appdome

MOBILE APPS FOR THE DIGITAL WORKPLACE

TABLE OF CONTENTS

Executive Summary

A COMPLETELY CHANGED MOBILE LANDSCAPE IN A ZERO TRUST WORLD

IT and Security professionals agree that enterprises today operate in a "Zero Trust" world. One that requires that every node connected to the networks is fully secured before it can be trusted with access to corporate or sensitive information. Every node, including workplace apps installed on untrusted devices, connecting from untrusted locations.

On top of that, the COVID-19 pandemic has fundamentally changed how work gets done and ushered in the rise of the remote workforce. Companies responded to this "new normal" by strategically allowing employees to permanently work-at-home. In turn, employees have embraced mobile apps to collaborate with each other and remain productive. In fact, in mere months, this embrace has advanced mobile usage by 2 to 3 years — accelerating our transition to a mobile-first world.

CISOs, as well as IT, Security and DevSecOps teams **have** to become agile and adjust rapidly to deliver consistently secured mobile apps that can easily installed on any device by their completely remote workforce. And Appdome's *Annual State of Mobile App Security Review*, showed that most apps lack one of several key security elements.

This Guide shares the top 5 trends driving the change to a mobile-first world and lays out the solutions Enterprises can implement to securely welcome the mobile (r)evolution in the digital workplace, instantly without code or coding.

Industry Backdrop

COVID-19 CHANGED THE WAY WE LIVE AND WORK - FOREVER

COVID-19 changed the way we work, forever. In the span of a few weeks, hundreds of millions of workers were sent home to 'shelter in place' and have been working from home ever since. And for now, it seems, work-at-home is here to stay, with the exception for "frontline" and "essential" workers. In fact, enterprises, large and small, have announced that employees should continue their work from home, well into 2021. For many, work-at-home is the norm. This change will have a lasting impact on the way we think of and perform our work for years to come.

So far in 2020, working from home underwent an exponential evolution in the wake of COVID-19. From a technology perspective, the working world went mobile and digital overnight and the virtual enterprise was born. For example, an organization with 5000 employees and 5 remote offices suddenly went to 5000 employees with many more remote devices accessing corporate data. Today's work from home employee taps into a fully digital existence, powered largely by mobile and online platforms and apps, to complete work. In this existence, mobile apps are quickly becoming the centerpiece for the modern remote workforce. And similarly, mobile apps allow frontline and essential workers to remain productive and abide by social distancing requirements. The research firm AppAnnie believes COVID-19 has accelerated the trend towards a mobile economy by 2 to 3 years. Now, everything from communication and collaboration, to CRM, to benefit and expense management, to social enterprise, business intelligence (BI), workflows, training and more are dominated by the mobile experience. In 2020, mobile app use is through the roof in just about any way it can be measured: downloads, subscribers, 'authorized' and 'shadow' user accounts, time and money spent in apps, etc. Apps are simply 'how work gets done.' And for the millenial generation, "enterprise apps" should behave like the consumer apps they use every day.

Cybercriminals understand these dynamics and have responded by increasingly shifting attack priorities to mobile apps designed for work. Traditionally apps for work are (1) not secure, (2) required to be downloaded by the employee, and (3) store, process or grant access to data that can be monetized. As was demonstrated with the release of EventBot malware earlier this year, apps for work can, albeit unwittingly, easily become trojans for malware that prey on unsuspecting corporate users. Even without the personal risk to corporate mobile users, the amount of confidential business information (and therefore valuable data) on mobile apps is increasing in relative and absolute terms. Corporate access and user credentials, confidential documents, CRM data about customers, PII, host URLs, certificates pinned in apps, new product and technology plans, and simply how the businesses functions are all resident inside mobile apps. As shown by the highly disruptive and costly advent of 'zoom bombing,' hackers don't wait and can strike quickly. They are increasingly organized, financially motivated, and heavily automated.

