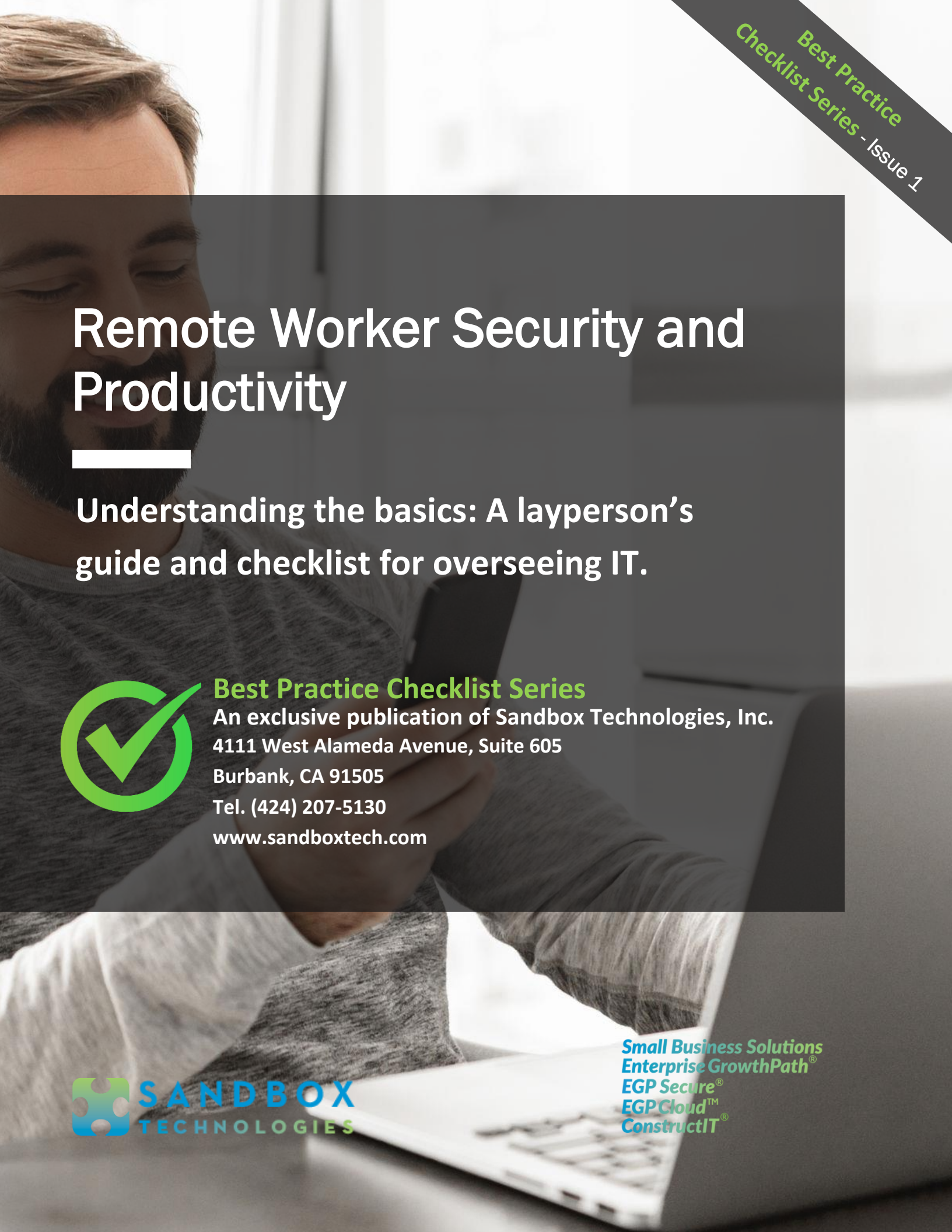


Best Practice Checklist Series - Issue 1

# Remote Worker Security and Productivity

## Understanding the basics: A layperson's guide and checklist for overseeing IT.

**Best Practice Checklist Series**
An exclusive publication of Sandbox Technologies, Inc.
4111 West Alameda Avenue, Suite 605
Burbank, CA 91505
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

# Remote Worker Security and Productivity

## Security

Once considered a luxury or perk by many, when unforeseen world events unfolded, remote work solutions became an overnight necessity for virtually every technology-dependent business in the US and Worldwide.

