A Successful Corporate-Liable Mobility Program Creates a Competitive Edge:

Moving Beyond BYOD Generates Cost Savings and Growth

FROST & SULLIVAN

A Frost & Sullivan White Paper

contents

INTRODUCTION

Frost & Sullivan research shows that more and more companies are going mobile, providing smart phones, tablets, and apps for their end users in record numbers. A 2016 survey of more than 400 IT decision makers in the United States reveals that nearly 80% of respondents provide smartphones for at least some of their employees to use for work, and about 65% offer tablets for business use. A 2015 survey of more than 500 IT decision makers in the US shows that almost three-quarters of companies use network management tools to control mobile devices, while more than half use mobile device management and/or endpoint security software.

But when deploying mobile devices to their end users, many companies do not have a clear picture of the total costs of doing so. IT resources, management applications and services, and security can comprise almost a third of the cost of these tools, and few companies account for less-tangible costs, such as reliability, extensibility, and productivity (or lack thereof when things go wrong). Deploying the right devices can lower these expenses, reduce risks, and improve overall performance.

This paper will guide readers in creating a successful corporate-liable mobility program, including the devices, security, and Enterprise Mobility Management (EMM) solutions available to help deliver advanced management and security, and offer best practices on supporting a truly mobile workforce.

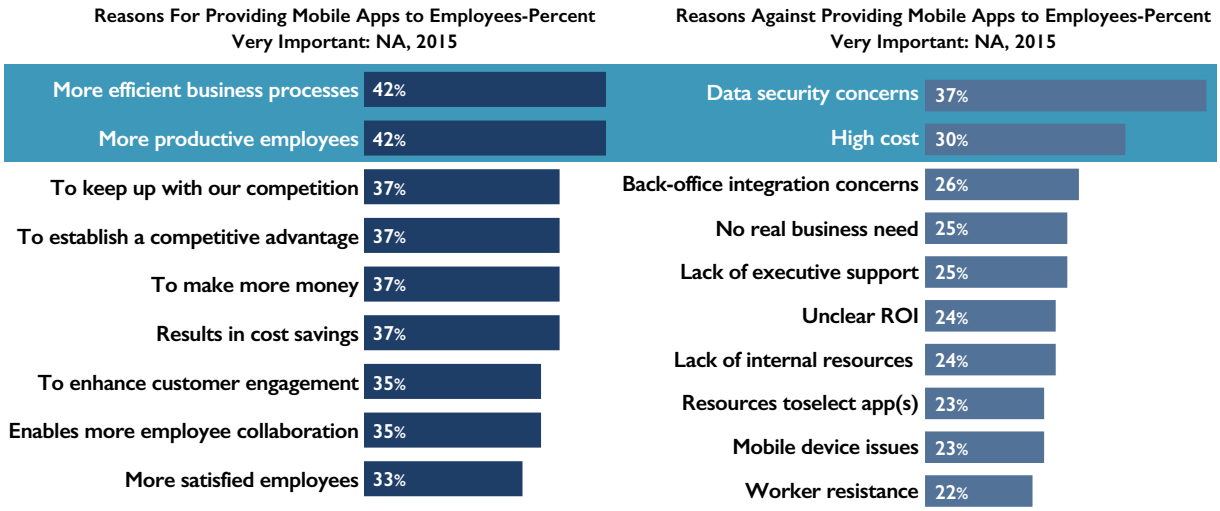
THE VALUE OF ENABLING A MOBILE WORKPLACE

With Frost & Sullivan research consistently showing that more than half of all employees routinely work outside of a traditional corporate office, the need for mobile devices and applications is clear; and indeed, our research also shows that the vast majority of companies provide smartphones and/or tablets to at least some of their employees to use for work. Anecdotally, our clients tell us that a good mobility plan results in improvements in employee productivity and accountability, higher customer satisfaction scores, and faster decision making—all of which can lead to increased revenues across the organization.

Businesses also continue to demonstrate high interest in mobile applications for their employees. In a 2015 Frost & Sullivan survey of 300 North American decision makers responsible for purchasing mobile software applications, 85% of respondents reported deploying at least one mobile worker app; the largest proportion of businesses (38%) have implemented between one and 10 apps. Looking ahead, 79% of respondent companies plan to deploy additional mobile worker apps by the end of 2016.

Top adoption drivers continue to focus on anticipated improvements in employee productivity and business process efficiencies, but a host of other benefits rank almost as high. In today's economy, businesses are clearly feeling the pressure from their competition, and they view mobile apps as a means to keep up with competitors or, even better, to establish a competitive edge. The probability of increased revenues and cost savings are also strong purchasing drivers, as are enhanced customer engagement and happier employees.

