HOW TO GUIDE

How To Secure BYOD & Unmanaged Devices for Remote Users

The COVID-19 pandemic accelerated the need for companies to implement remote access for their employees, partners, contractors, and other third parties. In a rush to get remote access implemented, many companies decided to implement a policy in which these users could leverage BYOD and unmanaged devices. The problem with this approach is that in their rush, companies only thought about authenticating the user without considering what may be on whatever device the user employs for access. This oversight can lead to security holes in corporate applications and business operations from potentially misconfigured or compromised devices.

Utilizing BYOD and unmanaged devices in existing remote access solutions lack robust security measures

A traditional BYOD policy allows users to access corporate applications from personal devices. These personal devices are typically not enrolled into management platforms for privacy concerns. While this helps protect the privacy of those users, this puts companies at a disadvantage because of a lack of visibility into what is on the devices and there is no way to ensure that the devices are secure.

AmZetta raises the bar on BYOD and unmanaged device security

AmZetta's BYOD platform facilitates enterprise mobility by giving users the freedom to choose the device they want to use to access corporate applications and data, all while keeping security in the hands of the company's IT infrastructure. By utilizing AmZetta's Digital Workspace solution with BYOD, a secure container is set up in any device that is used to connect, thereby enabling secure access to corporate applications and data. Security measures include blocking/limiting internet access, USB port control, and the prevention of copying data from the local device using features such as copy/paste and screenshots. Multi-factor authentication can also be enabled to ensure proper user access from any device where built-in identity verification methods prevent unauthorized access and use. All of this allows companies to focus on business continuity without the massive headaches of security compliance from BYOD and unmanaged devices.

Features:

Access Flexibility

Allow BYOD users access to corporate apps through either zGateway or zPortal, depending on need.

Device Compliance Scans

Give authorized users access to only their required assets in the proper context.

Multi-factor Authentication

Leverage strong MFA to add an extra layer of security and enable companies to have stronger control over data access.

Prevent Data Leakage

Ability to block printing, screen recording, screenshots, copy/paste as well as access to local PC storage or USB storage devices. Control endpoint device access to Internet while connected.

Simplified Management

Comprehensive remote manageability of devices, including installation, upgrades, OS patching, etc. This helps massively reduce the traditional burden put on an IT team.

AmZetta Technologies
5555 Oakbrook Parkway,
Suite 280
Norcross, GA 30093

Sales & Product Info
sales@AmZetta.com
1-877.991.1809
https://amzetta.com

Technical Support
support@AmZetta.com
1-800.892.6625