Successfully meeting this challenge with little to no planning or preparation time required left many organizations with few alternatives to implementing solutions that were fast and easy deploy yet required sacrificing some degree of security and stability.

Roughly a year later, uncertainty in the World still abounds. Yet, in the time that has lapsed, many businesses have found a silver lining – That the use of remote work workers can be surprisingly effective. As a result, some have made the decision to reduce or eliminate centralized workspaces entirely in favor of employing remote work strategies on a permanent basis.

Regrettably for many however, there exists a problem. Whether your organization's plans include the use of a remote workforce on a full, partial, or temporary basis, malicious actors have aggressively begun seeking to exploit residential vulnerabilities to gain illicit access to corporate networks.

Given the increasing threat of breaches and the likelihood of remote work solutions remaining a necessity for some time, we strongly urge all Sandbox Technologies customers to review the information that follows to see how your current security stacks up, and what, if anything, you can do to improve it.

## Productivity

It pleases us to say that in our experience, a vast majority of our client staff members eagerly adapted to remote work strategies with minimal transition pains.

Unfortunately, managing a remote workforce nonetheless still comes with its share of challenges. For this reason, we have included a brief section outlining our recommended approach to managing remote workforces, and we'll show you a simple tool that can aid in this endeavor.

As always, should you wish to discuss your remote worker security and productivity solutions, your Sandbox Technologies Engineer, Account Manager, or Consulting CIO will be happy to answer any questions you may have.

# Table of Contents

# Remote Worker Security Explained

In keeping with the conventions of our checklist series, this section includes a checklist of what we consider to be the optimal practices concerning the secure configuration of remote workforce solutions.

It should be noted however, that this specific area of focus is laden with numerous caveats, such that the optimal solutions can and will vary from one organization to the next based on numerous factors including infrastructure availability and employee workflows.

On the page that follows, we've begun by providing a matrix containing key attributes of various remote worker infrastructures. It illustrates how the presence or absence of these attributes may impact the corresponding level of security, and it highlights what we regard as some of the more salient vulnerabilities.

Following the matrix are explanations of the eight categories evaluated to help provide an understanding of their relevance and meaning to your organization. Lastly, we provide our customary checklist of these items to aid you in assessing your infrastructure and noting any questions you may have pertaining to these categories.

## How Does Your Remote Worker Security Rate?*

= Noteworthy Risk Exposure

| RATING ➡ | WEAK | WEAK | AVERAGE | PASSABLE | BETTER | BEST |
|---|---|---|---|---|---|---|
| Target Computers | Company Workstation | Company Workstation | Company Workstation | Company Workstation | Company Terminal Server | Company Terminal Server |
| Remote Computers | Employee Owned | Employee Owned | Employee Owned | Employee Owned | Company Owned and Managed | Company Owned and Managed |
| Access Solution | LogMeIn, GoToMyPC or Similar | SSL VPN Software Client | LogMeIn, GoToMyPC or Similar | SSL VPN Software Client | SSL VPN Software Client | Persistent VPN Connection between Company Firewall and Company Supplied Remote User Firewall |
| Multi-Factor Authentication | No | No | Yes | Yes | Yes | Yes |
| Connection Method at Remote Network | Wi-Fi | Wi-Fi | Wi-Fi | Hardwired | Hardwired | Hardwired |
| Remote Location Security | None or Employee Router (Minimal) | None or Employee Router (Minimal) | Software-Based Firewall on Computer | Software-Based Firewall on Computer | Software-Based Firewall on Computer | Company Owned and Managed Hardware Firewall |
| Antivirus | None or Unmanaged | None or Unmanaged | Free or Built-In Antivirus | Employee Managed | Company Managed | Company Managed |
| Internet Connectivity at Remote Location | Remote User's Internet Service | Remote Users Internet Service | Remote Users Internet Service | Remote Users Internet Service | Remote Users Internet Service, Separate Firewall Zone | Dedicated, Company Subscribed and Managed Internet Service |

*Example configurations for illustrative purposes only. Ratings based on the concurrent implementation of ALL items in each particular column. Individually, some solutions may rate lower when not used in connection with others.