Figure 1: Reasons For and Against Mobile Apps



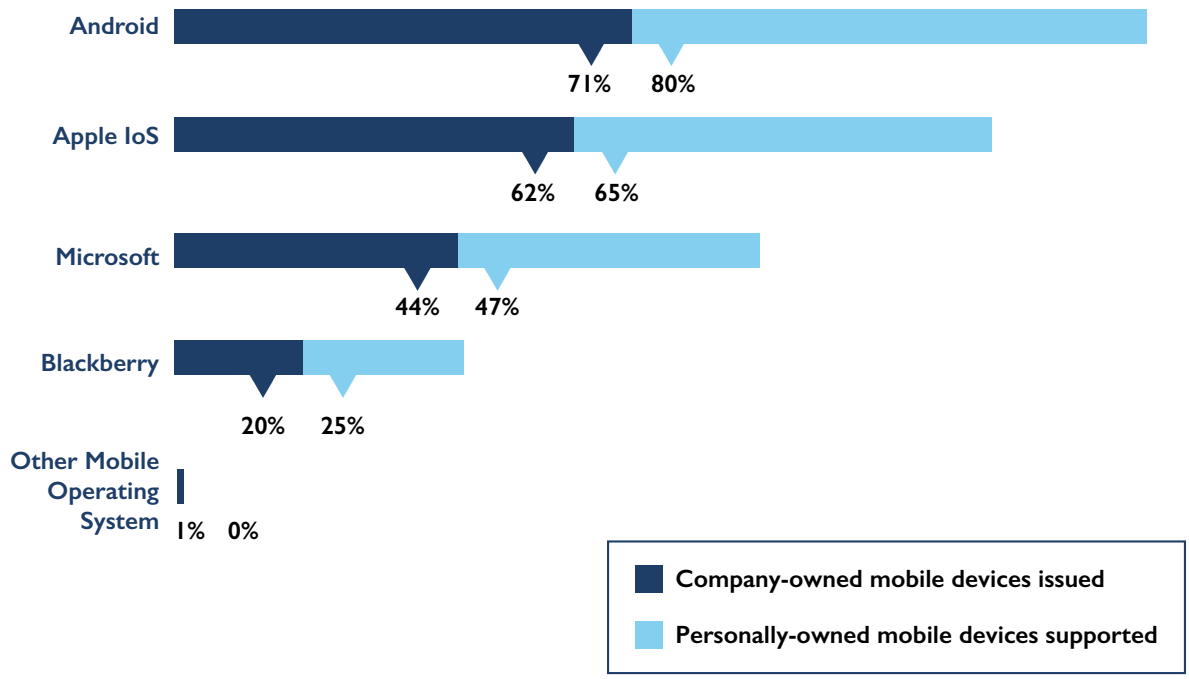
Source: Frost & Sullivan

But not everyone is buying in—primarily because of concerns over security and cost. Data security vulnerabilities remain executives' strongest concern, followed by (anticipated) high costs, integration issues, and the lack of business need.

Other concerns include the lack of a well-thought-out mobility strategy, rising employee use of unauthorized mobile apps, the instability and confusion caused by merger and acquisitions in the market, and the continued absence of end users in the mobile app decision-making process.

Reflecting the continued popularity of the "Bring Your Own Technology" (BYOT) trend, a higher percentage of companies support smartphones and tablets when they are owned by employees, as opposed to directly issuing the devices themselves. In fact, 11% of respondents report that their businesses do not issue company-owned mobile devices to employees at all. Just over two-thirds of respondents (68%) report that their companies support BYOT; Android is the top supported operating system for employees' personally owned devices, with Samsung the top manufacturer. If current non-BYOT companies were to start supporting employees using their own devices, they report that their top choice for a mobile operating system would be Android.

Figure 2: Snapshot of Mobile Operating Systems in the Enterprise



Source: Frost & Sullivan

THE NEED FOR A CORPORATE-LIABLE MOBILITY PLAN

Frost & Sullivan strongly believes that most companies today cannot afford to ignore the use of mobile devices within the organization. By allowing employees to work from anywhere with an Internet connection, be it cellular or Wi-Fi, mobile devices and applications ensure that employees can respond to opportunities quickly, shrink decision making and development times, boost productivity, and ultimately see the results in the company's bottom line.

