Remote Workers Drive Enterprise Mobile App Adoption

Security vulnerabilities in B2B apps put business, employee and customer data at risk.

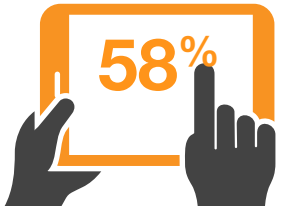
NowSecure™ MOBILE APP TRENDS

Use of mobile business-to-business apps skyrocketed in recent years and the pandemic only intensified demand as much of the workforce set up shop at home. 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 during the pandemic, 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.



of users access mobile productivity apps at least once per day[2]

Employees have proven that they can remain productive while working from home so most business leaders support flexible work schedules and remote work even after the pandemic ends. In fact, 87% of U.S. businesses expect employees to continue to work from home three or more days a week when mandatory closures are lifted and 90% of enterprises believe more of their workers will telecommute in the future.[1]

Global weekly downloads of business apps from the Apple® App Store® and the Google Play™ store skyrocketed from 33.3 million in October 2019 to 80 million in April 2020.[3] In that same time period, weekly downloads of video conferencing apps soared from 4.8 million to 52.1 million, according to App Annie.[4]

Zoom racked up 66 million downloads in Q2 and Q3 2020 to become the most downloaded app in the United States during that period, according to Sensor Tower.[5] Two other collaboration apps, Google Meet and Microsoft Teams, also ranked among the top 15 downloads worldwide in Q3.

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:

- **Redesigned apps**: Slack redesigned its mobile app to ease collaboration via features such as a navigation bar for quickly accessing new messages.[6]
- **Enhanced multi-app integration**: Workforce productivity tool makers extended integrations with third-party apps to improve the user experience. Cisco recently integrated Webex Teams with Box, allowing users to view Box content within a Webex Teams space.[7]
- **Artificial Intelligence**: Adobe recently added Liquid Mode AI technology to Adobe Acrobat. The app reformats files so they are readable on smartphones and other small screens.[8]

Collaboration Apps Top the Charts

The chart below shows Q3 2020 U.S. downloads of business productivity apps. Zoom amassed 25 million U.S. downloads in Q3 2020, while Google Meet and Microsoft Teams were also incredibly popular.[5]

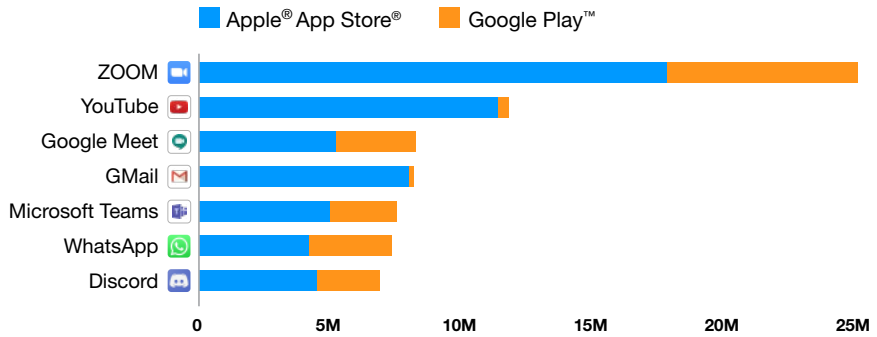


Image By: gpointstudio

NowSecure™
MOBILE APP TRENDS

Security and Privacy Risks Abound

As reliance on mobile apps grows, cybercriminals actively target apps to exploit weaknesses such as code flaws, insecure data transmission and poor or missing encryption. Loss of sensitive data puts entire companies and their customers and employees at risk.

A NowSecure review of popular Android and iOS business productivity apps found that 50% of

Leading enterprise business mobile apps suffered security breaches in 2020.

the top business productivity apps leak sensitive data. And several enterprise business mobile apps have suffered security breaches in 2020. Consider these recent incidents:

- **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.[9]

50%
of business productivity apps leak sensitive data

- **Twitter** fixed a Twitter for Android vulnerability that could allow an attacker to access private Twitter data including direct messages. The issue affected only 4% of Android users who used Android 8 or 9 and lacked a specific security patch.[10]

- **Samsung** patched four critical security flaws in its Find My Mobile app that enabled hackers to factory reset Galaxy S7, S8 and S9 phones, resulting in complete data loss. In addition, the vulnerabilities enabled attackers to track users' real-time locations, monitor phone calls and messages, and lock users out of their phones.[11]

- **Cisco Webex** fixed a vulnerability in Cisco Webex that allowed unauthorized users who have meeting ID numbers to attend password-protected meetings on the Webex mobile app without furnishing the password.[12]

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

About NowSecure

NowSecure offers a comprehensive suite of automated mobile appsec 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, government, et al. The company is SOC2 certified and was recently named a mobile security testing leader by IDC, a DevSecOps transformational leader by Gartner, and a Deloitte Technology Fast 500 member.

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

SOURCES

1 IDC, "Mobile Workers Will Be 60% of the Total U.S. Workforce by 2024, According to IDC," September 2020

2 Criteo, "App User Behavior in 2020, United States," April 2020

3 Business of Apps, "Downloads of Business and Video Conferencing Apps Skyrockets Due to Covid-19 Lockdowns," May 2020

4 App Annie, "Video Conferencing Apps Surge from Coronavirus Impact," March 2020

5 Sensor Tower, "Q3 2020 Store Intelligence Data Digest," October 2020

6 Slack, "A Simpler, More Organized Slack on Your Phone," May 2020

7 Box, "Enhance Remote Teamwork with Box and Cisco Webex Teams," June 2020

8 CNET, "Adobe Peps Up PDF on Smartphones with AI-powered Liquid Reformatting," September 2020

9 Threatpost, "Unsecured Microsoft Bing Server Leaks Search Queries, Location Data," September 2020

10 Twitter, "Twitter for Android Security Vulnerability," August 2020

11 Threatpost, "Samsung Quietly Fixes Critical Galaxy Flaws Allowing Spying, Data Wiping," August 2020

12 Cisco, "Cisco Webex Meetings Suite and Cisco Webex Meetings Online Unauthenticated Meeting Join Vulnerability," January 2020

Image By: twenty20photos