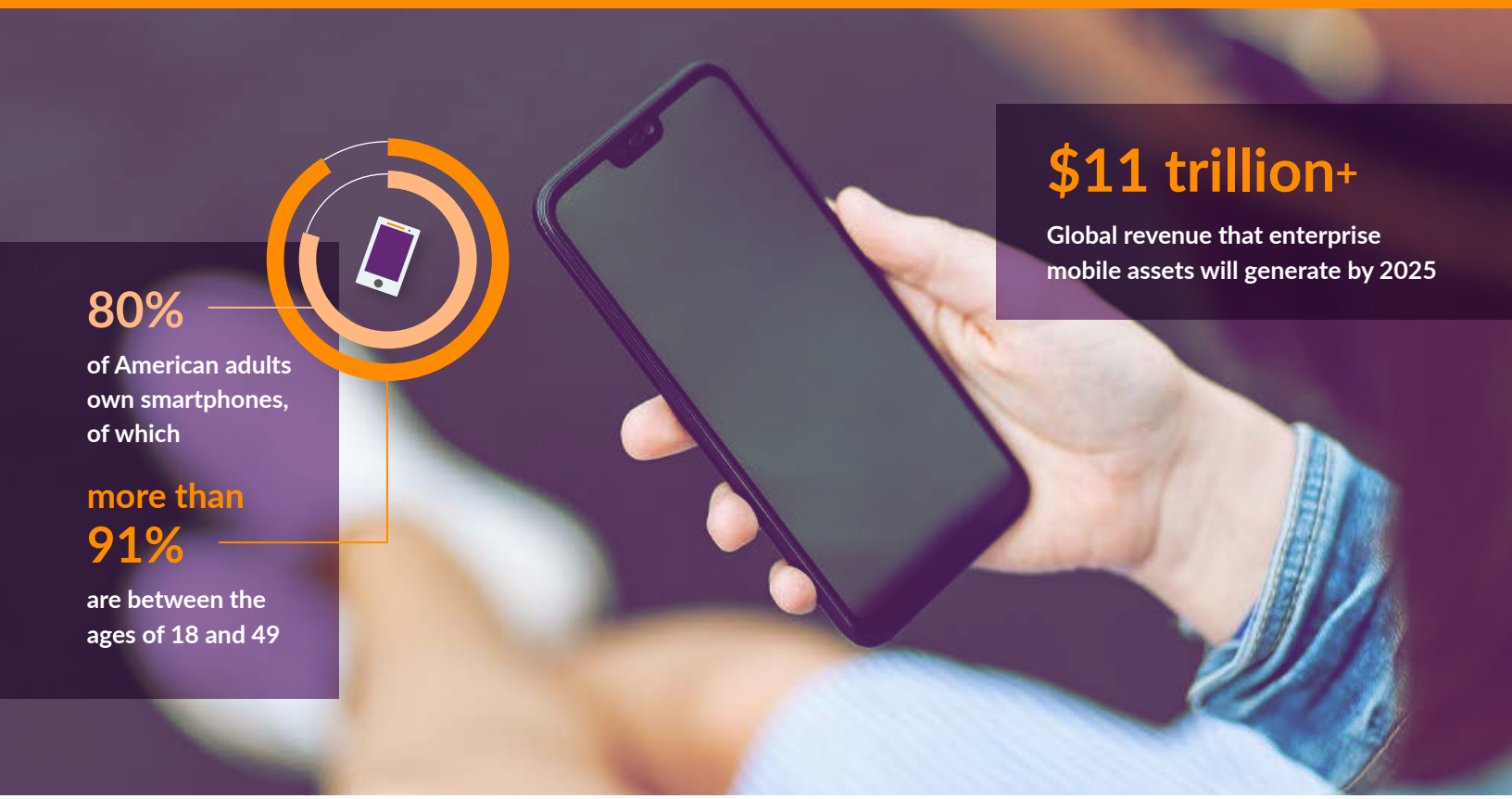
UNDERSTANDING THE IMPORTANCE

OF MOBILE DEVICE MANAGEMENT

Device Management in the Age of IoT

teligistics™



Today, almost 80 percent of American adults own smartphones, including more than 91 percent of those between the ages of 18 and 49.[1] These devices are part of an ever-expanding network of assets called the internet of things, which will include roughly 11 billion fixtures by the conclusion of 2018.[2] Smartphones and other mobile-ready tools have changed how people navigate daily life, offering them access to powerful applications that streamline activities once requiring manual effort.