But deciding to enable a mobile workplace and deciding on the best way to support mobile workers are two different things—and the latter can get complicated quickly. The most practical approach is for the company itself to purchase, deploy, and support mobile devices and applications for all employees who can reasonably be expected to need them. This so-called "corporate-liable" approach to mobility puts the power and control in the company's hands—the power to choose which devices, operating systems, and apps to support; the power to budget and control costs; the control to determine what data is available to which people and when; and the power to wipe endpoints clean if employees lose them, or when they part ways with the organization.

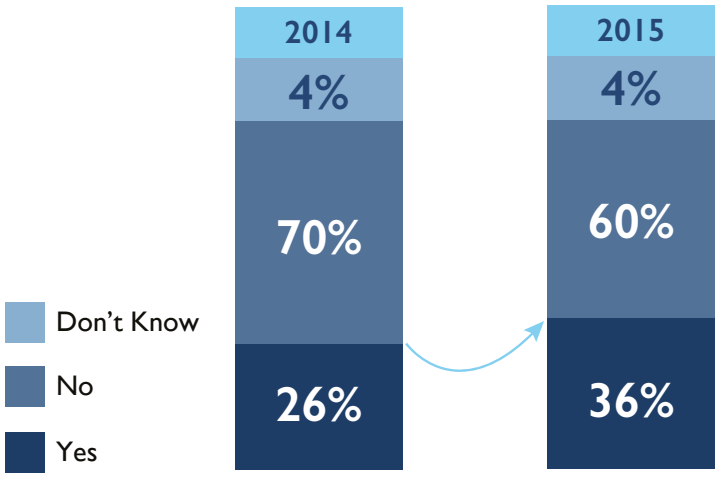
Perhaps even more important, a corporate-liable approach allows companies to maximize the value of the devices and apps employees use to get work done. IT decision makers, in conjunction with business leaders, can make decisions about what types of smartphones and tablets are best for their users and the organization overall, based on factors such as performance, hardened security, battery life, screen size, and so on. They can also offer and support mobile clients for select enterprise apps, as well as approve the use of whatever consumer apps they deem valuable—and block the ones they don't want running on their devices and networks.

The result is a much more effective mobile workplace—one that runs smoothly and seamlessly, consistent with the other IT-driven processes in the organization. Because while it's easy to sit back and let employees pay for and use their own devices and apps in the workplace, the mix of endpoints, operating systems, and applications will eventually cause havoc for the IT team. The first time a user can't access corporate email, salesforce.com, or other mission-critical data and services on her (personal) mobile device, she will contact IT—and IT may not have the resources or methodologies to fix the problem, at least not in a cost-effective and efficient way.

> **Think about it: you wouldn't let your employees source, purchase, and deploy their own productivity and back-office software, network management tools, compliance applications, or contact center solutions, so why would you give them complete control over the devices and apps they use the most?**

The best way to ensure that business processes are followed and effective is to ensure that employees have the tools they need to comply with them; these days, that means giving workers smartphones, tablets, and even wearable devices to run and support the enterprise and consumer apps you're building those processes around.

Employee Use of Unauthorized Mobile Apps as a Problem: NA, 2014 and 2015



Source: Frost & Sullivan

HOW TO LOWER COSTS AND IMPROVE PERFORMANCE

Of course, one of the biggest barriers to a corporate-liable mobility program is cost: when companies have to pay for hardware that they didn't have to budget for in the past, the reaction can be muted, at best. But the reality is that while corporate-liable plans may cost more initially, they often end up saving organizations money in the long run on maintenance and support, as well as by mitigating lost productivity and other opportunity costs.

During the *planning phase*, IT and line-of-business executives should think about three critical areas to ensure success. None of these should come as an afterthought:

1. **Rollout** When devising a corporate-liable mobility program, it's critical to consider both the hardware and the software employees will be using. For instance, your IT department may opt to support one smartphone and one tablet model based on a common OS and run only standard corporate apps. Or IT and business executives may decide that it's better to give employees some choice, allowing them to choose from an array of devices, and then offering them access to an enterprise app store so that they can download both enterprise- and consumer-grade apps as desired. Either way, the company should have identified the devices and applications that make the most sense for the business (or specific users), and which it can then support.

   It's also a good idea to develop a roadmap that clearly outlines where the company is today and where it plans to be in one, two, and three years. Most organizations start with a pilot program, issuing mobile devices to select users based on their location or job roles. Then, once that proof of concept has been completed, they expand delivery to most or all employees across the organization, offering different options for endpoints and applications, depending on what each employee's work requires. As they develop a long-term plan, IT executives should work closely with line-of-business managers—and their chosen vendor(s)—to make sure the rollout will meet their users' needs over time, with the right apps and security in place as soon as they are needed.

