Why High-Tech and Business Apps Are at Risk of Losing Sensitive Data

The importance of mobile app security for enterprise software continues to increase as remote work popularizes B2B app usage.

NowSecure™ MOBILE APP TRENDS

Many office employees continue to work from home full time or part time as the pandemic drags on, driving adoption of business-to-business (B2B) mobile apps. Today's enterprise software vendors compete to deliver top-notch, secure mobile apps that spur productivity, collaboration and business efficiency.

But in the rush to develop new capabilities that improve the user experience and attract new customers, some developers unknowingly build apps with security and privacy flaws that leak data and put everyone at risk.

Organizations Embrace Mobility

With telecommuting the norm in COVID-19 age, employees accustomed to working primarily on desktop or notebook computers also want to access data on smartphones and tablets. For example, many prefer to create content on a laptop but consume it on a tablet or respond to a Slack message on a smartphone while participating in a Cisco Webex or Zoom call.

Employees have proven that they can remain productive while working from home, so an increasing number of companies support permanent remote work policies or flexible work schedules in which staff divide their time working remotely and in the office.

Users spend an average of **4.8 hours** on their mobile devices **per day.**[1]

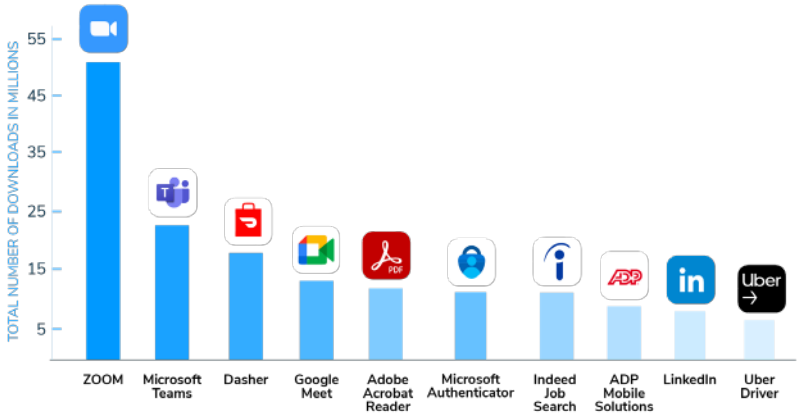
In fact, 67% of white-collar full-time employees and 45% of all full-time employees worked partially or fully remote in September 2021, according to Gallup.[2]

People downloaded 7.1 billion business and productivity apps in 2020, a 35% increase over 2019. Monthly downloads regularly topped 600 million, according to App Annie.[3] Worldwide spending of business apps jumped 59% between the first half of 2020 and the first half of 2021, SensorTower reported.[4]

Zoom racked up 52 million downloads in 2021, making it the most downloaded business app in the United States. Two other collaboration tools – Microsoft Teams and Google Meet – ranked among the top four downloads, according to Apptopia.[5]

Conferencing Mobile Apps Top the Charts

Virtual meeting apps had the most downloads of U.S. business apps in 2021, according to Apptopia. The Gig Economy drove growth of DoorDash Dasher and Uber Driver.[6]



Enterprise Apps Power the Workforce

Mobile B2B apps help automate operations, boost efficiencies and optimize sales, marketing and customer service. Some recent innovations in mobile apps include:

- **Video and audio messaging:** Slack introduced a feature that allows people to record and send short video messages to their colleagues and an audio feature that enables coworkers to hold short informal audio calls. The new features are intended to boost collaboration while reducing the number of formal meetings in a hybrid work environment.[7]
- **Enhanced multi-app integration:** Workforce productivity tool makers extended integrations with third-party mobile apps to improve the user experience. For example, Box recently integrated with Microsoft Teams to enable users to automatically save edits to Box.[8]
- **Artificial Intelligence (AI):** Adobe recently added Liquid Mode AI technology to Adobe Acrobat. The app reformats files so they are readable on smartphones and other small screens.[9]

Security and Privacy Risks Abound

As reliance on mobile apps grows, cybercriminals actively target mobile apps to exploit security and privacy vulnerabilities. Loss of sensitive data puts entire companies and their customers and employees at risk.