Enterprise IT and Security departments are facing an insatiable demand and critical need for more mobile apps, and overwhelming challenge to secure these apps for use by mobile employees. Inside the enterprise, developers are rapidly building and delivering apps for functionality first, at the expense of security. Outside, adversaries combine forces to hack mobile apps at scale. And both developers and hackers rely heavily on automation to achieve their goals (and in many cases, use the same tools). Enterprise IT and Security departments simply cannot stay ahead relying exclusively on the security tools, like MDM and UEM alone. They must adopt more agile and flexible layered models to protect apps and users. It's under that backdrop that we present 6 Key Trends in the latest edition of the "Mobile Apps for the Digital Workplace" guide.

Trend #1
THE MOBILE WORK-AT-HOME WORKFORCE

When COVID-19 struck, the shift to work-at-home home was unprecedented as virtually every company on the planet was forced to abruptly adopt this new and unfamiliar paradigm, just to keep the business afloat.

Many of the changes will be permanent, as enterprises large and small need to balance their employee's needs and safety, along with corporate objectives against the backdrop of public safety and increased social responsibility. This places a premium on flexibility and efficiency. A recent Gartner poll showed that 48% of employees will likely work remotely at least part of the time after COVID-19 versus 30% before the pandemic. In fact, in mid 2020, several major corporations including Google, Facebook, Twitter, Square, Slack and others announced that they extended their work-at-home policies into mid 2021 and will offer permanent remote working options for substantial portions of their workforce. And that's ok with the workforce. Forbes reported that 59% of people currently working from home due to COVID-19 are fine with it and plan to continue as long as they can.

Work-at-home post COVID-19 is uniquely different from other remote work use cases. Traditionally, remote work was a temporary or limited purpose consideration. By contrast COVID-19 work-at-home agility requires the entire corporate workforce to:

(1) Remain remote yet connected and productive for long periods of time;
(2) Use multiple digital devices and apps simultaneously to complete work, and
(3) Be capable of rapidly shifting context between work and family.

Traditional VPN access and mobile device management technologies are not flexible enough to accommodate these shifts, especially without making significant tradeoffs on functionality and usability – neither of which can really be sacrificed – especially now. IT and security teams will need to adapt to this massive shift towards work-at-home and offer more apps that offer a consumer-like experience. They need to plan for more agile and lightweight security models to enable a truly mobile workforce at scale.

Trend #2
BUSINESS CONTINUITY AND THE MOBILE APP

The demographics of the global workforce have shifted dramatically as millennials move into leadership positions and the younger Gen Z are entering the workforce in significant numbers.

These highly adaptable, privacy conscious and mobile native professionals are helping to usher in a new shift to user friendly, consumer-like, mobile paradigms at work. Millennials consider mobile apps in the workplace a key requirement to get their jobs done and job satisfaction. And frontline and essential workers flocked to mobile apps to get work done and abide by social distancing requirements. Mobile apps have allowed organizations to ensure business continuity, become more efficient and maintain a level of profitability and prevent loss in productivity. That now, more than ever, is required to keep our economy going.   And most of this was achieved using publicly available apps, downloaded to employee-owned devices.

This put Enterprise IT and Security organizations in a tough spot. Traditional mobile device management solutions, including Unified Endpoint Management (UEM) and Mobile Application Management (MAM) with enrolled devices, were not meant for this. Add to this that these systems can overreach in terms of user privacy, and it becomes clear why enterprise IT and security teams are implementing lighter weight security models like MAM without enrolled devices and zero-management mobile application security to support their work-at-home workforce.
In COVID-19, the trend towards true mobile application management has accelerated as more organizations race to give frontline are essential workers the tools they need and meet the consumer like demands of the Millennial and Gen Z workforce.

Mobile apps can be targeted to specific users or use cases, customized or developed to serve corporate specific workflows. As a result, the number of mobile apps to serve the digital workforce is on the rise.

Organizations and app developers are responding to this need by releasing more apps to support targeted workflows across the organization. They understand that their users will need to be able to install these apps to any device, company managed and BYOD. This is leading many enterprise organizations to develop mobile apps in house, secure those apps without an MDM, UEM or MAM and publish them to the public App Store and Google Play, to meet the needs of their workforce.

