Vonage® Business

BYOD IN 2018:

TOP TRENDS & BEST PRACTICES

INTRODUCTION

The ability to work on the go, or mobility, is so interwoven in the fabric of a business day, that most employees would be shocked to know that less than 20 years ago, working meant working at a desk. With this in mind, one of the latest trends in mobility is the idea of BYOD (bring your own device).

BYOD is often referred to as a mobile specific phenomenon. But in reality it refers to multiple devices including smartphones, laptops, tablets and in some cases even wearables like smart watches.

It's no surprise that BYOD has become so popular. The average worker already owns a smartphone, a laptop and a tablet, or all three. In many cases, employees are happy when a company has a BYOD policy allowing them to utilize their own technology for business purposes. One recent study shows that 72 percent of organizations are either using or are planning to allow employees to bring their own devices to work. The BYOD trend is clearly here to stay. While integrating BYOD into your communications systems is not hard, there are some protocols a company can take to ensure the best ROI, employee adoption and set up for scalability and privacy. This ebook outlines some of the best practices a company should take before they institute a BYOD policy.

Learn the benefits of BYOD for both employees and businesses, and find out how to roll out a BYOD policy that will empower your employees, maintain the integrity of your communications infrastructure, and benefit your bottom line.

CHAPTER 1:

BRING YOUR OWN DEVICE, NOT YOUR OWN HEADACHE: BYOD IN THE CLOUD

Employees want BYOD. Companies like the BYOD cost savings benefit. It should be a win-win situation. But there are some scenarios when a BYOD policy can be fraught with challenges—particularly if the business uses a traditional phone system that doesn't integrate with mobile devices. Fortunately, the route to a productive BYOD policy can be simplified when companies utilize a full-featured cloud communications phone system.

What to Expect With a Traditional Phone System

BYOD is possible when a business communications system is based in traditional landline providers. However, this route can be more costly and more cumbersome. Because it's more difficult to connect a personal mobile device to a traditional premise based phone system, it's likely your employees will simply use their personal numbers. If the employees uses their own mobile plans for business purposes your business loses control over the security of your company data while your employee is happily employed. What's worse, when they leave, your business has no way of ensuring your data, leads and clients don't leave with them.

Why BYOD in the Cloud is Better

With a cloud-based communications system, mobile employees can make and receive calls (and possibly text messages) via an app on their mobile phone. Caller ID indicates that the call is from the business, and employees can access the same calling features they enjoy back at the office. This is referred to as mobile integration: the seamless convergence of the company's business phone system with the employee's mobile device. And it's a huge advantage offered by cloud communications phone systems:

Your Employees Always Have a Professional Presence: Using a cloud-hosted mobile app, your employees' calls on their mobile phones appear on caller ID as a call from the business, not from the employee's personal account. This can also apply to text messaging, an increasingly popular mode of business communication.

Access to Robust Business Calling Features: When mobile solutions are integrated with the business phone system, on-the-go employees can access calling features as if they were in the office.

Employees Have Privacy Protection: There's no reason mobile employees should have to reveal their personal phone number on caller ID when doing business. Communicating through a business mobile app reveals their business phone number only.

Your Business Has Control Over Your Communications Security: Using security software like VPN for laptops and EMM for mobile devices, your business can create safeguards to protect your employee's work from potential threats.

Tracking Ability: With cloud-hosted phone service, integrated mobility enables the company to easily track the call activity of mobile employees, so you know they're working even when they're out of the office.

Building Better BYOD

When shaping a BYOD policy, integrated mobility from a cloud communications system can drive many benefits, including employee and customer satisfaction. With a mobile solution like Vonage Business Cloud Mobile App, a company can boost productivity and create a seamless, unified communications experience across devices: desk phone, desktop, laptop, mobile phone or tablet.

Most of all, a cloud phone system can turn BYOD from a challenging policy into a major advantage for any sized company. By empowering your mobile employees with a professional business appearance and feature-rich phone system functionality, they can effectively connect with customers, vendors and one another—wherever the business takes them.

CHAPTER 2:
10 BYOD BEST PRACTICES FOR BUSINESSES

BYOD, or "bring your own device," policies are increasingly typical at businesses today. The BYOD market is on track to reach around $318 billion by 2022—showing major growth from around $64 billion in 2012[1] BYOD delivers many advantages, reducing IT expenses while allowing employees to use the technologies that work best for them. It's a particularly powerful tool for connecting virtual or remote teams and offices.

