2016 Mobile Security Report

iPass

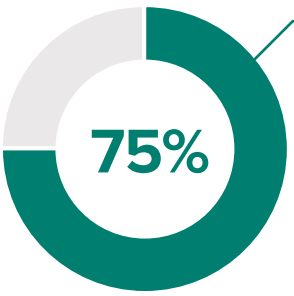
CONTENTS

According to industry analyst IDC, 75% of Europe's workforce will be mobile by 2018. Indeed, it expects mobile workers to account for nearly three-quarters of the U.S. workforce by 2020. Mobile working is here to stay.

The workplace of 2016 is a perfect storm of powerful, affordable and highly portable devices and cloud-based business tools. The deployment of technology to increase staff productivity has made mobile working prevalent in many organizations across the globe.

While mobile working can lead to increased levels of staff retention and productivity, it has also precipitated increased security concerns as employees look to access corporate data/systems from a number of different locations, using a multitude of devices and connection methods. Added to this is the explosive growth of free (and often unsecured) Wi-Fi hotspots, which are presenting cybercriminals with a playground for identity fraud and mass corporate data theft. Understandably, mobile security is becoming an overarching priority as organizations aim to keep their people productive and their data safe.

Surveying 500 CIOs and senior IT decision makers from the U.S., U.K., Germany and France, the iPass Mobile Security Report 2016 provides an overview of how organizations are dealing with the trade-off between security and enabling a mobile workforce.



According to industry analyst IDC, 75% of Europe's workforce will be mobile by 2018. Indeed, it expects mobile workers to account for nearly three-quarters of the U.S. workforce by 2020.

Mobile security is a worry for businesses in 2016

Being connected is the basic requirement of every mobile worker. However, with increasing numbers of businesses falling victim to security breaches, the number of organizations expressing a concern about mobile security is very high. The majority of businesses surveyed (92%) stated they are 'very' or 'somewhat' concerned about the mobile security challenges associated with a growing mobile workforce. Indeed, over a third of businesses (36%) described themselves as 'very concerned'.

When comparing responses across geographic regions, the research revealed that U.S. organizations (97%) demonstrated the greatest concern about mobile security, compared to 94% for French, 87% for German, and 83% for U.K. businesses.

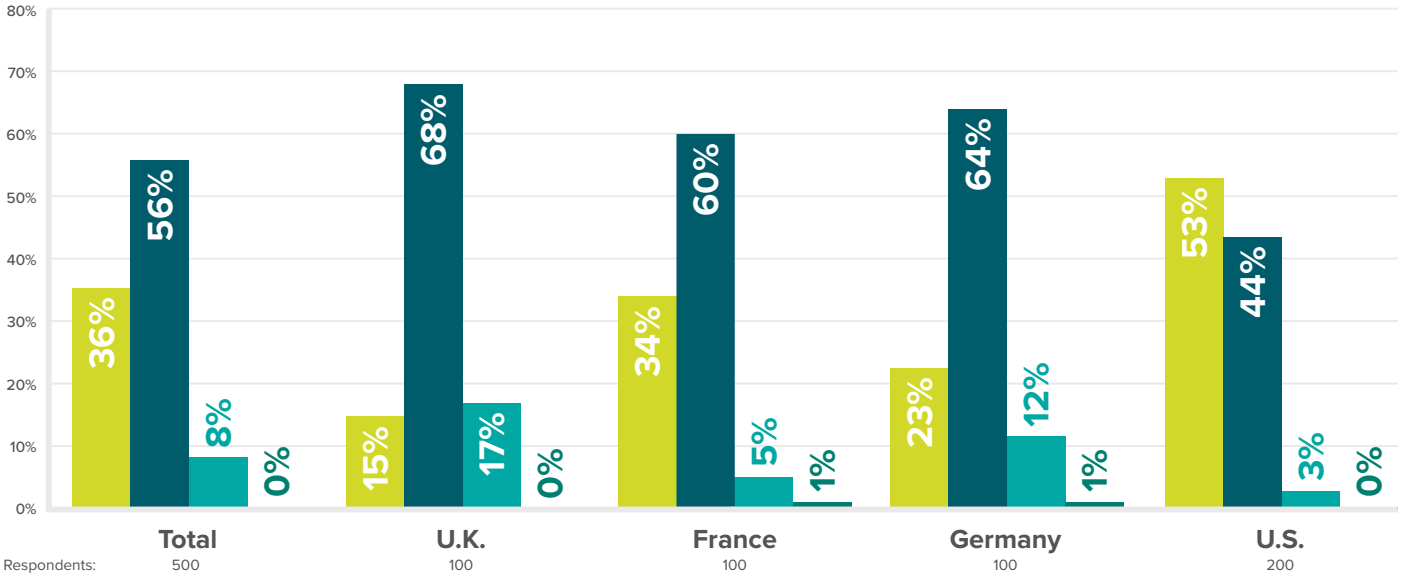
QUESTION 1:

