measure is password protection (67 percent), followed by remote wiping of data (52 percent) and use of encryption (43 percent).

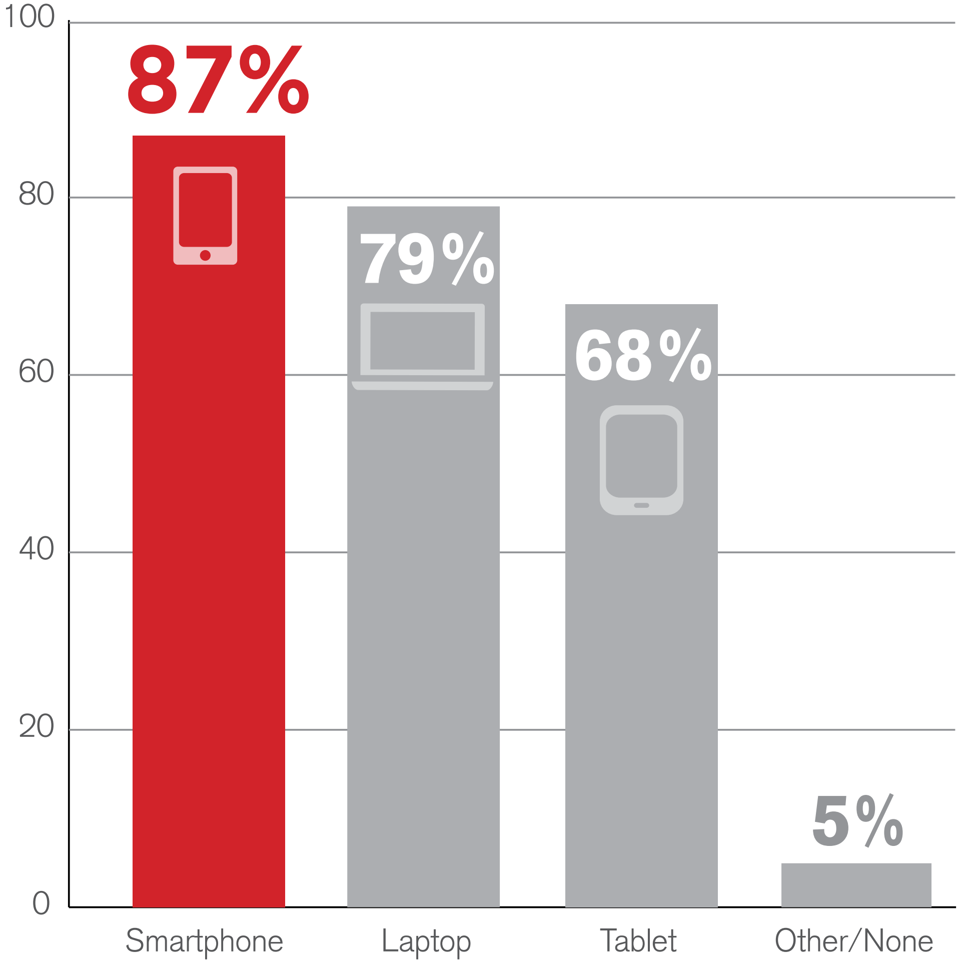
WHAT IS THE OVERALL STATE OF BYOD ADOPTION?

For 31 percent of organizations, BYOD is still under evaluation, followed by 26 percent of organizations with privately owned devices in limited use, and 24 percent with widespread use of privately-owned devices. Company-owned devices are widely used by 40 percent of organizations. 21 percent admit to having unsupported personal mobile devices in their organization.



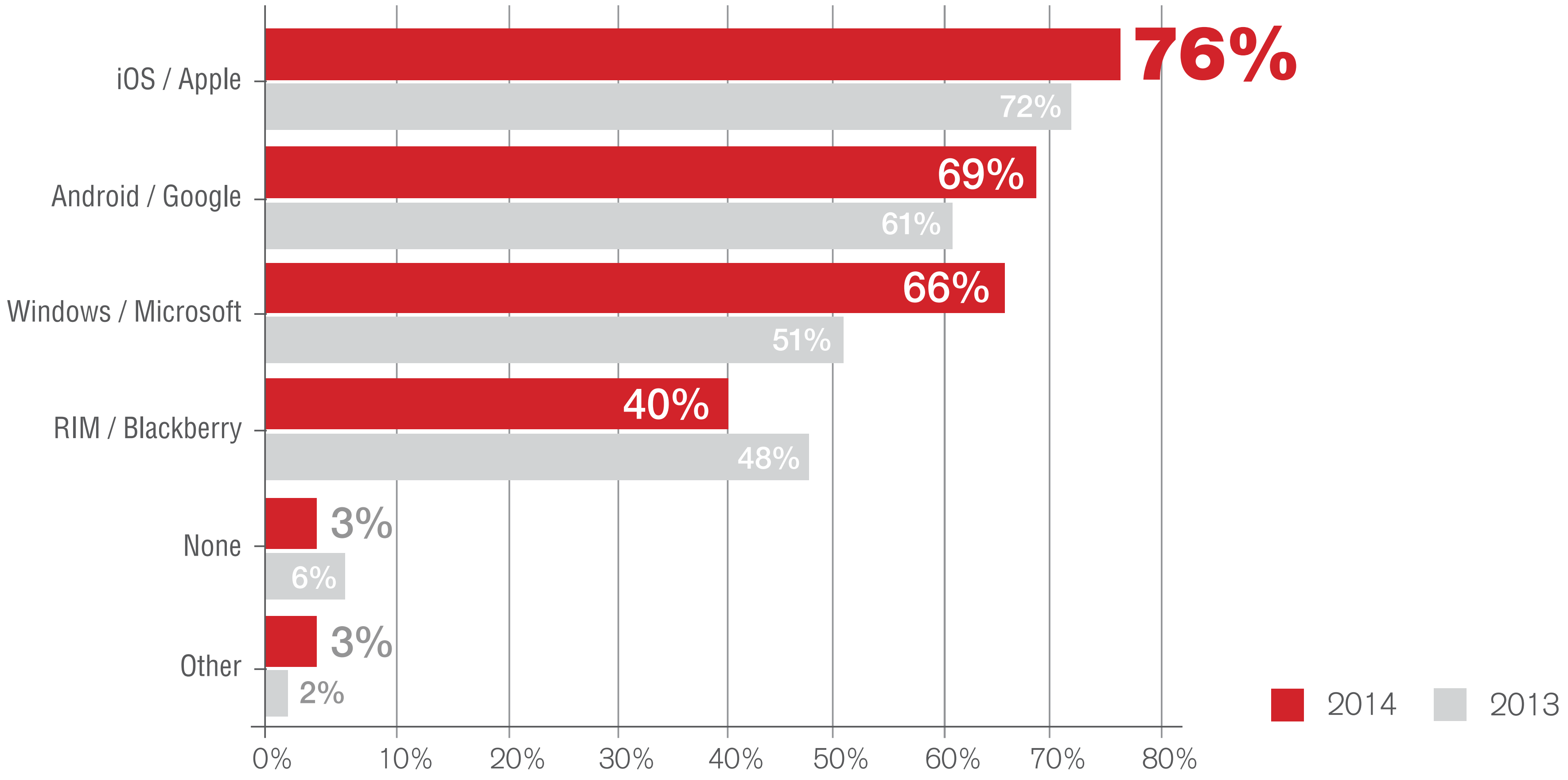
WHAT MOBILE FORM FACTORS DO YOU SUPPORT?

Smartphones (87 percent) are the dominant form factor among supported mobile devices, followed by laptops (79 percent) and tablets (68 percent).



