

"How to become BFFs with your CISO."

- Zero Trust

Merdio Con

2025 PALM SPRINGS

Agenda

Zero Trust: A state of mind

Mapping Zero Trust to NME security features

Let's play... The Weakest Link

Q&A final takeaways



Greg Roberson

Principal Enterprise Sales Engineer

Joined Nerdio 4 years ago

Based out of the United States





Doug Lind

Principal Architect

Joined Alchemy Tech Group 7 years ago

Based out of the United States







Zero Trust: A state of mind





Mapping Zero Trust to NME security features Authentication

- Enforce Multi-Factor Authentication (MFA) for AVD & W365
 - Identity and verify devices at every access request.
 - Biometrics
- Enable Conditional Access to protect access based on device, location and risk factors
 - Contextual authentication
- AD Join Account
 - Dedicated user account with minimal privileges to join session hosts
 - Separate OUs per Host Pool
- Supported authentication methods
 - Entra ID
 - Entra ID + AD DS
 - Entra ID + Entra DS
 - Entra ID + Entra DS + AD DS



Mapping Zero Trust to NME security features Nerdio RBAC

- Nerdio RBAC
 - Built in RBAC
 - AVD Admin: Full access to all areas
 - Desktop Admin: User sessions, view/restart VM, Images, Scripted Actions
 - End-User: Manage personal VM
 - Help Desk: Users sessions only
 - Intune: Applications, Update, Scripts, Bitlocker, AV
 - Segregate responsibilities
 - Windows 365/Intune management
 - Workspace and Host Pool
 - PIM (Privileged Identity Management)
 - Require permissions to be checked out on limited times schedules

Ω		
CONFIGURE INTUNE	r Entra ID usar group	
Intune integration can be limited by device type of	r Entra ID user group.	
CURRENT STATUS ①		
CONFIGURABLE FEATURES		
Intune managed devices* (i)	 Read-only 	O Manage
Group membership (1)	 Read-only 	O Manage
 Privileged operations (3) 	O Read-only	O Manage
Local Admin Password ③	 Read-only 	O Manage
Scripts ①	Read-only	— N/A
Cloud PC ④	— N/A	O Manage
Hide individual Cloud PC hosts page (recomme	ended) ④ On	
 Conditional Access policies (1) 	 Read-only 	O Manage
Intune Applications and App policies ①	 Read-only 	O Manage
✓ Device policies ④	 Read-only 	O Manage
DEVICE VISIBILITY SCOPE LIMITATIONS		
Device platform ④		
₩indows DioS/iPadOS × ÓmacOS ×		×
Windows Device type scope ④		
QAII X		×
Limit by Entra ID group ①		
OUser Groups (1) O Device Groups (1)		

Mapping Zero Trust to NME security features Assume breach

- Enforce Threat Protection: Implementation for Defender for Identity and Office 365
 - Prevent breaches, using proactive identity security posture assessments
 - o Detect threats, using real-time analytics and data intelligence
 - o Investigate suspicious activities, using clear, actionable incident information
 - Respond to attacks, using automatic response to compromised identities
- o NME actions
 - Intune policy configuration and enforcement
 - Enforcing at a global level
 - Compliance policy/baseline
 - Windows update policies
 - Conditional access policy
 - Alerts (CPC, Intune, Actions)
 - Monitoring deployment (AVD insights, ContolUp, Sepago) via policy
 - Nerdio AI KQL generation
 - Logging admin actions

	uues	Ta
		ta (V
	NAME ©	th co
	Intune certificate issues (Warning)	Ke
	Intune certificate issues (High)	ті
	Intune managed app install (Warning)	CC
	Intune managed app install (High)	Ca Us
	Intune patch issues (Warning)	kr
	Intune patch issues (High)	K
	Intune config policy issues (Warning)	
,	Intune config policy issues (High)	
	Intune compliance issues (Warning)	
	Intune compliance issues (High)	
	10 items	

write me a kusto query to discover all avd desktop users in the last 30 days

User's intent is to generate a query that identifies all unique Azure Virtual Desktop (AVD) users who have used desktop connections in the last 30 days.