With a growing mobile workforce are you concerned this presents an increasing number of mobile security challenges, as staff look to access corporate data/systems from a number of different locations using a multitude of devices and connection methods (e.g. free Wi-Fi hotspots)?

ANSWERS:

- A Very concerned
- B Somewhat concerned
- C Not very concerned
- D Not at all concerned

Source: Vanson Bourne



Safe mobile usage policies found difficult to enforce

In today's enterprise, mobile workers are utilizing a whole host of devices and connection methods to get online. In addition, the fact that many workers use mobile devices for both personal and business use exacerbates the challenge of enforcing safe mobile usage policies.

The survey found that 88% of organizations admitted to finding it difficult to consistently enforce a safe mobile usage policy. Indeed, when looking at how this played out geographically, the research revealed 94% of French businesses struggled to consistently enforce a safe mobile usage policy compared to 90% of German, 89% of U.S. and 79% of U.K. organizations.

This finding suggests businesses need to adopt more stringent measures in order to enforce security policies, while still providing mobile workers the flexibility they demand.

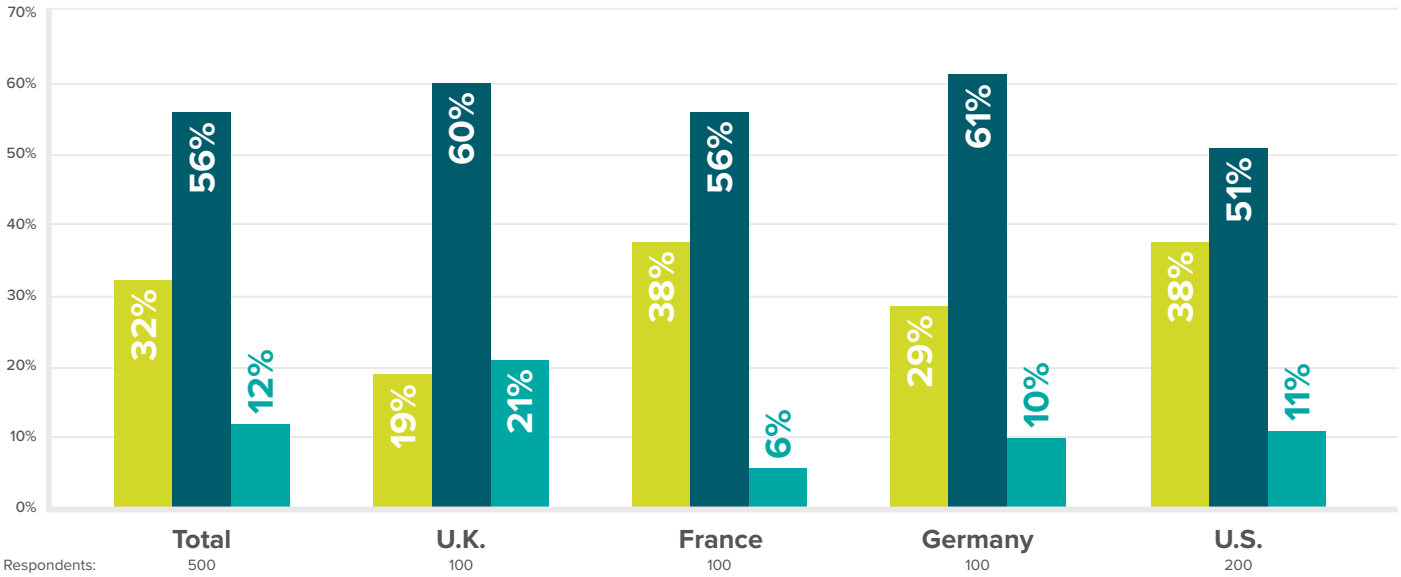
QUESTION 2:

With many workers using mobile devices for both business and personal use, does your organization find it difficult to consistently enforce a safe mobile usage policy?