## Target Computers

The target computer can be a company workstation or a company Terminal Server, both are acceptable. However, a Terminal server is generally the recommended solution. A terminal server hosts virtual "desktops" that users can log into and perform their daily tasks in much the same way that one would log into a regular remote computer.

Advantages to the target computer being a Terminal Server are: (1) Elimination of the need to concurrently maintain an individual remote computer and a company computer housed at the workplace for each user; (2) A Terminal Server lends itself much better to centralized management, security, and control; (3) Leveraging a Terminal Server may allow an organization to re-purpose existing computer workstations (subject to condition and viability) at remote locations. Drawbacks to using a company Terminal Server include (1) The Terminal Server represents a potential single point of failure in the event it should experience a problem. (2) If an office space is maintained and employees visit that space, they must bring their laptop or computer to the office or have an existing individual or shared computer there to access the Terminal Server. Overall, a Terminal Server is an industry-standard solution for remote workers, and more efficient and desirable to most than maintaining on-site workstations and connecting to them remotely.

## Remote Computers

Using employee-owned remote computers is not recommended. There are a few reasons for this: (1) Best practices call for computers used to conduct company business to be "Hardened" to NIST/DOD standards (to the extent the employee's job functions will allow.) (2) Company controlled and managed utilities, such as Cloud managed antivirus solutions, automated patch management, hard drive encryption solutions, trouble alerting, and software-based firewalls should also be installed and actively maintained.

These solutions can and often do impair the remote user's ability to install software for their own benefit. They are often regarded as intrusive and managing them in a manner similar to that of company-owned computers can potentially run afoul of employee privacy rights. Bring Your Own Device, or "BYOD" agreements can sometimes be secured to address these concerns (see Sample BYOD Agreement Here). However, BYOD agreements can still give rise to disputes between the employee and the employer, they may not sufficiently provide legal standing for the company to demand the return or inspection of the computer upon termination or in cases where malfeasance is suspected and should generally be avoided in favor of company owned and controlled remote computers.

## Access Solution

Cloud based remote access solutions are constantly evolving. Leading subscription-based products such as LogMeIn support two-factor authentication, making them attractive solutions for establishing remote connections to physical workstations maintained in office spaces.

To eliminate the need to procure, maintain and support both an on-premises computer and a remote computer for remote workers, connecting via an encrypted VPN tunnel to a Microsoft Terminal Server is often the recommended solution. A Terminal Server is a single (or virtual) server that facilitates hosting multiple remote "computers" virtually on a single machine. Users connect to the network via a secure tunnel, then connect to individual desktops hosted exclusively for each user. Terminal Servers can be hosted at an organization's headquarters, or to reduce on-site hardware, they can be hosted in co-location facilities, or via popular Cloud services such as Azure and Amazon Web Services.

## Multi-Factor Authentication

In addition to a password, multifactor authentication (also sometimes referred to as 2FA or Two-Factor Authentication) requires the entry of a unique security code generated by a token or a mobile device application to authenticate to protected systems. MFA greatly increases security by not only requiring the knowledge of a valid password (the 1st factor), but also the security code (the 2nd factor) to gain access to resources. Because each user's security code changes frequently (administrators often opt for every 60 seconds), multifactor authentication lessens the likelihood of a data breach in the event a user unwittingly allows their username and password to become compromised.

It is strongly recommended that all organizations that have not implemented multifactor authentication do so immediately to restrict access to computers, devices, and supported information technology systems, including cloud-based solutions.

Types of multifactor solutions vary and are often dictated by the platform(s) in use (Mac and/or PC), and by what multifactor solutions are supported by the applications in need of protection. Implementation methods range from simple and inexpensive configurations requiring manual entry of a mobile phone generated code for each protected solution, to more friendly "Push Based" solutions. More complex configurations also exist, such as SSO (Single Sign On) which can further lessen user burden by unifying credentials and thus allowing authentication to multiple systems at once.