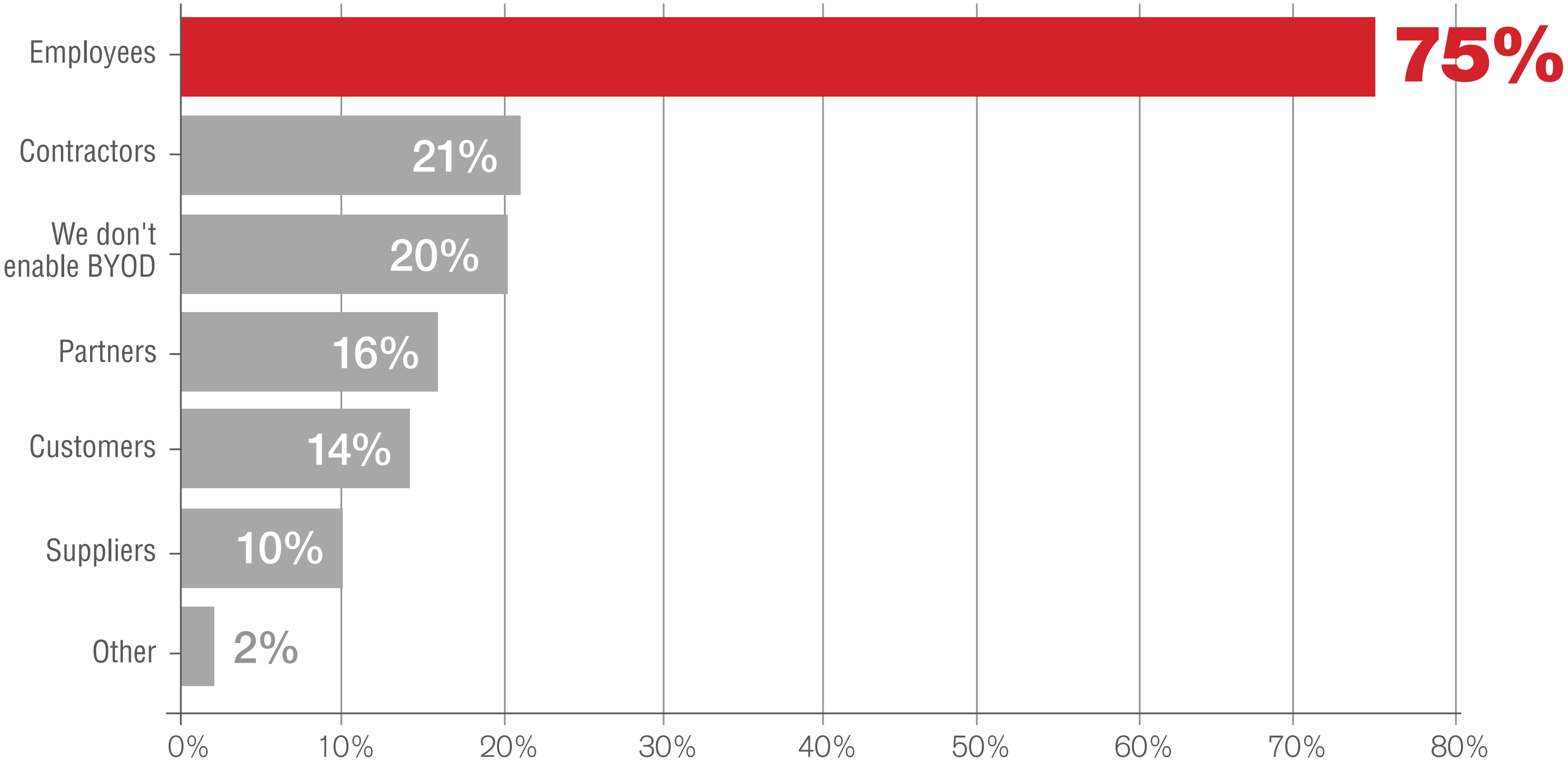
WHAT MOBILE PLATFORMS DO YOU SUPPORT?

Among all mobile devices considered for BYOD (including smartphones, tablets and laptops), Apple's iOS is still the dominant mobile platform with 76 percent. RIM (40 percent) declined in popularity compared to last year while Android (69 percent) and Windows (66 percent) are gaining popularity.



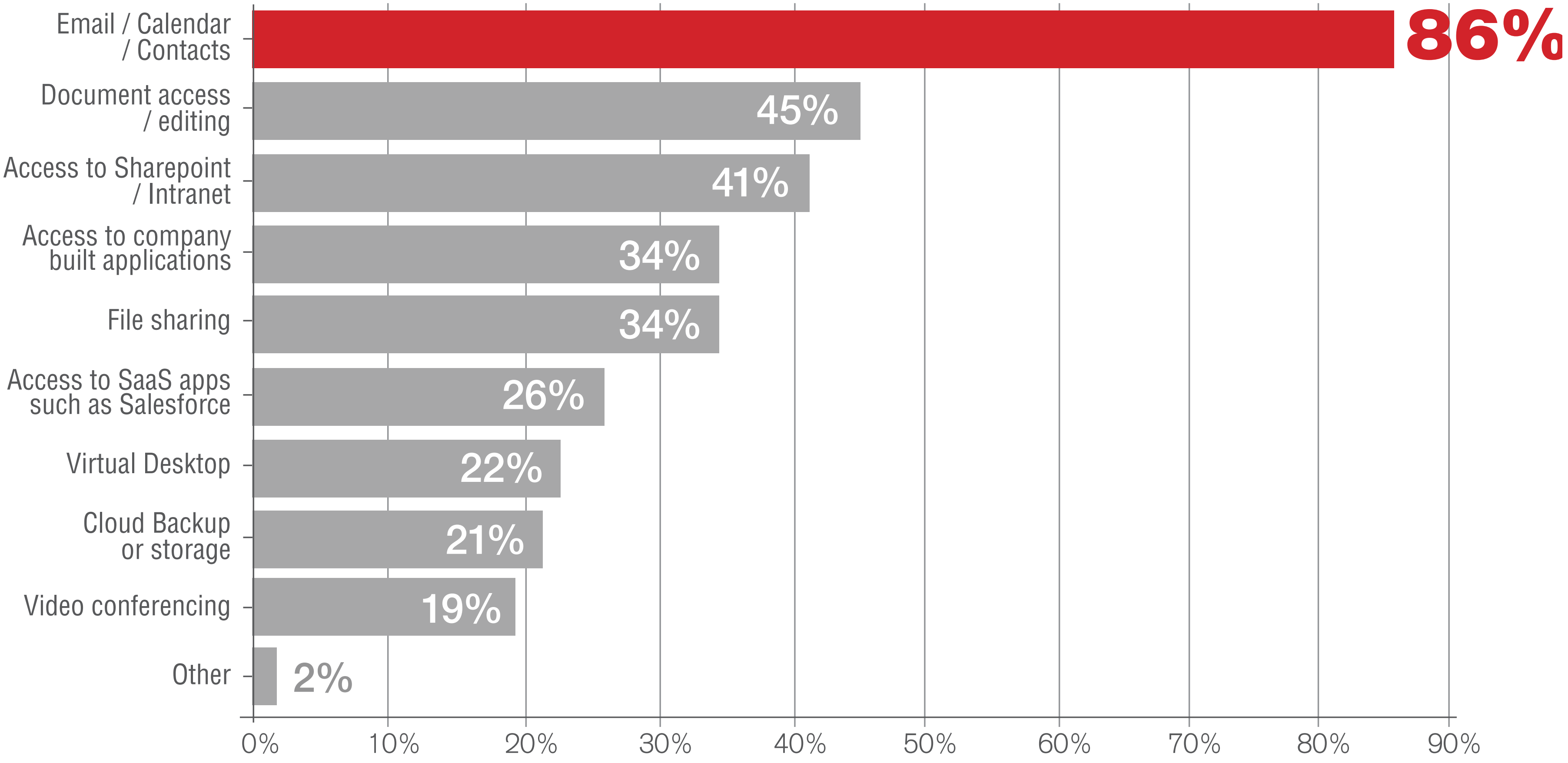
FOR WHAT USER GROUPS IS BYOD ENABLED?

Employees are the primary group of BYOD users (75 percent). The rise in extending BYOD to partners, customers and suppliers causes a continued dissolution of the traditional security perimeter and drives the need for new security strategies and architectures.



