WHITE PAPER

Neverfail

Neverfail Workspaces: Add Secure Remote Access & BYOD with Improved Security

A proven method for establishing secure IT environments that gives authorized personnel access to the tools they need from any device in any location.

Contents

Executive Summary

Security continues to be a major challenge for every type of business, including healthcare, finance, and legal services where regulatory compliance is also an important factor. New threats like ransomware can cost the business substantial amounts of money both directly and indirectly through their impact on operations.

People have come to expect that the professional IT systems they access to do their work will be as simple and easy to use as consumer products, while business owners and managers must be concerned about the security of their proprietary data. These goals are commonly in conflict, since “highly secure” rarely correlates to “easy to use”.

Neverfail Workspaces is a cloud- based platform that supports an intuitive user experience, remote access, Bring Your Own Device (BYOD), and other productivity-enhancing features, as well as enhanced data security.

The Neverfail Workspaces platform:

- Enables people working from home or on the road to access business-critical applications and data sources
- Offers end users the ability to use their own devices (BYOD), including tablets, without compromising data security
- Supports a wide range of deployment scenarios, including on premises servers combined with cloud-delivered applications.
- The platform also addresses the critical challenges associated with maintaining secure IT services. It provides increased visibility into who has accessed your data, and when, as well as enhanced protection from malware, and helps protect your systems from professional hackers. The system’s consumer-grade user experience also reduces the likelihood that individuals will attempt to circumvent security.

This approach also helps businesses save money by enabling them to:

- Continue using existing servers and client devices
- Eliminate the need to migrate sensitive data to new systems
- Greatly simplify configuration of new sites and new employees’ devices

The platform provides a full productivity solution that gives end users remote access to their applications and data without having to jump through hoops – and at a lower cost than legacy technologies like Virtual Desktop Infrastructure (VDI).

This paper explains the business benefits of deploying the Neverfail Workspaces platform and describes the most common deployment scenarios.

Workspace-as-a-Service is not only the best alternative to legacy tools, it offers improved security, a simplified user experience, and greater convenience for users.

Critical Security Challenges

There are four key features that platforms implemented in secured environment must address:

BYOD, Mobility, and Remote Access

Every type of organization is under pressure to operate more productively, including allowing workers to move around easily within a facility and to move between facilities while still being able to access all the information they need to do their jobs.

People working from home or on the road should be able to do productive work from any computer or tablet that happens to be available, without compromising system security.

Remote access and BYOD are closely linked since, in order to be effective and support good user acceptance, they cannot require special software to be installed on client machines or special configurations. Workers should be able to log in from any standard computer or tablet.

Enabling BYOD and remote access offer numerous business benefits:

- Increased productivity: Employees can now work anywhere and at any time, on the device that is most convenient for them.
- Improved employee satisfaction: Workers like being allowed the choice of using their personally-owned devices, which can eliminate the need for end users to carry multiple devices — one for personal use and one for business use.
- Cost savings: Organizations that support BYOD may not be required to buy and issue new devices to end users.

Obviously, the next big question is how to mitigate IT challenges and the organizational risks linked with BYOD and remote access, particularly in an environment that must maintain control over sensitive data. Key security risks with BYOD are:

- Application control: Uncontrolled and unsecured applications, including malware that could potentially hijack sensitive data, could be installed on the device by the user.
- Lost and stolen devices: End-user training for immediate reporting of loss or theft of a personal device with business access. The leading cause of data breaches continues to be the loss of physical devices containing sensitive data, and the increasing number of highly portable tablets being used within client organizations exacerbates this issue.

Addressing BYOD and mobility successfully while maintaining security above all requires that organizations implement systems that reduce or eliminate the possibility of any sensitive data residing on the device. If the device holds no useful data, even if it is misplaced or stolen, no breach has occurred.

People working from home or on the road should be able to do productive work from any computer or tablet that happens to be available, without compromising system security.

Logging and Reporting

A reliable audit trail is critical to establishing a secure IT infrastructure. In the event of a breach, an audit trail allows the organization to determine exactly who had access to the data in question, and how and when they accessed.

The logging system must record both failed and successful log-in attempts as well as log-outs to any areas that may contain sensitive data. The system must also log attempts at any malicious conduct, including malware infections and other attempts at disrupting services, as well as attempts to delete or modify the logs themselves.