Start by analyzing the requirements to determine which data table and fields are relevant:

Table: Based on the context, IMPConnect ions is the appropriate table. It stores connections related to Windows Virtual Desktop (WVD), where we can relate it to Azure Virtual Desktop (AVD) as these names are often used interchangeably in a technical context. Key Columns:

inegenerated: This column helps filter the data to capture nly the events from the past 30 days. prinectionType: We will ensure only desktop connections are aptured by filtering this column with "Desktop". serName: This is the key field of interest as the user wants to

ow distinct users, so we'll identify unique usernames

WVDConnections		
where TimeGenerated >= ago(30d)	//	Filter
for the past 30 days		
where ConnectionType == "Desktop"	//	
Specifically focus on desktop connection	ns	
distinct UserName	//	Extract
distinct usernames		
project UserName	//	Display
the usernames		

Enforce device health and compliance

- Intune policies—Safeguard
 - Backup
 - Scheduled backups
 - o Opportunistic Backup if changed
 - Restore
 - Recover deleted or modified polices
 - Compare
 - Compare old/new policies for policy creep
- Policy management
 - Compliance
 - Antivirus, BitLocker, Firewall, device
 - Configuration
 - Antivirus configuration, device
 - Security baselines
 - o Windows, Defender, 365 Apps, Edge

- Conditional access
 - Device, location, application, risk factors
- Applications
 - Protection policies
- Updates
 - o Ensure security updates are applied regularly



Secure access to applications & data

- Nerdio application access
 - o Enable Azure MFA
 - Access restrictions (IP, Internal, etc)-vNet integration
- Private endpoints
 - KeyVault, FSLogix, SQL, Automation Account, Nerdio App Service
- Enable script signing

Linked signing certificates (i)	GENERATE SELF-SIG	INED CERTIFICATE		
Link	KEY VAULT	Select	~	•
Generate	SUBJECT VALIDITY PERIOD	CN= 60	months	0
		Canc	el Crea	te

• SQL

- Add the app service's outbound IP addresses to the Azure SQL Server's firewall to ensure that only requests from your Nerdio Manager instance's IPs are able to reach the server
- CIS Hardened Images and Policy
 - o Images that come pre-hardened in accordance with the CIS benchmarks

CIS Hardened Image Level 1 on Microsoft Windows 11 Enterprise - Gen2 (single-session) [paid]

CIS Hardened Image Level 1 on Microsoft Windows 10 Enterprise Multi-Session - Gen2 (multi-session) [paid]

CIS Hardened Image Level 1 on Microsoft Windows 10 Enterprise - Gen2 (single-session) [paid]

CIS Hardened Image Level 1 on Microsoft Windows Server 2022 - Gen2 (multi-session) [paid]

CIS Hardened Image Level 1 on Microsoft Windows Server 2019 - Gen2 (multi-session) [paid]



Monitor and log all activity

• AI-Driven Personally-Identifiable Information (PII) Alerts

- Receive intelligent alerts when PII is discovered within Nerdio Manager logs. This feature requires
 Azure AI services to be enabled.
- Nerdio Log Shipping
 - Nerdio Manager allows for all console logs to be redirected to the Nerdio Manager Application Insights workspace. From here, the logs can be interrogated directly using standard workspace queries, exported manually for review, or accessed programmatically via API. This allows administrators to ingest Nerdio Manager logs into a log management SIEM solution.
- Diagnostic Logs
 - Collect all AVD Host logs for inspection

Event name	Error	Warning	Information
Application			
Microsoft-FSLogix-Apps/Admin			
Microsoft-FSLogix-Apps/Operational	•		
${\it Microsoft-Windows-TerminalServices-LocalSessionManager/Oper}$			
${\it Microsoft-Windows-Terminal Services-RemoteConnection Manage}$			
System			

Use network & micro segmentation

- Azure Firewall with TLS
 - Nerdio Script Deploy
 - Inspect incoming traffic
 - Azure Bastion
 - VPN/Express Route
 - DDOS Protection to all spokes vnets
- Segmentation
 - Conforms to CAF Landing Zone topology
 - Deploy vNets in a Hub and Spoke topology
 - Individual vNet spoke cannot directly communicate without going through a Hub vNet
- Breach
 - With network segmentation, the ability to spread past the Azure Firewall is limited. Only the same workload would be allowed through.