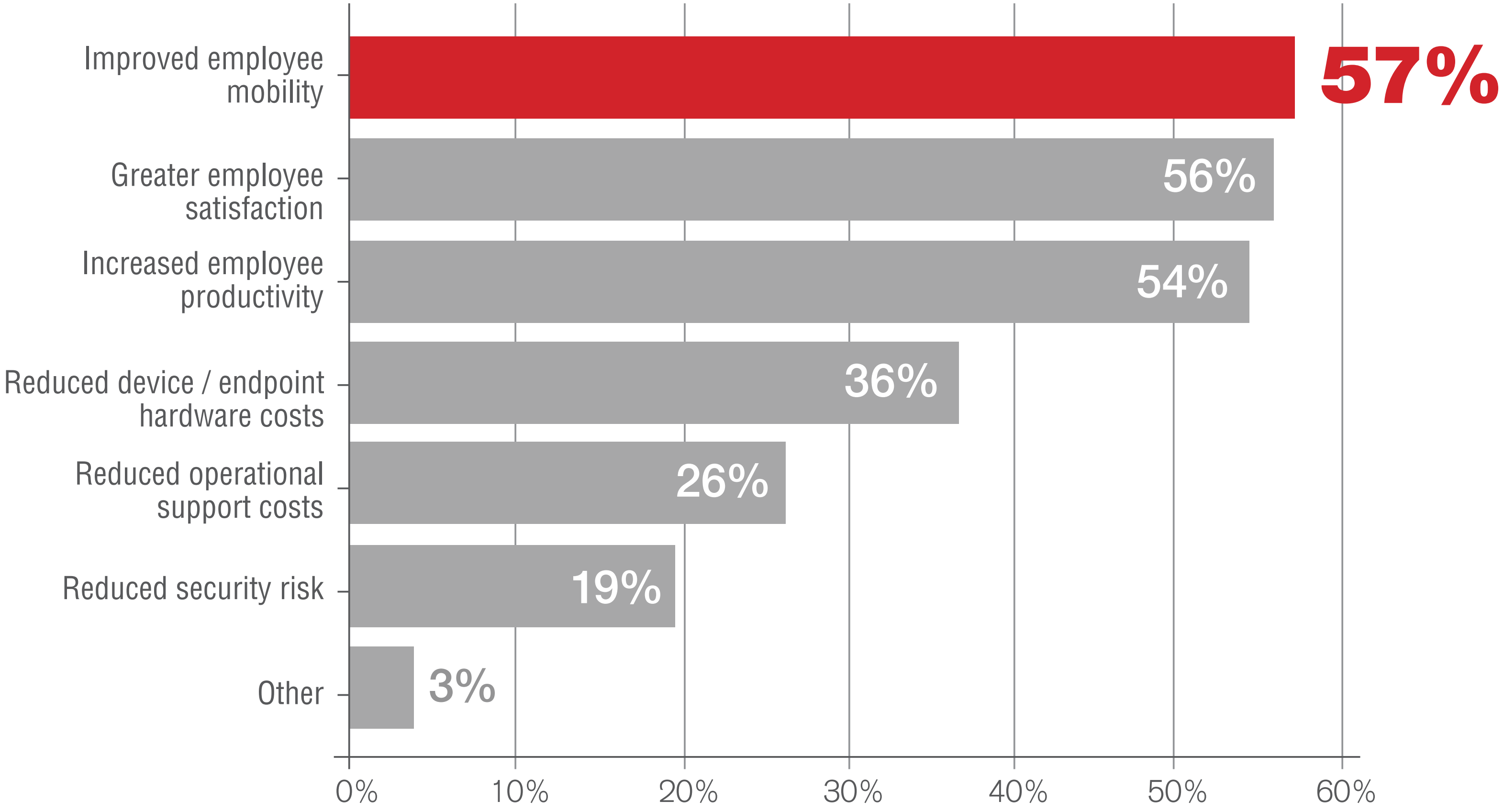
WHAT ARE THE MOST POPULAR BUSINESS apps on BYOD devices?

Email, calendar and contact management are the most popular mobile apps (86 percent). The applications designed to boost productivity are the very same applications that can increase the risk of data breaches, intrusions or malware incidents. Finding the right balance between productivity and security will be critical to the success of BYOD initiatives.



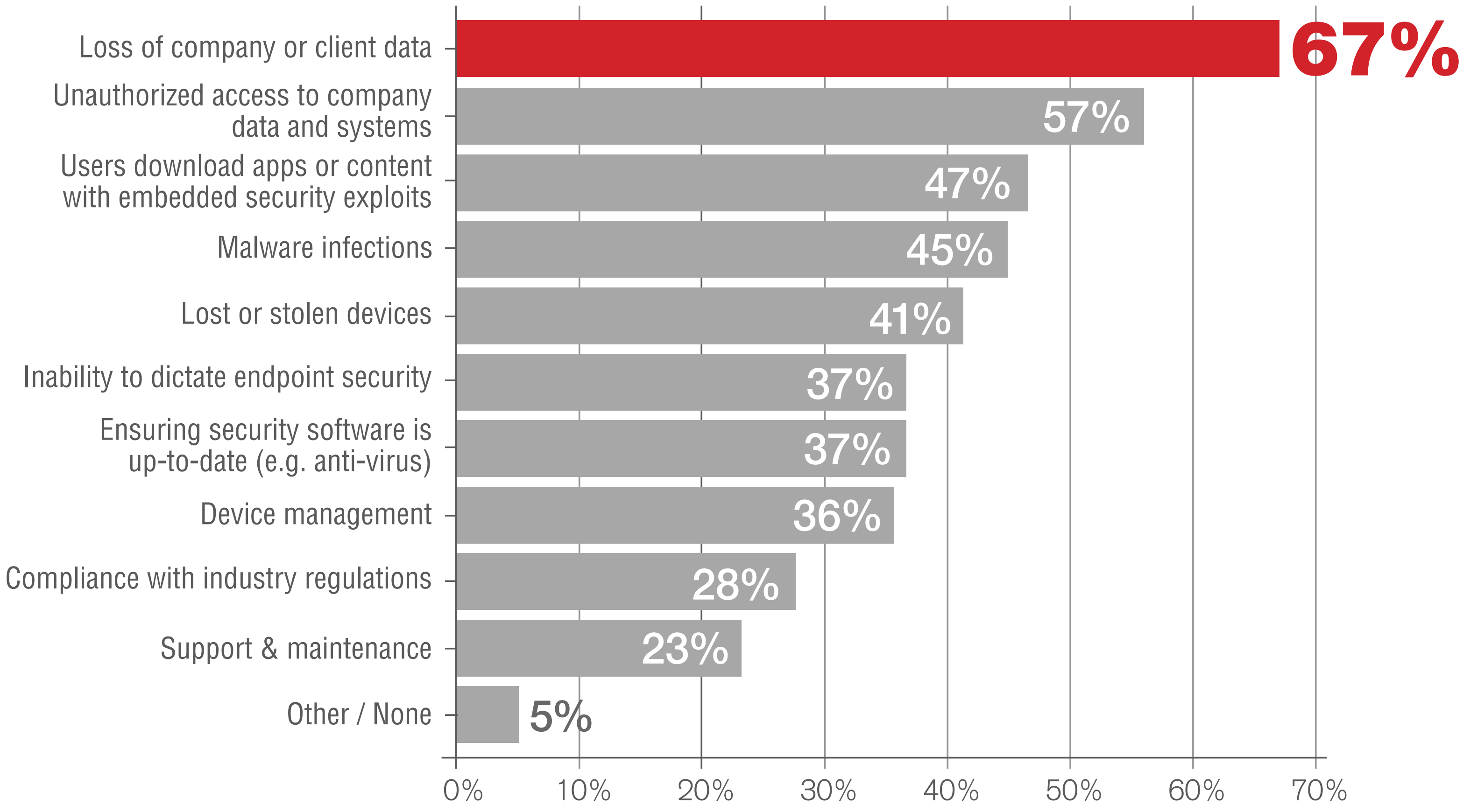
WHAT ARE THE MAIN DRIVERS AND benefits of BYOD?

The key drivers for BYOD are about keeping employees mobile (57 percent), satisfied (56 percent) and productive (54 percent). Reducing cost for mobile devices (36 percent) and support cost (26 percent) is important but secondary to employee-related benefits.