## Connection Method at Local Remote Network

"Connection Method" refers to connecting the remote computer via a wired ethernet connection, or via Wi-Fi. Wi-Fi connections should be avoided when at all possible for numerous reasons, including (1) Residential users often have poor Wi-Fi passwords and security and rarely change them, if ever. (2) Residential users often share their Wi-Fi passwords freely with others. (3) Residential Wi-Fi rarely segments business-use computers from home users, leaving unprotected computers open to virus infections and breaches when the security of another computer on the network is compromised. (4) Residential Wi-Fi users often use default passwords, outdated hardware, and/or fail to ensure that a minimum of WPA2 Encryption is in place, making them easy targets for would-be hackers. (5) Wi-Fi is inherently less secure than hardwired connections, such that even businesses with robust security protections in place are advised to limit Wi-Fi use to Internet Access Only and no access should be granted to other local devices present on the network. When this is unavoidable for iOTS (Internet of Things) devices, such as smart TV's and streaming appliances, a dedicated, separate Wi-Fi network should be configured for this purpose.

When at all possible, residential users should connect via hardwired connections. When this is not possible, the best method of securing the environment entails the deployment of a modest, company-owned, and controlled firewall to segment separate home "business" networks from "personal" networks and activity, and aggressively limiting activity on the "business" side. Unfortunately, doing so sometimes poses difficulties for home users, which is elaborated upon below.

## Remote Location Security

Many residential users have minimal or no firewall security protecting the perimeter of their network. This represents a significant vulnerability to being breached by outside attackers seeking to use residential computers as a pivot point into more lucrative corporate targets. At a bare minimum, remote computers should be protected by a software firewall. Optimally, a modest company-owned

and controlled firewall should be deployed at each remote use location to segment networks and regulate the flow of traffic. It should be noted that the deployment of a residential firewall offers the employee many added benefits, such as greater security overall, and the ability to prioritize bandwidth availability for business-specific devices over other less essential family devices when utilization is at its peak and it is scarce.

Regrettably, the addition of a firewall to previously "open" residential environment is likely to create occasional hardships for non-business applications, the most common complaint being that households with children playing online console games will occasionally encounter Network Address Translation or "NAT" incompatibility messages that impair their ability to play certain games with other players not employing similarly configured networks. When undertaking the task of deploying a hardware firewall to remote locations, it should be expected that periodic support may be required to remediate such reasons. For this reason, the optimal approach is to deploy remote location firewalls in concert with dedicated, company paid and controlled Internet circuits, thus eliminating these and other potential concerns.

## Antivirus

Workstation-based antivirus software is one of the fundamental safeguards a network has against the propagation of security threats. A properly configured antivirus solution can help mitigate outbreaks on a network. An effective antivirus suite offers protection against Internet-based threats, and infected resources that are permitted to connect to an organization's network. Antivirus solutions can also mitigate the use of rootkits and backdoors by malicious actors in the event of a compromise.

Despite the protections of stand-alone antivirus products, it is strongly recommended that that all organizations deploy a centrally managed antivirus solution to every workstation accessing company resources to provide the visibility necessary to ensure remote antivirus installations are properly configured and being updated.

## Remote Internet Connection

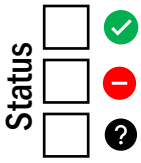
A separate, company-provided Internet circuit at the work remote location has several benefits. (1) It automatically segregates the remote business user from other users at the location who could (intentionally or unintentionally) become compromised and serve as a pivot point for hackers to enter the corporate network. (2) A separate Internet connection permits a locally maintained company firewall appliance to be deployed to protect the user and filter content without the employee objecting to the fact that a company firewall on their personal Internet service might allow their non-business Web activity to be monitored by the company. (3) It eliminates potentially costly troubleshooting of connectivity issues stemming from the use of non-company devices, and (4) It may provide some degree of legal protection concerning user expectations of privacy and permit exercising control over the use of the circuit if needed.

