bitglass

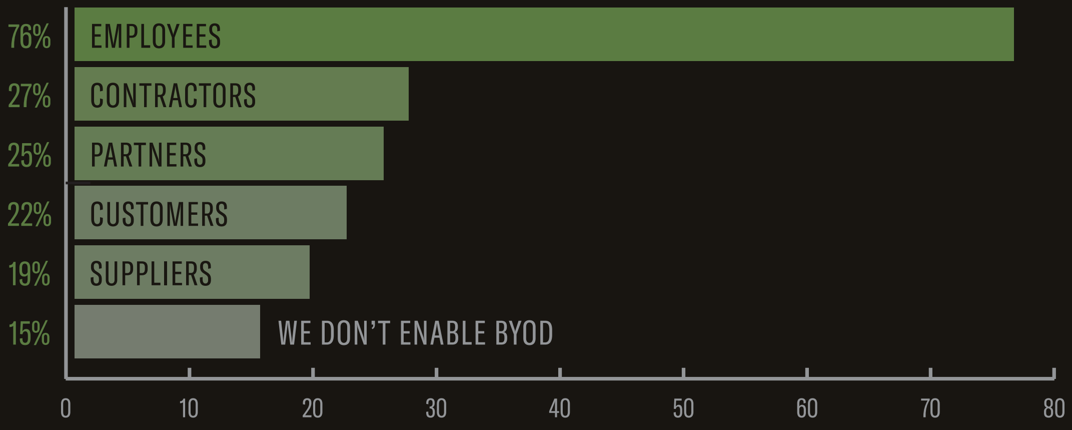
MISSION IMPOSSIBLE : SECURING BYOD

The rise of the cloud has enabled employees to perform an ever-growing amount of work from mobile devices, forcing organizations to rethink how they protect their data. Bring your own device (BYOD), whereby employees work from their personal smartphones and tablets, has proven particularly challenging for the enterprise to secure.

Bitglass wanted to learn more about what organizations are doing to protect data on mobile devices. So, in partnership with a leading, cross-industry, cybersecurity community, Bitglass surveyed IT experts and uncovered the state of BYOD security in the modern enterprise.

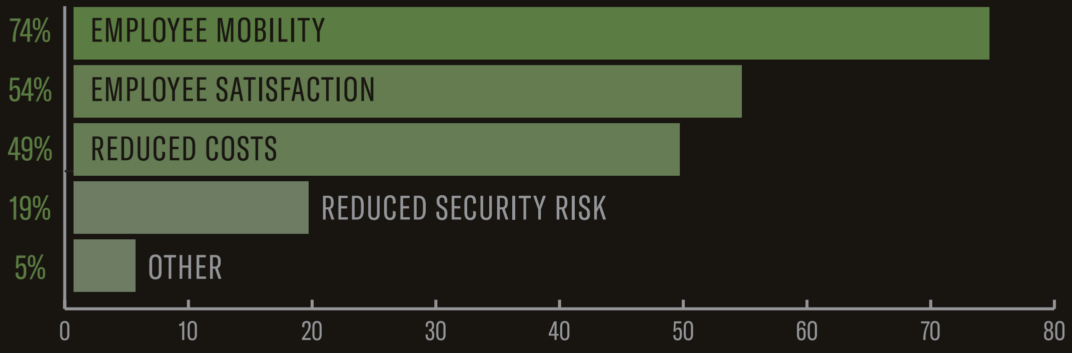
THE RISE OF BYOD

FOR WHICH GROUPS DOES YOUR ORGANIZATION ENABLE BYOD?



85% of organizations enable BYOD; those that deny data access to personal devices are now the minority.

