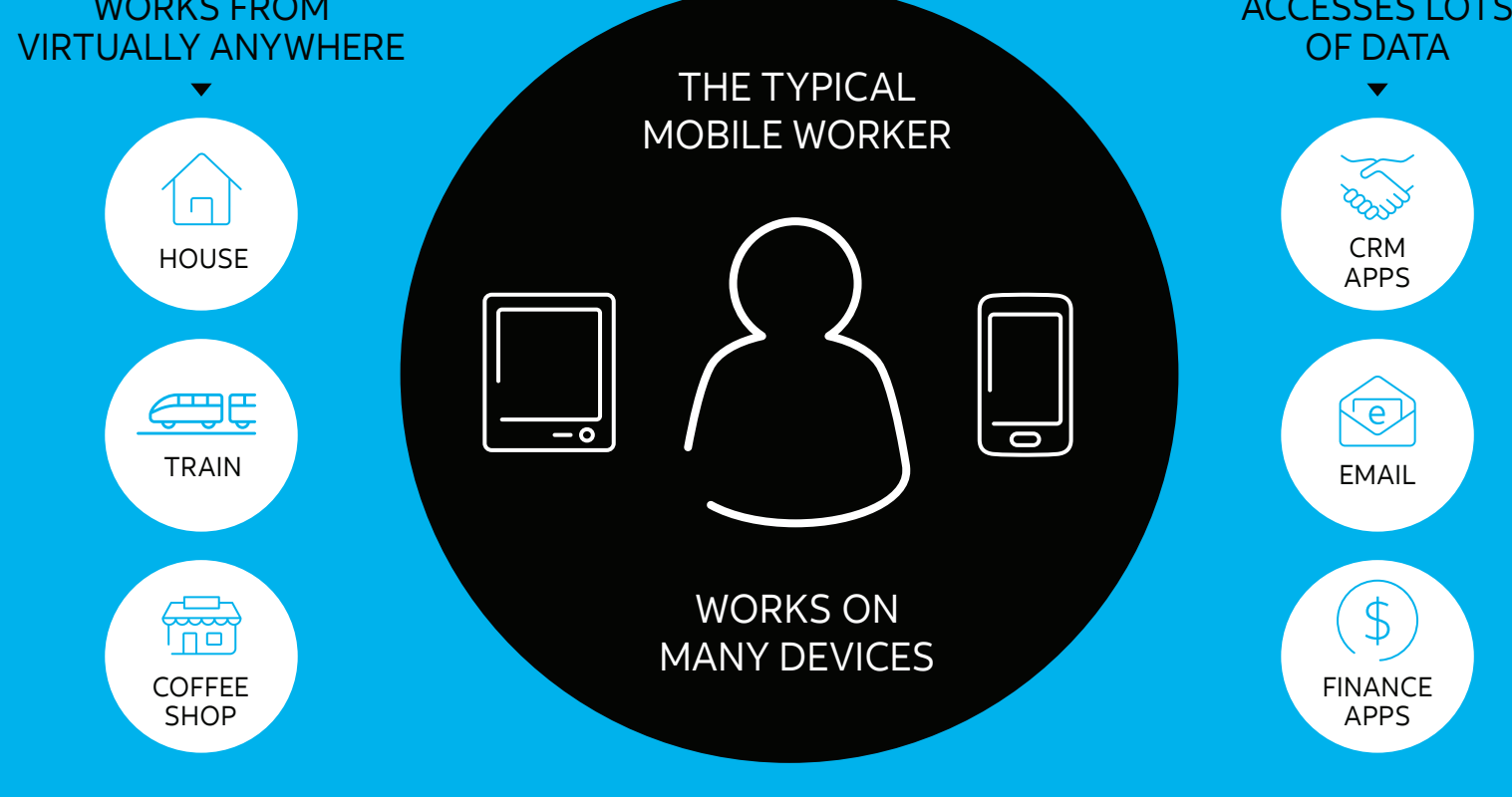
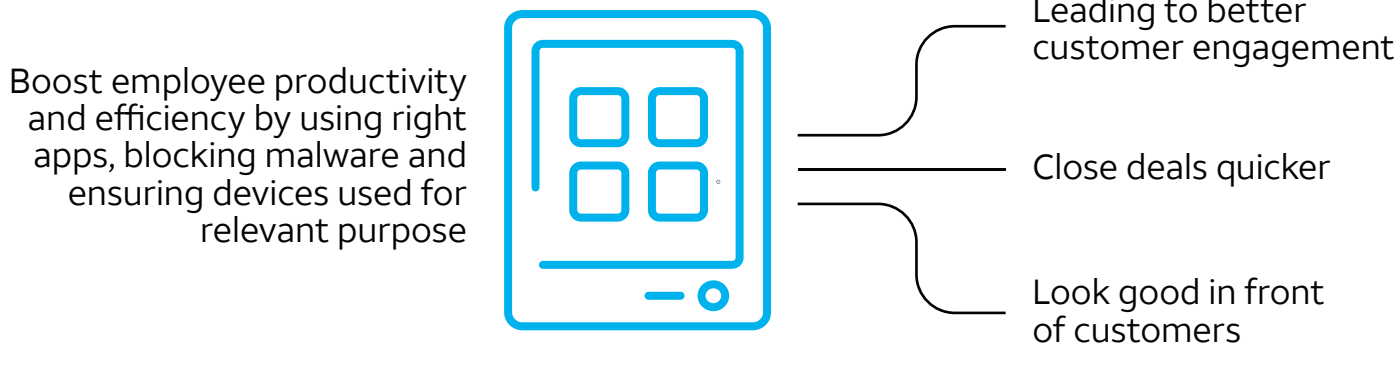


Mobilize your workers



Improve your business performance



AccessMyLAN™ supports employee productivity

- Employee smartphones and tablet devices become productivity tools when connected to AccessMyLAN™
- Effectively manage your mobile data with better control over who has access to what websites and apps.
- Improves employee productivity with data policies that help block time wasting websites and apps.



