Devolutions

Improving Security and Productivity for the MSP and IT

THIS ARTICLE WAS WRITTEN BY THE PETRI TEAM IN PARTNERSHIP WITH DEVOLUTIONS.

Overview

There is no doubt that IT has always undergone rapid and sweeping changes. However, over the past year, it is safe to say that with the continuing pandemic, remote connectivity and security have a greater focus than ever before. The pandemic has resulted in a huge increase in remote workers as well as the need to perform remote support.

At the same time, security continues to be a primary concern as well. The increase of remote support has been accompanied by an increase in phishing and ransomware attacks that are aimed at taking advantage of the potential holes created by a larger and more diverse remote workforce. Today's remote workforce provides cybercriminals with a larger attack surface than ever before. Once cybercriminals have access to an organization's network, the threats they pose include disrupting operations, stealing proprietary information, and extorting ransom.

In addition, several high-profile security breaches like the SolarWinds exploit have resulted in many businesses redoubling their security efforts and enforcing stricter security policies. These security restrictions often hinder Managed Service Providers (MSPs) and enterprise IT personnel from being able to effectively perform remote support tasks.

MSP and enterprise IT have similar needs for remote support and connectivity. Both need to provide secure remote support and connectivity for multiple remote locations that often have quite different security requirements. For instance, MSPs need to connect to a diverse array of businesses to perform remote support, maintenance, and troubleshooting. Enterprise IT frequently performs the same type of support for remote locations and branch offices. Improving Security and Productivity for the MSP and IT

"MSPs and IT need to find a balance where their remote connections are as secure as possible yet still be productive enough to be effective in their remote support requirements."

MSPs and IT also need to perform these remote support tasks in the most secure way possible. However, in many cases, the need for efficient and productive remote connections is often at odds with the needs for security. As organizations work to lock down the security of their remote connections, the measures they take can adversely impact the ability of remote support personnel to efficiently accomplish their tasks; administrative privileges are often revoked and access to remote resources can be severely restricted. When you need to perform some type of support that's required to keep the business running, you do not want to be in the position of being so confined that you are not able to get anything done. MSPs and IT need to find a balance where their remote connections are as secure as possible yet still, be productive enough to be effective in their remote support requirements.

In this whitepaper, we will look at some of the challenges that MSPs and enterprise IT face in order to implement secure yet productive remote support for their customers, branch offices, and remote sites. We will cover many of the hurdles that MSPs and IT need to deal with to provide secure remote connectivity. And then you will see how Devolutions' Wayk Bastion and Remote Desktop Manager can help provide secure and managed remote connectivity without impacting remote access productivity.

Challenges of secure remote connectivity

MSPs must manage servers for their customers as well as supporting users who have problems with their computers and applications. Enterprise IT also needs to perform these same sorts of tasks for their remote and branch office installations. Cloud billing and managing support for multiple accounts are also concerns for an MSP. When it comes to remote access, keeping track of who accessed what, when, and for how long with proper auditing and reporting is vital to meet the billing, security, and compliance requirements. This is particularly true for MSPs that frequently connect to machines in separate networks to support their customers. For many businesses, security is about defining the remote support capabilities.

Some of the main requirements for secure remote support include:

- Secure on-demand remote sessions
- Easy connectivity to multiple remote locations
- Remote access to multiple heterogeneous operating systems
- Encrypted remote session connections
- Centralized password management
- Easy remote access deployment
- Real-time session tracking
- Audit trials for remote sessions

Many businesses use Virtual Private Networks (VPNs) to provide secure remote connections, but VPNs have drawbacks that can impede productivity and even hinder security. First, VPNs have overhead that makes VPN connections slow. And VPNs can be difficult to manage – especially for MSPs with many different customers that could require connecting to dozens of different VPNs. While VPNs do provide an added level of security, a VPN is not part of a zero-trust network architecture. Instead, VPNs typically provide perimeter level security. Once you're inside the VPN, you essentially have a trusted connection and potentially extensive access to the organization.

Wayk Bastion solves the problem of remote security and connectivity

Wayk Bastion is designed to provide secure remote connectivity for MSPs and enterprise IT. Wayk Bastion's secure connection architecture leverages a centralized management platform that provides attended and unattended

access to all types of remote systems. Wayk Bastion is based on a self-hosted server and this server component must be accessible to all of its different connections. It can be installed in the cloud, or it can be installed on your own on-premise infrastructure. The server is entirely under your control. The Wayk Bastion server provides security, management, and control of all of the remote sessions that flow through the server.

