ZIMPERIUM.

Gartner
Peer Insights.

Trends in Securing Mobile Access to Productivity Apps

Mobile devices allow employees to stay connected in today's increasingly distributed workforce. Microsoft Office 365 and other productivity apps are critical tools that can quickly and easily send emails, share documents, and collaborate in real-time from anywhere.

Productivity tools are now commonplace on both corporate and personal BYO mobile devices. While the use of these apps on mobile is increasing productivity, the truth is, they are also exposing more intellectual property (IP) and personally identifiable information (PII) than ever before. Security teams around the world are faced with unprecedented challenges to secure corporate data on mobile devices without compromising productivity. If not addressed, organizations face increased risk, including security breaches, privacy issues, and regulatory compliance violations.

In order to understand how to protect corporate data in a BYOD environment, Gartner Peer Insights and Zimperium examined how organizations approach the challenge of securing access to corporate data through productivity tools like Office 365.

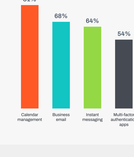
Data collection: May 22 - August 8, 2022

Respondents: 250 IT and security leaders

Business communications and productivity apps are leading use cases for enterprise enabling BYO devices. As a result, security best practices are cited as a top concern for security teams due to the risks associated with storing and transmitting sensitive corporate information.

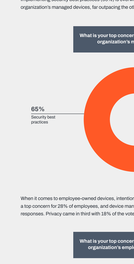
More than two thirds (68%) of organizations have enabled access to productivity tools on mobile devices for the past 1-2 years.

IT and security leaders cite calendar management (81%), business email (68%), and instant messaging (64%) as the most common use cases for mobile productivity tools.

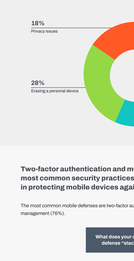


Exercising security best practices was by far the top concern cited by IT leaders, while employees were more concerned about data privacy and device management in a BYO setting.

Implementing security best practices (65%) is overwhelmingly the top concern related to securing the organization's managed devices, far outpacing the other options.



When it comes to employee-owned devices, intentionally erasing the device's data due to a security issue is a top concern for 28% of employees, and device management garnered one quarter (25%) of the responses. Privacy came in third with 18% of the vote.



Two-factor authentication and mobile device management are the most common security practices, but there is still work left to be done in protecting mobile devices against advanced persistent threats.

The most common mobile defenses are two-factor authentication (80%) and mobile device management (76%).

42% of IT and security leaders claim they have high visibility into compromised devices, while just 24% have high visibility into third-party app stores.

For nearly half of IT and security leaders (47%), "high-risk" devices are dealt with by simply alerting the employee with either email (34%) or a notification on the device (13%), both of which leave the action in the employee's hands to complete.

About half (50%) of respondents' security teams are able to address a zero-day vulnerability within 24 hours. 43% of respondents' security teams responded that they are able to address and mitigate against zero-day vulnerabilities within one week.

At least half of respondents cite mobile endpoint security must comply with GDPR (70%), PCI DSS (53%) and CPRA/CCPA (50%) regulations.

Respondent Breakdown

Gartner

Source: Gartner Peer Insights, Securing Mobile Access to Productivity Apps survey