A NowSecure benchmark review of 1,223 popular high-tech mobile apps found that 80% have privacy risks. 86% used dangerous permissions, 42% used weak cryptography and 21% leaked personally identifiable information.[10]

Several enterprise business mobile apps have suffered security and privacy breaches.

Leading enterprise business mobile apps suffered security breaches in recent years.

Consider these recent incidents:

- **Slack** fixed a bug in its Android app that stored users' credentials in plain text, meaning other mobile apps on a device could theoretically gain access to them. Slack said it did not see any unauthorized access but urged users to reset their passwords as a precaution.[11]
- **Samsung** patched security flaws found on its preinstalled mobile apps which could have allowed attackers to steal users' personal data. Samsung said no data was breached, but the flaws could have allowed malicious apps on the device to change settings and steal photos, videos, contacts, call records and messages.[12]
- **Microsoft** fixed an unsecured database that exposed Microsoft Bing app search records including users' location, search terms in clear text, type of device and a partial list of the websites the users visited from the search results. Microsoft said no personal information was exposed.[13]

Enterprise software vendors can better protect their B2B customers by adopting best practices for security and privacy by design and testing for issues throughout the software development lifecycle.

Automated mobile application security testing tools empower AppDev, AppSec and DevSecOps teams to test apps on demand or perform integrated security testing directly in the development pipeline. NowSecure Platform analyzes risks of Android and iOS mobile apps so organizations can quickly address them and ultimately deliver high-quality secure mobile apps faster.

80%
of high-tech mobile apps have privacy risks.[14]

About NowSecure

NowSecure offers a comprehensive suite of automated mobile app security and privacy testing solutions, penetration testing and training services to reduce risk. Trusted by many of the world's most demanding organizations, NowSecure protects millions of app users across banking, insurance, high tech, retail, healthcare and government. The company is SOC certified and was named a mobile security testing leader by IDC and a DevSecOps transformational leader by Gartner.

Visit www.nowsecure.com to discover strategies for strengthening the security of enterprise business mobile apps without slowing down developers.

NowSecure™
MOBILE APP TRENDS

SOURCES

[1] App Annie, "State of Mobile 2022," January 2022
[2] Gallup, "Remote Work Persisting and Trending Permanent," Oct. 13, 2021
[3] App Annie, "Working Well: Downloads of Business & Productivity Apps Hit 7.1 Billion in 2020 – Up 35% in a Year," March 4, 2021
[4] SensorTower, "Global App Spending Approached $65 Billion in the First Half of 2021," June 28, 2021
[5] Apptopia, "Worldwide and U.S. Download Leaders 2021," Dec. 27, 2021
[6] Apptopia, "Worldwide and U.S. Download Leaders 2021," Dec. 27, 2021
[7] The Verge, "Slack Launches Clips, Video Messages That Help You Avoid Meetings," Sept. 21, 2021
[8] ZDNET, "Box Adds New Integrations with Microsoft, Slack, Steps Up Security," Oct. 6, 2021
[9] CNET, "Adobe Peps Up PDF on Smartphones with AI-powered Liquid Reformatting," Sept. 2020
[10] NowSecure, "Mobile RiskTracker," Jan. 13, 2022
[11] The Verge, "PSA: If You Use Slack on Android, You Might Want to Update Your Password," Feb. 11, 2021
[12] TechCrunch, "Security flaws Found in Samsung's Stock Mobile Apps," June 10, 2021
[13] Threatpost, "Unsecured Microsoft Bing Server Leaks Search Queries, Location Data," Sept. 2020
[14] NowSecure, "Mobile RiskTracker," Jan. 13, 2022

NowSecure™