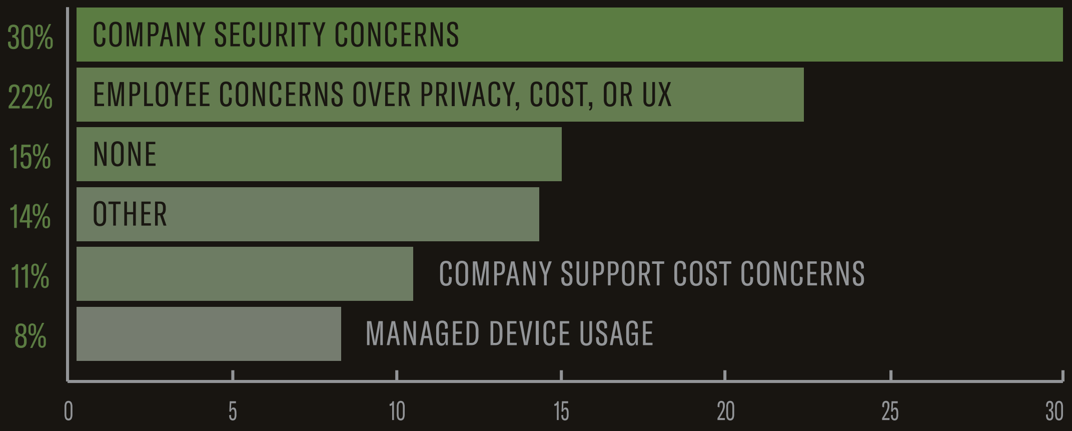
WHAT ARE THE MAIN BENEFITS OF BYOD?



BYOD increases employee mobility and, consequently, organizational flexibility, efficiency, and collaboration.

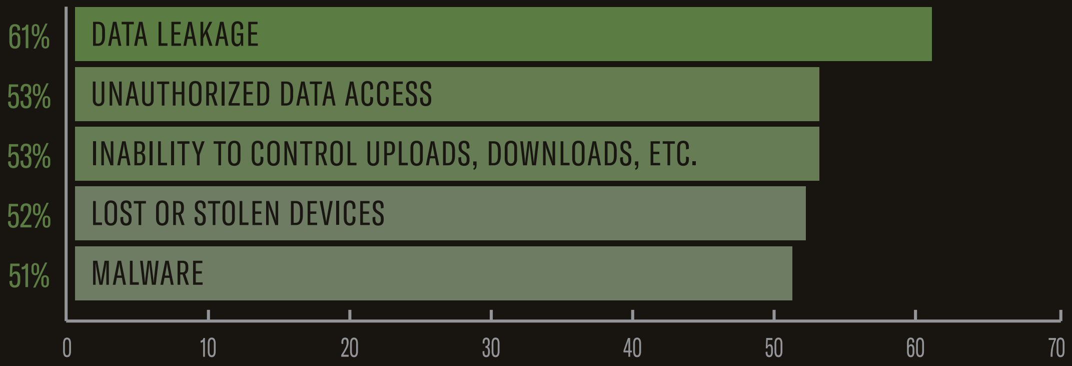
LACKING THE STATE OF THE ART

WHAT IS THE LEADING INHIBITOR TO BYOD IN YOUR FIRM?



Despite its benefits, some organizations are still hesitant to embrace BYOD—primarily because of security and employee concerns.

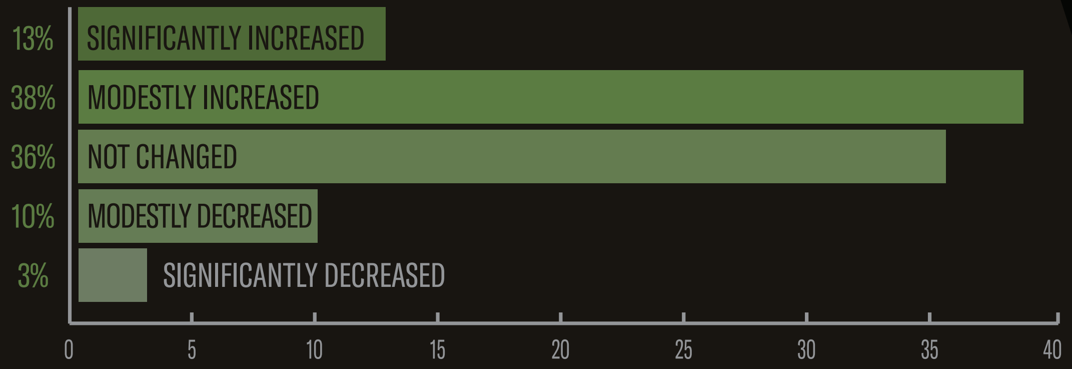
WHAT ARE YOUR MAIN BYOD SECURITY CONCERNS?