You should approach your corporate-liable rollout as you would any other. Pay close attention to:

- ***Delivery:*** Do you want the devices to be shipped to the MIS department for customization and vetting, or directly to each end user? What apps and services do you want pre-loaded, what will you or the user need to download, and how will you manage that process?
- ***Training:*** Don't overlook the need to train end users on their new hardware and software. This should include the usage of the technology itself, as well as company policies around business-versus-personal use, security and intellectual property protection, data limits, and so on.
- ***Support:*** Before you deploy a single mobile device, make sure you have a clear and consistent plan for supporting the hardware, apps, and services. What will you do if a user calls for help outside of normal business hours—a common occurrence with mobile devices? Will you support consumer apps, and if so, which ones and how? If a user needs to send a device to you for maintenance, what will they use to get work done in the interim?

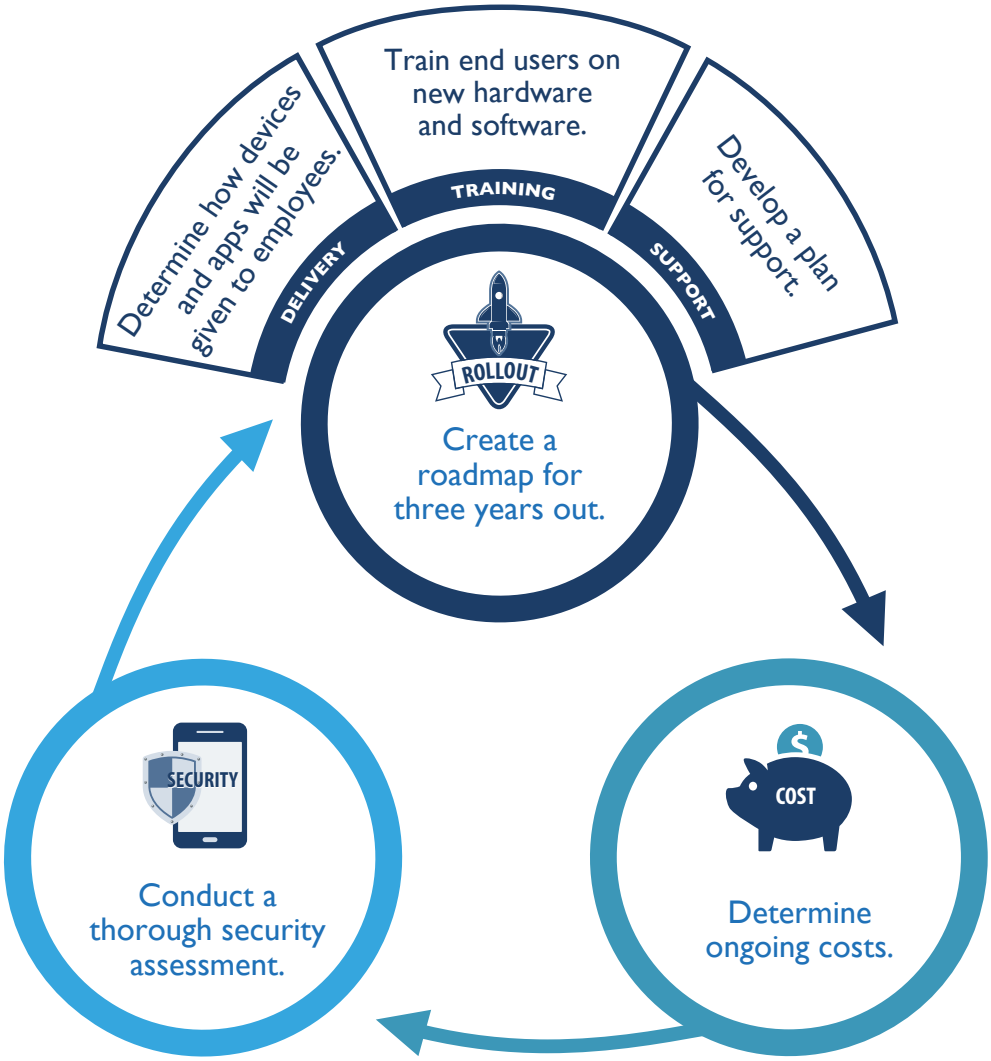
2. **Cost** Investment considerations start with the devices and apps a company plans to deploy. Will you rollout smartphones, tablets, or both? Will you pay for corporate mobile apps, and if so, which ones and for which users? What about accessories like protective cases, Bluetooth headsets, chargers, and extra batteries?