But you need BYOD best practices in place to make sure that it works best for all involved. Here are 10 considerations for creating a policy that protects the company while still boosting business productivity and supporting a better work-life balance for employees.

When approaching the question of how to create a BYOD policy, it's always best to strike a meaningful balance between employee productivity and business security.

10 BYOD Best Practices

1. **Lay the Ground Rules:** First and foremost, you'll need to set clear eligibility criteria for the program. This includes how much—if at all—the company will pay toward each device, which types of devices will be allowed, who is eligible to participate in the program, and what sort of availability they're expected to provide the company. Be sure to consider smart devices, such as smart watches, that employees may also want to use. All employees participating in BYOD should sign an agreement indicating they understand the policy and will comply with it.

[1] Crystal Market Research

2. **Go to the Top:** Make sure all executives are covered by your BYOD policy. They're likely to be enthusiastic mobile-device users, and chances are good that they're viewing and exchanging privileged business information that needs to be secured. In order to properly manage the risk that their mobile-device or smart device use presents, it's wise to take special care to include executives when rolling out BYOD at your workplace.

3. **Great Internal Marketing:** Providing clear, consistent communications to all employees about what to expect is essential for success with BYOD, both during the transition and afterward, as well as when new employees join the company and need orientation. By proactively managing change during the crucial moment of transition to BYOD, your company will be better able to ensure enthusiasm among employees and, in turn, enhanced long-term productivity.

4. **Start on the Same Page:** If you're launching BYOD for the first time, make a point of reaching out to wireless providers well before launch so you can secure better company rates. After your organization has been up and running with BYOD for a short while and has worked out any kinks that may have arisen during implementation, you can work with providers to refresh company discount rates and let them know that employees are going to be shopping around for the best prices on devices.

5. **Take Precautions:** Proper security is a must under BYOD, as employees' mobile devices will be connecting directly to the company's systems. With that in mind, ensure that any participating devices are secured with strong, regularly updated passwords and best practice authentication methods such as two-factor authentication. If your company has an existing password policy, make sure employees' devices are in compliance—and if your company doesn't yet have a password policy in place, now would be an ideal time to create one.

6. **Stay Current:** Likewise, you'll need to ensure that any participating devices are consistently patched with the latest software updates and are as carefully managed as any business-owned smartphone, tablet, or computer would be. Employee devices that are left running outdated or insecure versions of their operating systems or applications pose a security risk to the company.

7. **Know Your Networks:** Devices shouldn't be allowed to connect to insecure, open wireless networks. If you have an existing information security policy that specifies this restriction in writing with regard to company-owned devices, make sure participating BYOD users adhere to it as well.

8. **Back it Up:** One of the most important BYOD restrictions involves the ability to remotely wiping devices in the event of loss, theft, or unauthorized access. There are options available to wipe only company data that resides in the EMM application, or the entire device. Employees should be advised that they're responsible for backing up their devices on a regular basis so that they don't lose any important data in the event that this occurs. The cloud-based email and calendaring services that come with a cloud communication system can be helpful in just these sorts of scenarios, since they automatically back up employees' calendar and contact data.

9. **Endpoint Management:** When developing a BYOD policy, make sure that your IT team has the right tools in place to make it work. This includes enterprise mobility management (EMM) or mobile device management (MDM) systems, which put the security-related aspects of your policy—for example, remote wiping—into practice. You may also want to ensure that, with regard to wireless network security, you take advantage of virtual private network (VPN) solutions that allow your laptops and mobile devices to connect securely to company resources from remote locations.

10. **Set Boundaries:** BYOD, it should be noted, is not the same as Bring Your Own Cloud (BYOC). Although you're granting employees the ability to use mobile devices at the workplace, that doesn't mean you've automatically permitted them to deploy and use their own cloud software for work purposes without proper vetting and a green light from IT. Because this form of shadow IT can result in unintended consequences such as data breaches or worse, it must be addressed in your BYOD policy so that expectations are clear from the beginning.

When approaching the question of how to create a BYOD policy, it's always best to strike a meaningful balance between employee productivity and business security. By following these BYOD policy tips, you help ensure a smoother and safer rollout so that both the company and its employees are able to enjoy the many benefits enhanced mobility offers.

CHAPTER 3:

WHY YOUR EMPLOYEES WANT BYOD

Smartphones, laptops and tablets are not just business tools, they are multi-tasking consumer toys that people want for personal communication, social media engagement and entertainment. For many, they are even an electronic extension of personality. With this logic, it's not surprising that 53% of employees say using their own devices boosts productivity.[2]

Keeping your employees happy and productive is key to positive corporate culture and booming bottom line. Here's a three reasons why BYOD can help.

