
NerdioCon
2025
PALM SPRINGS

NerdioCon
2025
PALM SPRINGS

“How to become BFFs with your CISO.”

- Zero Trust

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


NerdioCon
2025
PALM SPRINGS
Zero Trust: A state of mind

ZERO TRUST PRINCIPLES

Verify explicitly

Use least privileged access

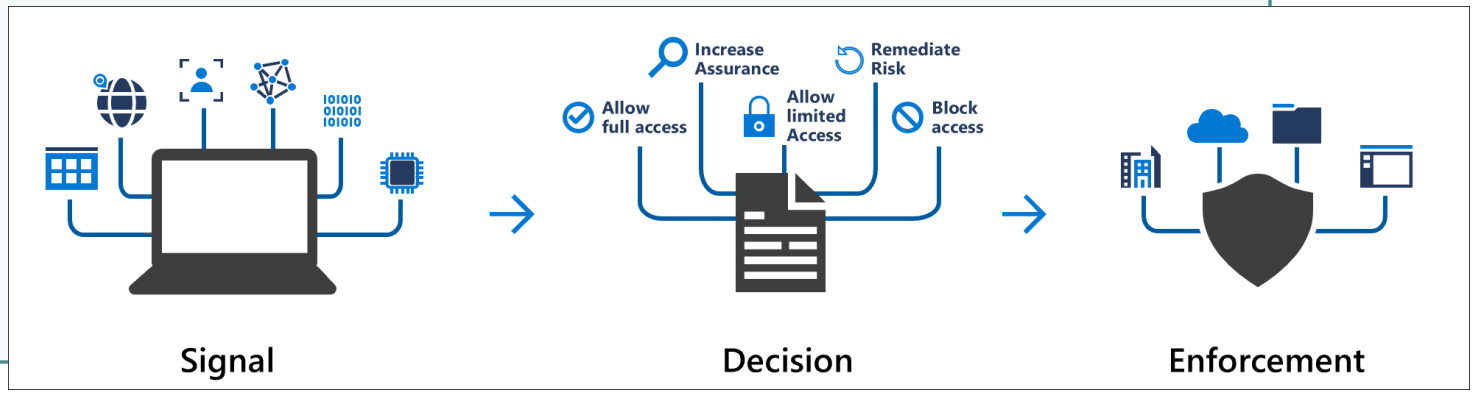
Assume breach

Mapping Zero Trust to NME security features

Mapping Zero Trust to NME security features

Authentication

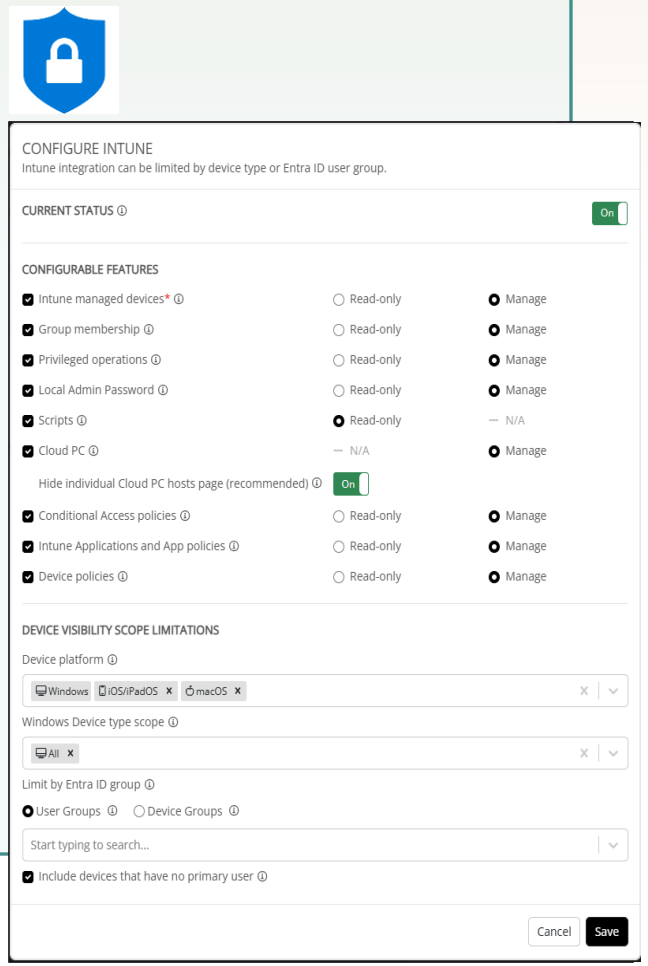
- Enforce Multi-Factor Authentication (MFA) for AVD & W365
  - Identity and verify devices at every access request.
  - Biometrics
- Enable Conditional Access to protect access based on device, location and risk factors
  - Contextual authentication
- AD Join Account
  - Dedicated user account with minimal 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