Trend #3

BUSINESS AGILITY AND APP-CENTRIC SECURITY MODEL

The shift to mobile apps in the enterprise - which was already well underway - is now in overdrive. Mobile apps are being used for increasingly more business-critical functions and transactions which generate highly valuable data. On top of this, enterprises are developing new apps that usher in an expanding mobile app estate across a more diverse set of use cases such as: sales process, employee enablement, operations, supply chain management, calendaring and collaboration. Finally, apps are helping companies to get ready for the return to the office scenario. when they can leverage mobile apps for contactless activities such as reserving resources, time and attendance tracking, access to building and emergency communications. And to avoid the expense and complexity inherent with MDM and UEM, companies are looking for ways to bypass their traditional enterprise mobility methods, when rolling out apps company wide.

In fact, a 2019 Appdome study found that 1 in 3 of the Fortune 1000 are building internally facing mobile apps designed especially for the workplace and publishing these apps on public app stores (Google Play and Apple's Appstore).

The coronavirus crisis has only accelerated this. Since the beginning of the pandemic, we've seen an 80% increase in the download of business apps. COVID-19 has dramatically reshaped the importance of mobile apps, and they are now the primary channel to conduct business, as employees who work-at-home reach for mobile apps to perform the same functions they would perform in the office. In fact, the mobile app research firm AppAnnie believes the pandemic has advanced mobile usage by 2 to 3 years — accelerating our transition to a mobile-first world.

Speed is key to remain agile in this dramatically changing environment. Enterprise IT needs to remain vigil and has to adopt light weight security models that can address the changing needs of the digital workforce quickly. Companies that are not ready for this mobile-first world, will suffer the consequences, ranging from being left behind commercially to becoming a prime target for mobile-based cyberattacks.

1 in 3

FORTUNE 1000 Companies Publishing Internal Workplace Apps to App Stores

31%

214 apps

Event and Meeting Apps

Mobile apps built for customer conference engagement used to be the only internally facing mobile apps on the app store. Now, they barely lead the pack. These apps facilitate corporate and customer meeting and conferences, provide real time feed, conference schedules and more.

21%

146 apps

Sales Process/Enablement Apps

Enterprise organizations are building more mobile apps than ever to facilitate sales, quote generation, product demonstration and product selection. These function specific apps are used by internal sales people to speed sales and improve the buying process for everyone.

20%

139 apps

Operational Process Apps

Mobile apps that improve the way organizations work, collect information, process claims, confirm values on remote systems, manage payloads and inventory, enroll clients, project and workflows management and more have emerged as a leading category in the enterprise mobile app landscape. These special purpose apps help mobile workers increase productivity and efficiency in every aspect of work.

15%

104 apps

Workplace safety / training Apps

It shouldn't be surprising that enterprises have started to build mobile apps for HR, training and workplace safety. What should be surprising is that these apps cover more than mere text or video based training programs, payroll and standard healthcare benefit information. These apps include finding mentors, employee reward programs and perks, employee scheduling and time tracking, training games, work permitting, virtual reality training and more.

12%

83 apps

Team collaboration Apps

Enterprise built team collaboration apps are definitely on the rise as organizations race to leverage the power of mobile to foster better peer review and support, teamwork and overall collaboration.

1%

7 apps

Partner-SPECIFIC Apps

These apps are semi-public usually meant for partners of the enterprise developer. These apps allow the partner to register deals, confirm royalties, track shipments, get company or product news, and similar activities.

Organizations are finding that legacy device management and vendor specific solutions cannot meet the demands of a mobile-first organization. (data is from 2019, pre-pandemic)

Trend #4
MOBILE THREATS TO THE ENTERPRISE

As more users turn to mobile apps, there is an assumption and expectation that the apps are safe, and the environments in which they connect to are secure – especially in a work environment. The data shows otherwise. Mobile threats are on the rise in every category, from fake apps, to data theft to general and purpose-built mobile malware to tampering.

Mobile threats are not only growing in volume, they are increasingly more diverse and sophisticated – often using different methods of compromise within the same attack, across longer time periods. Mobile attacks are also becoming increasingly more automated, like we saw with the recent emergence of EventBot and other malware. According to Check Point's annual Cyber Security Report, malicious botnets and other mobile malware are up fifty percent. And more than 28% of all enterprises were affected by malicious mobile botnet attacks, where the attacks were executed remotely by command and control botnet networks.

