36 Azure Virtual Desktop Security Guidelines Cheat Sheet – v1.0

36 AVD / Azure related security measures, with and without Nerdio divided into six distinct categories to get you started. There is a PDF available for download, which includes links to each item mentioned for additional information.

Introduction

This checklist / cheat sheet is meant as a starting point to secure your Azure Virtual Desktop environment, with and without Nerdio. This list gives you an overview on some of the most important and common security measures regarding the lockdown of your AVD / Azure estate. The below security measures are split up into distinct categories, some are additional paid for services and could be part of a Microsoft subscription / license you already own. Have a look **here**, a very well put together resource on all different MS 365 licensing models – credits: **@AaronDinnage**

Contents

Nerdio security checklist

Name: Harden the SQL service ✓
Additional information: Click here
Description: By default, communication between the app service and the SQL database is encrypted. The same applies to data at rest. Further harden security by adding the app service outbound IP address to the SQL firewall. This ensures that only requests from your Nerdio Manager instance's IPs are able to reach the server. Route traffic from the app service using a vNet. Create an Azure SQL service endpoint in the vNet. Traffic to the SQL Server can then be restricted to allow only traffic coming from the vNet.

Name: Harden storage account ✓
Additional information: Click here
Description: Storage Accounts are used by both AVD and Nerdio Manager to store various sorts of data. Most notably, storage accounts are used for holding end user's FSLogix Profiles, boot diagnostics, custom scripted actions, and MSIX app attach packages. This topic covers key steps and important considerations when implementing tighter security for common scenarios using storage accounts.

Name: Harden app service ✓
Additional information: Click here
Description: Nerdio Manager consists of a number of PaaS services. The entry point into the Nerdio Manager application is the App Service. By default, the Nerdio Manager app service is protected with Azure AD authentication, including MFA and conditional access, and is accessible from any internet location. It is possible to further protect the Nerdio Manager app service by using Access Restrictions or enabling a Private Endpoint. Removing the FTP service is another way to further lock down the service.

Name: App gateway and web app firewall ✓

Additional information: Click here

Description: The application gateway should be associated with a new URL/domain that can be directed to the gateway. For example, nmw.contoso.com. Obtain an SSL certificate: For secure HTTPS connections, you need an SSL certificate in PFX format to install on the gateway. The CN of the certificate should correspond to the domain you chose above. Public or Private: Decide whether the gateway is accessible from the public internet or restricted to your Azure network.

Other (Nerdio) considerations:

Name: Role Based Access ✓

Additional information: Click here

Description: Configure Role-based Access Controls (RBAC) to allow admins in your organization to sign in to Nerdio Manager and control which actions they can perform once signed in. Creating custom RBAC roles is optional as well. As a best practice, apply the “least privilege” principle.

Name: Scripted Actions ✓

Additional information: Click here

Description: Scripted Actions are PowerShell scripts that run either in the context of a Windows VM or an Azure Automation Account. When using sensitive information as part of your scripts Nerdio Manager allows you to manage these using Global Secure Variables. The variables are stored securely in an Azure Key Vault and can be passed to scripted actions using the $SecureVars.Variable_Name variable name.

General security best practices:

Name: Enable logging ✓

Additional information: Click here

Description: When using Nerdio logging is automatically enabled and accessible directly from the main console. Everything that happens within your environment is automatically logged, including date, day, and time stamps. It will also show you if it was an automated action (by auto scale, for example) or if a task was executed manually, by one of your admins. It also allows you to download various logs directly from an VM, when applicable for troubleshooting and analytic purposes. Of course, there are several ways outside of Nerdio to enable logging as well, like Azure (and Azure AD) activity logs, for example.

Name: Security awareness ✓

Additional information: Click here

Description: Probably step one in preventing unwanted access to your environment or machines and other components being infected (or taken over) with malicious software is security awareness training. Making sure you users are aware of phishing attacks and other types of threads while providing insights in how to recognize these attempts and educate them on the appropriate actions to take.

Name: Microsoft Secure Score ✓

Additional information: Click here

Description: Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more recommended actions to take. Following the Secure Score recommendations can protect your organization from threats.

Name: Azure Security Baseline for AVD ✓

Additional information: Click here

Description: The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Virtual Desktop. You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud.

Name: Azure Monitor ✓

Additional information: Click here

Description: Monitor your Azure Virtual Desktop service's usage and availability with Azure Monitor. Consider creating service health alerts for the Azure Virtual Desktop service to receive notifications whenever there is a service impacting event. Other third-party solutions include Control Up (DaaS), EG Innovations, Sepago Azure Monitor, and more.

