Verizon Wireless Private Network

Take control of your network with Verizon Wireless Private Network and 4G LTE.

verizon

Wireless devices challenge control.

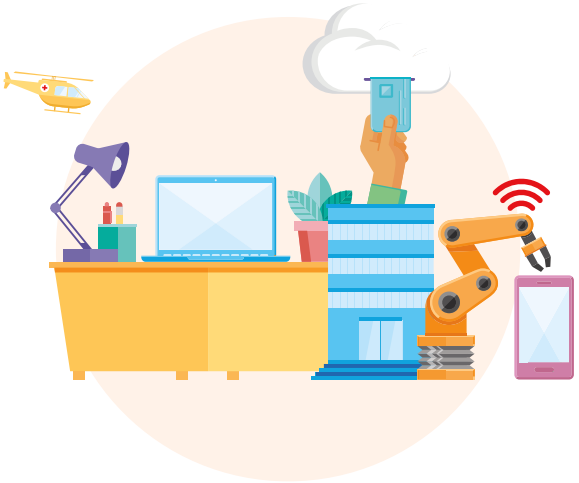
As networks evolve, companies need to manage risk.

More wireless devices are being added to the workplace every day and are challenging organizations to safely integrate these devices into their infrastructures. Depending on the role, these devices can be used to do anything from accessing email to managing a generator. But any change to an IT network can introduce potential vulnerabilities and weaken the security posture of the company. Companies have invested time and resources into maintaining the integrity of computing networks. As the modern network footprint changes, they need a solution that delivers the same level of management and control over their wireless networks that they have over their IP networks.

Verizon Wireless Private Network is a comprehensive solution that joins wireless devices to the company's internal IP network using a dedicated connection that isolates data from the public Internet. It extends a corporate IP network to wireless devices, while enabling IT to maintain the control and manageability that they need.

With Verizon Wireless Private Network, companies can take charge of their evolving networks by:

- Avoiding the exposure of wireless devices and internal networks to the inherent risks of unsolicited public Internet traffic.
- Controlling which wireless devices can connect to the network.



- Controlling which network resources the wireless devices and machines can access.
- Leveraging the convenience of mobility and wireless to introduce new opportunities.

The network footprint is evolving.

Networks look and behave differently now that wireless devices and machines have been added into the ecosystem.

The increasing number of wireless devices that are accessing mobile networks worldwide is one of the primary contributors to traffic growth. Each year, several new devices in different form factors, and with increased capabilities and intelligence, are being introduced into the market. By 2017, there will be 8.6 billion handheld or personal mobile-ready devices and 1.7 billion machine-to-machine (M2M) connections (e.g., GPS systems in cars, asset-tracking systems in shipping and manufacturing

sectors or medical applications making patient records and health status more readily available, et al.).[1]

Mobile data traffic will reach the following milestones:

- Monthly global mobile-data traffic will surpass 10 exabytes in 2017.
- The number of mobile-connected devices will have exceeded the world's population in 2013.
- Due to increased usage on smartphones, handsets will exceed 50% of mobile-data traffic in 2013.[1]

The number of wireless devices used by employees—smartphones, tablets, notebooks, printers, routers, monitors, keyboards, data-storage devices and more—is exploding exponentially. Add that to the number of new wireless devices those companies can use to improve operational efficiency and customer service, such as vehicles, ATMs, kiosks, appliances and machines. Enterprises are faced with the control, management and security issues that go along with an evolving IT infrastructure.

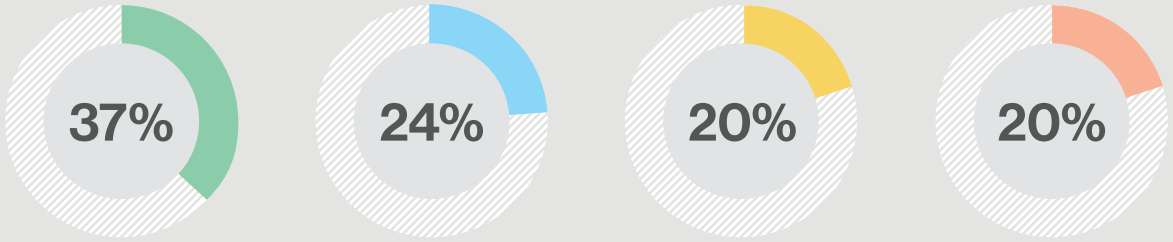
The value of Private Network

Avoid the risks associated with unsolicited traffic.