Employees Like Choice

People are a creature of habit. One of the benefits of BYOD is that employees can use the technology they feel the most comfortable with at home, at work. Ramping up on a new platform, type of phone or laptop is not impossible, but it can be annoying. And as new technology savvy generations join the workforce, they come to employment with strong opinions on what they consider best. Allowing them to exercise their choice is an easy way to build loyalty.

Employees Like Perks

BYOD policies often involve having the company pay for part of their personal cell phone plans. That combined with employee discounts on many of the major carriers can add up to what may be seen as a significant employee perk

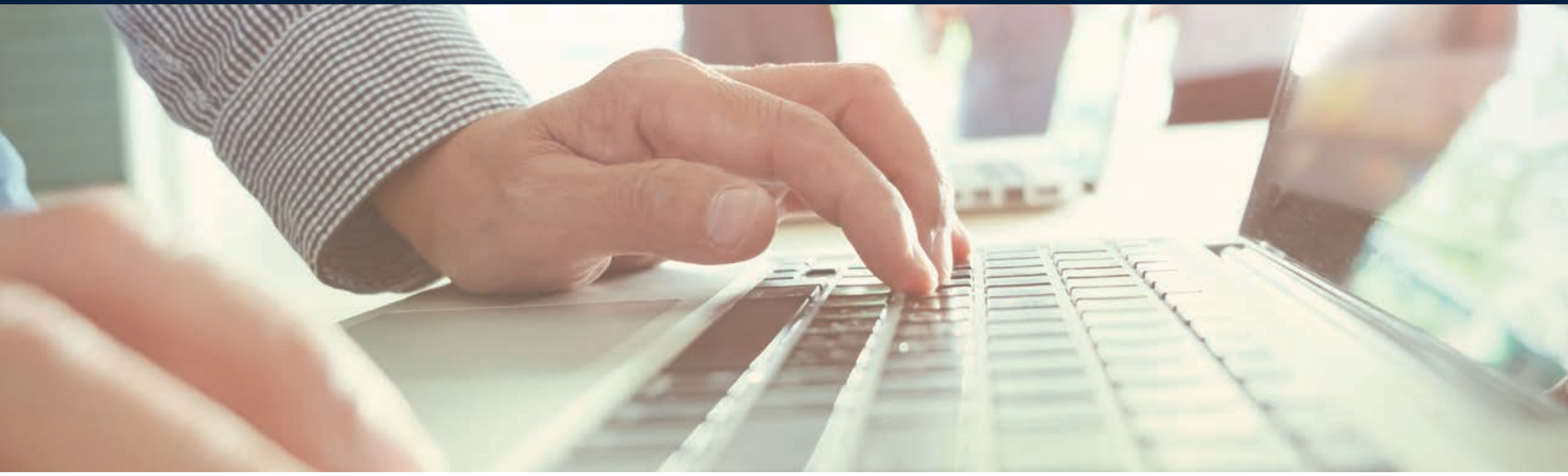
Employees Like Convenience

Company issued devices once were seen as a perk. However, today most employees have their own smartphones, laptops and tablets. Rather than a benefit, having a company issued device can be seen as an annoyance or even a stress. Two phones? Two tablets? Two laptops. Today's employees don't feel the need for extra technological clutter—not when they can easily use a mobile app to turn a personal phone into an business number or log in to the office crm via a VPN from their personal laptop.

The impact of BYOD is not just the significant financial incentive to your business. BYOD also can do a lot to making your employees feel valued and be more productive.

53% of employees say using their own devices for work boosts productivity.

[2] Executive Enterprise Mobility Report



CHAPTER 4:

ENDPOINT MANAGEMENT: HOW AN EMM SYSTEM CAN HELP

The integrity of the private and confidential information and business data that resides within your business technology infrastructure is one of your most important resources. Protecting that data from being deliberately or mistakenly stored on insecure personal devices, and/or transmitted over insecure networks, where it can potentially be accessed by unsanctioned resources, is critical. A breach could mean the loss of confidential and/or proprietary information and damage to critical applications—not to mention loss of revenue and a PR nightmare. But when your employees are using their own devices, there's a chance you can lose control.

What's the Worst That Can Happen?