   But the cost discussion should go well beyond your initial outlay to consider ongoing maintenance and support. Will you keep those services in house, and if so, how will you manage calls? Will you outsource them, and if so, to whom—the same vendor from which you purchased the devices? The software providers? Some combination of the two? A third-party outsourcer that can handle hardware and software trouble tickets? Consider geography and job roles—will you have different help desks available to different users depending on the time of day and the nature of their call, or their importance to the business? (If a VP of sales needs his phone to work at 11 p.m. ET, that's more important than if a first-year intern does; how will you distinguish between the two?)

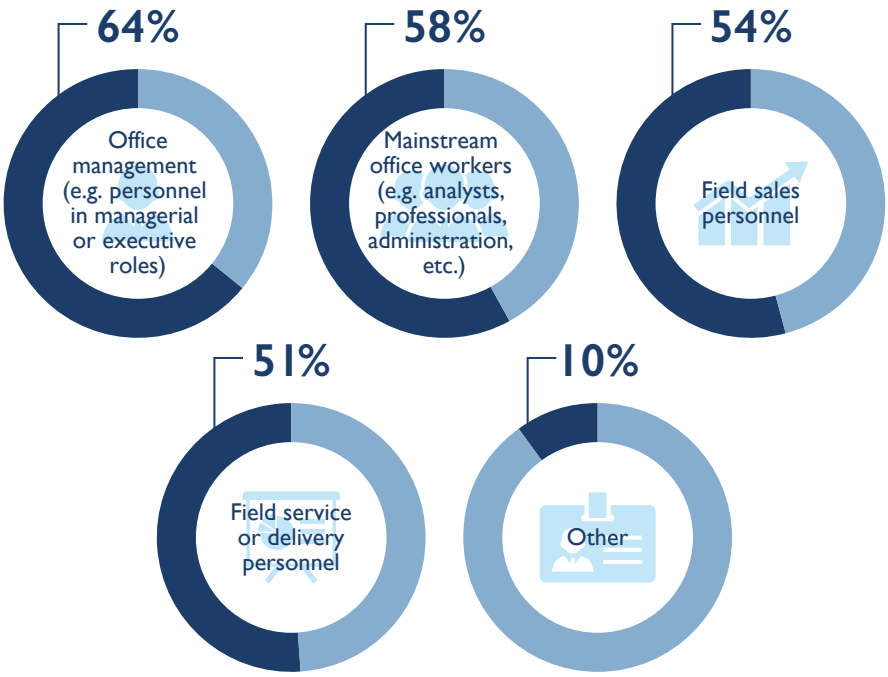
3. **Security** Companies should conduct a thorough security and risk assessment during deployment planning—if you think about it after you've selected your devices and processes for deployment and support, you're doing it too late. Malicious or compromised applications are the most significant risks for mobile devices; as

a result, application- and application-store management are especially important to mobile security. You'll need to protect against everything from viruses, backdoors, Trojans, and worms to spyware, trackware, and adware.

But IT managers need to be aware of other security risks, too. One commonly overlooked threat is the end user himself, who often, knowingly or not, takes action that puts the device, network, and business at risk. In many cases, employees will leverage personal devices where possible, bypassing the security needs of the company if the company-issued device is too constrained or doesn't provide sufficient functionality, which increases the risks to the company. Some tech-savvy users will even try to hack their corporate-liable devices to get around pre-set limits, which makes the risk of a security breach even greater. As you think about how you'll handle mobile security, it's critical to weigh benefits of restricting use (and increasing security) versus enabling use (and deploying the necessary security tools to ensure any and all use is safe). A so-called "walled garden" approach—implementing solutions that enable a personal-use environment that is separate from enterprise applications and data—can be very effective; companies should consider leveraging solutions that provide for a secure environment for corporate data and one with less restrictions for limited personal use.



Users of Mobile Worker Apps, by Title



Corporate policies that ban the process of hacking devices to run desired apps will greatly minimize an organization's risk, but only if such a ban can be enforced. The challenge lies in identifying which apps present a true threat—a difficult task, because many malicious apps blur the line between useful features and exploitative functionality. That's where strong mobile security services and software come in.

