

BYOD SECURITY

2015 RISE OF THE EMPLOYEES

 bitglass

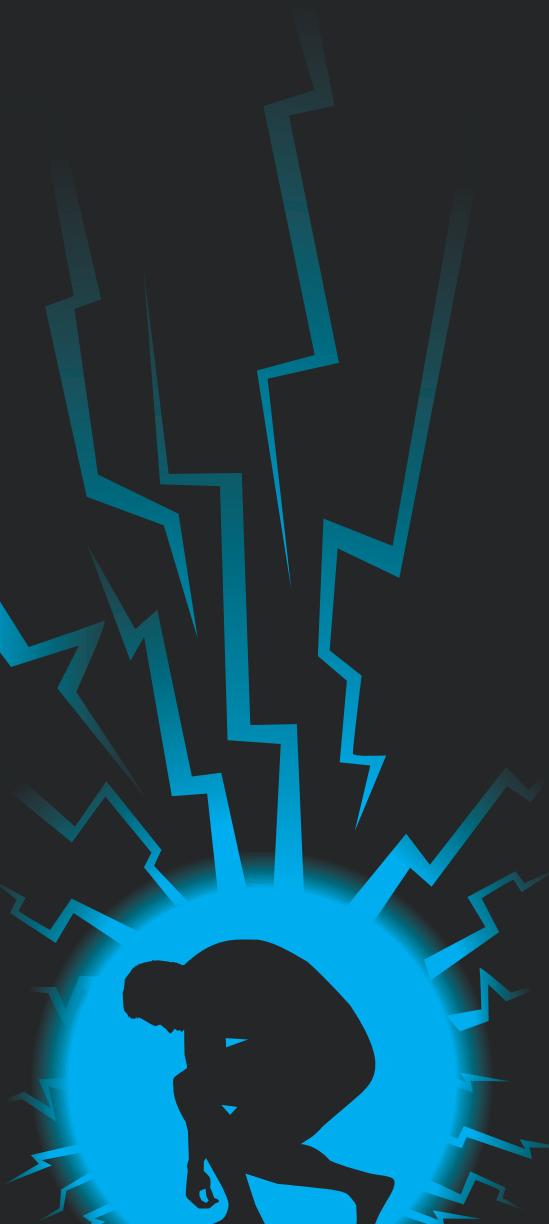


Bring Your Own Device (BYOD) and Mobility have completely transformed the way that IT departments provision devices to employees. The first attempt at providing secure mobility was to control and lock down devices via enterprise mobility solutions like Mobile Device Management (MDM) or Mobile Application Management (MAM). Unfortunately, employees frequently reject these solutions as too oppressive or too invasive into personal privacy. The result is that millions of dollars are spent on MDM/MAM solutions for BYOD programs that never achieve anticipated broad adoption. So will BYOD be relegated to the dustbin or does it simply need a fresh approach?

For this report, Bitglass conducted two surveys on BYOD adoption, challenges, and overall effectiveness. One survey focused on end users—capturing opinions from 2,021 smartphone toting employees. The second survey captured the distinct view of 227 IT security professionals with responsibility for mobility in their organization. The findings showcase a growing disconnect between end users and IT, signaling that 2015 is turning out to be the year of the Rise of the Employees.

BYOD has room to grow substantially, but the path forward requires a look forward to next-generation mobile security with data-centric approaches that honor personal privacy and eschew agents and configuration on personal devices.

TOP FINDINGS



57%

57% of end users (and 38% of IT professionals) do not participate in a company BYOD program because they do not want employers' IT departments to have visibility into their personal data and applications.

1/3

Since MDM/MAM solutions take control over personal devices, privacy has been an issue in almost 1 out of 3 BYOD programs.

67%

IT and employees agree—67% of employees would participate in a BYOD program if employers had the ability to protect corporate data, but couldn't view, alter or delete personal data and applications. 64% of IT pros believe such a solution would make their BYOD program more successful.