Of course, these devices have had a similarly transformative effect within the workplace, where they are used to optimize customer service operations, bolster operational visibility and develop fresh business models.[3] These improvements are stimulating significant returns as businesses unlock efficiency and deliver higher-quality products and services. In fact, by 2025, enterprise mobile assets will generate more than $11 trillion in additional annual global revenue.[4]

Firms watching this activity from afar should certainly consider doubling down on IoT workflows centered on the latest mobile devices. However, entities in this position should also examine the complexities that come with mass IoT adoption—most notably, the oversight of numerous connected assets.

Organizations with extensive IoT-powered processes often develop and deploy mobile device management strategies to help information technology teams more easily manage the dozens or perhaps hundreds of assets under their purview. As of 2017, an estimated two-thirds of the businesses with active IoT programs had adopted MDM software solutions to strengthen such protocols.[5] MDM adoption is expected to grow further in the years to come, pushing the global market for this software near the $8 billion mark.[6]

Why are businesses investing so much time and money into comprehensive MDM programs and the requisite technological solutions? They optimize enterprise IoT usage in multiple ways.

64%

of mobile device owners use these assets for work, and

40%

do so without IT oversight

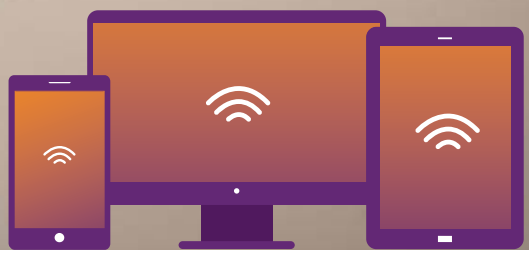
RIGHT-SIZING MOBILE WORKFLOWS

The average consumer owns more than three internet-enabled mobile devices.[7] Approximately 64 percent of these individuals use such assets for work purposes, including the 40 percent who do so without IT oversight.[8] This excess of connected devices drastically complicates the MDM equation, forcing organizations to take responsibility for numerous assets, along with sensitive enterprise data contained on what are effectively shadow IT fixtures.

Effective MDM strategies with tried-and-true software solutions at their centers can help firms cut through the mobile clutter and cultivate right-sized IoT networks that are easily monitored. This reduces the burden on the IT department and paves the way for increased cost savings and stronger data security.

the average consumer

owns more than 3 internet-enabled mobile devices.

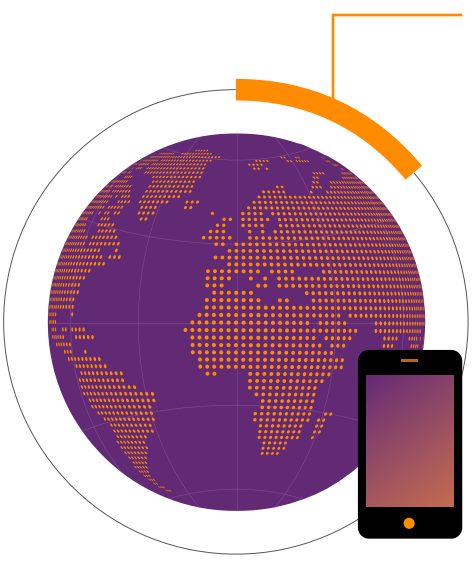


BOLSTERING ENTERPRISE DATA SECURITY

Mobile data security is an increasingly serious concern for organizations navigating the IoT age. In fact, an estimated 64 percent of enterprises believe mobile security threats have increased.[9] Additionally, 85 percent believe they face moderate risk linked to the presence of smartphones and other on-the-go company devices.[10] Unfortunately, this fear is founded in reality.

Digital strikes conducted against mobile devices running the Android operating system grew by 40 percent in 2017.[11] For context, more than 85 percent of smartphone users worldwide now run Google's flagship OS.[12] Even individuals with Apple devices running iOS—roughly 14 percent of all smartphone users globally—are encountering new threats capable of compromising their systems, something once considered highly unlikely.[13]

Of course, these external dangers represent only half of the data security equation. Employees often create problems for themselves by misusing or losing devices. In fact, misplaced assets were linked to approximately 14 percent of all data breaches recorded in 2017.[14] As more IoT devices enter the workplace, the likelihood of device loss grows.



