Mobile networks matter.

What CIOs should know about mobile network security

verizon

The mobile workforce is exploding.

The size of the workforce that depends on mobile devices continues to increase exponentially. Forrester Research characterizes 29% of the global workforce as so-called "anytime, anywhere information workers—those who use three or more devices, work from multiple locations and use many apps." By 2020, the mobile workforce population is expected to reach 105 million—nearly three-quarters of the total U.S. workforce.[1]

Enterprise and government organizations face challenges on multiple fronts.

Even with an advanced mobile security infrastructure in place, companies and agencies face a variety of obstacles in protecting their data.

Worker negligence
Employees deliberately ignore security rules, placing corporate data and, potentially, customer information at risk.[2]

Application vulnerability
On average, employees access 160 unique IP addresses per day from their devices. And 24.7% of mobile apps include at least one high-risk security flaw.[3]

Bring your own device
More employees using mobile devices—including their own personal devices—present CIOs with a number of security challenges.

Business apps are three times more likely to leak login credentials than the average app.[3]

Verizon Wireless makes protecting your data the top priority.

As mobility usage increases, so does the variety of threats and vulnerabilities for enterprise and government. Addressing security needs is paramount to delivering solutions that meet the demands of a mobile workforce. Verizon Wireless deploys a multipronged strategy for network security that combines the expertise and resources of our internal engineering teams, external software development partners and vendors of the various commercial applications and products we offer.

Verizon works behind the scenes to thwart malicious attacks.

The Verizon Wireless network security team works vigilantly to protect your data as it travels across our network. Our current network security capabilities include:

LTE security

Using the most advanced mobile broadband security architecture available (3GPP Specification 33.401), Verizon protects your privacy on five different levels:

Firewalls and routers
Taking advantage of software- and hardware-based tools to filter traffic between the internet and the Verizon Wireless network, we apply intelligence to identify and prevent hackers, viruses and other threats from affecting the network. Each router is configured with a specific list of permissions, which regulates network access. These tools allow the network to continue performing at a high level while guarding against malicious attacks.

Domain Name System (DNS) analysis
Some data thieves exploit unsuspecting users in an attempt to create botnets with their devices. These botnets perform automated tasks on behalf of the data thieves without the user's knowledge. Verizon uses sophisticated DNS analysis tools to stymie would-be attackers.

Internet and mail analysis tools
Verizon uses complex software tools to strip out malicious attachments that are sent to a user's SMS/MMS mailbox. Network-based anti-virus protection helps stop phishing scams and other malicious activity.

Intrusion detection systems
Verizon constantly monitors the network for malicious traffic. If suspicious traffic is detected, a team of certified security professionals investigates, analyzes and remediates the threat.

Risk management programs
Verizon Wireless conducts a prelaunch security risk assessment for all branded applications and devices, as well as all internal applications and devices. This program uses third-party security professionals to identify security weaknesses and help make devices more bulletproof.

Vulnerability management program
Verizon continuously monitors and secures its wireless network. We create a stable and secure environment by implementing a four-stage model.

Why Verizon

Your organization expects performance, reliability and security from your wireless network. The increasing numbers of factors that are beyond your control heighten that expectation.The security team at Verizon Wireless works tirelessly behind the scenes to keep the network running while monitoring, identifying and eliminating security threats and malicious attacks before they reach a single mobile device under your supervision. Our reputation for reliability and peak performance depends on the security of our network. Our sophisticated security infrastructure utilizes firewalls, routers, monitoring systems, software, device standards and security expertise to keep mobile communications and data out of the hands of hackers and data thieves, so you can keep your workforce productive, connected and mobile.

Choose the best network.

The service is one part of the equation for helping your business. A widely available, stable wireless network is the other. That's why it makes sense to choose America's largest 4G LTE network: Verizon Wireless.

1 IDC study, *U.S. Mobile Worker Forecast, 2015-2020.*
2 http://www.computerweekly.com/news/2240180185/Employees-ignore-security-rules-say-infosec-pros
3 2016 NowSecure Mobile Security Report, https://info.nowsecure.com/rs/201-XEW-873/images/2016-NowSecure-mobile-security-report.pdf
Network details & coverage maps at **vzw.com**.
SB01870716