When a person loses a device, there's always the worry of losing personal data that could have sentimental value like personal photos, as well as the worry about the cost of replacing the device. But when your employee loses or compromises a device that has business data on it, there are more ramifications. Here are some potential scenarios where an individual employees actions can impact the company:

- **Lost and Stolen Device:** A lost or stolen device can mean compromised or stolen company data
- **Malware:** Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device

What is Sensitive Information?

Confidential or sensitive information can be classified as information that is not publicly known. That can includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form like an email, a document, or a note. There are a few different types of confidential information that you need to protect.

- **Information Relating to Your Business:** This might include source code, designs and plans, beta and benchmarking results, patent applications, production methods, roadmaps, customer information, prospect information, promotional plans and competitive information.
- **Private Employee Information:** This might include names, salaries, skills, positions, pre-public financial results, and organizational charts.
- **Third Party Information:** Confidential information also includes any information received by your company from a third party under a non-disclosure agreement.

How Does EMM Work?

Enterprise Mobility Management (EMM) application is a unified way to ensure that an employees mobile device allows your employees to function in a secure environment.

Think of it like this.... Your company communications are contained in a virtual room. The device is a door to that room. All the work that happens in that virtual room is protected. Regardless of where the employee is located, the work is actually happening in that private, secure space.

Your IT always has access to that room. They can open or close the door. And if, something funny happens—like a device is lost or stolen, they can delete the contents of that room so intruders don't have access. And when an employee is terminated, IT has the ability to remotely remove company-only data from a device after the employee termination.

What To Look For in an EMM System?

Of course, your EMM system should be unified, flexible and secure, but here are a few other things it should be able to do to ensure it fits within your company culture:

- **Support Different Technology and Platforms**
  One of the benefits of BYOD is that employees can use the technology they feel the most comfortable with. Your EMM platform should support Apple aficionados and Android fans alike.

- **Support End Users Quickly**
  Like any business technology your BYOD will only be compliant if users can easily adopt it and get support. If support issues interrupt their ability to do their job, they will rebel.

- **Keeps Up with the Latest Updates**
  Technology is constantly evolving. Your EMM system needs to keep up or again employees will look for other less secure but simpler options for the business communications.

- **Have A Secure Log In**
  Having a strong password policy and even two factor authentication is imperative to ensure only authorized users are accessing these personal devices.

- **Have A Back Up Plan**
  In the event of a lost or stolen mobile device it is important that employees understand what to do. They should know to report the missing device as soon as possible and have a clear point of contact 24/7, 365 days.

When you think about it, your employees do business with the help of a wide variety of mobile computing devices. Mobile work can happen on laptops, notebooks, tablets, PDAs and other hybrid devices, wearables, and all portable storage media, including flash drives, smart cards, tokens, etc. That's a whole lot of other devices out there that need to have top notch security. An EMM system is definitely a core part of making sure your company and its data stay safe—no matter what device your employees chose to use for work.

CHAPTER 5:

HOW BYOD AFFECTS YOUR BUSINESS FINANCIALLY

Employees love BYOD because it allows them to utilize the technology and platforms they feel the most comfortable on. In fact, many employees have come to see mobile phone reimbursement as an employee benefit. But beyond employee satisfaction, here are some sound business reasons to pursue a BYOD policy.

Device Acquisition Savings

Let's start with the most obvious cost savings—the cost of hardware. Devices. Laptops, smartphones and tablets can suck up a large portion of your operational budget. You want your employees to be using the most up to date technology tools. Today, a two year old device can be lacking in performance and features. Plus, since most upgrade cycles are in the range of two to three years, the general feeling is that beyond two years a device is both "old" and bordering on obsolete. Since employees already are in the mindset to upgrade within that one to two year cycle, a BYOD policy means your business is sharing the cost of the initial purchase and keeping pace with innovation through upgrades.

Service Provider Savings

BYOD allows your business to include cell phone and data plans as an employee benefit. You may be able to draft your policy so that more senior staff are offered a larger or full reimbursement—do some research to find out what works for your company. And keep in mind that for the majority of your company, you'll probably be able to pay a percentage of their bill rather than the whole bill, which would be the case if they were issued a company cell phone. This adds up to cost savings.

Half of employees who left their jobs in the last 12 months kept confidential corporate data—and forty percent of those planned to use it in their new jobs.

Cloud Savings

Businesses employing traditional phone systems may choose to purchase separate mobile accounts for mobile employees, or even separate devices. Within the cloud environment, however, separate accounts aren't necessary—mobile apps integrate the employee's device with the business communications system. That's both a cost savings to your business and to your employee.