Identity and access controls:

Name: Multi Factor Authentication ✓

Additional information: Click here

Description: Using Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password. You can enforce MFA for Azure Virtual Desktop using Conditional Access and can also configure whether it applies to the web client, mobile apps, desktop clients, or all clients.

Name: Conditional Access Policies ✓

Additional information: Click here

Description: Conditional access policies can be combined with MFA to enforce the use MFA to be applied. Other forms of CAP can be applied to geo-located based access and device-based access for AVD users. This way you make sure that only certain devices are allowed to connect to your (AD) environment and only from locations you approve.

Name: Risk based policies ✓

Additional information: Click here

Description: Another form of conditional access are risk-based policies (based on Azure AD). These allow you to automate the response to risks and allow users to self-remediate when a risk is detected. Being the Admin you can control the risk level to minimize the impact on the overall user experience. Organizations can choose to block users when a risk is detected or enable self-remediation based on MFA and secure password change.

Name: Azure policies ✓

Additional information: Click here

Description: Using Azure policies you can control the types of resources that are allowed to be created and deployed into a subscription. This way you make sure no unnecessary network resources are deployed, for example, public IP addresses, only allow the creation of certain virtual machine types / families, and more.

OS, machine, and data level security:

Name: Patch strategy ✓

Additional information: Click here

Description: Patching your applications (including any agents) and applying security updates is a recuring task. At least once a month security updates will have to be applied to your Windows operating system, for example. Nerdio offers several ways to help you automate this process. We are not the ones telling how and when to do it, though we do provide the tools to make this process as easy (and automated) as it possible can be. Think about an approach that best fits your practice and execute with consistency.

Name: Session time limits ✓

Additional information: Click here

Description: Within Nerdio you will find session time limits as part of a hostpools' properties (also configurable via GPO's). Giving these some thought will help you secure your environment by signing users out when they are inactive, preserving resources and it prevents access by unauthorized users. It is always going to be a fine line between the users' productivity and overall security, finding the right balance can be challenging but worth the effort. Nerdio auto scale can be used in combination to make sure machines are shut down (or removed completely) to save on additional resource cost and make sure machines are not exposed while not in use.

Name: Control device redirection policies ✓

Additional information: Click here

Description: This will help in making sure data can not be accidently shared and stored. Again, it is all about finding the right balance between productivity and security. Nerdio offers RDP "profiles" for you to configure and apply per host pool. The most obvious ones to think about are printers, USB devices, local drives, clipboard, screenshots, and the camera.

Name: Microsoft Defender ✓

Additional information: Click here

Description: Make sure all your AVD hosts are part of Microsoft defender for Endpoint and schedule regular scans. A third-party anti virus solution is also optional. Excluding the VHD extension, when using FSLogix, for example. Endpoint Detection and Response (EDR) capabilities, also part of Defender for Endpoint provides advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats. NOTE… Do not confuse MS Defender for Endpoint with Microsoft 365 Defender (or the Cloud version, see below), they are different (and separate) products, though they can work side-by-side and can be integrated as well.

Name: Microsoft Defender for Cloud ✓

Additional information: Click here

Description: It probably should not be lister under “OS and machine level security” but since I highlighted Microsoft Defender I thought it would make sense to mention it here. Defender for Cloud will help to strengthen the overall security of your (AVD / Azure) environment and can help with managing various vulnerabilities and assess compliance with common frameworks like PCI. It also lets you configure enhanced security policies over multiple tenants and / or workspace as well as use Microsoft Defender for Cloud to help you identify problem spots through the Microsoft Defender for Endpoint's threat and vulnerability management solution.

Name: Data Loss Prevention ✓

Additional information: Click here

Description: Use Microsoft (Purview) Data Loss Prevention (DLP) to monitor the actions that are being taken on items you have determined to be sensitive and to help prevent the unintentional sharing of those items. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

Name: Microsoft Purview Information protection (formerly MIP) ✓

Additional information: Click here

Description: Another one from the Purview suite. According to Microsoft: Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels. These information protection capabilities give you the tools to know your data, protect your data, and prevent data loss.

Name: Security Policy Advisor (Office 365) ✓

Additional information: Click here

Description: In addition to securing your session hosts, it is important to also secure the applications running inside of them. As we all know, Office pro Plus is one of the commonly used pieces of software. Using the Security Policy Advisor helps you to identify policies that can be applied to your deployment. It will recommend policies based on the impact on overall security and productivity.

Name: Trusted Launch ✓

Additional information: Click here

Description: Available directly from within Nerdio. Azure offers trusted launch as a seamless way to improve the security of generation 2 VMs. Trusted launch protects against advanced and persistent attack techniques. Trusted launch is composed of several, coordinated infrastructure technologies that can be enabled independently. Each technology provides another layer of defence against sophisticated threats. Be sure that the desktop image used for this host pool supports Trusted Launch. It must be an Azure Marketplace image or an Azure Compute Gallery image with Trusted Launch enabled.