9%

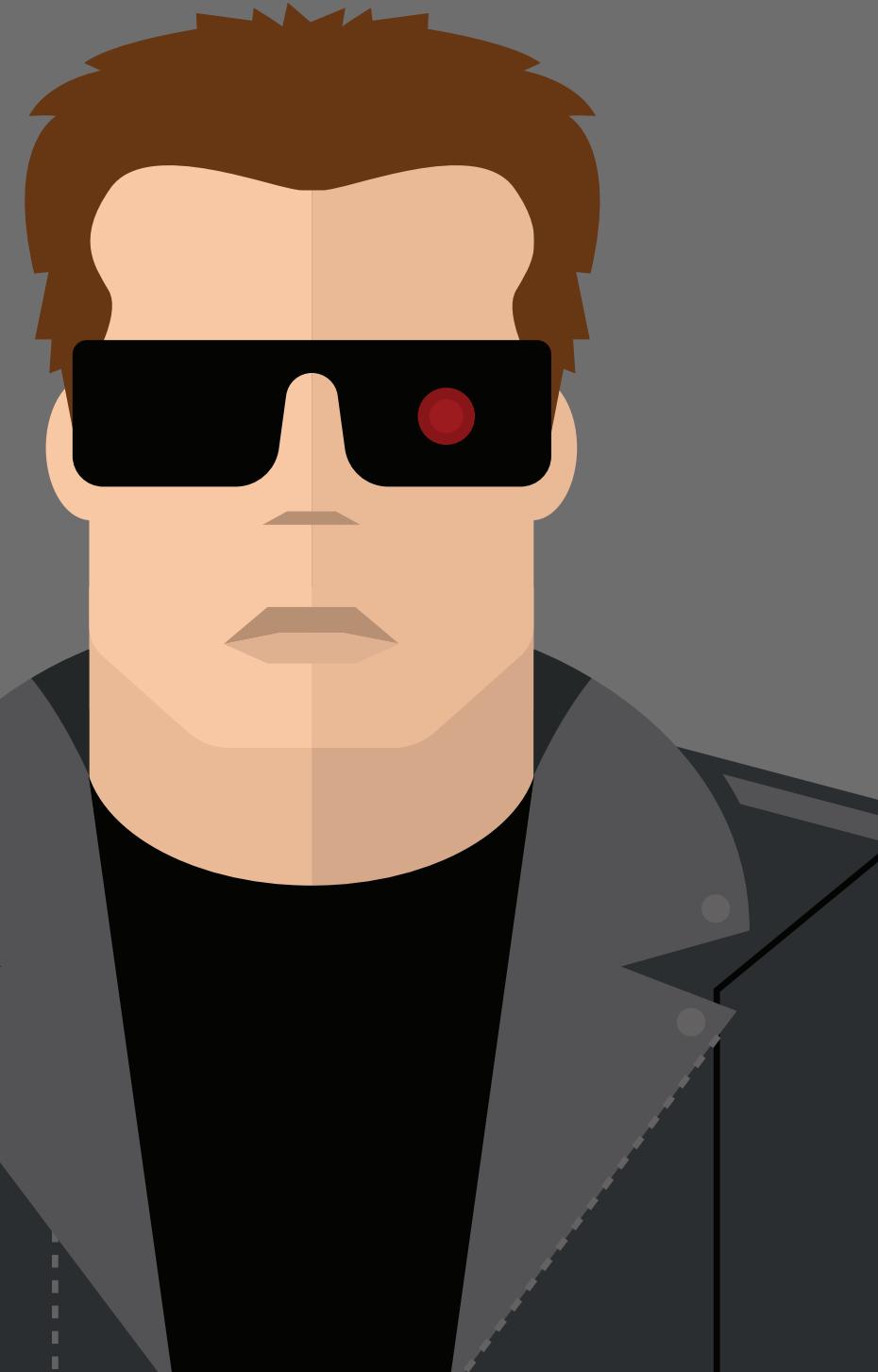
MAM is DOA. Despite a huge push by EMM vendors, only 9% of organizations have deployed a MAM solution. Violations of application licensing agreements and fragile "wrapping" approaches have softened the impact of MAM.