ANSWERS:

- A Yes—we find it very difficult to enforce a safe mobile usage policy all of the time
- B Yes—we find it difficult to enforce a mobile usage policy some of the time
- C No—we don't find it difficult to enforce a safe mobile usage policy

Source: Vanson Bourne



Free Wi-Fi poses greatest mobile security threat

When asked to identify the greatest mobile security threat they face, 37% of respondents pointed to unsecured Wi-Fi.

Mobile workers are very resourceful when it comes to finding wireless connectivity. But mobile workers need to anticipate and avoid common threats associated with remote working. For instance, by connecting to unsecured Wi-Fi hotspots, mobile workers risk falling prey to cyberattacks like 'man in the middle' attacks and 'packet sniffing,' which compromise personal and corporate data. In today's Wi-Fi first world, it is therefore paramount to educate mobile workers about how to find secure connectivity while on the go.

Indeed, employees' lack of diligence, whether choosing poor passwords, losing devices or failing to adhere to corporate policies, poses a significant threat to mobile security for businesses. According to the report, 36% of respondents cited employees as the greatest threat to mobile security. Interestingly, the choices varied across geographic regions, with the majority of U.K. respondents (64%) citing employees as the greatest threat, but only slightly more than half of U.S. respondents (53%).

This finding indicates that U.K. and U.S. organizations, in particular, still have a long way to go to ensure their mobile workers are properly educated regarding safe mobile working practices.

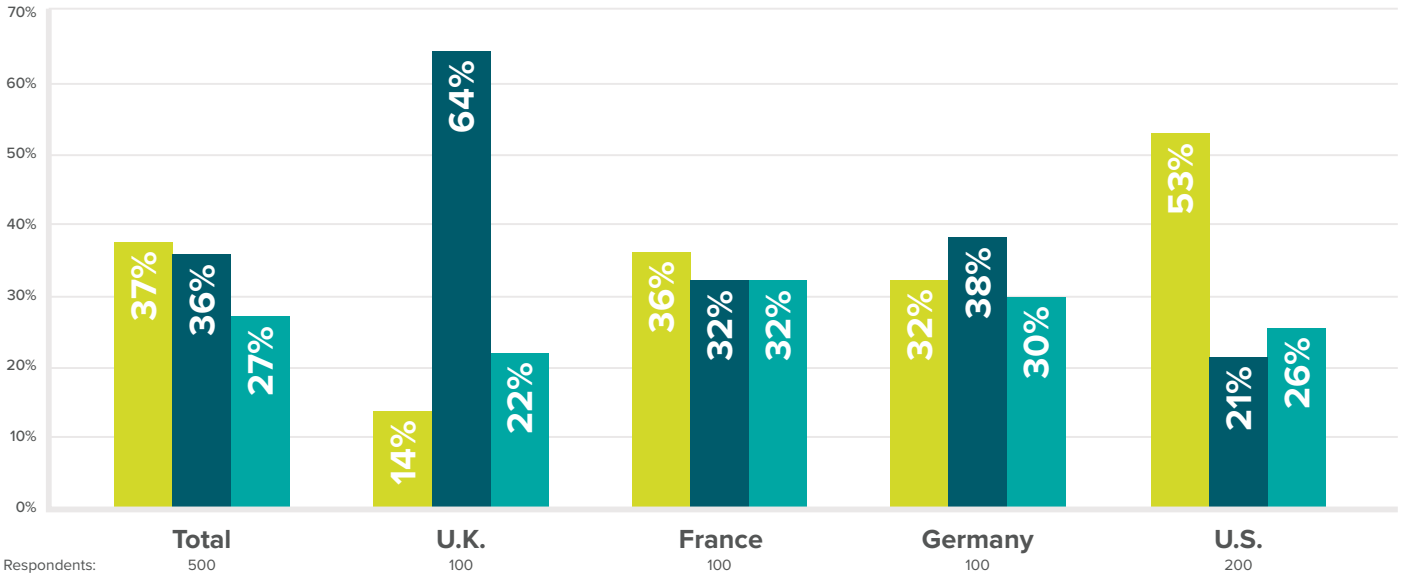
QUESTION 3:

When it comes to keeping your corporate data/systems safe, which of the [following] do you think is the biggest mobile security threat?