Making employees and other users aware of the existence and capabilities of the logging system helps deter consciously attempted breaches as well.

Implementing a good logging system greatly reduces risk and helps the organization ensure the overall and should ensure that the requirements do not become unmanageable, overwhelming, or too expensive.

User Authentication

A secure system must verify that people seeking access to sensitive information are who they say they are.

In general, there are three accepted methods of authentication:

- Something you have: Smart card, token systems, or other unique physical identification
- Something you know: User ID, unique question/answer, personal ID number, and password.
- Something you are: Biometrics such as a facial image, finger image, voice scan, or iris or retina scan.

Nearly all security experts agree that, in order to provide the best security, IT systems should require something beyond simple usernames and passwords.

In addition, many experts recommend that organizations implement an authentication system that prevents authorized access from unauthorized locations or devices, or at unauthorized times of day and/or days of the week. For example, the organization may wish to prevent selected staff members from accessing systems containing sensitive data after business hours or on weekends.

Data Encryption

In nearly every circumstance, businesses concerned about security should encrypt all sensitive data both at rest and in transit. They must also take care to utilize documented, carefully thought-out methods for ensuring that all such data is encrypted and that relevant software and decryption keys are stored in such a way that only authorized personnel can access the encrypted data.

There are numerous encryption systems available, but many are burdened by significant challenges of their own, including increased latency, higher costs, and increased complexity.

Choosing the appropriate encryption system that fits the unique needs of the business is critical for keeping productivity as high as possible while enjoying increased protection and overall security assurance.

BYOD: Why It Matters

BYOD is one of the most significant trends in the IT industry today.

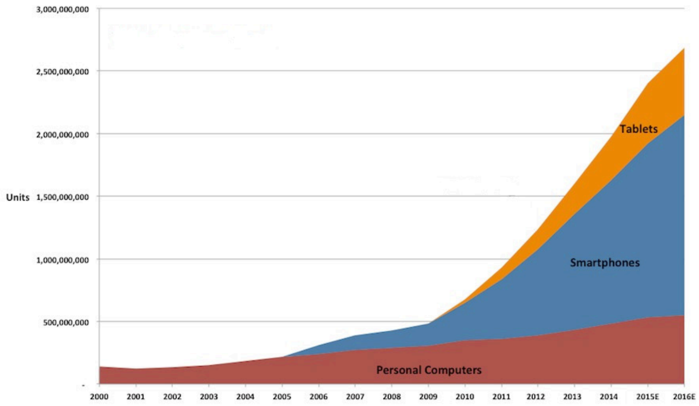
The evidence for this is clear: A recent Tech Pro Research report found that 72% of organizations polled were already permitting BYOD or were planning to do so. Gartner predicts by 2017, 50% of employers will require employees to supply their own device for work purposes, and a further study by Juniper Research concluded that by 2018, there will be more than one billion devices used in BYOD programs worldwide.

An IDC survey of 508 US-based companies found that more than 90% had employee-owned devices that were accessing corporate data. In other words, nearly every organization in the US is confronting some form of BYOD in their work places already, whether they have policies and appropriate security safeguards in place or not.

The primary drivers behind the BYOD trend are cost savings, employee satisfaction, and productivity. However, as CompTIA reported in their Trends in Enterprise Mobility study, cost savings were not the most important factor for 66% of businesses; they were more a by-product of a BYOD project, while productivity improvements are the core focus, as shown in the chart on the right:

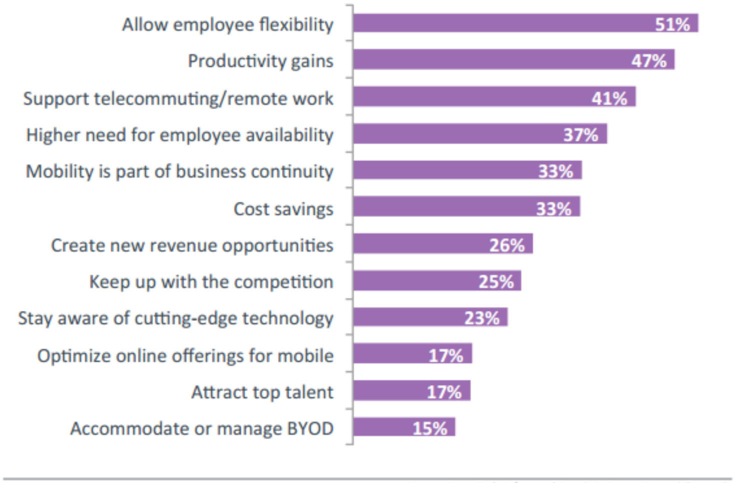
The greatest barrier to adopting BYOD is security, followed closely by compliance issues, and these challenges are further compounded by the fragmentation of the mobile operating system market. The release cycle of new versions of operating systems is measured in months instead of the average three-year refresh cycle of Windows in a desktop PC.