Name: vTPM ✓

Additional information: Click here

Description: A sub technology of Trusted Launch mentioned above. It stands for Virtual Trusted Platform Module. (vTPM) is TPM2.0 compliant and validates your VM boot integrity apart from securely storing keys and secrets. It is actually a software-based representation of a physical Trusted Platform Module 2.0 chip normally found in desktop, laptops, and such.

Name: Secure Boot ✓

Additional information: Click here

Description: Again, another sub technology that falls under the Trusted Launch umbrella. Secure boot helps protect your VMs against boot kits, rootkits, and kernel-level malware. Once Trusted Launch is enabled in Nerdio (though, it is available outside of Nerdio as well, of course), both vTPM and Secure Boot becomes available as separate options to enable.

Name: Host encryption ✓

Additional information: Click here

Description: When you enable encryption at host, that encryption starts on the VM host itself. The data for your temporary disk and OS/data disk caches are stored on that VM host. After enabling encryption at host, all this data is encrypted at rest and flows encrypted to the Storage service, where it is persisted. Encryption at host encrypts your data from end-to-end. Encryption at host does not use your VM's CPU and does not impact your VM's performance. Make sure to have a look at the prerequisites and restrictions.

Name: Watermark (preview) ✓

Additional information: Click here

Description: Watermarking, alongside screen capture protection (see below), helps prevent sensitive information from being captured on client endpoints. When you enable watermarking, QR code watermarks appear as part of remote desktops. The QR code contains the connection ID of a remote session that admins can use to trace the session. Watermarking is configured on session hosts and enforced by the AVD client.

Name: Screen capture ✓

Additional information: Click here

Description: Helps prevent sensitive information from being captured on client endpoints. When you enable screen capture protection, remote content will be automatically blocked or hidden in screenshots and screen shares. Also, the Remote Desktop client will hide content from malicious software that may be capturing the screen. It can be used in combination with Watermark, as highlighted above.

Name: Sandbox ✓

Additional information: Click here

Description: Some users need to be able to instal software on their virtual machines, power users and developers are good examples. Windows Sandbox provides a lightweight desktop environment to safely run applications in isolation. Software installed inside the Windows Sandbox environment remains "sandboxed" and runs separately from the host machine. Please note that Windows Sandbox enables network connection by default. These can be disabled using the Windows Sandbox configuration file.

Name: AppLocker ✓

Additional information: Click here

Description: AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers. When a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organization if a user knowingly or unknowingly runs malicious software. AppLocker can help mitigate these types of security breaches by restricting the files that users or groups are allowed to run.

Network security

Name: Machine exposure ✓

Additional information: Click here

Description: Make sure to not expose any machines directly to the internet through RDP. Instead, consider using an Azure Bastion host. Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal, or via the native SSH or RDP client already installed on your local computer. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software. Also, AVD uses a technology named; Reverse Connect, meaning all inbound traffic can (and should be) be disabled. It uses outbound connectivity to the AVD infrastructure over a HTTPS connection (there is no TCP listener).

Name: Network Security Groups ✓

Additional information: Click here

Description: You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. AVD network traffic can be limited using service tags.

Name: Proxy Server ✓

Additional information: Click here

Description: It is recommended to bypass proxies for Azure Virtual Desktop traffic. Proxies do not make Azure Virtual Desktop more secure because the traffic is already encrypted. Also, they cause performance related issues in the form of latency degradation and packet loss. If your organization's network and security policies require proxy servers for web traffic, you can configure your environment to bypass Azure Virtual Desktop connections while still routing the traffic through the proxy server.

Name: Azure Firewall ✓

Additional information: Click here

Description: The Azure virtual machines you create for Azure Virtual Desktop must have access to several Fully Qualified Domain Names (FQDNs) to function properly. Azure Firewall provides an Azure Virtual Desktop FQDN Tag to simplify this configuration. Your AVD hosts need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic. When VNet integration is applied to the Nerdio Manager app, the network connectivity flow changes. In most cases, the subnet has outbound access restricted. To overcome that, the following addresses need to have access allowed in order for Nerdio Manager to work as required. Also see **this article** for an overview.

Name: Network segmentation ✓

Additional information: Click here

Description: In most AVD deployments some form of testing will be necessary. Security patches, new applications, image updates, and more. As a best practice make sure to separate production and non-production environments at a network level. Separate networks based on vNets / Subnets. By default, subnets on Azure are able to communicate. You can create custom routes overwriting Azure's default behaviour, creating your own security boundary.

Thank you very much for reading, I hope this was helpful. Please, let me know when you have any suggestions on what to add, remove, change, or other comments.