Respondents highlighted all BYOD security concerns quite equally; no threat is too small to overlook when enabling bring your own device.

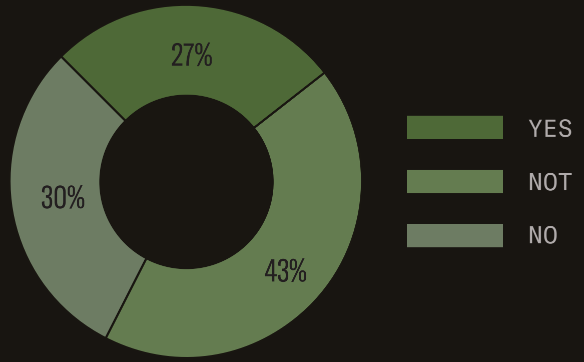
MOBILE THREATS MOUNTING

THIS YEAR, THREATS TO MOBILE DEVICES HAVE

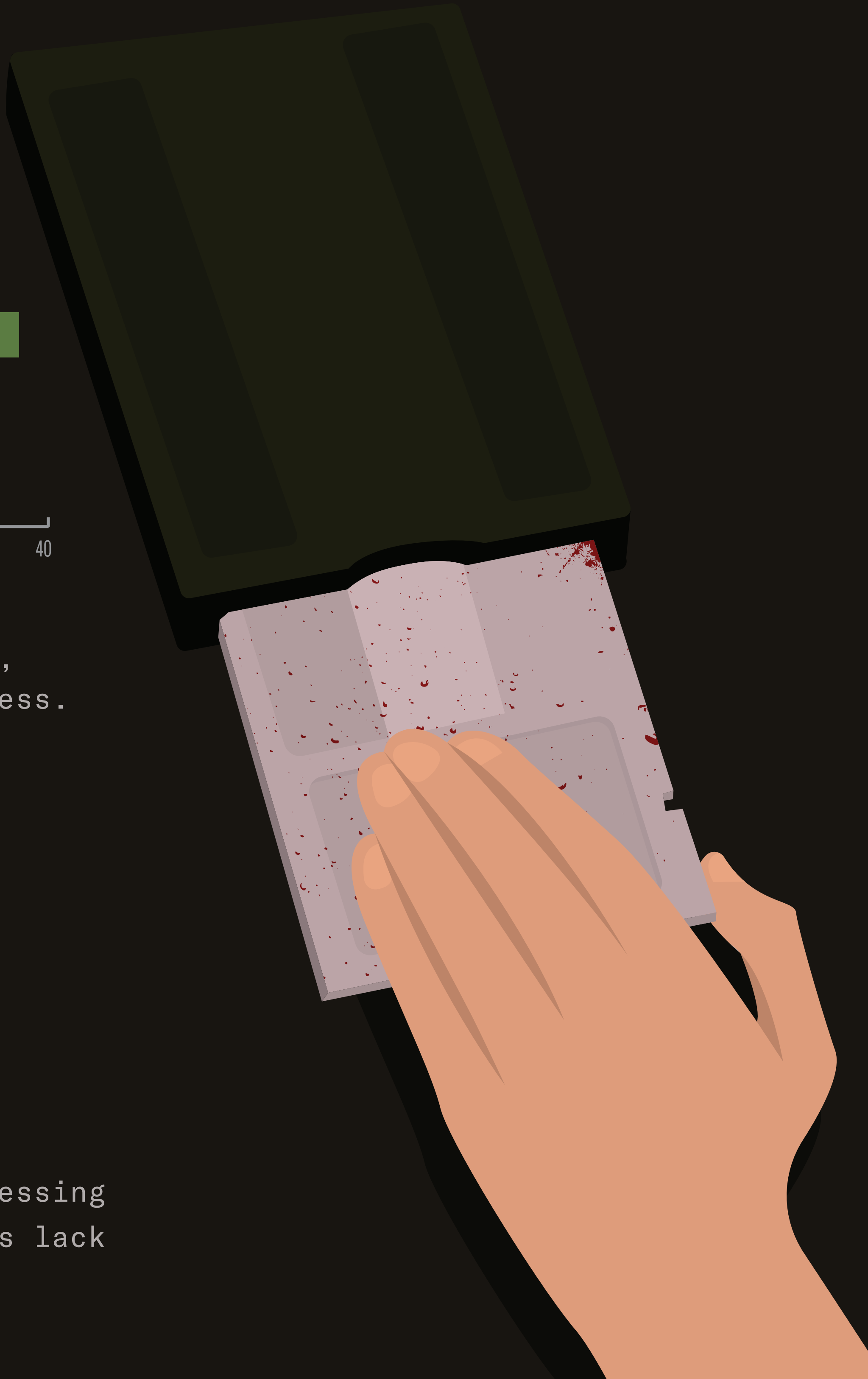


51% of respondents stated that the volume of threats targeting mobile devices is increasing, following the rise of BYOD and mobile data access.