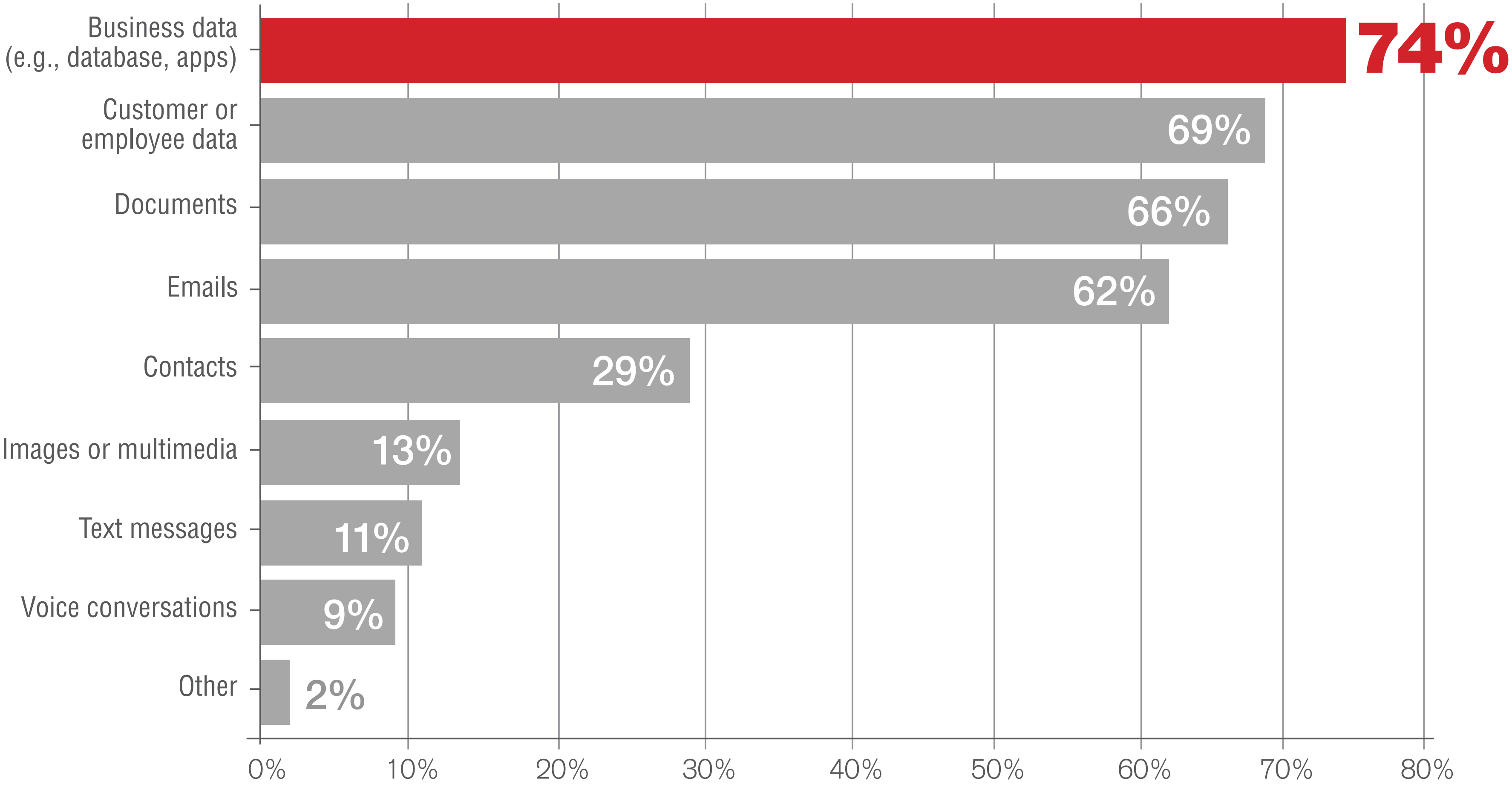
WHAT ARE YOUR BIGGEST BYOD SECURITY CONCERNS?

While security technologies are maturing, BYOD security concerns remain. Loss of company or client data (67 percent), unauthorized access to company data and systems (57 percent) and fear of downloading content or apps with security exploits (47 percent) top the list.



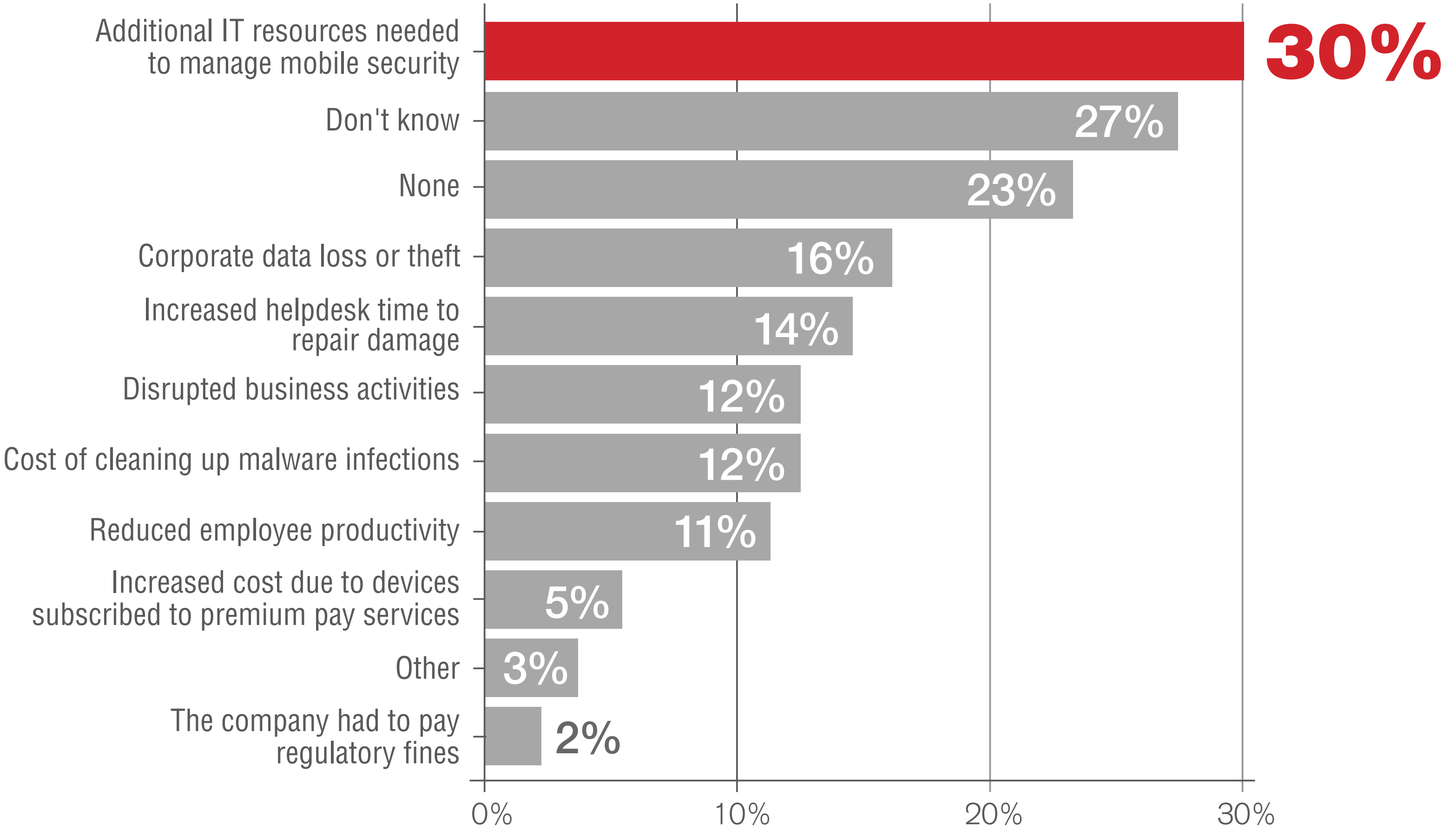
WHAT TYPE OF SENSITIVE DATA AND INTELLECTUAL property are you most concerned about?

A majority of organizations are most concerned about protecting business data (74 percent), followed by customer and employee data (69 percent).