ANSWERS:

- A Insecure Wi-Fi hotspots
- B Employees
- C Mobile devices

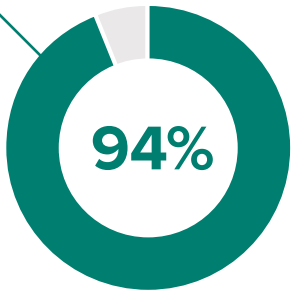
Source: Vanson Bourne



Indeed, with the proliferation of public Wi-Fi hotspots, it is now possible for any small business to set up a free Wi-Fi hotspot. However, this has meant that the security credentials of individual hotspots vary considerably.

Free Wi-Fi hotspots might be fast, simple and convenient, but they can also be one-way tickets to identity fraud and mass corporate data theft. When asked, 94% of organizations stated they saw free Wi-Fi as either 'very much' or 'somewhat' of a threat.

When asked, 94% of organizations stated they saw free Wi-Fi as either 'very much' or 'somewhat' of a threat.



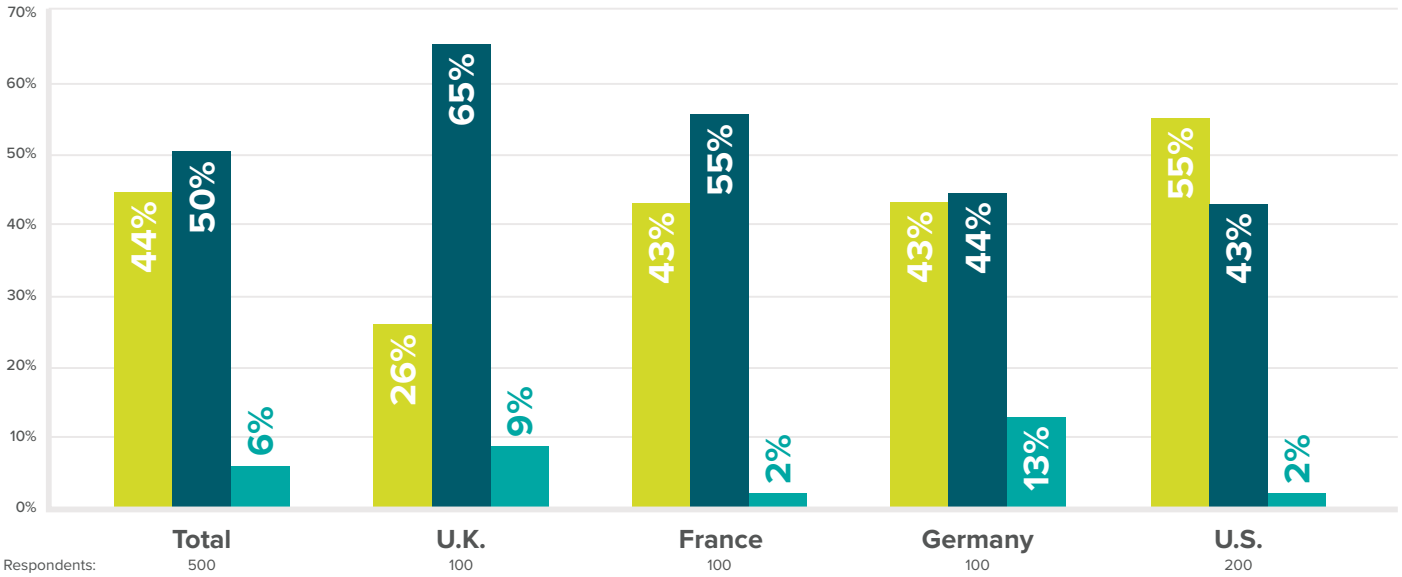
QUESTION 4:

How much of a mobile security threat do you see free Wi-Fi hotspots as?

ANSWERS:

- A Very much a threat
- B Somewhat of a threat
- C No threat at all

Source: Vanson Bourne



Organizations struggle to enable safety via VPNs

Many organizations use virtual private networks (VPNs) to provide secure remote access to their data and systems. Typically, these VPNs have to be enabled by end users each time they connect. However, considering employees may have divergent levels of technical expertise and that the process of using a VPN itself differs from device to device, there is no guarantee that mobile workers will use them every time they go online.

Just 26% of organizations are confident that their employees utilize the company VPN all of the time.

Of all the geographic regions surveyed, U.S. businesses were least confident about their mobile workers using a VPN to access corporate networks on the move, with 79% displaying a lack of confidence in their workforces' cyber-savviness.