All data sent from devices configured for a specific Private Network is segregated from all other traffic. No unauthorized traffic can travel over this network, eliminating the risk of unsolicited traffic from external sources.

There are many different wireless device types that businesses employ today for a variety of solutions. As businesses grow and evolve, these devices are becoming integral parts of their operations and infrastructures. IT organizations are faced with the challenge

The *2013 Verizon Data Breach Investigations Report* revealed some important insight:



No industry is impervious to attack. Network intrusions occur across a broad range of industry sectors, including retail, manufacturing, food services, professional services, finance, transportation and utilities.

of determining how best to integrate wireless devices without exposing unnecessary risk.

Unsolicited Internet traffic is data sent to a wireless device that was not solicited by the wireless device owner. This data could be a result of random queries from unknown third parties, or it could be malicious in nature, attempting to cause a service disruption. Either way, it is critical to understand how this could impact a business.

Unsolicited traffic without malicious intent
Even though there is no identifiable malicious intent, it does not mean there is no cost. For example, if an M2M device is being pinged by an external source, it takes time and resources to investigate, and potential corrective actions are limited.

Unsolicited traffic with malicious intent
This type of traffic is meant to be negatively disruptive. This could cause downtime, reduced productivity, lost revenue and more.

Unsolicited traffic can be dangerous. Although businesses take precautions to ensure critical assets are not accessible by external sources, any change to the network footprint adds risk. Organizations can block unsolicited traffic by attaching to the Verizon Private Network in one of three ways: Verizon Private IP, VPN over Internet or a dedicated circuit. Of the three options, Verizon Private IP provides a complete, end-to-end, enterprise-class system from one provider, capable of supporting connections from multiple customer locations.

Control which wireless devices can connect to a network.
IT organizations need to know what is connecting to their networks in order to understand how to maintain the integrity of their networks. Wireless device utilization is making this increasingly difficult, not only because it's increasing year over year, but also because companies need to expose internal services to maximize the benefit of these devices.

The statistics speak for themselves. Wireless devices are penetrating every aspect of business from remote tools for users to infrastructure components. IT isn't always aware of which endpoint is connecting and to whom it belongs. This makes it difficult to understand where the end of a network actually is.

In order for IT to deliver viable services to users or its business via wireless devices, some sort of connection needs to be made. The downside is that the connection often exposes internal services to the external, connected world. Best practices can be followed to ensure the proper security is in place, but it's still difficult to control what's being connected.

Access only what you need.
Private Network sends all of the data through the Private Network to the company's network for handling. This includes everything from the Internet to application requests.

Common IT best practices are to allocate only the resources and permissions that are needed. Doing so protects networks by eliminating unnecessary exposure to incidents caused by threats or mistakes. Private Network enables companies to control not only what

The *2013 Verizon Data Breach Investigations Report* revealed some important insight:

92%

In 2012, 92% of threats—malicious or nonmalicious, intentional or unintentional, causal or contributory—to enterprise data came from external sources.

internal resources wireless devices can connect to, but also what mobile-to-mobile connectivity is allowed. This allows them to deploy wireless solutions and retain control over all of the data from the device.

For example, if a device is used for a specific application, it should access that application only. This protects a company if the device is lost, stolen or otherwise compromised. Controlling what it can access also helps to dictate the security requirements needed on the wireless endpoint.

Private Network in action

Corporate email servers

Corporate email servers provide an easy example of the considerations for expanding a network to include wireless devices. A company can expose an email server to provide remote access to email and calendars, but can it limit the devices that can connect to this service? Now, think about a more critical operation or service, such as a point-of-sale system. Would it be a best practice to expose that type of service to a network without access control?

Device authentication

When a device is authenticated to the network, it is recognized as a Private Network device. Traffic is routed to an access point predefined for the company and the network is instructed to send all data to a connected wireless gateway.

Companies determine what devices can connect to a private network. Doing so provides a level of network control for wireless devices that has previously been reserved for internal, wired IT assets. Controlling what can connect limits threats and helps IT maintain network integrity.