Mobile Ransomware is emerging and a next mobile threat. In fact, another Check Point study reports a sharp rise in the spread of mobile ransomware. Ransomware attacks are almost always related to previous attacks where a cybercriminal harvested information from an app through static or dynamic analysis or by intercepting a mobile user's session to sniff the data in real time (using a Man-in-the-Middle attack for example). All of which are relatively easy to do for mobile apps. And even junior hackers know that valuable data is often stored unencrypted as plain-text strings inside app preferences, resource files, or other common storage areas inside a mobile app).

If a developer or an Enterprise IT team didn't take specific measures to encrypt or obfuscate the data inside their app, then all of this info sits in the app in human readable format and as such is vulnerable to theft.

And most apps are an under-defended access point to corporate data. In fact, Appdome's *Annual State of Mobile App Security Review* showed that:

- 95% are vulnerable to OWASP mobile top 10 risks;
- 95% lack encryption;
- 90% lack application shielding;
- 80% lack code obfuscation;
- 80% lack mobile privacy and data loss prevention;
- 75% lack man-in-the-Middle protection;
- 70% lack Jailbreak or Root prevention.

Trend#5
INCREASED CONSUMERIZATION OF WORK

Even before COVID-19, Enterprise Security, IT and DevSecOps teams were struggling to deliver remote mobile experiences that are seamless, easy, useful and secure. Legacy mobile management, access and security technologies (like UEM, MDM, static VPNs) are not flexible enough to meet the dynamic needs of the mobile-first organization; these systems impose one or more of the following painful trade-offs:

- **Device Control** – BYOD is the now the dominant use-case in the enterprise. Controlling user-owned devices is problematic for many reasons, including privacy concerns, spiraling licensing costs, and a giant operational burden in provisioning, managing, updating and supporting.
- **Traditional VPNs Are Inflexible** - They impose operational burdens on IT and end users, including introducing authentication friction and a cumbersome user experience. On top of this, most mobile apps not 'VPN-aware', putting additional configuration management burdens on IT.
- **Lack of 3rd Party App Coverage** – Enterprises use a lot of 3rd party apps, which they don't control or own. More often than not, these apps either do not meet the unique security requirements of the enterprise. This forces the enterprise compromise on security, functionality, or user experience/mobile privacy – none of which are good options. It is good to see that ISVs and app makers are starting to take greater responsibility for securing their apps and delivering MAM compatible versions of their apps.
- **Mobile App Security Deficiencies** – None of the above technologies provide comprehensive mobile app security. They are mainly designed to manage mobile devices or secure the transport via encrypted tunnel, not to secure the app or the data stored in the app. The majority of mobile hacks focus on exploiting security deficiencies in the mobile app itself (unencrypted data at rest or in memory, partially or non-obfuscated code, user data stored in clear text in app preferences, lack of MFA, weak certificate chains or reliance on public CAs, lack of tamper-protection, lack of reverse engineering protection, etc).

The technologies enterprises use to secure mobile apps were built for a 'device-centric' security model, where there is a well-defined perimeter. Today's reality for mobile apps is different. Enterprises cannot control devices, the perimeter has disappeared, and apps operate in a hostile, Zero-Trust environment. COVID-19 has forced work patterns that are dynamic and fluid, which means that the security and management model must also be dynamic, adaptable and fluid. In other words, enterprises need to shift from a device-centric security model to an app-centric security model.

They need to focus on securing the app and data, not the device.

Solutions
APPDOME MAKES BUILDING APPS FOR THE DIGITAL WORKPLACE EASY

Enterprises face a huge challenge in securing the apps their employees need and also making those apps compatible with their enterprise environments (including conditional access, authentication and access policies, SSO systems, mobility management, etc). All this is happening all at a time when their employees have moved to mobile en-masse, both due to COVID-19 and their mobile native workforce.

