

Mobile security threats

Intermingling personal and business data and apps on mobile devices



BYOD is on the rise.

More workers are using personal mobile devices for business.



41% use personal smartphones



37% use personal tablets

Blurred lines:

Mixing personal and business-owned devices creates business risk.

Top five mobile threats:



Data loss

from lost, stolen, or decommissioned devices



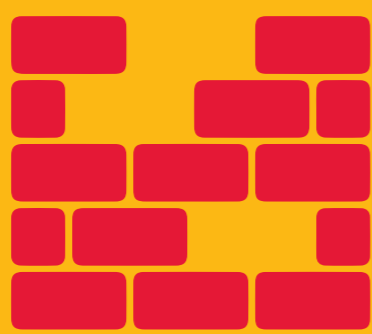
Data hijacking

by mobile malware



Data leaks

from third-party apps



Exposure

from mobile OS and app vulnerabilities



Security risk

from unsecured public Wi-Fi

The Dell secure mobile access solution:

Enable BYOD, while keeping your company protected.



Provide secure mobile access:

- › To corporate data
- › To apps and resources



Prevent rogue access and malware threats:

- › Validate user, mobile app and device integrity
- › Restrict VPN access to allowed mobile apps



Enforce and manage mobile device policy terms:

- › Limit BYOD risks
- › Maintain compliance



Centrally manage access and control:

- › User/group
- › Mobile app and device security posture
- › Resources, web apps, client/server, virtual desktop



Support mobile device platforms:

- › Microsoft Windows
- › Apple iOS, OS X
- › Google Android
- › Amazon Kindle Fire



Deliver safe mobile access and boost productivity with Dell secure mobile access solutions.

[Learn More](#)

Sources:
IDG, CloudSecurityAlliance.org

© 2015 Dell Inc.
ALL RIGHTS RESERVED.
Dell, the Dell logo, and Secure Mobile Access are trademarks of Dell Inc.
Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.
26394 FB

