Mobility has rapidly moved into the mainstream of the enterprise and changed IT and business processes in profound ways. Today, it’s next to impossible to find an organization that doesn’t incorporate at least some mobile devices—smartphones, tablets and laptops—into the fabric of the business. In fact, according to various industry statistics, somewhere in the neighborhood of 90 percent of companies have adopted some form of bring your own device (BYOD). Yet, despite rapid adoption and a growing focus on mobility, many business and IT executives cling to myths and misconceptions. In many cases, organizations are adopting strategies and security protections that aren’t in the best interests of the organization, points out Bill Conner, CEO of security firm Entrust. He believes that it’s critical to understand the current state of mobility and to build a strategy and protections around actual risks. To clarify things, Entrust has provided the following common myths about mobile security, along with a fact-based explanation of the true situation.
Mobile Security: Myths Vs. Reality

Myth #1: Company-issued devices are the only way to ensure mobile security.
Fact: Personal devices can be used safely. By separating corporate and personal apps in different containers, you can build a protective barrier between the two.
Mobile Security: Myths Vs. Reality

Myth #2: There is no way to know who is on a WiFi network.
Fact: You can assign a separate identity to each personal device, which makes it possible to know who is connected and what device they are using at any moment.
Mobile Security: Myths Vs. Reality

Myth #3: Mobile malware is more malicious than conventional malware.
Fact: Mobile devices use a sandbox to separate apps. This means malware from one app cannot jump to another app, reducing potential damage and risks.
Mobile Security: Myths Vs. Reality

Myth #4: Android devices lack essential security.
Fact: While Android devices are subject to side-loaded apps containing potential malware, users must choose to allow these apps to be installed. The Google Play store represents negligible risk.

MOBILE SECURITY: MYTHS VS. REALITY

MYTH #4
Android devices lack essential security.

FACT
While Android devices are subject to side-loaded apps containing potential malware, users must choose to allow these apps to be installed. The Google Play store represents negligible risk.

Baseline
Mobile Security: Myths Vs. Reality

Myth #5: If a device is stolen, confidential information goes with it.
Fact: A layered, identity-based mobile security solution that uses a PIN or biometric key blocks access to confidential data.
Mobile Security: Myths Vs. Reality

Myth #6: Mobile devices cannot be fully trusted.
Fact: Mobile devices can be used to enhance physical and logical security throughout the enterprise. A mobile credential can be used for all types of physical and virtual access.
Mobile Security: Myths Vs. Reality

Myth #7: Employees can accidentally jailbreak a mobile device.
Fact: Jailbreaking requires a number of active steps, including tethering the device to a PC. A phone can’t be jailbroken without the purposeful involvement of a user.
Mobile Security: Myths Vs. Reality

Myth #8: Mobile devices lack security features required to digitally sign and authorize sensitive transactions.
Fact: A mobile device with a smart credential protects sensitive online transactions by notifying the user that a transaction requires the individual’s explicit confirmation or digital signature.
Mobile Security: Myths Vs. Reality

Myth #9: Mobile browsing offers the same level of security as mobile apps.
Fact: Mobile apps automatically connect to a legitimate service provider and protect all interactions, but mobile browsers allow users to be duped into accessing rogue Websites.
Mobile Security: Myths Vs. Reality

Myth #10: SMS is a safe and secure tool.
Fact: While SMS simplifies communication, hackers can redirect messages and spoof communications without the user’s knowledge.