Global Internet Device Sales



Source: Gartner, IDC, Strategy Analytics, company filings, BI Intelligence estimates

Drivers for Mobility Adoption



Source: CompTIA's 3rd *Annual Trends in Enterprise Mobility* study
Base: 400 U.S. end users

This pace of change and the fragmented market complicate things for MSPs that do not have the right tools and architecture at hand.

In 2015, Aruba Networks, part of Hewlett Packard Enterprise, surveyed over 11,500 workers across 23 countries worldwide to learn about security threats created by today's mobile workforce. The study suggests that businesses are not nearly as well prepared as they should be for the explosion in use of mobile devices, and the increasing demand for remote access, with over a third (37%) of businesses not having any type of basic mobile security policy in place.

Software Advice, a Gartner company, found that only 39% of organizations have a formal BYOD policy, and another 20% aren't sure whether their organization has a policy or not. But as Software Advice notes, "employees will find a way to use their own devices, no matter what." This lack of preparation creates significant business opportunities for MSPs that can deliver affordable, easy-to-use BYOD capabilities suitable for the mid-market.

Neverfail Workspaces uses industry- standard protocols and supports for all popular operating systems. This means that businesses using it can be confident that BYOD will not create new security problems for them and also give their workers a flexible, intuitive way to get their work done using their own computers and tablets.

Ransomware: A New Threat

Ransomware is a growing problem. For example, as many as 75% of hospitals in the US were hit with ransomware in 2015, according to the survey released by Healthcare IT News and HIMSS Analytics. Many of them might not even be aware that they've been hit — about 25% of them are either unsure or have no way of knowing whether ransomware attacks were perpetrated against them or not.

The ransomware epidemic is far from being limited to the healthcare industry though. Any organization can make a good target; in fact, ransomware has gone from a niche attack to a booming criminal market since its introduction in 2013.

Attacks are being reported in a number of organizations both large and small in several verticals. For example, one virus, "CryptoLocker," infected more than 250,000 computers around the world and was used to target businesses and consumers. The virus enabled the extortion of about $27 million from infected users in a single two month period.

The FBI issued an alert in early April 2016 reporting that losses from "business email compromise" scams — basically phishing schemes — totaled more than $2.3 billion from October 2013 through February 2016. The cases involve some 17,642 businesses of all sizes scattered across at least 79 countries.

Ransomware is now an industry unto itself and, like any forward- thinking tech vertical, there's a big emphasis on speed and innovation. Malware developers are looking to ramp up their infection volume while also coming up with new ways to slip past corporate defenses.

Protecting Your Business from Ransomware

Anyone working in IT today knows that one of the most difficult challenges involves getting people to be aware of hacking and ransomware threats, and to take reasonable security precautions as a matter of routine. However, people being people – and busy people at that – means that security isn't always their top priority. Changing their behavior is difficult, and that's how ransomware infections spread.

Here's a mantra that business owners need to keep in mind at all times:

Keeping your data safe means protecting it from your least technically savvy employee.

Neverfail Workspaces helps protect your business from that technically naive employee by changing the game. If an employee does install ransomware on a computer, that machine will not contain any of the data the thief is looking for. Wiping the PC gets rid of the ransomware and the previously infected machine can be returned to service in a few minutes.

Workspaces also prevents the infection from getting to the servers and, even if a black hat tries that, they won't succeed. A Workspaces-enabled server is locked down and secured to prevent a server-based attack as well.

> ***"What we're seeing is the macroevolution of ransomware and the tactics that are being used by organized crime to continue to expand the revenue generated from ransomware. The most productive way to do that is by targeted campaigns."***
> **— Chris Ensey, COO, Dunbar Security Solutions**

Rethink and Replace VPNs

Over the years, many businesses have implemented VPNs to support secure remote access to applications and data. This has been particularly true when remote workers need access to legacy client/service applications and a typical setup involves running thick client software end user devices connected through the VPN to a database server.