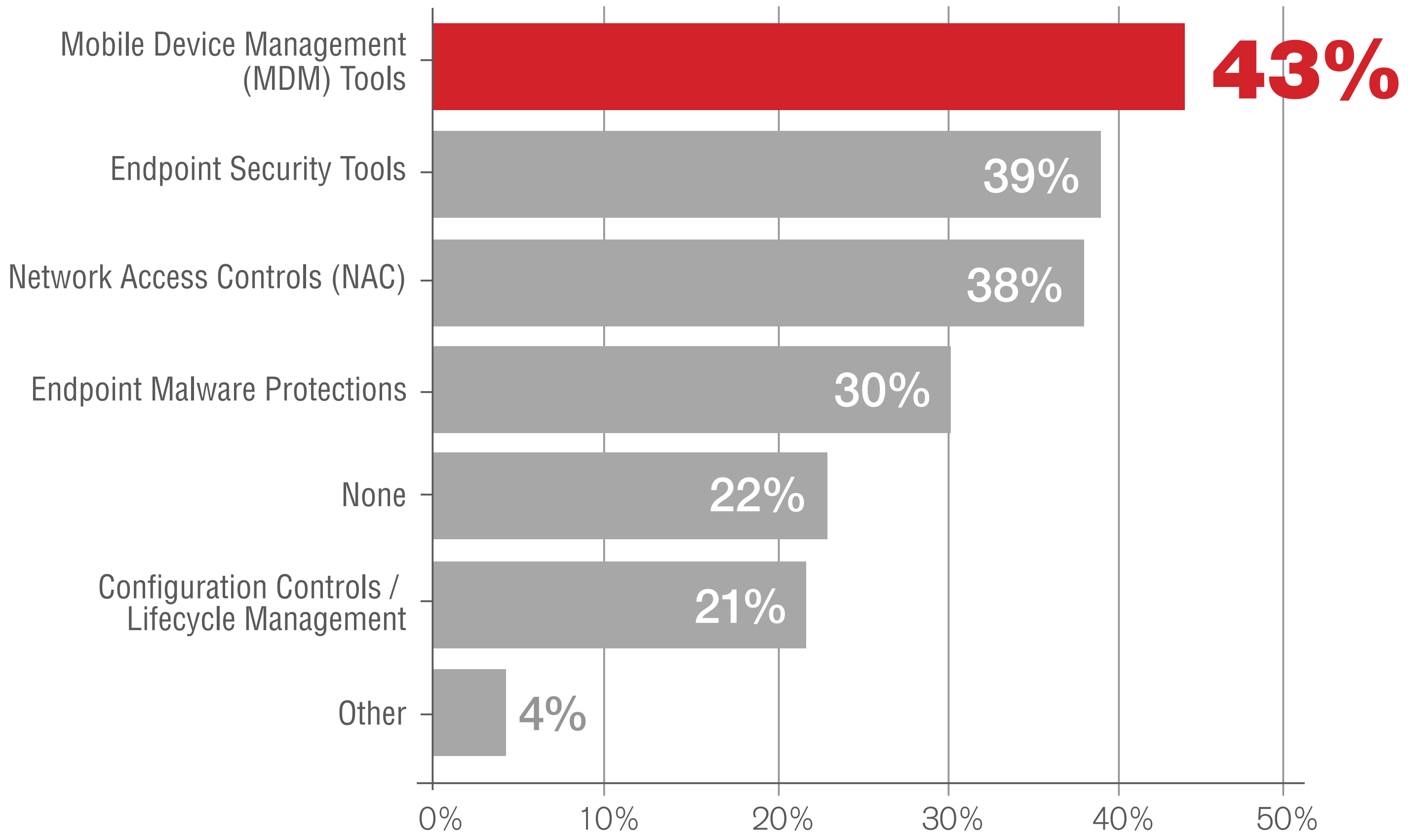
WHAT NEGATIVE IMPACT DID MOBILE SECURITY threats have on your organization?

Additional IT resources to manage security incidents (30 percent) are by far the biggest negative impact of mobile security threats.



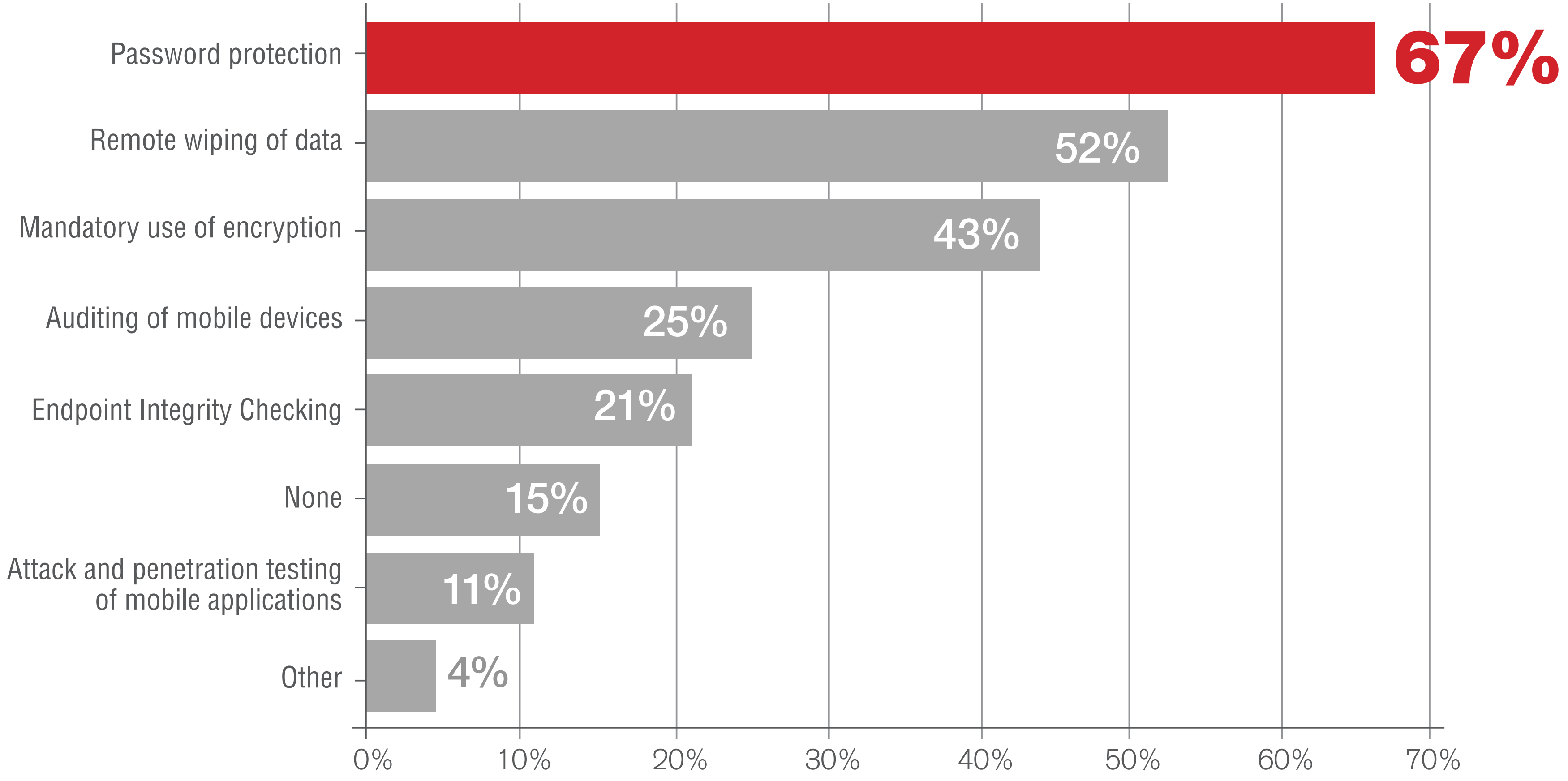
WHAT TOOLS ARE USED TO MANAGE MOBILE DEVICES?

43 percent of organizations use mobile device management (MDM) tools to monitor and manage mobile devices, followed by endpoint security tools (39 percent) and Network Access Controls (NAC) with 38 percent.



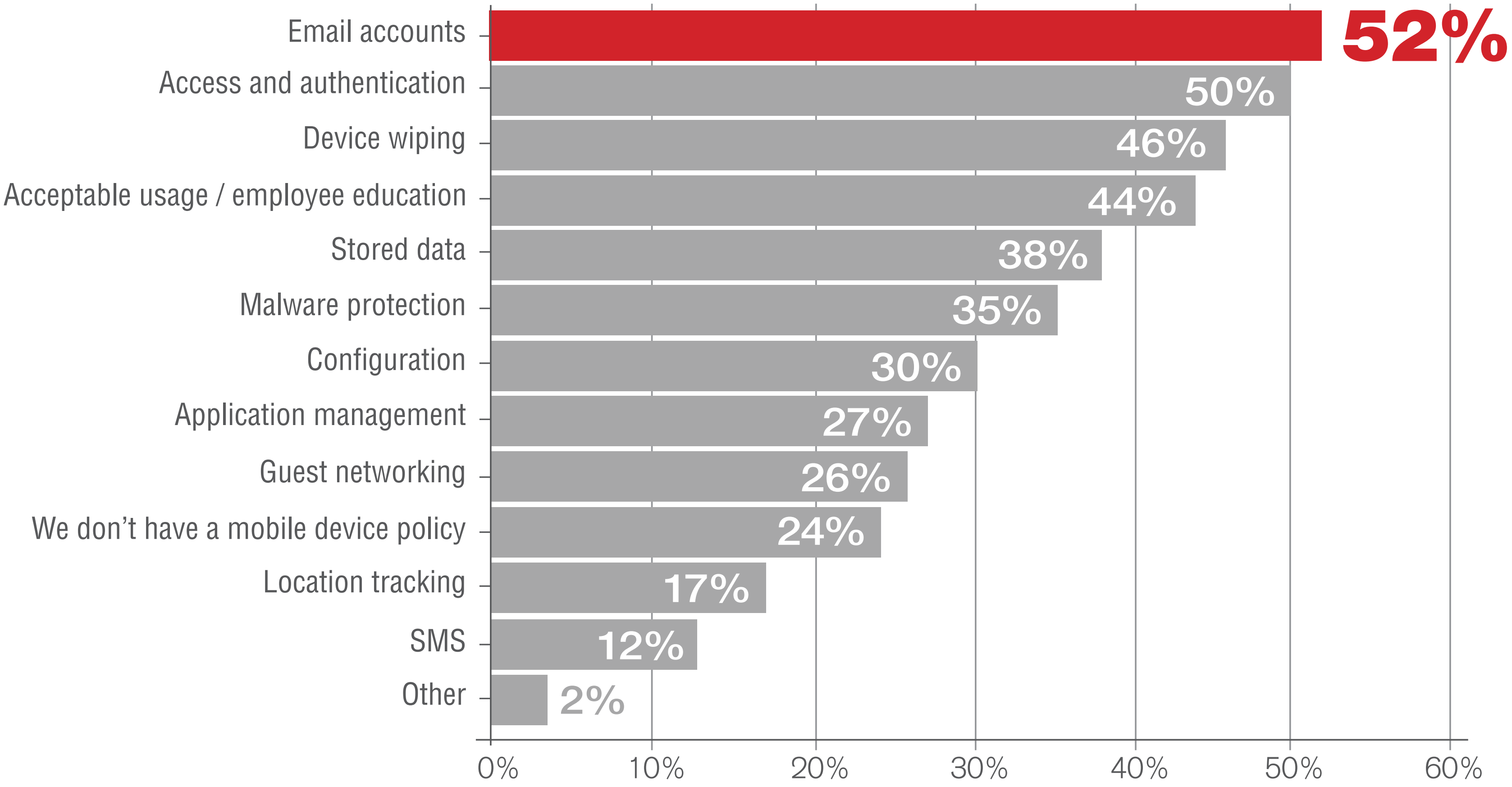
# WHAT RISK CONTROL MEASURES ARE IN PLACE
for mobile devices?