14%

of smartphone users globally run Apple iOS

Despite these developments, a significant number of businesses have not taken action to protect their mobile networks. A mere 14 percent of companies have adopted key IoT data security best practices such as changing default passwords, leveraging encryption services, restricting system access and conducting regular network tests.[15] Even worse, only one-quarter of internal IT teams have control over the proprietary information contained within employee mobile assets.[16] Sadly, 32 percent of organizations have knowingly sacrificed IoT protections in an effort to boost performance.[17]

This state of affairs is unacceptable, something enterprises staring down advanced new threats are beginning to realize. In fact, companies worldwide are on track to spend around $176 million on mobile data security technology in 2018.[18] What kinds of solutions are these firms investing in?

MDM platforms have become common targets, as they provide the data-driven infrastructure needed to properly track smartphones and other vulnerable mobile fixtures. They also support remote data management, functionality that is mission-critical in the context of enterprise IoT and its use in bring-your-own-device setups.

EXPEDITING INTERNAL IoT OPERATIONS

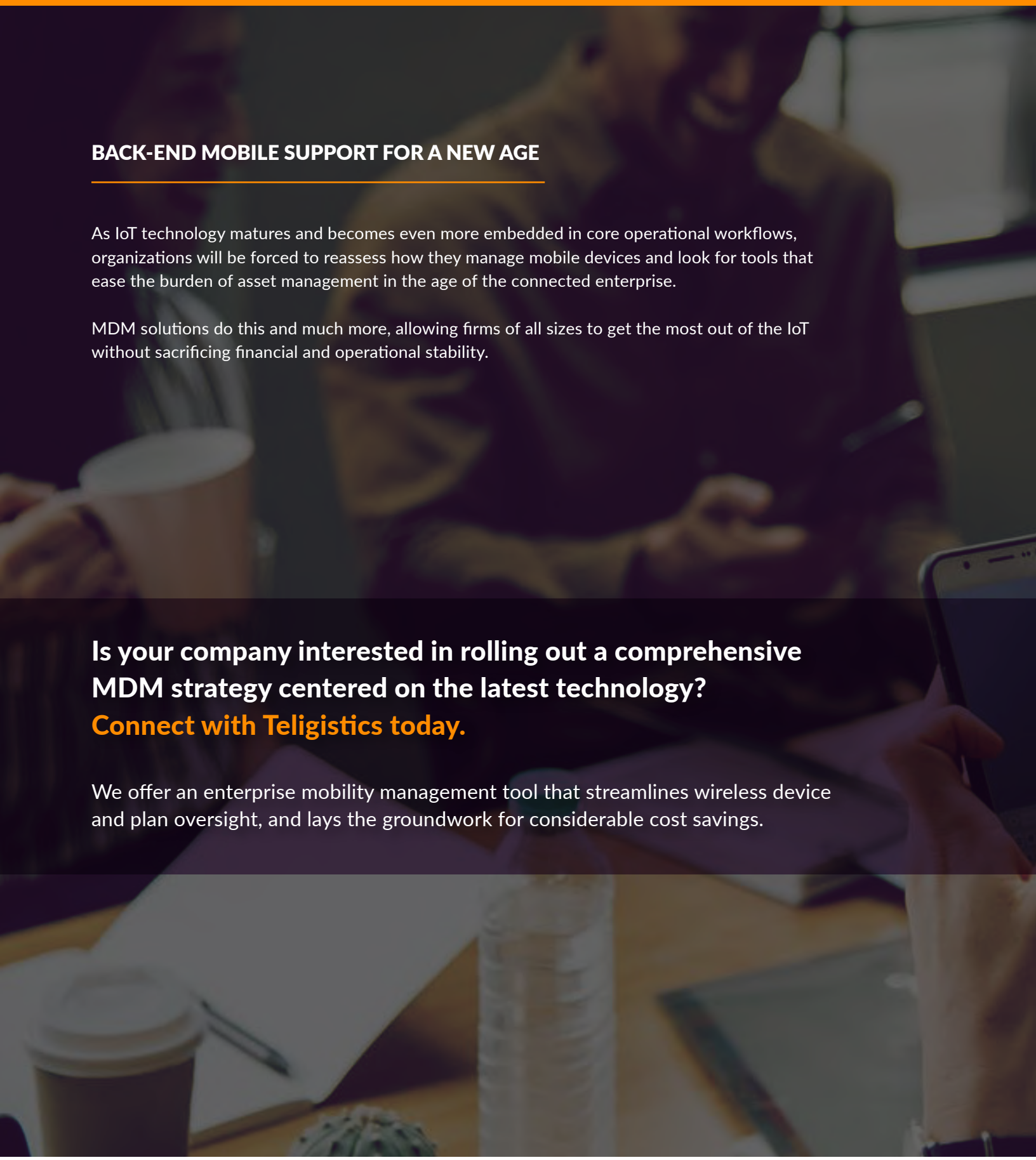
Mobile devices are at the center of modern business models. As mentioned above, this can greatly benefit businesses of all sizes. However, these assets add complexity to the operation, especially where it concerns employee device issuance, troubleshooting and deactivation. IT teams often set aside significant amounts of time to dole out physical assets or configure and manage voice and data plans. Deactivation is a similarly time-intensive task, as data security specialists have to assess and wipe corporate information from devices of departing employees. While these complications clearly do not prevent organizations from embracing the IoT, they can certainly increase resource usage and cause internal dysfunction.[19]

