appthority

ENTERPRISE MOBILE THREAT PROTECTION

5 SIGNS YOU NEED A MOBILE SECURITY GAME PLAN

EBOOK

INTRODUCTION

> Mobile devices are one of the weakest links in corporate security. Executives are wrestling with managing a proliferation of devices, protecting data, securing networks, and training employees to take security seriously.[1]

In our view, all companies need mobile threat protection. But, if you're wondering whether this is the right time for your organization, we've compiled a list of five signs that you might be at risk.

If any of these describe your company, you need a mobile security game plan.

45% of tech executives and employees in a recent survey[2] identified mobile devices as their company's weakest security link.

As mobile devices and apps are used in enterprise environments more often and more extensively, the potential for mobile attacks and the risks to both corporate and personal data continue to increase. Privacy is also at risk as employees are targeted as a means to access corporate information.

1. https://hbr.org/2016/09/your-biggest-cybersecurity-weakness-is-your-phone
2. https://hbr.org/2016/09/your-biggest-cybersecurity-weakness-is-your-phone

1 BYOD AND BYOA ARE EXPLODING IN YOUR ENTERPRISE

A recent poll[3] showed 72% of companies now permitting or planning to permit BYOD (Bring Your Own Device) programs. As employee owned mobile devices proliferate along with corporate owned devices, so too do the apps employees bring into your enterprise environment. As BYOA (Bring Your Own Apps) grows, you'll need a game plan and an automated solution to keep up with the growing security risks in your enterprise's dynamic mobile environment.

72% say Incident Response processes are informal, relying on spreadsheets and open-source tools[4]

75% say Incident Response processes can be disrupted if key individuals are unavailable[4]

HALF

Gartner predicts that, by 2017, half of employers will require employees to BYOD for work[5]

3. http://www.techrepublic.com/blog/10-things/10-ways-byod-will-evolve-in-2016/
4. http://resources.idgenterprise.com/original/AST-0170622_How_does_your_security_stack_up.pdf
5. http://www.gartner.com/newsroom/id/2466615

2 MOBILE RISK IS YOUR SECURITY BLIND SPOT

Do you know all the of mobile devices and apps accessing your corporate networks and data? Many apps have privacy invasive behaviors, leak data or even contain malware. And, shadow IT, or employee use of unsanctioned cloud apps via mobile, is on the rise and often hidden. If you can't see what's in your mobile environment, you can't be sure it's safe. Whether you use an EMM or not, you need to increase your visibility into mobile risks by knowing as much as you can about the devices, apps and behaviors that are impacting your enterprise security.

68% Users who say IT is blind to the apps they use[7]

20x Number of cloud apps actually in use vs IT estimates[6]

841 Average number of cloud apps used in the enterprise[8]

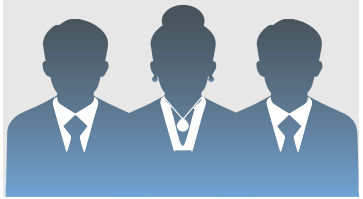
6. http://searchsecurity.techtarget.com/feature/CISOs-face-cloud-GRC-challenges-as-services-take-off
7. http://www.eweek.com/security/why-visibility-into-enterprise-apps-is-still-major-security-issue.html
8. http://searchsecurity.techtarget.com/feature/CISOs-face-cloud-GRC-challenges-as-services-take-off

3 YOUR BOARD IS ASKING

Cyber security is now a board-level concern and, as more and more work is done on mobile devices, mobile security is a top priority for boards looking to keep their enterprises safe and in compliance. If your board isn't yet asking for your plan to protect your increasingly mobile workforce, it will be. It's time to get in the game with a mobile security threat defense solution.

40% say their boards participate in security strategy, budget and policy[9]

2015 saw a double-digit up-tick in board participation of security issues[10]



9. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
10. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

4 YOU FEEL A SECURITY BREACH LOOMING

Whether you've had a digital security breach or know peers who have, you understand that a breach is to be avoided at all cost. If your organization doesn't yet have cybersecurity protocols that cover mobile security risks, prioritize investing in a comprehensive mobile security solution that provides early warnings, real-time alerts, and an automated ability to shut down compromised devices and apps quickly.

25% Organizations who rate their ability to protect apps from a security exploit or compromise as high[11]

38% more security incidents were detected in 2015 than 2014[12]

56% Increase in theft of "hard" intellectual property in 2015[13]

SECURITY BREACH

11. http://www.eweek.com/security/ibm-ponemon-say-app-security-still-lags-in-the-enterprise.html
12. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
13. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

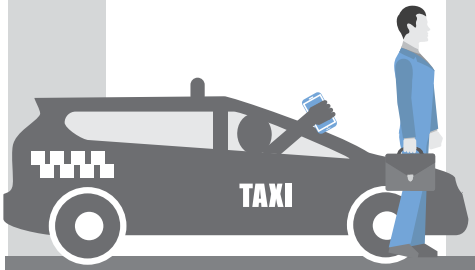
5 COMPLIANCE IS A REQUIREMENT IN YOUR INDUSTRY, SECTOR OR GEOGRAPHY

An expanding number of mobile devices combined with risky app behaviors mean that, at any time, devices and apps can be out of compliance. If you don't know whether your employee devices are in compliance with your privacy, data and security policies, it's time to find out. Avoid increased risk as well as regulatory fines with a mobile security solution that keeps your enterprise in compliance and your data and employees safe.

2/3 Users with underground BYOD[14] who would not disclose loss of their device or a hack.

53% Organizations with at least one non-compliant device. For government orgs the number increases to 61%[15]

50+% Technology and security pros operating without cloud privacy and security compliance measures[16]



14. http://searchcio.techtarget.com/feature/Promiscuous-users-redefine-bounds-of-good-mobile-security
15. http://www.multivu.com/players/English/7754351-mobileiron-security-risk-review/
16. http://searchsecurity.techtarget.com/feature/CISOs-face-cloud-GRC-challenges-as-services-take-off

COMPLETE ENTERPRISE MOBILE THREAT PROTECTION

Appthority helps organizations ensure mobile security in an era of BYOD and IT consumerization. Our automated and scalable mobile threat defense solution proactively detects malicious and risky apps, plays well with major EMMs, and helps employees assist with security via a mobile app that protects their devices and your enterprise. With Appthority, security teams are informed, employees are productive and enterprise data is kept private and secure.

GET STARTED today to stop data loss in its tracks while improving your mobile security.

Appthority Sales
sales@appthority.com
+1 844-APP-RISK
(+1 844-277-7475)

www.appthority.com

appthority