The *2013 Verizon Data Breach Investigations Report* revealed some important insight:

52%

Fifty-two percent of network data breaches are due to hacking.

4/5

Authentication-based attacks (guessing, cracking or reusing valid credentials) factored into about four of every five violations.

The convenience of mobility and wireless creates opportunities.

One of the reasons that wireless device utilization is on the rise is because of the mobility and convenience that it offers. The lack of a physical connection combined with the speeds available with Verizon Wireless 4G LTE are helping create new opportunities and reduce the time required to implement solutions.

Private Network extends a corporate IP network so companies can get the benefits of wireless without compromising on control. Private Network setup and configuration is simple. There is no need to purchase or install additional clients or deploy and manage device-level configurations to establish and maintain connectivity. Once Private Network is established, compatible devices can be activated quickly and easily. That means it is completely scalable and will grow with the business. And it reaches anywhere the Verizon Wireless mobile network does.

Private Network offers businesses a way to isolate data from the public Internet, removing the potential for unsolicited requests and attempts to access the corporate network. Example use cases include:

- Meeting industry-specific regulatory mandates
- Mobile and wireless access to corporate networks for road warriors, field workers and those working at temporary locations, such as construction sites, conventions or mobile medical centers
- M2M ecosystems that send and receive critical data, including pumps, generators, oil rigs and other operations that should not be connected to the public Internet
- Residential and commercial security monitoring systems
- Utility smart-grid infrastructure
- Any challenge that can be solved by connecting to an IT network

The convenience and ease of deployment associated with wireless makes it possible to connect wireless devices when on the go, introducing endless possibilities. Companies aren't limited to making existing connections wireless, but can look at new ways to leverage connectivity.

Enhanced features of Private Network

Private Network brings wireless devices into the company's IT network with features that deliver the level of management and controlit needs:

Dynamic Mobile Network Routing (DMNR), only from Verizon, is a network-based mobile technology that makes the management of wireless devices comparable to wired device management.

DMNR allows companies to remotely access IP addresses of devices that are connected to a Private Network, through a wireless router, for easier support and management.

Parent/child relationship support uses tiered hierarchy and closed user groups to separate the billing and data for departments or companies with parent/child relationships.

It allows the financial cost to be attributed to the correct company or department. This creates the opportunity to model a private network after a business or supply chain.

Self-service capabilities allow users to take immediate action via different portals—My Business Account, Verizon Enterprise Center and the Machine to Machine Management Center—to provision and manage Private Network devices.

Self-service reduces the time required for the management and administration of Private Network devices. Companies can take action, as needed, when needed.

The Service Based Access option allows customers with Private Network–eligible 3G devices to track mobile devices as well as access Visual Voice Mail (VVM) and Multimedia Messaging Service (MMS) on 3G smartphones. Subscribers can locate Open Development–certified 3G devices, as well as track fleets and other high-value assets using Verizon assisted Global Positioning System (aGPS). Service Based Access provides access to VVM on 4G LTE smartphones. Service Based Access 4G LTE does not support aGPS and it is not required for MMS.

Expand your network with Verizon Wireless Private Network.

With Verizon Wireless Private Network, line-of-business operations and employees can connect to the network from more places, while keeping IT firmly in control of management. Businesses can add devices to their own internal networks, with their own IP addressing, to be managed by their own support personnel. This empowers them to make wireless solutions part of their infrastructure and extend their core-computing networks farther, faster and easier.

With Verizon Wireless Private Network, there's no need for complicated device configuration, no need to worry if the connection is on or off and no complicated support practices. And companies can be confident knowing that their private network is backed by the coverage, speed and reliability of Verizon Wireless. Verizon can help businesses make the most of wireless communications to securely and cost-effectively power their networks.

1 *Cisco Visual Networking Index™: Global Mobile Data Traffic Forecast Update, 2012–2017.* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

Service Based Access is not supported for customers utilizing Closed User Group, Zero Tunnel Private Network features or Virtual Customer Private Network.

Network details & coverage maps at vzw.com.

SB02690316

Learn more.

To learn more about Verizon Wireless Private Network, contact your Verizon Wireless business specialist or visit us at **VerizonEnterprise.com/contact-us.**