HAVE ANY BYO OR MANAGED DEVICES IN YOUR ORGANIZATION DOWNLOADED MALWARE?

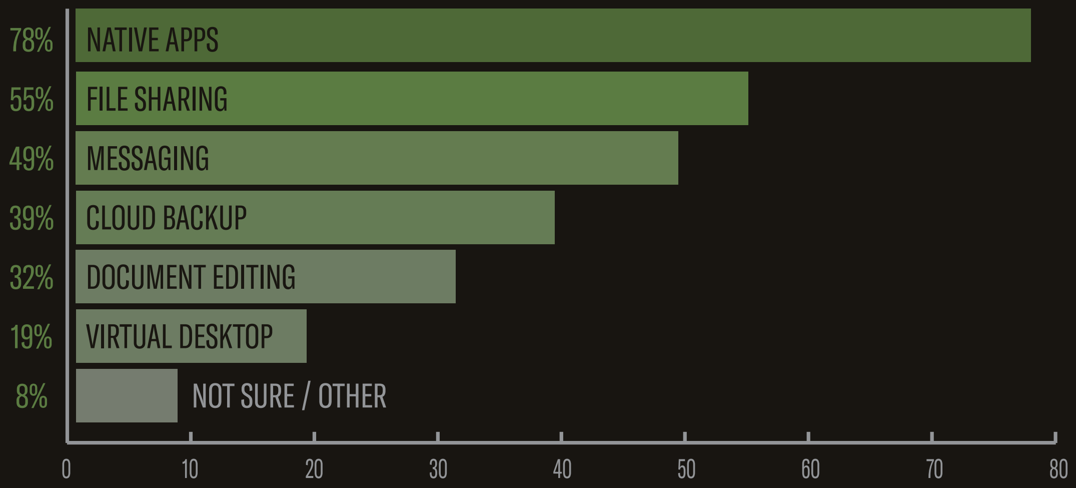


43% of respondents did not know if devices accessing corporate data were infected with malware. This lack of visibility is highly concerning.



NO ONE SEES MAX

INTO WHICH APPS DO YOU HAVE VISIBILITY ON BYO DEVICES?



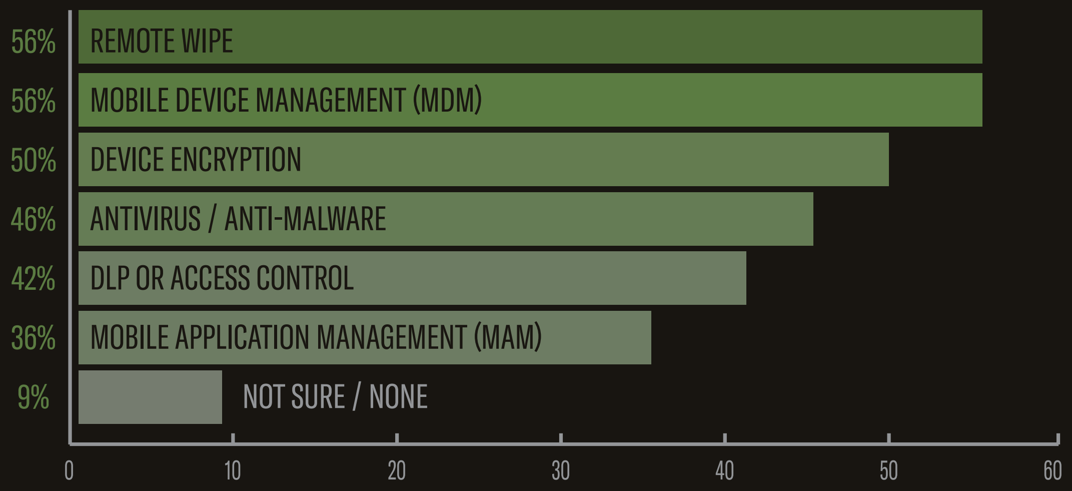
One in five organizations lacks visibility into basic, native mobile apps (like email) on BYO devices.