VPNs have the advantage of being easy to setup at the server level. Getting one running is, for most installations, as simple as checking a box on a router or installing an appliance and punching some holes in a firewall. However, user setup can be onerous and can quickly become a support headache. In addition, VPNs often suffer from performance issues, including random disconnections.

PNs are also not as secure as many people would like to believe and they can be hacked fairly easily. Many VPN solutions use protocols or configurations that don't encrypt the traffic. They may also allow packet sniffing technology to snag user names or passwords. For example, PPTP is one of the most widely adopted VPN technologies, and it is the easiest to attack; most hackers can get usernames and passwords in just a few minutes.

Another problem with VPNs is that they do not monitor access, which creates two significant challenges: First, they are rarely tied in with Active Directory or other centralized user directories, which makes broad spectrum password policy enforcement and user management impossible. Tying VPNs in with Active Directory is feasible, but it is complicated to do this and adds unnecessary costs to the system. The second challenge is that users with VPN access often have unfettered access to all intranet resources and they could be moving sensitive data to personal machines, which in turn could already be hacked.

In addition to the poor user experience, difficult management, and poor security model, VPNs do not address mobility very efficiently. People want and expect a seamless experience these days, including BYOD, regardless of which device they happen to be using. They don't want to deal with fiddly or unreliable client applications.

These trends create huge security, supportability, and user acceptance headaches if a VPN is part of the infrastructure. Neverfail Workspaces is the best option to replace VPN. It gives end users that seamless experience they want and supports much better security for the organization.

> ***Neverfail Workspaces is the best option to replace VPN. It gives end users that seamless experience they want and supports much better security for the organization.***

Neverfail Workspaces: A New Approach

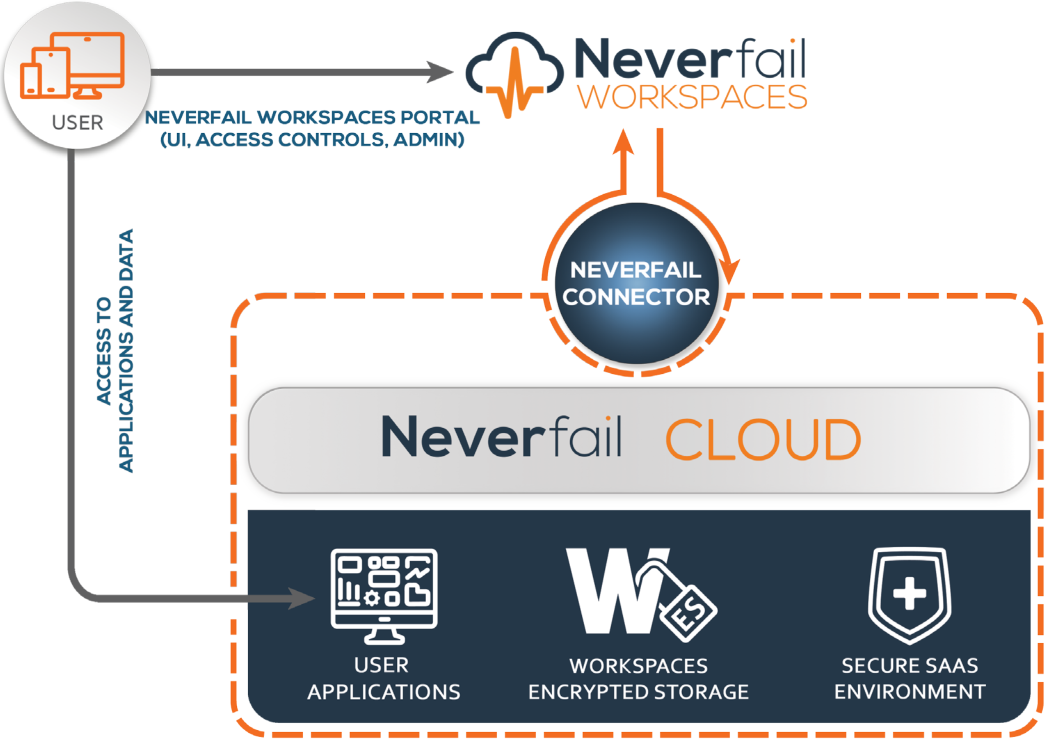
Neverfail Workspaces is a new, secure way for MSPs to secure the IT infrastructures for their clients. It controls access to sensitive data and applications and ensures that client devices do not become weak points in the security system.