The most common risk control measure is password protection (67 percent), followed by remote wiping of data (52 percent) and use of encryption (43 percent, which includes technologies such as VPN and disk encryption). 15 percent of organizations have no specific mobile security controls in place. Only 11 percent of respondents are running attack and penetration tests on mobile devices.



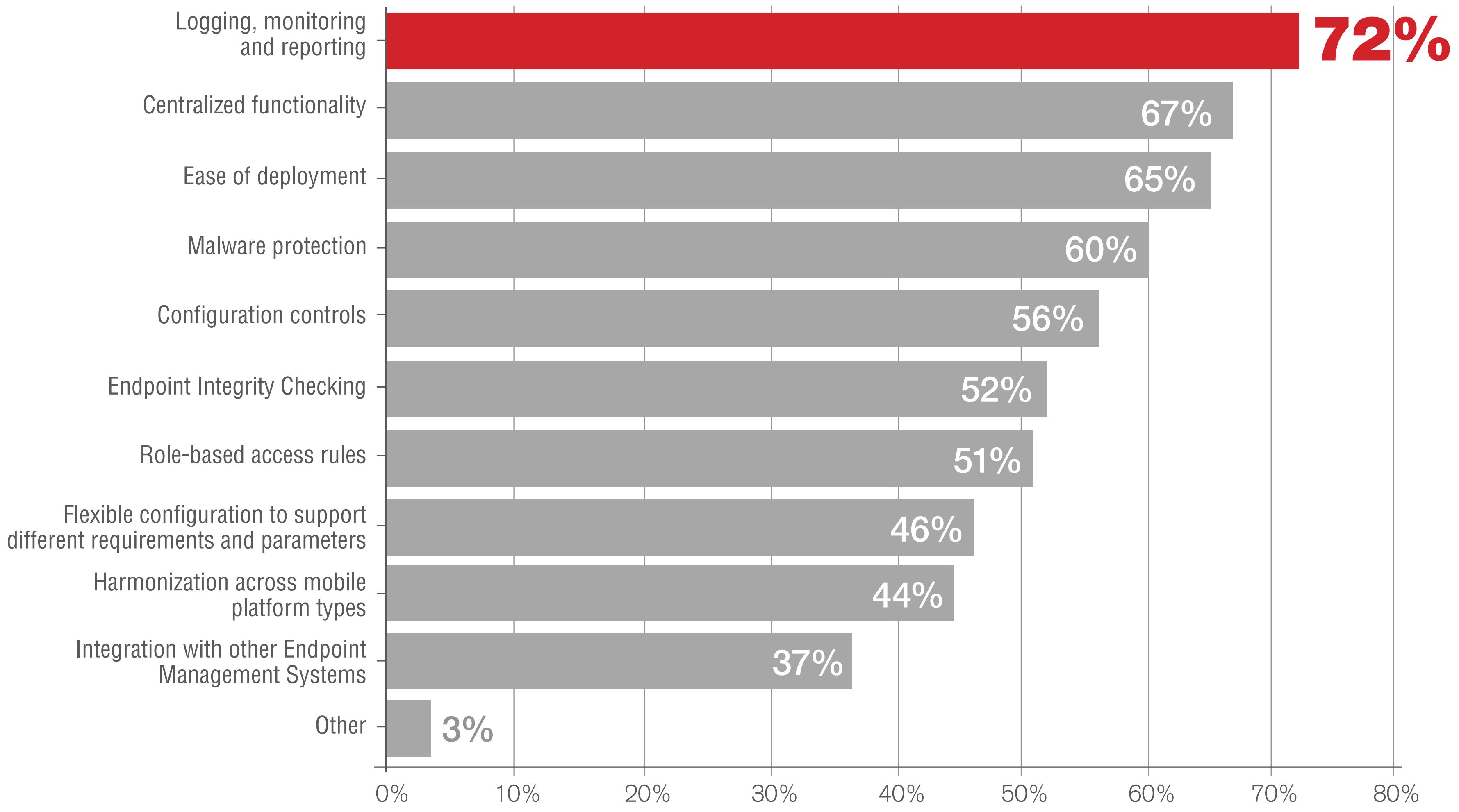
WHAT AREAS ARE COVERED BY YOUR organization's mobile device policy?

Email accounts (52 percent), access and authentication (50 percent), and acceptable usage & employee education (46 percent) are the top-3 mobile device policy topics for organizations. Malware protection (35 percent) scores relatively low considering that threats can easily walk past perimeter security by mobile devices.



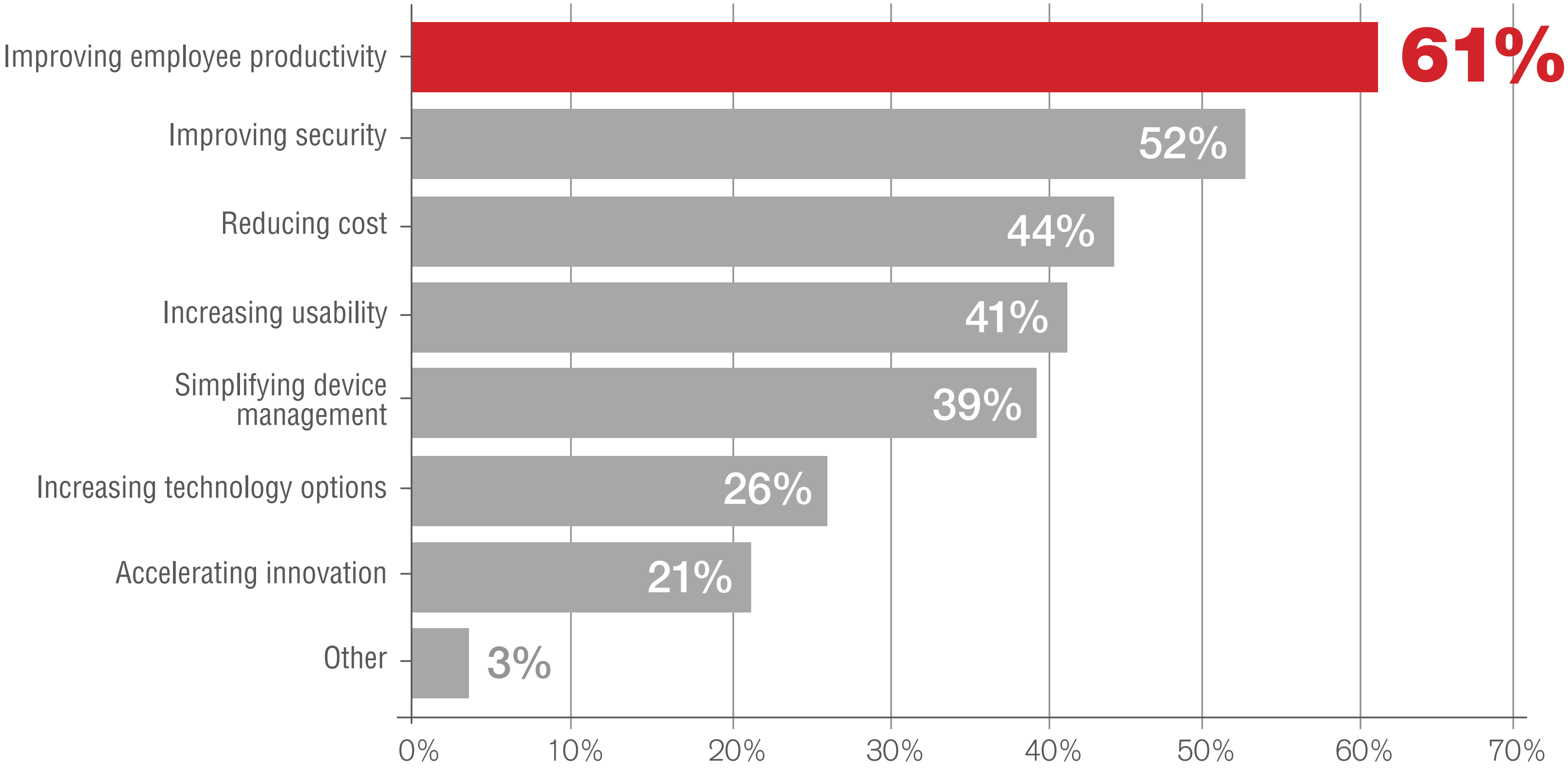
WHAT ARE THE KEY CAPABILITIES REQUIRED
for mobile device management?