As you cannot secure what you cannot see, visibility into cloud apps is the first step towards data protection. Unfortunately, as the above chart shows, organizations do not have sufficient visibility into applications on BYO devices.

Only 55% of firms can monitor file sharing apps, like Box and Dropbox, that can easily be used to share highly sensitive files. Likewise, only 49% of enterprises can see what is done with their information in messaging apps like Slack. Obviously, this level of oversight is simply not enough.

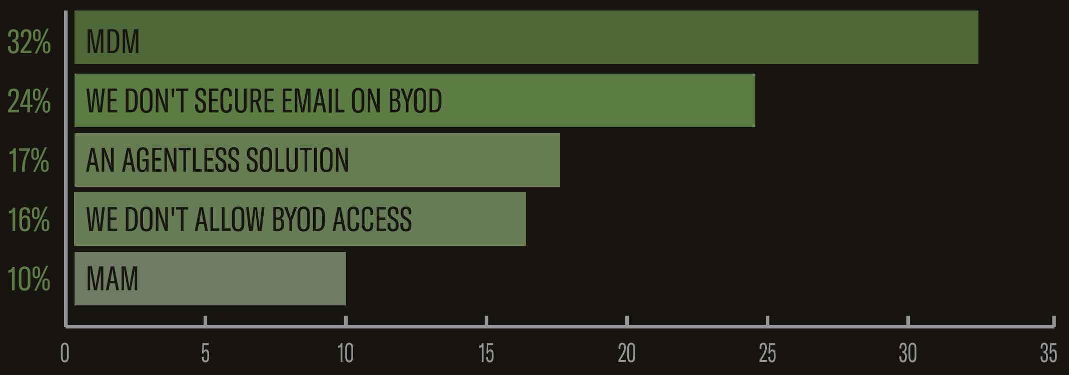
CHOOSE YOUR WEAPONS

WHAT IS USED OR PLANNED FOR MOBILE SECURITY IN YOUR ORGANIZATION?



To secure mobile and BYOD, organizations must use solutions that boast a variety of the above security capabilities

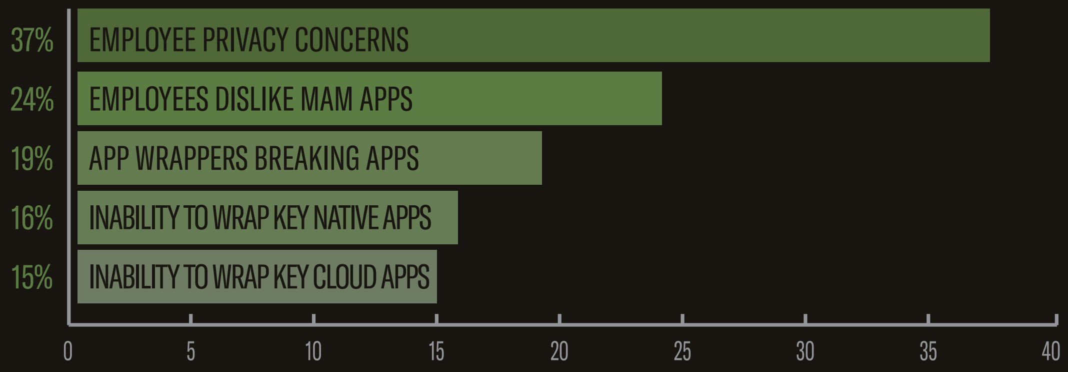
HOW DO YOU SECURE EMAIL ON BYO DEVICES?