Before, during, and after any mobility rollout you must ensure security is as high as necessary for your business and the industry it plays in. One option is to install critical security software to protect the hardware and its apps from a variety of malware. You can also opt to deploy security software in conjunction with a hardened device. (Hardened devices have unnecessary software and services removed and may incorporate security protocols built into the silicone, significantly increasing the security of the device.)

Finally, don't overlook management and control. You will need to ensure that you have sufficient capability in place to adapt security configuration and controls on the device over its lifetime to address the ever-changing risk environment. Such tools should be able to help you find lost devices, wipe stolen devices, and deploy updated tools and applications. Depending on the industry you're in, you also may need to archive (and make accessible) data and other content for regulatory or legal purposes.

> **IT and the C-level suite remain the most involved when it is time to approve the deployment of a major mobile business application. As many as 35% of businesses also pull in their operations, finance, and/or sales and marketing staffs. Unfortunately, end users remain an untapped resource.**

Cloud vs. On-premises

Most organizations will need to make the decision of how and where to manage their mobile infrastructure based on a variety of criteria, including geographic location, the percentage of virtual or remote employees, use cases, and IT resources. According to the Frost & Sullivan survey of 300 IT decision makers with control of mobile apps, on-premise vs. cloud-based vs. hybrid implementation of mobile applications continues to evolve, with an increase in the use of premises-based solutions. Hosted or cloud solutions remain stable at 25%, with hybrid solutions dropping to 19%. This year, security and privacy concerns have leaped forward as a significant barrier to implementing cloud-based mobile apps. In addition to the usual cost and control issues, internal politics has also risen as a significant barrier to adoption.

IDENTIFYING THE KEY COMPONENTS FOR A CORPORATE-LIABLE PARTNER

Clearly, companies must protect any mobile devices they deploy to their end users. And it appears that most organizations are realizing that fact: according to Frost & Sullivan research, more than three-quarters of companies see value in deploying an Enterprise Mobility Management (EMM) platform. In the research, 44% of decision-makers report that their business currently has an EMM platform or suite in place, while another 29% plans to introduce an EMM platform for the first time within the next year. Less than one-quarter of the respondents report that their businesses have no plans to introduce an EMM platform.

> “With a corporate-liable mobility program, the decisions about security and support remain where they belong—with the business whose data, contacts, and processes are most at risk.”

But choosing the right EMM partner can be tricky. When evaluating the options, it’s important to look at the following criteria:

- **Anti-malware** to identify, block, and remove malicious programs or applications.
- **Content filtering** to avoid traffic from known malicious Web hosts.
- **Call and message filtering** to block unwanted calls and texts.
- **Remote wipe and lock** so users and/or administrators can remotely erase data or lock a mobile device that is lost or stolen.
- **Anti-loss and anti-theft** to remotely locate a lost or stolen mobile device.
- **Content controls** for monitoring and limiting user access to websites, messaging and calls based on location, time, or content type.
- **Mobile Virtual Private Network (VPN)** to enable secure VPN connections and persistence over wireless and mobile networks.
- **Encryption** to secure files and any data exchanged on the device.

- **Separation of corporate and personal data** to let users rely on one device for both personal and business use.
- **Cloud-based management** to give IT a simple, efficient way to see and manage all devices from a central console.

Finally, consider devices with security software pre-loaded, or even so-called "hardened" devices, which go beyond traditional network or software solutions by using security embedded in the machine's semiconductor to make mobile devices much more secure from end to end. Paired with the right security software, the combination can make even the most security-focused organizations comfortable with embracing a fully mobile workplace.

CONCLUSION

As more companies embrace the need to support a fully mobile workplace, many IT and business executives are struggling with how to best deploy and support smartphones, tablets, and other devices. Frost & Sullivan recommends taking a corporate-liable approach, which allows the organization to maintain complete control over the devices, operating system, and the mobile apps—without sacrificing any of the benefits mobile workers want and need.

To ensure success with any corporate-liable program, IT decision makers should work with line-of-business managers and end users to choose the right devices and apps for each use case and business process. They should also carefully select a partner that can offer top-of-the-line security for the device, the network, and the end user. Look for a wide range of features, including anti-malware, content controls, remote-locator capabilities, tools to let admins wipe data remotely, containers for personal and corporate data, and encryption. Also consider the device itself for added protection—a hardened smartphone can deliver even more peace of mind, without sacrificing benefits or performance.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

MELANIE TUREK
Vice President | Enterprise Communications | Frost & Sullivan
P: 970.871.6110
E: melanie.turek@frost.com

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041