Workspaces removes the challenges typically seen with disparate end points and creates a standardized method for accessing applications and data, without the issues associated with traditional methods.

Neverfail Workspaces incorporates extensive automation that handles the most complicated aspects of configuring the infrastructure to become secure, thereby freeing up the most experienced engineers within the MSP to work on higher value projects.

This method provides several key benefits:

- Servers containing sensitive data can be securely located on the client's premises, in the MSP's data center, or both
- Manage how data is accessed inside or outside of a cloud-based third party systems, including accounting and HR systems
- Exposes only a very narrow cross section of the infrastructure the public internet, reducing the potential attack surface and thereby helping to deter hacking attempts
- Low capital cost for software — Neverfail utilizes a SaaS business model with pay-as-you-go licensing, and combined with your Microsoft SPLA, can be combined to create a very margin rich offering
- Support for a wide range of end user devices, including tablets, and ability to use "low horsepower" devices, including thin clients and zero clients
- Vastly simplified and less expensive deployment requiring substantially less engineering time compared to methods utilizing a mix of third party tools and complex system configurations



Neverfail Workspaces' architecture allows organizations to incorporate servers located on the business's premises, in a data center, or both, into secure deployments.

Neverfail Encrypted Storage

Neverfail Workspaces incorporates a reliable method for segregating and protecting data. We can implement the encrypted virtual disk on standard hardware with as much capacity as needed, which helps to keep costs low.

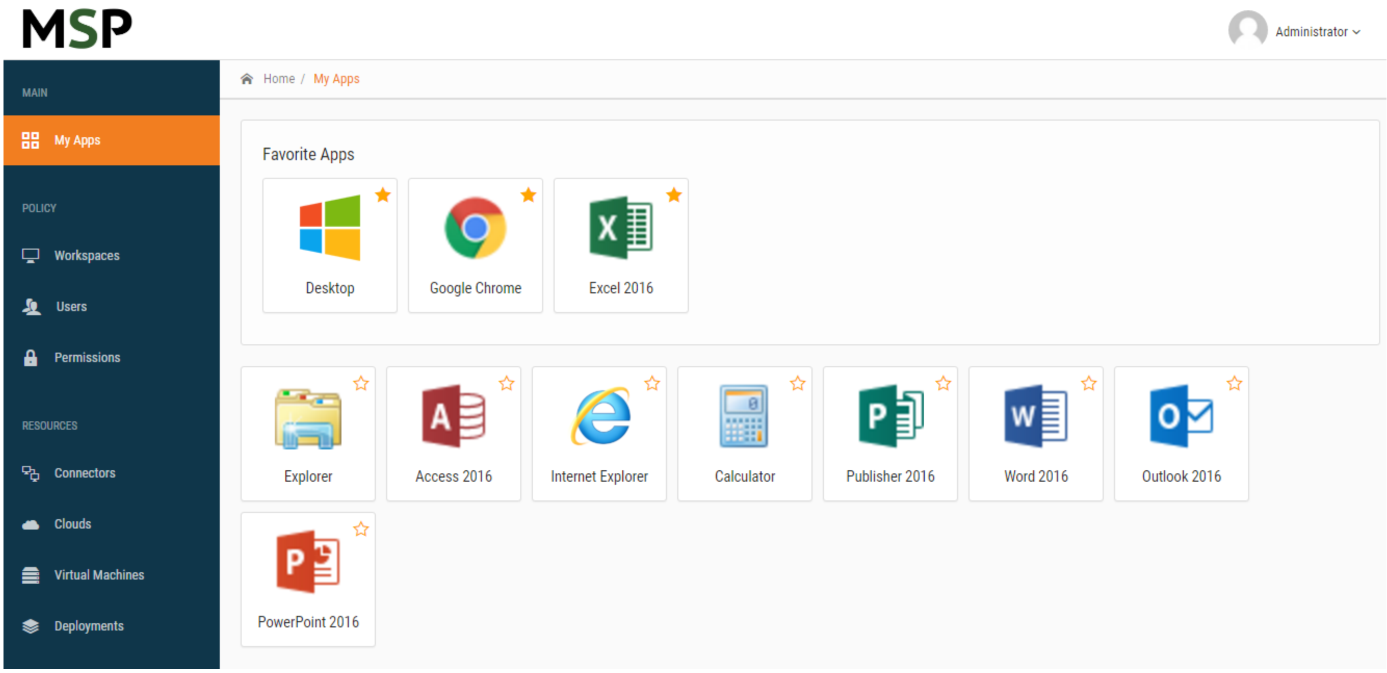
All data in the sub-system is encrypted both at rest and in transit using proven tools incorporated into the system architecture. It allows authorized users to save files of any kind, including documents, scans, images, databases, and so on, in conveniently-accessed storage, but completely disallows access by users who do not have the appropriate permissions.