Mobile data usage is growing¹

- “ 75% lack real-time visibility of mobile usage. Nearly 90% saw overages in the past one year.”
- “ Mobile data grew by 44% in 2016. ”
- “ By 2020, 30% of IT mobile and endpoint resources will be dedicated to enabling frontline workers. ”
- “ In North America, traffic per smartphone is expected to increase from 7.1GB per month at the end of 2017 to 48GB by the end of 2023². ”

Remote workers face security challenges

THERE WAS A 54% INCREASE IN MOBILE MALWARE VARIANTS IN 2017³



“ Nearly 86% of U.S. organizations will increase their spending on security in 2018.⁴ ”

MOBILE MALWARE | PHISHING ATTACKS | BOTS | MALWARE | RANSOMWARE | SPYWARE

AccessMyLAN™ controls



PROTECT company data on the mobile network. AccessMyLAN™ helps block access to the 3.4 billion malicious requests that happen monthly.



DETECT suspicious malicious behavior on the device, app and network. AccessMyLAN™ provides observations and actionable insights.



RESPOND to mobile threats. AccessMyLAN™ helps ensure the business has the means to respond to malicious attacks, and stolen devices.

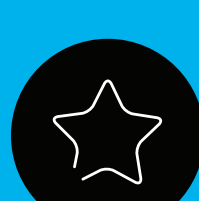
AccessMyLAN™ helps protect, detect and respond to mobile threats

Why should your company care?



FINANCIAL COST

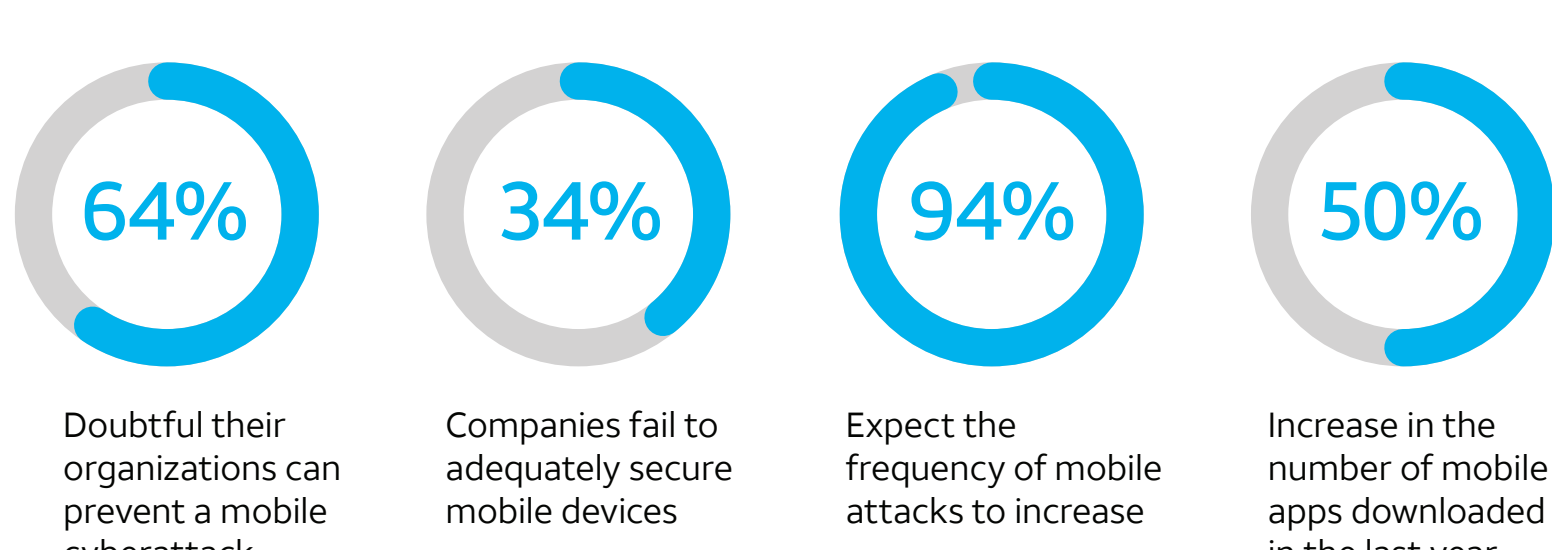
60% of small businesses were unable to sustain operations six months after a cyber breach



REPUTATIONAL RISK

Loss of data not only has potential legal consequences, but also practical damage to reputation (e.g. being "named and shamed")

Security professionals are concerned⁶



Safety checklist

SMART PHONES, TABLETS ARE **EASY TARGETS FOR CYBER-ATTACKS. STAY SAFE!**

- 1. Password protect all devices and data
- 2. Locate misplaced devices remotely
- 3. Lock down all data on lost or stolen devices
- 4. Wipe devices automatically if unrecovered
- 5. Block malicious attacks before they happen
- 6. Comply with regulatory, company & HR policies
- 7. Control app and website usage
- 8. Provide insights on inappropriate usage
- 9. Respond to the observed threats
- 10. Protect traffic on cellular and wi-fi

¹CISCO VNI 2017
²A study conducted by Forrester Consulting on behalf of Cisco Jasper, September 2017
³Ericsson Nov 2017
⁴2018 Symantec ISIR
⁵Thales 2018 Data Threat Report
⁶Dimensional Research | April 2017
 © 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. | 12/53-100418