*In some territories, employers may be bound by law to provide or reimburse remote work employees for the use of computers, tools and services that are required to perform their respective job duties. Sandbox Technologies is not qualified to provide legal advice, and it is advised that any organizations considering the implementation of any of the measures herein consult their legal counsel to determine any legal obligations under Federal, State and Local law.

# Recommended Practices – Remote Access

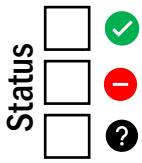
## Target Computers

Are target computers properly secured remote workstations or hosted via a suitably configured Microsoft Terminal Server solution?



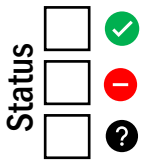

## Remote Computers

Are remote computers company-owned and managed devices, rather than employee-owned devices?



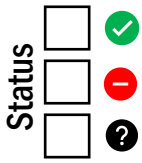

## Access Solution

Has the organization standardized on a secure and robust remote access platform suitable to its needs and consistent with security requirements? (SSL-VPN or Persistent Firewall-Based VPN's combined with restricted implementation of Remote Desktop or Microsoft Terminal Server are optimal in many situations. Others may be better suited to third-party remote access products such as LogMeIn and GoToMyPC.)



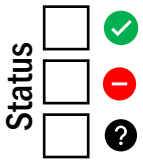

## Multifactor Authentication

Is remote access to all company resources secured by an acceptable form of multi-factor authentication?



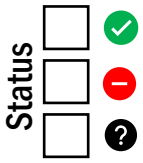
## Connection Method at Remote Network

Are remote users connecting to their local remote network via a hardwired connection as opposed to a Wi-Fi connection?



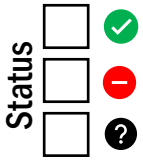

## Remote Location Security

Is the remote computer being used to access company resources secured by a company-owned and managed firewall appliance or by a properly configured software firewall?



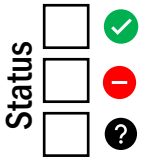

## Antivirus

Is the computer being protected by a suitable company-owned antivirus solution that is actively managed and updated?




## Hardware VPN Connections

If a hardware VPN is in use, is VPN traffic restricted to a designated work computer or device at the remote location?



## Internet Connectivity at Remote Location

Is Internet connectivity at the remote location provided via an Internet circuit that is paid for and managed by the company or organization?

Status ☐ ✓ ☐ – ☐ ?

_____

_____

_____

## Segmentation of Devices

### <Answer only if you checked – in response to the previous question>

Are security measures in place to suitably segment business-use device(s) from all other Internet-enabled devices (computers, laptops, mobile devices, streaming and other appliances, smart TV's, etc.)?

Status ☐ ✓ ☐ – ☐ ?

_____

_____

_____

# Remote Worker Productivity Explained

While developing and making proper use of Key Performance Indicators (KPI's) for various roles is by far one of the most effective means of ensuring productivity, many metrics are difficult to measure until it's too late. Although the development of KPI's is largely a managerial and human resource issue, there are software tools to aid in this task, which we may address in a future installment.

To help identify and address suspected productivity issues, businesses may opt to utilize one of several inexpensive and easily to deployable audit utilities that provide visibility into user activity. Some solutions are very aggressive, and capable of collecting virtually every keystroke along with actual video of activity that takes place on a given computer or computers. Storage of this data can be costly however, and many organizations find such levels of data collection excessive and unnecessary.

Other solutions exist that are more moderate in their configuration, logging only basic activity data and periodic screenshots as needed. These minimally invasive solutions often provide ample information to identify problem areas before they are permitted time to worsen.

On the following page is an example report from such a solution.

# Example Productivity Report

The fictional report below illustrates the activities of user Bob Smith. Under normal circumstances, Bob's supervisor would have no need to request an activity report, however as of late, Bob has missed several deadlines. In fairness to Bob, the shaded area could reflect preparation for a Zoom meeting with client that's an avid sports enthusiast. Conversely, Bob could also be suffering from distractions and in need of coaching and encouragement to help him improve.