Most Enterprise network infrastructure is ill equipped to secure or manage the mobile apps that users are demanding and bringing into the workplace to remain productive in their jobs.

A new way is needed. And that new way is Appdome.

APPDOME IS A NO-CODE MOBILE SECURITY AND DEVELOPMENT PLATFORM

Appdome's no-code mobile security and development platform enables organizations to automate mobile app security as part of the app lifecycle. Developers, SecOps or DevSecOps use Appdome to build app security, threat defense, authentication, identity, and app management functionality directly into any Android and iOS apps – no matter how the app was built. This enables organizations to meet the demands of the mobile-first workforce for any mobile app (internally developed or 3rd party) without changing source code or degrading the user experience. With Appdome, you can overcome constraints to make your existing authentication or management solutions work with any app.

ZERO MANAGEMENT SECURITY

When the pandemic forced the world's largest businesses to figure out how enable tens of thousands of employees to do their jobs remotely, many came to the Appdome self-service platform to build zero management security in enterprise apps. Using Appdome Zero Management Security, developers, CISOs and SecOps teams can instantly build secure versions of existing mobile apps that work with the Enterprise's existing authentication (SSO) and secure remote access (VPN) solutions - all within minutes, without any coding

Using Appdome enterprises can deliver their choice of comprehensive app security without the overhead of a separate VPN proxy or identity service. And most importantly, without forcing device enrollment or installing management profiles. With Appdome, employees don't need to sacrifice privacy or lose control over their personal devices, and the enterprise gets all the mobile app security it needs - all with less work.

ENTERPRISE MOBILITY CONTROL

Implement any mobile management solution in any app - instantly with no coding. Achieve instant compatibility between any mobile app and your chosen enterprise mobility vendor, including VMWare Workspace ONE, Microsoft Intune, IBM MaaS360, MobileIron, Blackberry and more. Appdome easily overcomes the limits of app wrapping or manually coding the SDK and bridges the gaps that exist in UEM, EMM and MAM SDKs, including support for modern frameworks, non-native applications, WKwebviews and more! And most importantly, no source code access is required. This makes it easy for Enterprise to add any app (internally developed or from a 3rd party app maker) to their mobile management solution. Moreover, with Appdome, Enterprises are not locked into any solution and have the flexibility to easily switch between management solutions. All it takes is 5 minutes to complete a new build on Appdome.

ALL-IN-ONE MOBILE SSO

Appdome's all-in-one mobile SSO solution delivers complete enterprise authentication, cross-app identity, and cloud identity services to Android and iOS apps. Using Appdome, Enterprise build and secure mobile apps that work with any identity provider (including Microsoft, Okta and others) using any authentication standard. With Appdome, there's no prerequisite to build SAML, OpenID Connect, OAuth or any other standard into the app manually. Appdome's platform handles that for you, so you don't need to worry about it.

SECURE PROGRESSIVE WEB APPS (PWA)

Don't have a mobile app yet? No problem, go from zero to mobile-first in seconds. Using Appdome you can build brand new progressive web apps (PWAs) that deliver native functionality and user experiences that are secure from the start. Appdome converts any website, web app, or cloud app into a secure progressive web app (PWA) that runs on any iOS or Android device - all without coding. Add more security features, SSO, or mobile management services as your needs evolve. Eliminate reliance on 3rd party app vendors to deliver the features you need. Build your own versions of apps to access any gated resources

Conclusion

Organizations are also placing a premium on the Appdome platform's full mobile app lifecycle feature set, including digital workflows, teams, templates, approval, and audit trails. These features empower functional groups - from development, to line-of-business, including IT, Security, Mobility, SecOps and DevOps - to collaborate and work together to create, improve and release mobile apps to the workforce.

With Appdome, organizations take control of the mobile app lifecycle to create, secure, enhance and deliver mobile apps quickly and easily, on demand – all without writing a single line of code.

SECURE MOBILE APPS FAST!
fusion.appdome.com

appdome

3 Twin Dolphin Drive Suite 375
Redwood City, CA 94065
+1.650.567.6100
+1.844.360.FUSE (3873)
info@appdome.com
www.appdome.com