While, BYOD has many financial benefits, the picture is not completely rosy. Security breaches because of human error or malevolence could cost your business a bundle. However, if you properly protect your business, you can protect your company data from breaches and financial losses.

Cost of Losing Leads & Business Opportunities

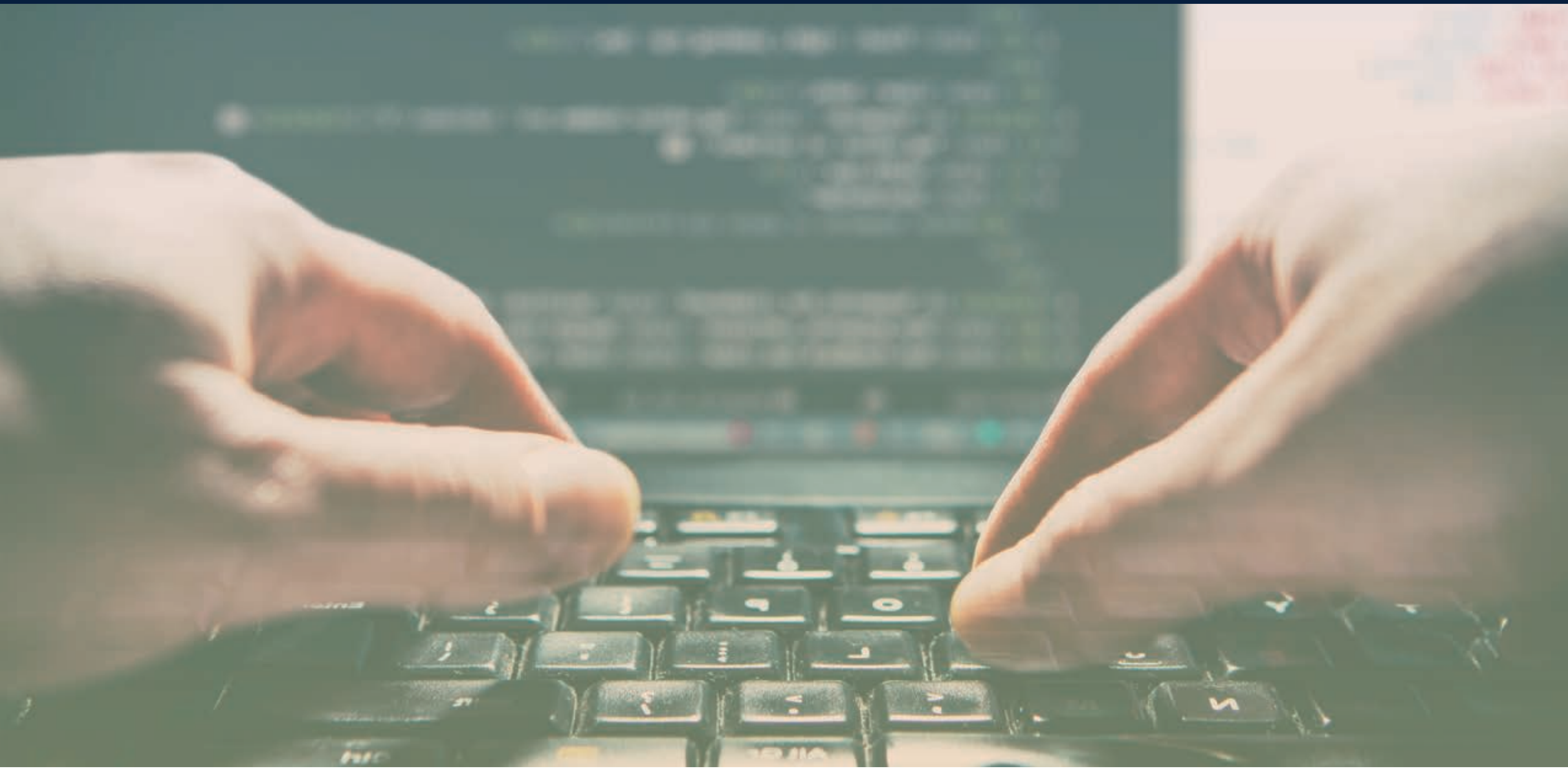
According to a global survey from Symantec, half of employees who left or lost their jobs in the last 12 months kept confidential corporate data[3]. Even worse, forty percent planned to use it in their new jobs! Without a strong BYOD policy coupled with security measures, it could be easy for an employee who is leaving a company to keep business contact information, if the device is a personal device without an EMM in place, as those business contacts may be co-mingled with the employees' personal ones. But this data goes beyond business leads' phone numbers—it could include sensitive emails and other internal company documents, including third party information. The cost implication runs from lost business to potential legal action if for some reason private information is leaked.