The Wayk Bastion server works by integrating the Wayk Agent and Wayk Client. All of the connections to the server from the Wayk Client and the Wayk Agent are outbound. This simplifies the remote connection requirements and eliminates the need for VPN and firewall exceptions. The Wayk Client is used by your technical personnel to establish remote desktop connections to systems managed by Wayk Bastion. The Wayk Agent is installed on all of the remote machines that are managed by Wayk Bastion. This agent reports its state to the central Wayk Bastion server and provides remote desktop connectivity to the Wayk Client. You can see an overview of the Wayk Bastion architecture in Figure 1.

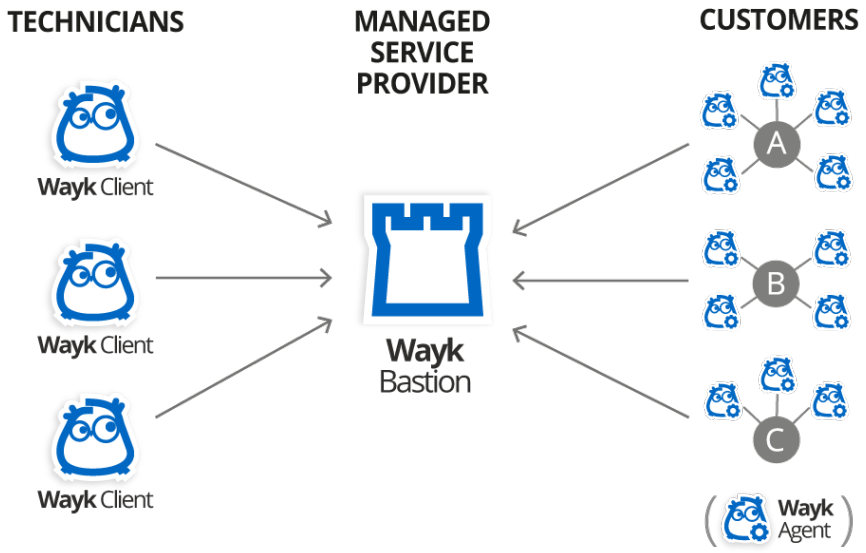

Figure 1- Wayk Bastion Zero Trust Architecture

The Wayk Agent allows remote access and management of registered machines from Wayk Bastion. It is not a direct connection between the Wayk Client and the Wayk Agent. The Wayk Agent connects to the Wayk Bastion server to report its state and it acts as a remote desktop server for the Wayk Client. It is authorized and managed by the Wayk Bastion server. When a remote connection is requested, the Wayk Client first gets permission from the Wayk Bastion server, and then the Wayk Bastion server connects to the Wayk Agent.

The Wayk Bastion server can be installed on Windows Server 2019, Ubuntu, or Red Hat Enterprise Linux. It uses native containers for the OS on which it is installed as well as PowerShell and Docker. The Wayk Bastion server is exposed externally as a web service. It can be installed in any location that you choose so long as it can be reached by the Wayk Clients and Wayk Agents. This design ensures independence from third-party cloud services and provides full control over remote session data traffic. Some of the secure remote connection capabilities that Wayk Bastion provides for the MSP and enterprise IT include:

1) Self-hosted zero-trust security

Wayk Bastion provides secure remote connectivity without the need for a VPN. The Wayk Agent and Wayk Client both use outbound connectivity to the Wayk Bastion server. No VPN or inbound traffic firewall exceptions are required. With Wayk Bastion, the network does not provide any form of trust. There's no need to open a VPN or to use multiple VPNs to deal with multiple different remote networks. Wayk Bastion is compatible with zero-trust networks where the philosophy is "Never trust, always verify". Devices on the corporate network are all untrusted.

Even if an attacker gets in, lateral movement and access is very difficult. In contrast, VPNs are not zero-trust. VPNs provide perimeter security, but once an attacker is inside there's implicit network trust and easy lateral access to business resources. Wayk Bastion's zero-trust approach to security reduces security exposures and simplifies remote access because the network location no longer matters.