IT teams must come to terms with reality—participation in BYOD programs is low because employees are worried about IT control over personal devices. The next-generation of secure mobility solutions takes a data-centric approach, preserving privacy and the user experience, while securing corporate data without any footprint on the device.

THE SURVEYS—STRAIGHT FROM THE SOURCE

The **2,242** enterprise employees that carry smartphones and/or tablets surveyed tell the story of enterprise mobile security today, and shine light on the need for a more effective method for securing BYOD devices in the enterprise.

This survey data came straight from the source; employees that own smartphones and/or tablet, and IT security professionals with insights into BYOD and mobility programs at their organizations.



PUT AN END TO THE "LOCKDOWN"

45%

PERCENT OF ENTERPRISES HAVE AN
MDM AND/OR MAM SOLUTION DEPLOYED

36%

PERCENT OF ENTERPRISES
USING MDM SOLUTIONS

9%

PERCENT OF ENTERPRISES
USING MAM SOLUTIONS

57%

PERCENT OF EMPLOYEES THAT
REFUSE TO USE MDM/MAM

28%

PERCENT OF ENTERPRISES DOING
NOTHING ABOUT MOBILE SECURITY

15%

PERCENT OF ALL DATA BREACHES
DUE TO LOST MOBILE DEVICES

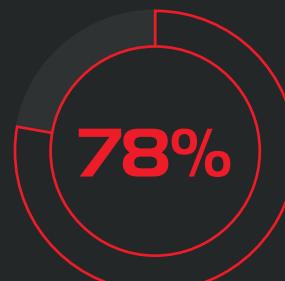
0501510578459797278240789279801
1810558508550108427980182179011
9712097100207201278901280712780
120981306838306371981307900192
7120790801029101092109907102480
120897813205280440871028027801
078248041040834080430317801387





THE USER REVOLT

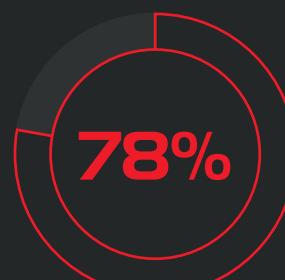
Analysts are predicting that 2016 will be the year of the revolt from oppressive MDM and MAM solutions. But the revolt has already begun. Users want the ability to work from anywhere, at any time and from any device. But they also fear "big brother" snooping into their personal applications, which is why they are revolting against BYOD programs en masse.



of employees said they are not likely to participate in a BYOD program if their employer has visibility into personal applications/locations.



would not participate in a BYOD program at work where their employer has the ability to wipe their personal mobile device to protect their proprietary information if they leave the organization.



understand that companies need to protect their own proprietary information, but that they should not have the ability to wipe personal data from the mobile device.

MDM/MAM: JUDGMENT DAY

Employees aren't the only ones who like the idea of BYOD within the workplace. IT security teams want to use their new iOS or Android device for work as well. And as it turns out, neither employees nor IT security teams are fans of company owned MDM/MAM software being installed on their personal devices.

— 38% —



38% of IT security professionals do not personally participate in their own BYOD programs because they do not want software on their personal devices.

BYOD: SALVATION

BYOD in the workplace has rendered MDM and MAM solutions obsolete. Personal privacy issues, changes to the user experience, and complicated deployments have slowed down BYOD adoption, causing many to question BYOD's future. In order to meet the needs of both IT security and employee needs, ensuring secure, widespread adoption of BYOD in the enterprise, it's time to for a data-centric approach to mobile security.

More users are looking for a mobile security solution that doesn't require an invasive agent or configuration management... Bitglass Mobile Edition meets that need. The solution represents the next generation of mobile security—data security with no agents, no changes to the user experience, no privacy concerns, no hassles.

ABOUT BITGLASS

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company 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.



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

www.bitglass.com