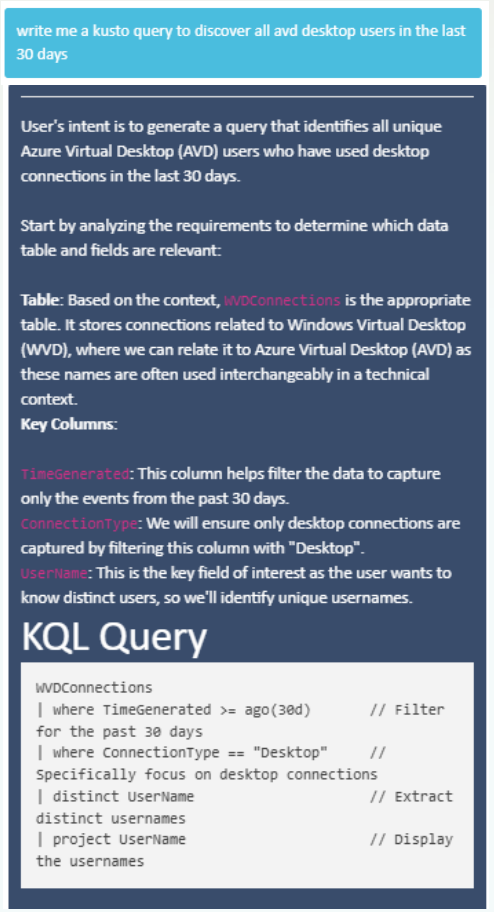
- Nerdio RBAC
  - Built in RBAC
    - AVD Admin: Full access to all areas
    - Desktop Admin: User sessions, view/restart VM, Images, Scripted Actions
    - End-User: Manage personal VM
    - Help Desk: Users sessions only
    - Intune: Applications, Update, Scripts, Bitlocker, AV
  - Segregate responsibilities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



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
  - Detect threats, using real-time analytics and data intelligence
  - Investigate suspicious activities, using clear, actionable incident information
  - Respond to attacks, using automatic response to compromised identities
- 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



Mapping Zero Trust to NME security features

Enforce device health and compliance

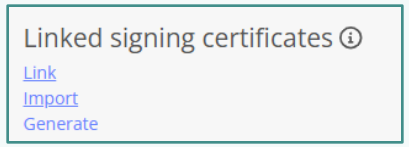
- Intune policies—Safeguard
  - Backup
    - Scheduled backups
    - Opportunistic Backup if changed
  - Restore
    - Recover deleted or modified polices
  - Compare
    - Compare old/new policies for policy creep
- Policy management
  - Compliance
    - Antivirus, BitLocker, Firewall, device
  - Configuration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

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

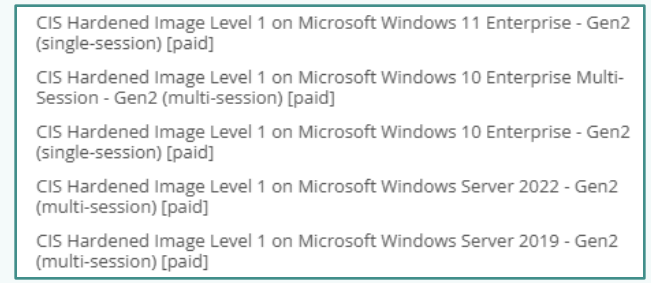
Mapping Zero Trust to NME security features

Secure access to applications & data

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



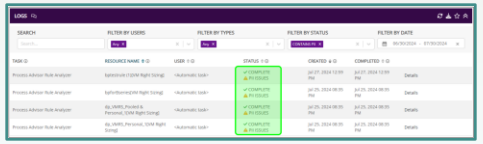
- SQL
  - Add the app service's outbound IP addresses to the Azure SQL Server's firewall to ensure that only requests from your Nerdio Manager instance's IPs are able to reach the server
- CIS Hardened Images and Policy
  - Images that come pre-hardened in accordance with the CIS benchmarks



Mapping Zero Trust to NME security features

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.