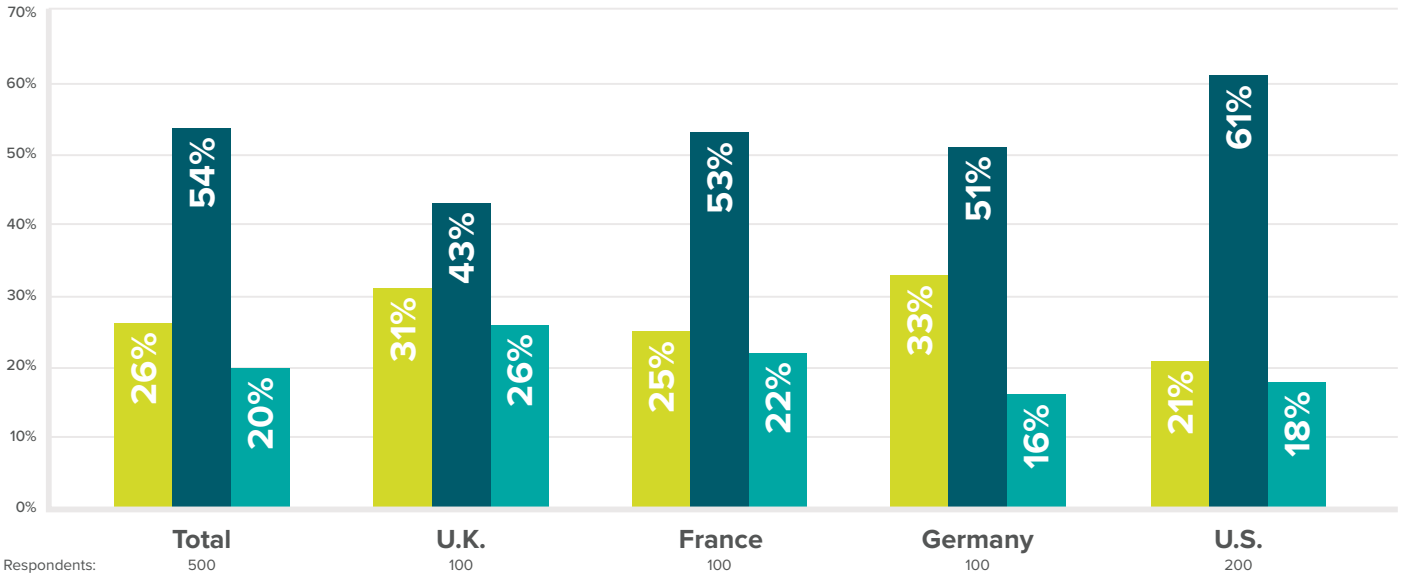
QUESTION 5:

Considering employees have differing levels of technical expertise and that the process of using a VPN can differ from device to device, how confident are you that your organization's mobile workers use a VPN every time they go online?

ANSWERS:

- A I am 100% confident that our mobile workers use a VPN every time they go online
- B I am somewhat confident our mobile workers use a VPN every time they go online
- C I am not confident our mobile workers use a VPN every time they go online

Source: Vanson Bourne



Organizations ban the use of free Wi-Fi hotspots

Given the challenges of enforcing a safe mobile usage policy, sporadic corporate VPN use and the threat posed by mobile workers choosing unsecured Wi-Fi hotspots, it is not surprising to see so many organizations beginning to enforce bans for mobile workers. Well over half (62%) of the organizations surveyed actively ban their employees from using free Wi-Fi hotspots, with 22% enforcing this rule without exception and a further 20% of organizations planning to put bans in place in the future.

A significant number of French companies (73%) actively enforce bans for free Wi-Fi hotspots, making France the surveyed country with the highest incidence. In fact, nearly 30% of French companies do so without exception.

Interestingly, U.K. businesses seem less strict when it comes to employees using free Wi-Fi. Nearly half (47%) of respondents stated they do not actively ban employees from using free Wi-Fi services and do not plan to.

With many companies already enforcing bans and with others likely to enforce more stringent policies in the future, organizations clearly have a balance to strike to keep employees safe as well as connected. But prohibiting access to free Wi-Fi can have unintended consequences. Free Wi-Fi bans may cause employees to connect via more expensive and potentially slower means (such as 3G/4G or via a Mi-Fi device), and then charging those costs back to the company.