2) Cross platform multi-tenant management

Wayk Bastion enables MSPs to manage multiple customers using a single multi-tenant deployment that enforces isolation and security for all its remote connections. You can manage multiple remote connections simultaneously and quickly navigate between them. All of the connections to the Wayk Bastion server use TLS 1.2 encryption to secure the in-transit data and are backed by a built-in certificate authority. Wayk Bastion can provide remote desktop connectivity to virtually all popular systems ranging from Windows, macOS, and Linux as well as connections from Android and iOS. It provides a uniform feature set on all platforms, giving technical personnel a common remote management experience across all platforms. With Wayk Bastion, MSPs and IT only need to deploy a single remote desktop solution to cover all of their remote system support requirements.

3) Extensive remote management capabilities

It's not enough to simply provide remote connectivity. To provide productive remote support, the remote connection also needs to provide the tools that you need for your remote support tasks. Wayk Bastion supports the ability to seamlessly send and receive files between the Wayk Client and the remote systems. In addition, it enables you to copy clipboard data between your local system and the remote systems. For auditing and analysis, Wayk provides the ability to record remote desktop sessions. These recordings can be saved as video files and viewed later. Wayk Bastion also provides a built-in chat window to facilitate communication between you and an end-user on the remote system.

4) Role-Based Access control with Active Directory Integration for user management

To help simplify role assignments for a large number of users, Wayk Bastion supports Role-Based Access Control (RBAC). Creating role assignments for different users and groups simplifies central management and provides granular control over remote resources. For enterprise authentication, Wayk Bastion provides LDAP integration with Active Directory

5) Centralized management dashboard

Wayk Bastion's server enables you to manage all of your machines from a centralized dashboard that displays and monitors the real-time status of the remote sessions. You can choose between the web client and the native remote connection application when launching remote sessions from the browser. You can also automatically deploy the lightweight Wayk Agent on a large number of machines that are registered with the Wayk Bastion server.

6) Auditing for remote access session tracking

To better secure and manage your remote sessions, Wayk Bastion provides real-time auditing that tracks who is using each remote session. This enables you to see who is currently connected to each remote system as well as how long each connection has lasted. It also provides a detailed remote activity audit log that you can later use for remote session analysis. The audit log enables you to examine remote session history and includes information like session time, user, and session duration as well as client
and server information.

Integrating Wayk Bastion with Remote Desktop Manager

Remote Desktop Manager (RDM) is Devolutions' primary remote desktop management platform for the enterprise. RDM centralizes all remote connections on a single platform that is securely shared between users and across the organization. RDM provides support for hundreds of integrated technologies including multiple remote access protocols and VPNs. It also provides built-in enterprise-grade password management tools, support for multifactor authentication, and RBAC for granular management.

Wayk Bastion can be used as a standalone remote access management solution and it can also integrate with RDM. RDM provides a built-in remote connection option for Wayk Bastion. RDM connects as a client to the Wayk Bastion server just like a native Wayk Client. RDM provides full Wayk Client support and you do not need the Wayk Client installed in addition to RDM. The Wayk Bastion server securely manages and controls the RDM connections exactly the same as it does Wayk Client connections.

Securing and Simplifying Remote Access

Wayk Bastion provides secure remote access without interfering with MSP and IT productivity. Providing highly secure zero-trust connection capabilities along with powerful remote support tools, Wayk Bastion addresses the two main pains points of remote access for the MSP and enterprise IT. Wayk Bastion is essentially licensed per

remote user. The Wayk Bastion server is free. The Wayk Agent is also free, and you can install the agent on an unlimited number of remote systems. The only license requirement is for the Wayk Client. Wayk Bastion Client Access Licenses (CALs are assigned to individual users. Users with a CAL can make use of all of the functionality of Wayk Client through the native app or the web-based client that is built into Wayk Bastion. There is also an option to purchase
a Site license.

Devolutions offers a free 90-day trial of Wayk Bastion that you can use to see how Wayk Bastion can address your own remote connection requirements. The free trial includes an instance of the Wayk Bastion server plus a Wayk Client Site License that can be used by all the support personnel at your location.

Additional Information

For more detailed information about SMB cybersecurity challenges and solutions, be sure to check out Devolutions State of Cybersecurity in SMBs in the 2021 report.