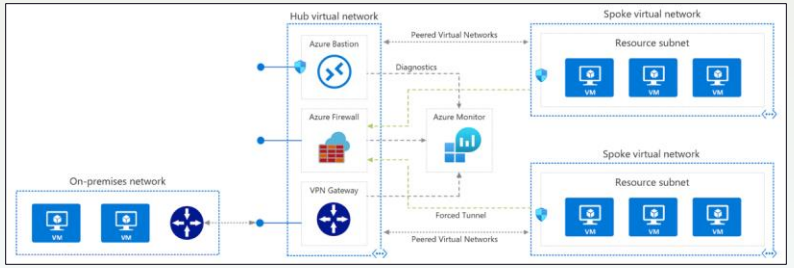


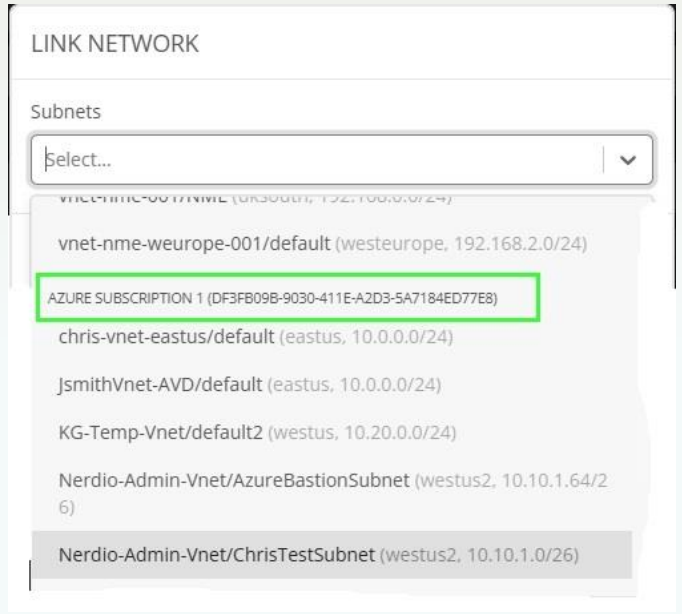
- Nerdio Log Shipping
  - Nerdio Manager allows for all console logs to be redirected to the Nerdio Manager Application Insights workspace. From here, the logs can be interrogated directly using standard workspace queries, exported manually for review, or accessed programmatically via API. This allows 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	☑	☑	☑
Microsoft-Windows-TerminalServices-LocalSessionManager/Oper...	☑	☑	☑
Microsoft-Windows-TerminalServices-RemoteConnectionManage...	☑	☑	☑
System	☑	☑	☑

Mapping Zero Trust to NME security features

Use network & micro segmentation



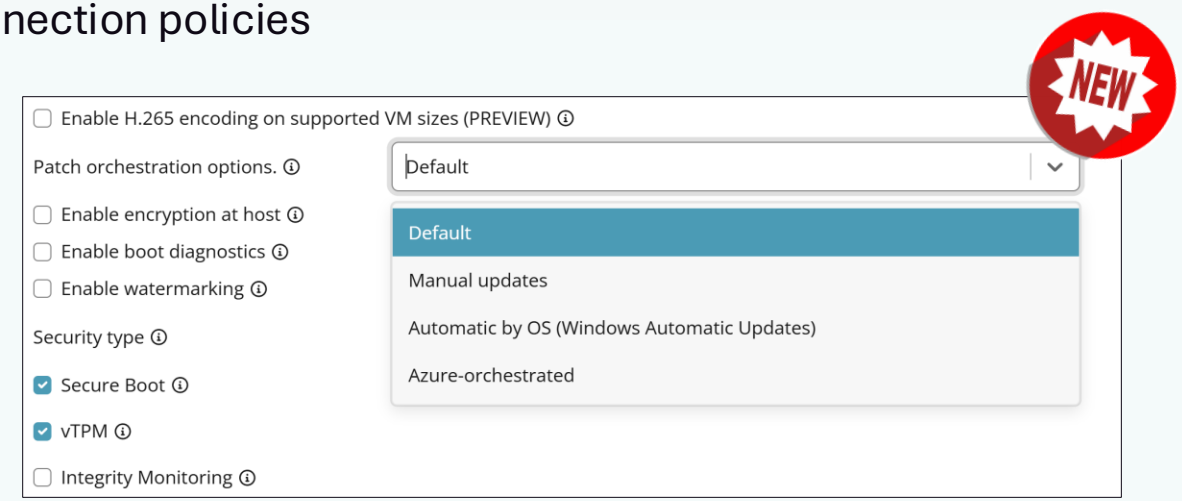


- Azure Firewall with TLS
  - Nerdio Script Deploy
  - Inspect incoming traffic
  - Azure Bastion
  - VPN/Express Route
  - DDOS Protection to all spokes vnets
- Segmentation
  - Conforms to CAF Landing Zone topology
  - Deploy vNets in a Hub and Spoke topology
  - Individual vNet spoke cannot directly 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.