Workspaces logs each time a user accesses encrypted storage, and this data is stored in the cloud platform.

Connecting to On-Site Peripherals

Most customers need to incorporate peripheral devices, including everything from scanners to digital cameras to credit card readers, into their secured infrastructure.

Since each of these can handle or contain sensitive data, Neverfail Workspaces is designed to make it easy to include them within the system's security wrapper, whether they be network devices like printers or USB-connected devices.



Using Neverfail Workspaces, each user sees a personalized "App Store" which presents a full desktop experience and/or a series of applications that are assigned to them based on credentials. In this example, users are presented with an "App Store" that includes the option of launching a full desktop if needed.

Incorporating Cloud-Based Services

Many business have already made the shift to using cloud-based applications like Salesforce, Office365, or Concur. Mistakenly, many also believe that by utilizing such systems, they have made their entire facility secure. Of course this is not the case, since such systems cannot authenticate, log, or manage users' access to other systems in use within the organization that contain sensitive data.

The biggest challenge with cloud-based applications is security for the client devices. Workspaces addresses this by creating a templated browser environment that domain-wraps the entire user interaction with the application, thereby securing communication with the application's servers. Through its management of browser and disk access, Neverfail Workspaces also controls how data moves into or out of the application.

General Purpose Office Applications

In order to make a reasonable claim of offering a secure IT environment, the organization must ensure that sensitive data incorporated into word processor documents, spreadsheets, presentations, and the like are only accessible by authorized personnel.

Of course, no technical solution can prevent people from emailing data or printing out and distributing proprietary information to unauthorized people. However, we can make it so easy for people to access sensitive data within a secure environment that casual disclosures of such data for the sake of convenience are minimized. In addition, if users know that the system is logging each time they access sensitive data, they are less likely to try and bypass security controls.

Neverfail-enabled businesses can also control which users have access to specific applications, including Word, Excel, and other Microsoft Office tools, whether a user can save files to external devices, access copy and paste functions, or have write access to a local drive.

Conclusion

Flexible working hours, work-from-home, and other trends are creating new security challenges for businesses, creating a demand for secure remote access and BYOD solutions.

Individual users also have developed preferences based on their experiences with consumer products and want easy-to-use systems and features like remote access, while business owners and managers must be concerned about the security of their data.

Neverfail Workspaces is a proven method for establishing secure IT environments that also gives authorized personnel access to the tools they need from any device in any location — without imposing undue operational burdens on the organization or the individuals involved.

Neverfail

About Neverfail

Neverfail delivers continuously available clouds through a single pane-of-glass SaaS platform. This platform is the industry's first secure, comprehensive, multi-tenant, multi-cloud management solution for BC/DR solutions, solution catalogs, cloud service billing, service orchestration, monitoring, cloud workspaces and unified communications. Neverfail serves a global partnership of managed service providers, systems integrators, telecommunication providers, data center operators, independent software vendors, governments, healthcare institutions and enterprises exclusively through the channel.

Neverfail provides solutions across the globe and operates data centers in the United States and Europe. Neverfail is headquartered in Austin, Texas with offices in Melville, Chicago, Denver, Kansas City, Portland, Edinburgh, Scotland and Cluj, Romania. For more information on Neverfail solutions, contact the company at +1 512-600-4300 or **www.neverfail.com**. Follow Neverfai on Twitter at **twitter.com/Neverfail**

2016-9-08