The most required MDM features include logging, monitoring and reporting (72 percent).



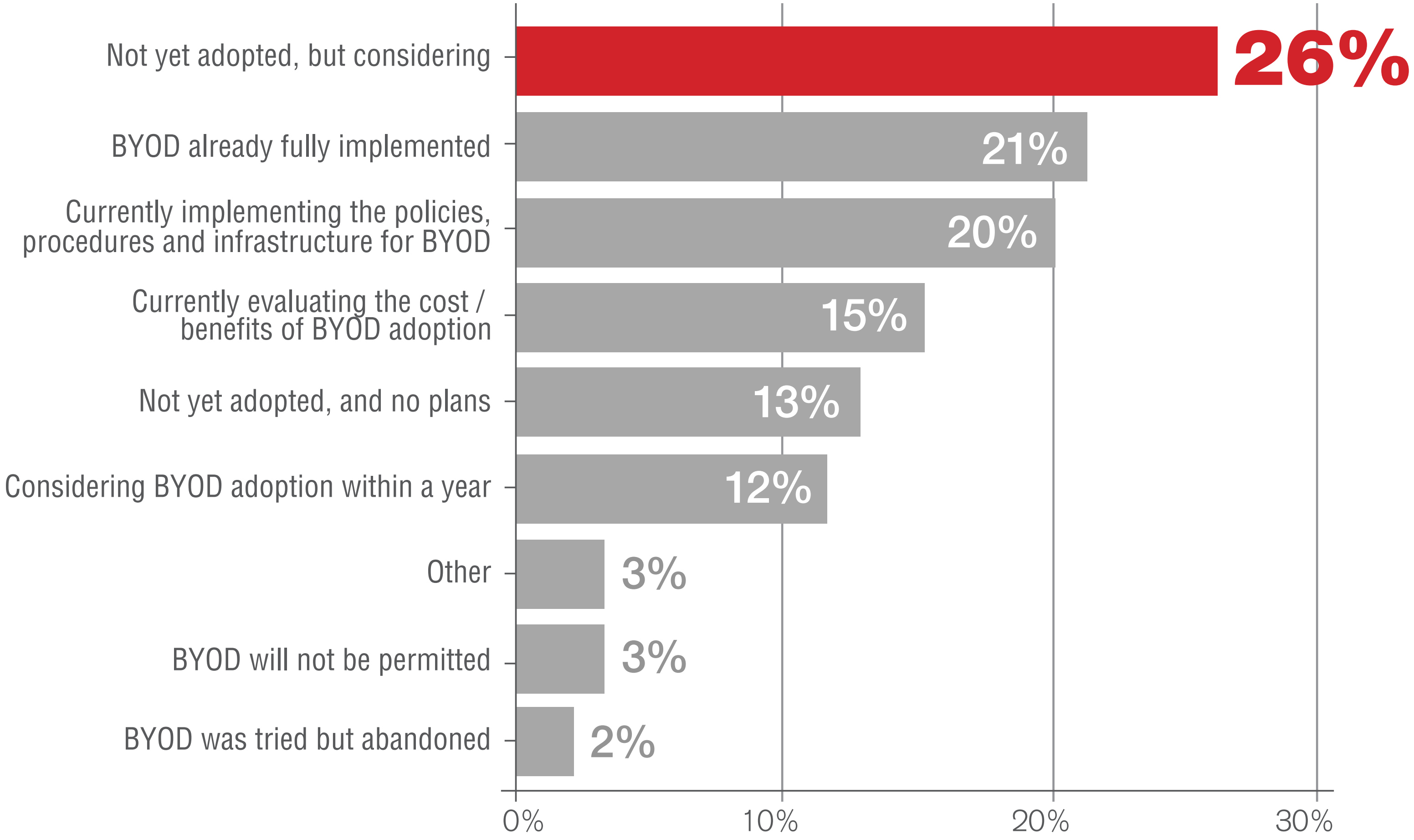
WHAT ARE YOUR MOST IMPORTANT MEASURES of BYOD success?

Employee productivity (61 percent) is the single most important measure of BYOD, which is aligned with 'increasing employee productivity' receiving 54 percent when we asked about the main drivers for BYOD. Improving security of the BYOD initiative ranks second with 52 percent.



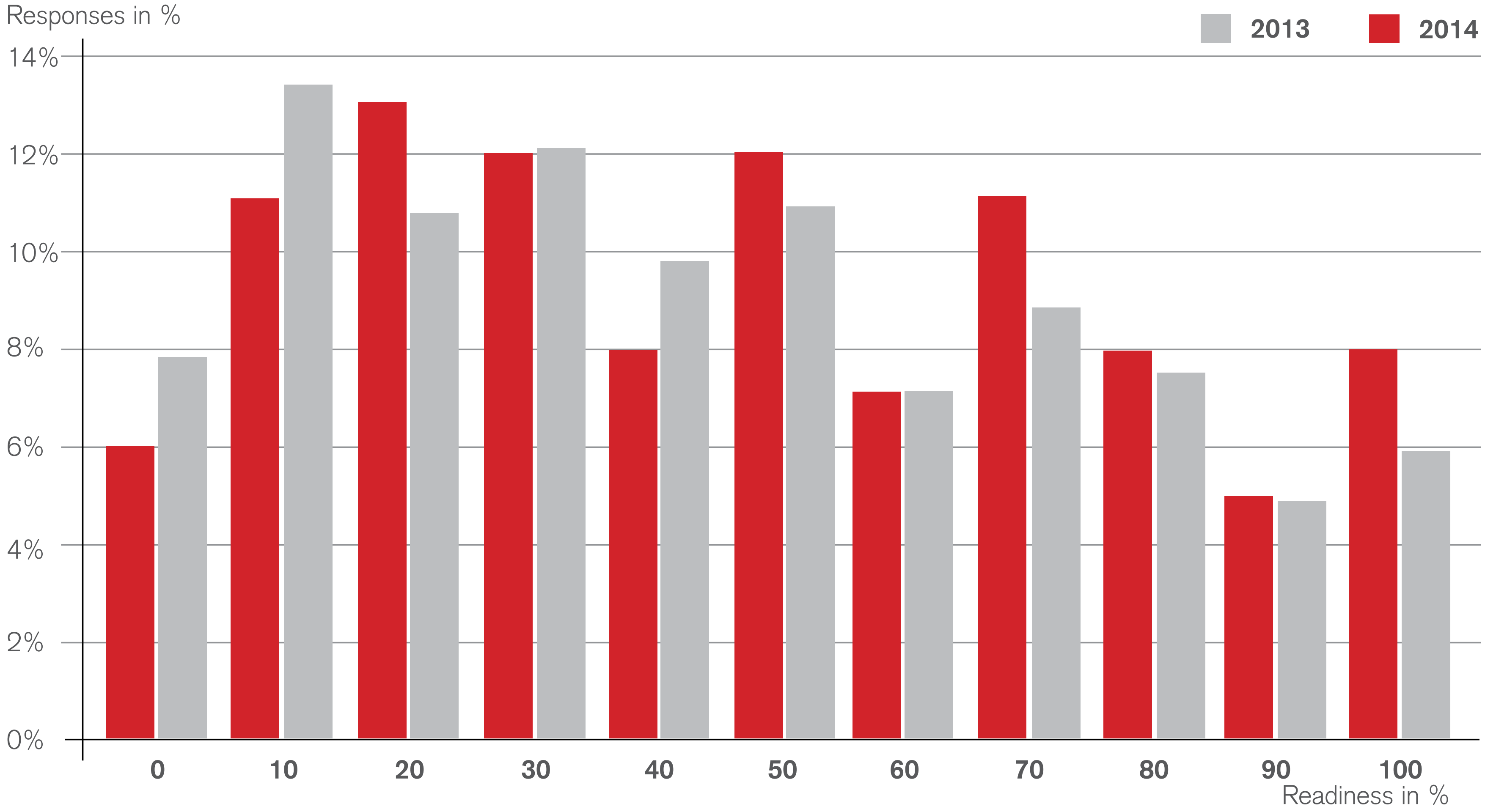
WHAT STAGE OF BYOD ADOPTION HAVE YOU REACHED?