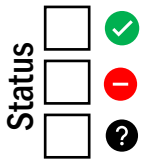
Activity logs are a helpful way of mitigating the loss of on-site visibility that managers might otherwise benefit from when team members are working in the same location.

| Activity | Device | User | Time |
|---|---|---|---|
| Lacerte Tax for Windows \| Sign In | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:15 |
| Lacerte Tax for Windows \| 2019 Lacerte Individual Tax | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:15 |
| LogMeIn Host Launcher \| LogMeIn | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:15 |
| Microsoft Outlook \| Inbox - Bsmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:16 |
| Microsoft Outlook \| Junk E-mail - BSmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:16 |
| Microsoft Outlook \| Inbox - BSmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:16 |
| Microsoft Outlook \| Fwd: 1099 Request - Message (HTML) | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:16 |
| Microsoft Outlook \| Inbox - BSmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:17 |
| Microsoft Outlook \| Re: Fwd: 1099 Calculation Question - Message (HTML) | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:17 |
| Microsoft Outlook \| Inbox - BSmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:17 |
| Microsoft Excel \| Opening - Excel | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:18 |
| Microsoft Excel \| Book1 - Excel | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:18 |
| Microsoft Outlook \| Re: Re: Fwd: 1099 Calculation Question - Message (HTML) | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:18 |
| CCH ProSystem fx Practice Management \| Time Entry - Smith, Bob - 11/10/2020 | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:18 |
| CCH Axcess \| ProSystem fx Document | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:18 |
| Microsoft Outlook \| Inbox - BSmith@xyzco.com - Outlook | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:19 |
| Microsoft Edge \| Falcons vs. Saints - Box Score - November 22, 2020 - ESPN - Profile 1 | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:21 |
| Microsoft Edge \| Falcons vs. Saints - Game Summary - November 22, 2020 - ESPN - Pr | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:28 |
| Microsoft Edge \| ESPN: Serving sports fans. Anytime. Anywhere. - Profile 1 - Micros | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:31 |
| Microsoft Edge \| NBA - National Basketball Association Teams, Scores, Stats, Rumor | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:31 |
| Microsoft Edge \| CBS Sports - Anticipating a normal bracket in an abnormal year - Pr | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:35 |
| Microsoft Edge \| ESPN: How will coaches fare in the upcoming recruiting cycle - Prof | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:38 |
| Microsoft Edge \| Amazon Search - Profile 1 - Microsoft Edge | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:42 |
| Microsoft Edge \| Amazon Search - NBA Memorabilia - Profile 1 - Microsoft Edge | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:42 |
| Microsoft Edge \| eBay Search - Profile 1 - Microsoft Edge | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:46 |
| Microsoft Edge \| eBay Search - Autographed Basketball - Profile 1 - Microsoft Edge | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:46 |
| Microsoft Edge \| eBay Search - Autographed Basketball Bryant - Profile 1 - Microsoft | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:48 |
| Lacerte Tax for Windows \| Sign In | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:53 |
| Lacerte Tax for Windows \| 2017 Lacerte Tax | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:54 |
| Lacerte Tax for Windows \| 2017 Lacerte Individual Tax | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:54 |
| Lacerte Tax for Windows \| Organizer | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:54 |
| Zoom Meetings \| Loading Zoom Meetings | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:54 |
| Zoom Meetings \| Zoom Meetings | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:55 |
| Google Chrome \| Untitled - Google Chrome | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:55 |
| Google Chrome \| Google - Google Chrome | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:58 |
| Google Chrome \| Section 7 Deductions - Google Search - Google Chrome | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:58 |
| Adobe Acrobat DC \| Federal Return - Saunders.pdf - Adobe Acrobat Pro DC | ws1-win10.xyzco.local | xyzco\bsmith | 11/25/2020 9:58 |

# Recommended Practices – Productivity

## Key Performance Indicators

Has the organization created formal key performance indicators for each employee and implemented a system whereby indicators are routinely reviewed and acted upon as needed by supervisory personnel?




## Productivity Support Utility

Does the organization have a solution in place to generate logs to aid in the assessment of remote and on-premises user productivity when required?