MDM strategies and associated technologies reduce the operational burden that comes with managing enterprise mobile devices, giving IT administrators the power to easily set up service for employees, oversee active assets and decommission them remotely. Some even connect users directly to third-party support services, removing IT from the troubleshooting equation altogether. Together, these features allow companies to fully embrace the IoT without suffering operational disruptions that risk the continuity of mobile workflows and organization at large.

REDUCING TELECOMMUNICATIONS COSTS

In addition to complicating IT functionality, enterprise mobile devices can have a less-than-ideal effect on the bottom line. Untracked IoT assets and overly expansive service plans can lead to significant cost overruns. If left unchecked, these expenses could outweigh the revenue gains attributed to increased efficiency, resulting in net losses.

MDM programs and the solutions that anchor them protect businesses from overspending on IoT technology by allowing IT teams to track usage and offer tailored service plans that meet the needs of employees but do not run up the budget. Especially advanced MDM software can use business intelligence to pinpoint cost-saving opportunities that are invisible to the naked eyes of system administrators.



BACK-END MOBILE SUPPORT FOR A NEW AGE

As IoT technology matures and becomes even more embedded in core operational workflows, organizations will be forced to reassess how they manage mobile devices and look for tools that ease the burden of asset management in the age of the connected enterprise.

MDM solutions do this and much more, allowing firms of all sizes to get the most out of the IoT without sacrificing financial and operational stability.

Is your company interested in rolling out a comprehensive MDM strategy centered on the latest technology?
Connect with Teligistics today.

We offer an enterprise mobility management tool that streamlines wireless device and plan oversight, and lays the groundwork for considerable cost savings.

SOURCES

[1] Pew Research Center, "*Mobile Fact Sheet*," 2018.

[2] Gartner, "*8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016*," 2017.

[3] McKinsey and Company, "*Taking the Pulse of Enterprise IoT*," 2017.

[4] McKinsey and Company, "*The Internet of Things: Mapping the Value of Beyond Hype*," 2015.

[5] Gartner, "*Two-Thirds of Enterprises Will Adopt Mobile Device Management Solutions for Corporate Liable Users Through 2017*," 2012.

[6] MarketsandMarkets, "*Mobile Device Management Global Forecast to 2023*," 2018.

[7] GlobalWebIndex, "*Device*," 2018.

[8] Clutch, "*How Employees Engage With Company Cybersecurity Policies*," 2018.

[9] Verizon Wireless, "*Mobile Threat Index*," 2018.

[10] Ibid.

[11] Avast, "*Avast Reports 40% Increase in Mobile Cyberattacks*," 2017.

[12] International Data Corporation, "*Smartphone OS*," 2017.

[13] Symantec, "*iOS Trustjacking—A Dangerous New iOS Vulnerability*," 2018

[14] Verizon Wireless, "*Data Breach Investigations Report*," 2018.

[15] Verizon Wireless, "*Mobile Threat Index*," 2018.

[16] Gemalto, "*The State of IoT Security*," 2018.

[17] Verizon Wireless, "*Mobile Threat Index*," 2018.

[18] International Data Corporation, "*IDC Spending Guide*," 2018.

[19] EY, "*Bring Your Own Device*," 2013.

www.teligistics.com | info@teligistics.com | 800-530-1063

1836 Spirit of Texas Way Suite 200, Conroe, TX 77301