42% of firms rely upon ill-suited, agent-based tools to secure email on BYOD. Surprisingly, 24% don't secure it at all.

MAM CHALLENGES

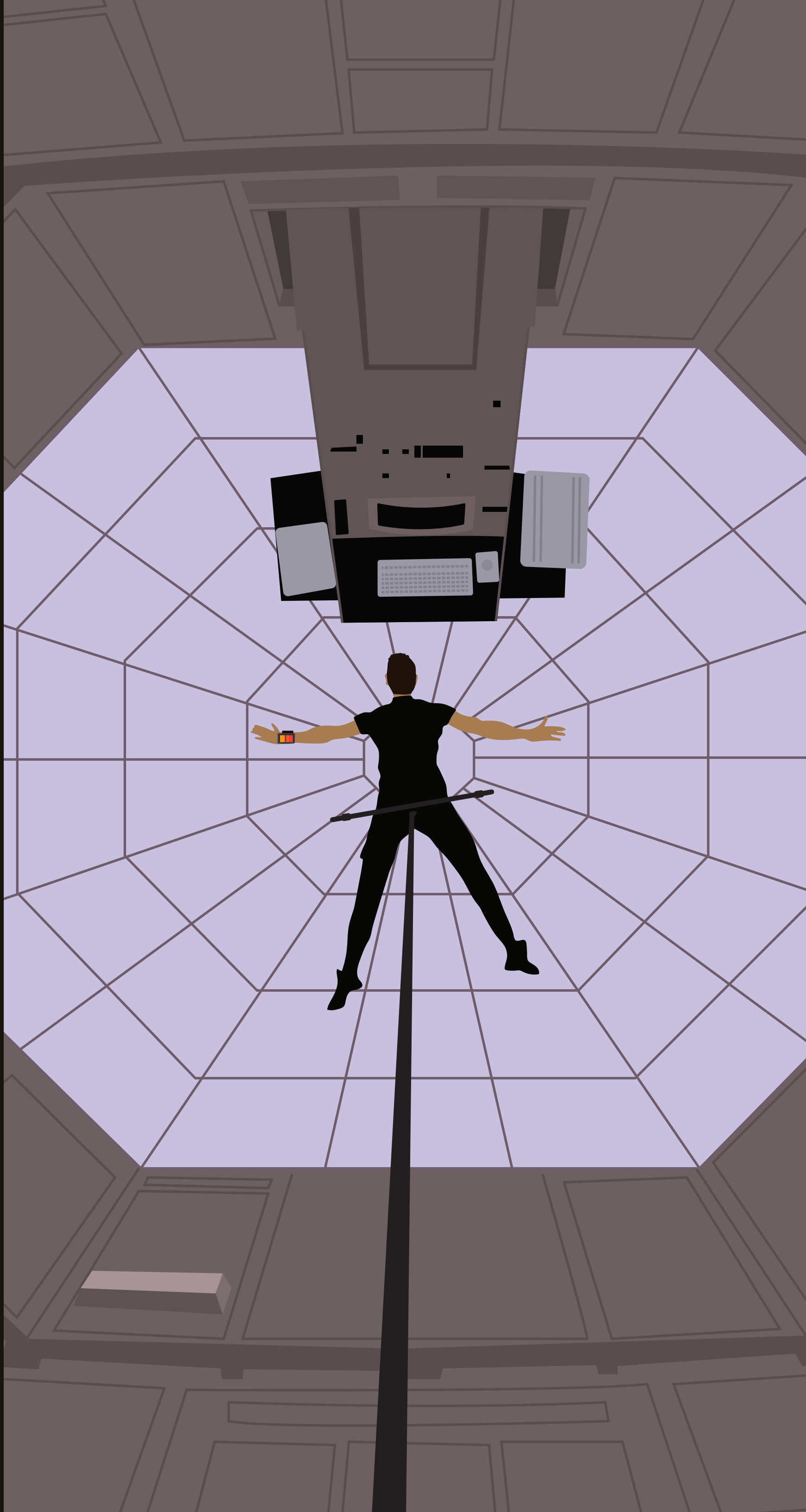
WHAT ARE YOUR TOP MAM CHALLENGES?