Cost of Data Breach

Security remain the major challenges around BYOD implementations. Lack of compliance with BYOD policies and human error (loss of phones) open up your company to the risk of your most valuable assets—your data. According to the 2017 Cost of Data Breach Study from the Ponemon Institute, sponsored by IBM, the global average cost of a data breach is $3.6 million[4]. BYOD is not the culprit for all of these security instances. However, remember, every unprotected device opens your business up to potential data and public relations catastrophe. A strong BYOD security system with the ability to auto-lock and remotely wipe devices, and a strong password policy can decrease your risk revenue loss from a data breach.

Data breach is always a business risk even without BYOD. But with proper security and employee compliance, your company should be able to reap the financial benefit of BYOD. That means, not only will your employees be happy, so will your bottom line.

[3] Symantec Press Release



CHAPTER 6:
BYOD & VPN

What is a VPN? This question gets asked more and more as the uncertainty of web privacy looms large. On a very basic level, a virtual private network (VPN) is a technology that lets you secure network communications from prying eyes.

What Is a VPN?

A VPN is technically just a rerouting and encryption of your normal network communication. In a traditional network setup, every time you browse the web, packets of information are sent and received between remote hosts, whether it's websites, file downloads, or cute cat videos.

This traffic typically takes a route from your computer through your ISP to a predetermined route across the globe to its final destination. Communication this way is completely out of your control once it leaves your network. This leaves it vulnerable to hijacking or snooping by unauthorized users. Think of it like chatting with your buddy down the street on those old walkie-talkies. By simply changing channels, you can waltz right into another person's line of communication and listen in, due to its use of public bandwidth.

With a VPN, instead of communicating through public channels, you create a private, encrypted line of communication directly to your destination—primarily through secure shell (SSH) tunnels. In essence, you use the Internet in an intranet setting, free from prying eyes and cybercriminals.

When are VPNs Most Frequently Used?

Though net neutrality and privacy concerns may have sent the consumer market searching for VPN solutions, the enterprise arena has been at it for some time now. Similarly, while consumers look to a VPN for anonymity, the business world is in it for other reasons—chief among them, security.

How does this enable BYOD? VPN can be an important tool for keeping your company data safe no matter where your employees are logging on. Using VPN, an employee can log on to the company network from their home office, a client meeting, or even the local coffee shop and your data will be protected.

VPNs are particularly easy to deploy in cloud-based environments. All that's needed is a VPN server—the brains of the operation—and clients for each device.

Think about it this way: You wouldn't want someone looking over your shoulder as you type your PIN into the ATM, would you? And yet that's exactly what so many organizations do with network communication, whether it's chatting over VoIP connections or leveraging instant messaging for office chatter. Because of this, enterprises can use VPNs as a way to secure communication between data centers, remote offices, and traveling users.

Do You Need a Degree in Cryptology?

As mysterious as a VPN may have once been, the technology is surprisingly easy to deploy. All that's needed is a VPN server —the brains of the operation—and clients for each device. All clients can be pointed to the server to automatically encrypt communications and keep sensitive data from falling into the wrong hands.

VPNs can be surprisingly flexible, too. In a basic setup, all network traffic is encrypted and rerouted to the VPN server. However, other setups do exist. For example, perhaps your organization only sends sensitive communications across a very specific application or ports. A VPN solution can be set up to only tackle that specific traffic, while all other network communication takes its normal path. Since the encryption, routing, and oversight of traffic through a VPN is only as good as the curator of the server or service, you'll want to choose your vendor wisely.

With a definitive answer to the question, "What is a VPN?" in mind, it's time to take the next step. Whether you're building your own VPN tunnel or spinning up a prepackaged solution, securing your organization's communication and establishing your company as a virtual enterprise has never been so important or easy to do.

CONCLUSION

GET STARTED TODAY

Do you have the mobility tools in place to support a secure BYOD policy?

Empower your employees. Support your IT. Protect the integrity of your organization's data. A well thought out and executed BYOD system creates a corporate culture that can help your employees to thrive and your business to grow.

Contact a Vonage Mobility Specialist Today.

1.844.771.1267 | vonage.com/business