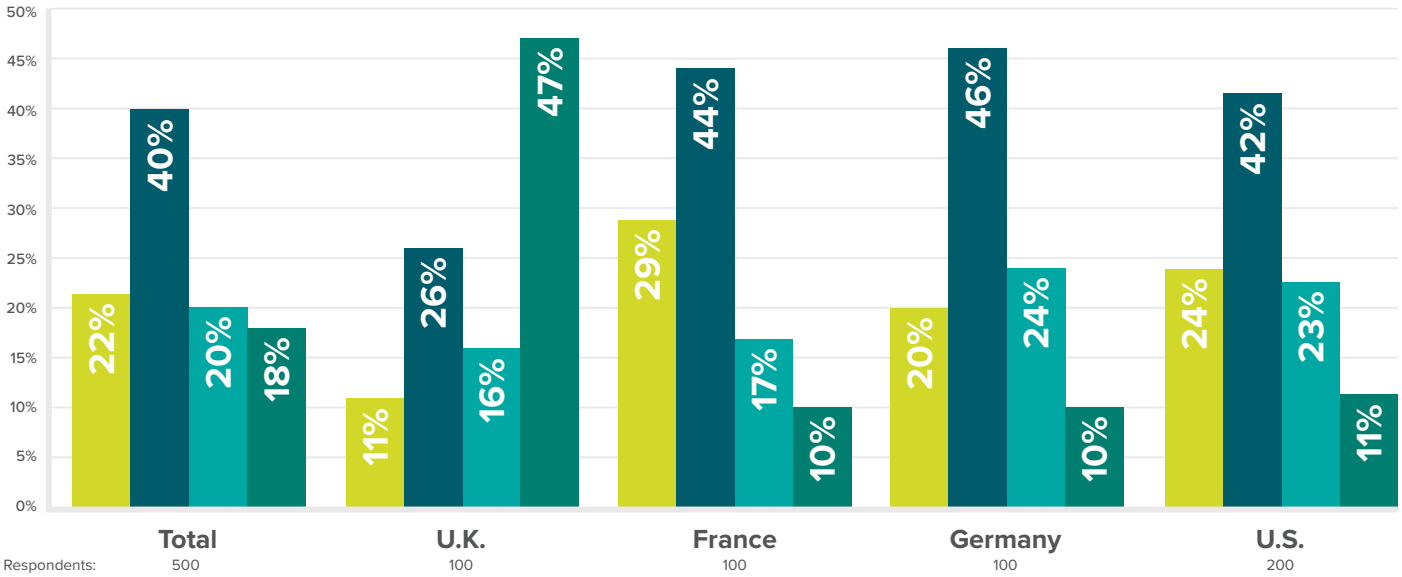
QUESTION 6:

Based on increasing security risks, does your organization currently ban your mobile workers from using free Wi-Fi hotspots?

ANSWERS:

- A Yes, all the time
- B Yes, sometimes
- C No, but we plan to in the future
- D No, and we do not plan to

Source: Vanson Bourne



Conclusion

The draw of mobile working is evident to workers and businesses alike, but as the research reveals, mobile security is a growing concern. For organizations, the use of free and unsecured Wi-Fi hotspots in particular is posing a conundrum, as businesses balance the need for low-cost and convenient connectivity solutions against the potential threat posed by hackers. The fact is that for convenience and guaranteed service, mobile workers will seek out Wi-Fi connectivity, despite security flaws. In today's 'Wi-Fi-first' world, it is imperative that mobile workers are equipped with the requisite tools to get online and remain productive, while simultaneously ensuring the security of corporate data.

*The research was carried out during March 2016 and was conducted by independent research company Vanson Bourne.

About iPass

iPass (NASDAQ: IPAS) is the leading provider of global mobile connectivity, offering simple, secure, always-on Wi-Fi access on any mobile device. Built on a software-as-a-service (SaaS) platform, the iPass cloud-based service keeps its customers connected by providing unlimited Wi-Fi connectivity on unlimited devices. iPass is the world's largest Wi-Fi network, with more than 50 million hotspots in more than 120 countries, at airports, hotels, train stations, convention centers, outdoor venues, inflight, and more. Using patented technology, iPass SmartConnect™ takes the guesswork out of Wi-Fi, automatically connecting customers to the best hotspot for their needs. Customers simply download the iPass app to experience unlimited, everywhere, and invisible Wi-Fi.

iPass Corporate Headquarters
3800 Bridge Parkway
Redwood Shores, CA 94065

phone: +1 650-232-4100
fax: +1 650-232-4111

www.ipass.com