While 20 percent of organizations are working on the policies, processes and infrastructure for BYOD, 21 percent have fully implemented BYOD. 26 percent of survey participants are considering BYOD but have not adopted it yet.



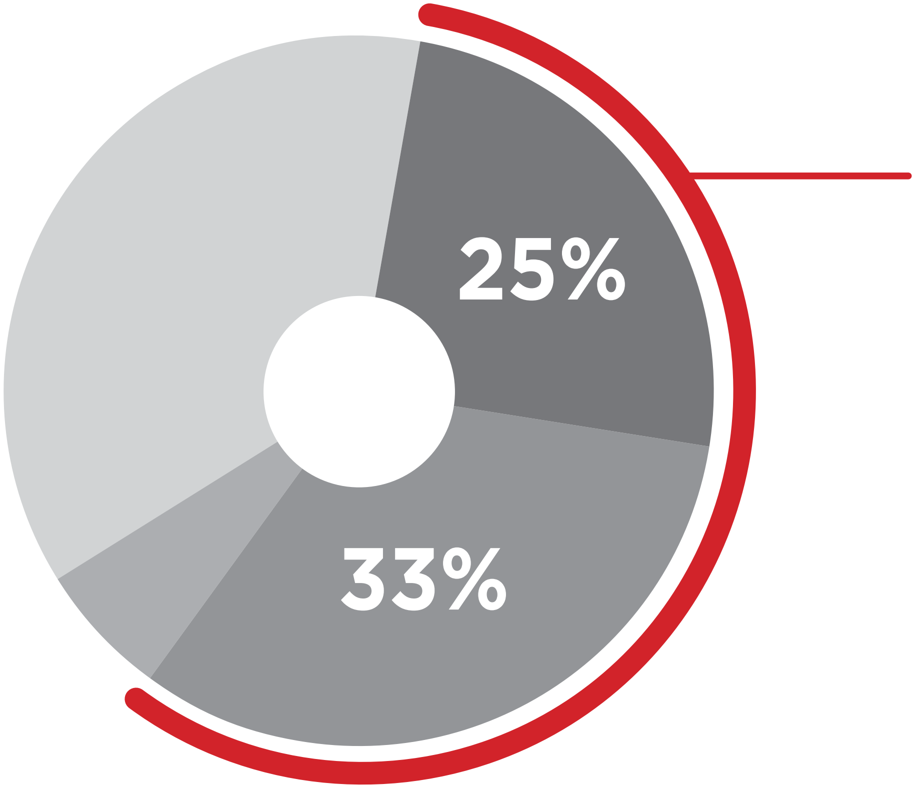
HOW READY ARE ORGANIZATIONS FOR BYOD?

While we still have some way to go toward broad BYOD adoption, organizations are somewhat better prepared for BYOD than a year ago. This year, 40 percent of respondents rank their readiness at 60 percent or higher compared to 34 percent last year.



HOW ARE BYOD BUDGETS CHANGING
over the next 12 months?

For 25 percent of organizations, BYOD budgets will increase while budgets will remain flat for 33 percent. Only 6% anticipate budget decreases.



58%

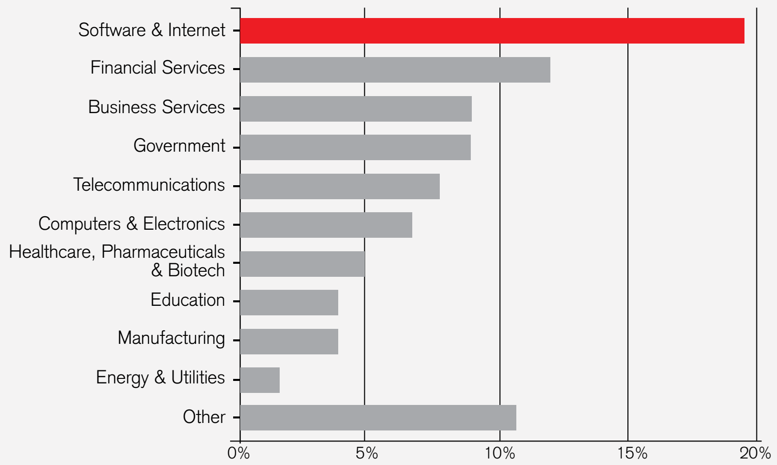
Budgets will increase or stay flat

- ■ **25%** | BYOD budget will increase
- ■ **33%** | BYOD budget will stay flat
- ■ **6%** | BYOD budget will decline
- □ **37%** | Not sure

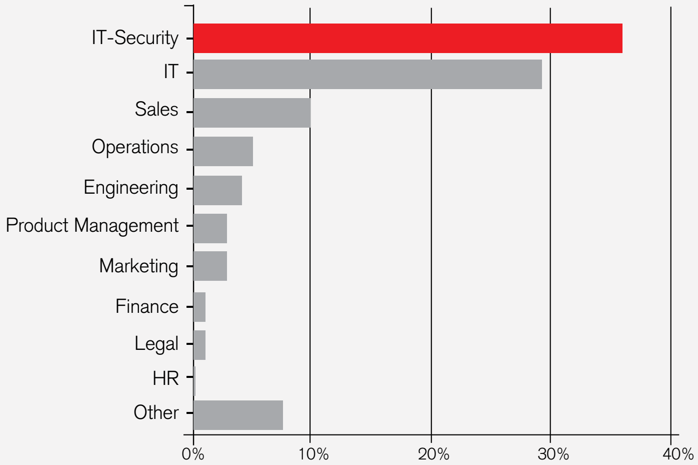
DEMOGRAPHICS & METHODOLOGY

This survey was conducted from April through June 2014. We collected 1,122 responses from information security professionals across the world – here is a detailed breakdown of the demographics.

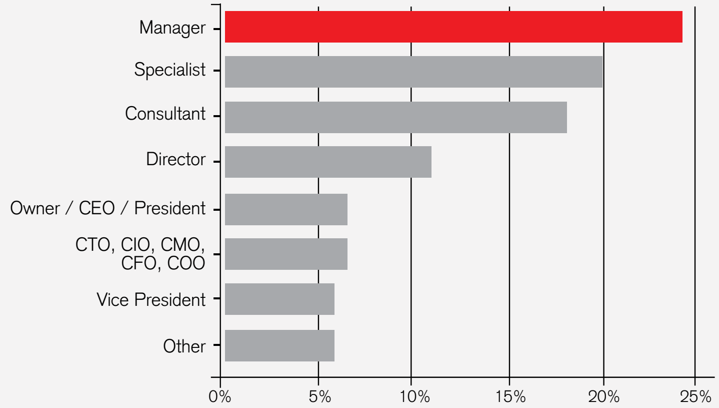
INDUSTRY



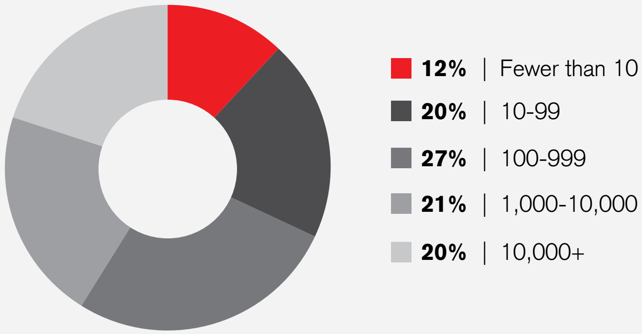
DEPARTMENT



SENIORITY



SIZE (Number of Employees)


12% | Fewer than 10
20% | 10-99
27% | 100-999
21% | 1,000-10,000
20% | 10,000+