At 37%, employee privacy concerns topped the list of MAM challenges.

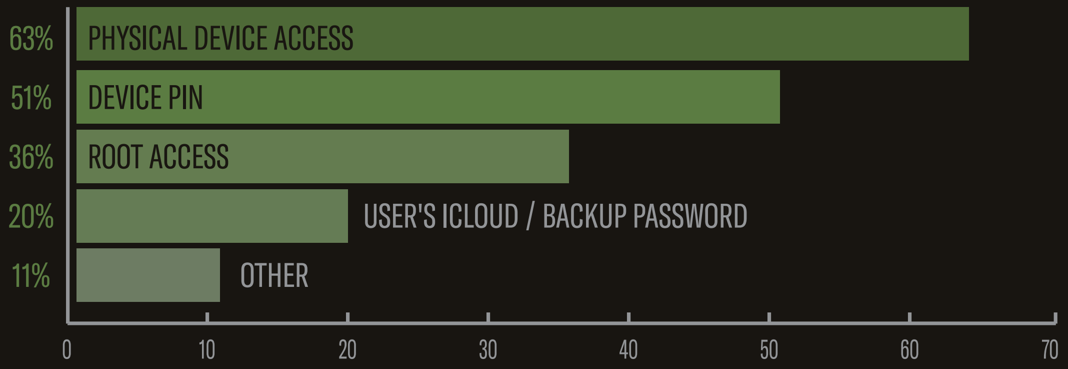
Mobile application management (MAM) is an agent-based security tool that requires employees to use corporate-sanctioned, “wrapped” apps. However, agent-based approaches to security rarely work in organizations that enable BYOD.

When installed on endpoints, agents give employers deep visibility into all device activity, including personal internet traffic, geographic location, files, and more. Naturally, this is a large concern for employees. As such, agentless security is critical wherever BYOD is enabled.



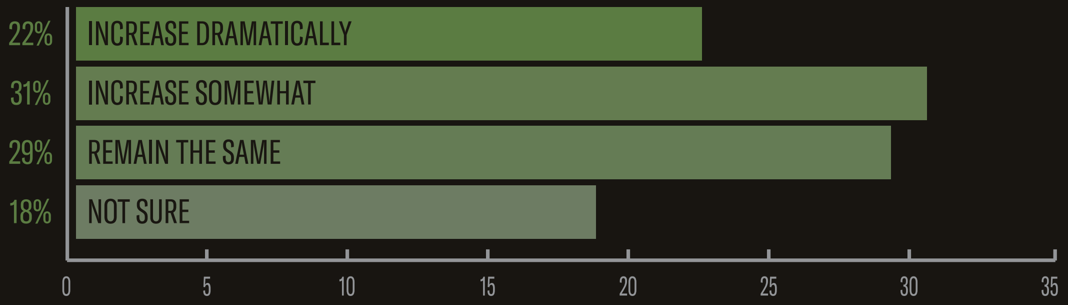
PRIVACY IN PERIL

WHAT DO YOU NEED TO PROVISION MOBILE DEVICES?



To provision mobile devices, 63% of firms need physical access and 51% require users' PIN codes. This is not ideal for enabling BYOD.

IF IT COULDN'T VIEW PERSONAL DATA, BYOD ADOPTION WOULD



Over 50% of respondents said BYOD adoption would increase if IT couldn't view or alter personal data.

WRAP-UP

Organizations are enabling BYOD more and more, seeking benefits like employee mobility, efficiency, and satisfaction. This new style of performing work on the go is clearly here to stay. However, mobile-based threats are on the rise, and there are valid security concerns around BYOD. As such, organizations must adopt advanced solutions that can protect data in any type of device, including personal mobile phones. It is only through comprehensive, real-time security that the enterprise can succeed in today's dynamic business world.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

ABOUT BITGLASS

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.