ubnets	
Select	
VICCTINC-00 (TRIVE (URSOUCH, 192, 100.0.0/24)	
vnet-nme-weurope-001/default (westeurope, 192.	168.2.0/24)
AZURE SUBSCRIPTION 1 (DF3FB09B-9030-411E-A2D3-5A7184ED77E8))
chris-vnet-eastus/default (eastus, 10.0.0.0/24)	
JsmithVnet-AVD/default (eastus, 10.0.0/24)	
KG-Temp-Vnet/default2 (westus, 10.20.0.0/24)	
Nerdio-Admin-Vnet/AzureBastionSubnet (westus2, 6)	. 10.10.1.64/2
Nerdio Admin Vnet/ChrisTectSubnet (westus2 10)	10.1.0/26)

Automate threat detection and response

• RDP

- Ensure RDP settings are not changed. Keep the consistent at the Host Pool level
 - Eg. Copy/paste, local drive redirection, local US B redirection
- Session time limits
 - Establish maximum inactive time and disconnection policies
 - Screen lock for idle sessions
- Patch orchestration
 - Automatic for AVD + Windows server
 - Script updates on a regular basis
- Encryption at Host
 - Encrypts your data from end-to-end
- Watermarking
 - Protect sensitive data
- Enforce Intune compliance at the Host Pool level

•		NEW
Enable H.265 encoding on supported	VM sizes (PREVIEW) ③	
Patch orchestration options. ④	þefault 🗸	
🗌 Enable encryption at host 🕄	Default	
Enable boot diagnostics ③		
Enable watermarking ④	Manual updates	
Security type 🛈	Automatic by OS (Windows Automatic Updates)	
Secure Boot ④	Azure-orchestrated	
VTPM 🛈		
Integrity Monitoring ③		

Apply encryption everywhere

Secure variables

- Run scripted actions utilizing encrypted variables
- All variables are encrypted at rest and in transit
- BitLocker
- Nerdio can setup and track BitLocker keys and configuration
- Security Type
- Trusted Launch
- Secure boot: OS boot components
 - TPM: (virtual trusted platform module)
 - Confidential compute
 - Protect data in use by performing computation in a hardware-based, attested trusted execution environment

lame ④		
APIKey		
alue 🕄		
	SI	how
Allow usage within shell apps ④		
Pass variable to specified scripted actions or	ily 🛈	
cripted actions ④		
1. 🕂 Install 7zip via Chocolatey (Combined) [Nerdio, A	vpp 🗸	
1. 📫 Install 7zip via Chocolatey (Combined) [Nerdio, A s install, Chocolatey]	^{ypp} × X	~
1. Install 7zip via Chocolatey (Combined) [Nerdio, A s install, Chocolatey] Scripted actions: Use \$SecureVars.APIKey with action.	hin the scripted	4
1. Install 7zip via Chocolatey (Combined) [Nerdio, A s install, Chocolatey] Scripted actions: Use \$SecureVars.APIKey with action. Shell app scripts: Read the Parameterization s to learn about parameterization.	hin the scripted	~ н
1. Install 7zip via Chocolatey (Combined) [Nerdio, A s install, Chocolatey] Scripted actions: Use \$SecureVars.APIKey with action. Shell app scripts: Read the Parameterization s to learn about parameterization.	^{pp} x X	ч са

Adopt a Zero Trust mindset across the organization

- Provide role-specific access insights and enforce compliance reporting to educate users on secure access practices.
 - Let's play the weakest link!





Let's play... The Weakest Link



What percentage of all security issues originate with one single user?







Adopt a Zero Trust mindset across the organization

- 94% of security breaches involve human error (phishing, weak passwords, accidental data exposure).
- Security policies alone won't stop a well-crafted phishing attack or social engineering attack.
- If users don't know why a policy exists, they will find ways to bypass it. Or simply won't apply it all.
- People have different roles and therefore will encounter different types of threats.
- Mapping ideas to competence...



Make security personal. Make it relevant. Make it role-based.

Train for context, not checklists Adapt to roles, not departments Explain the why, not just the what





Thank you...

Enjoy the rest of NerdioCon