Mapping Zero Trust to NME security features

Automate threat detection and response

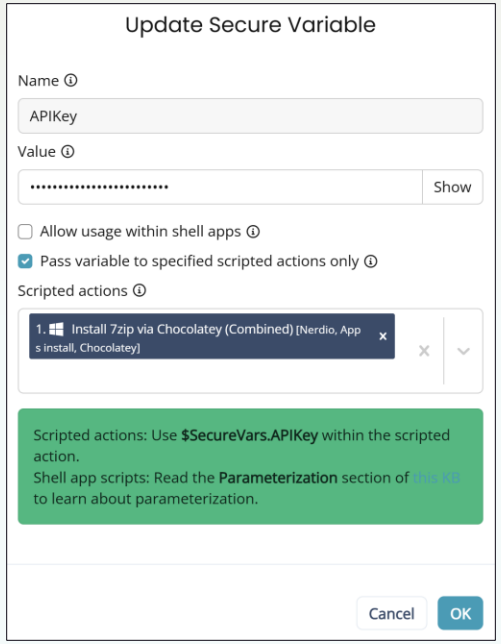
- RDP
  - Ensure RDP settings are not changed. Keep the consistent at the Host Pool level
    - Eg. Copy/paste, local drive redirection, local US B redirection
- Session time limits
  - Establish maximum inactive time and disconnection policies
  - Screen lock for idle sessions
- Patch orchestration
  - 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



Mapping Zero Trust to NME security features

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



Mapping Zero Trust to NME security features

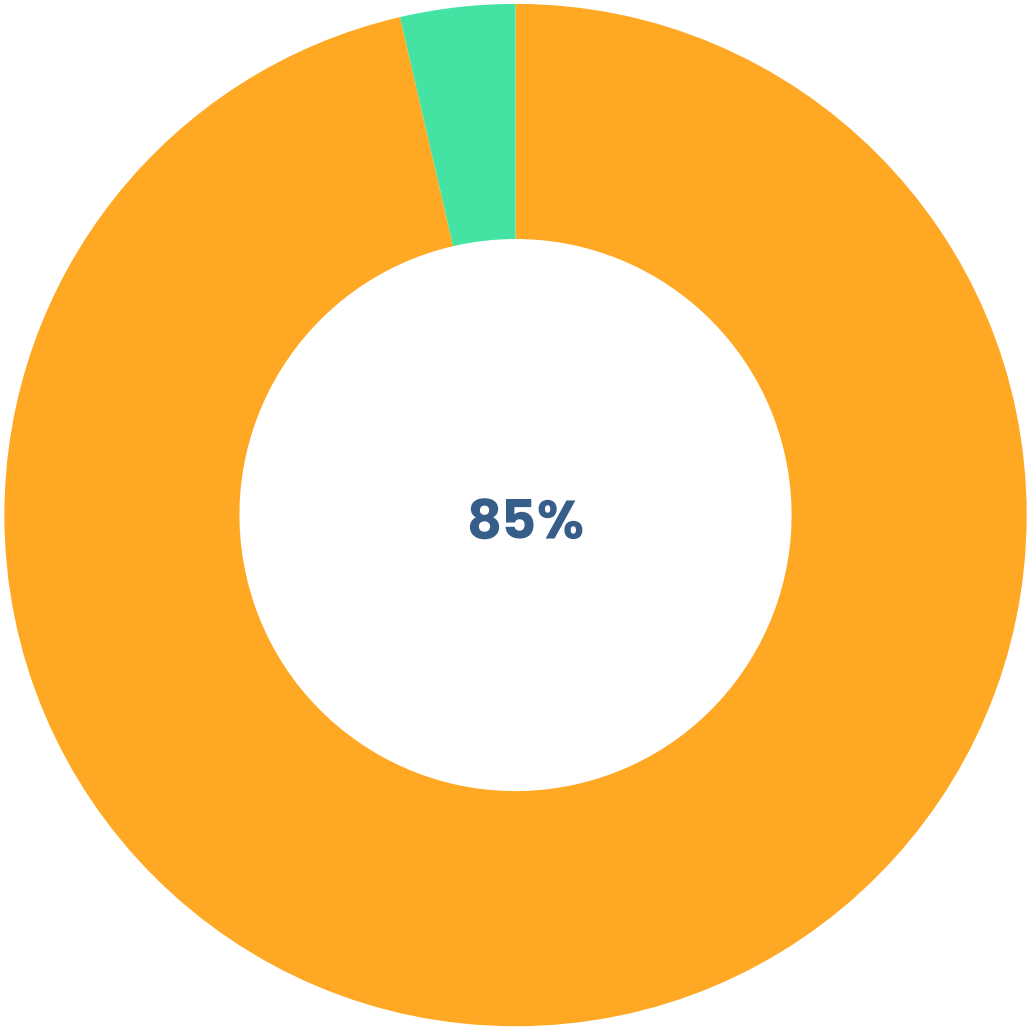
Adopt a Zero Trust mindset across the organization

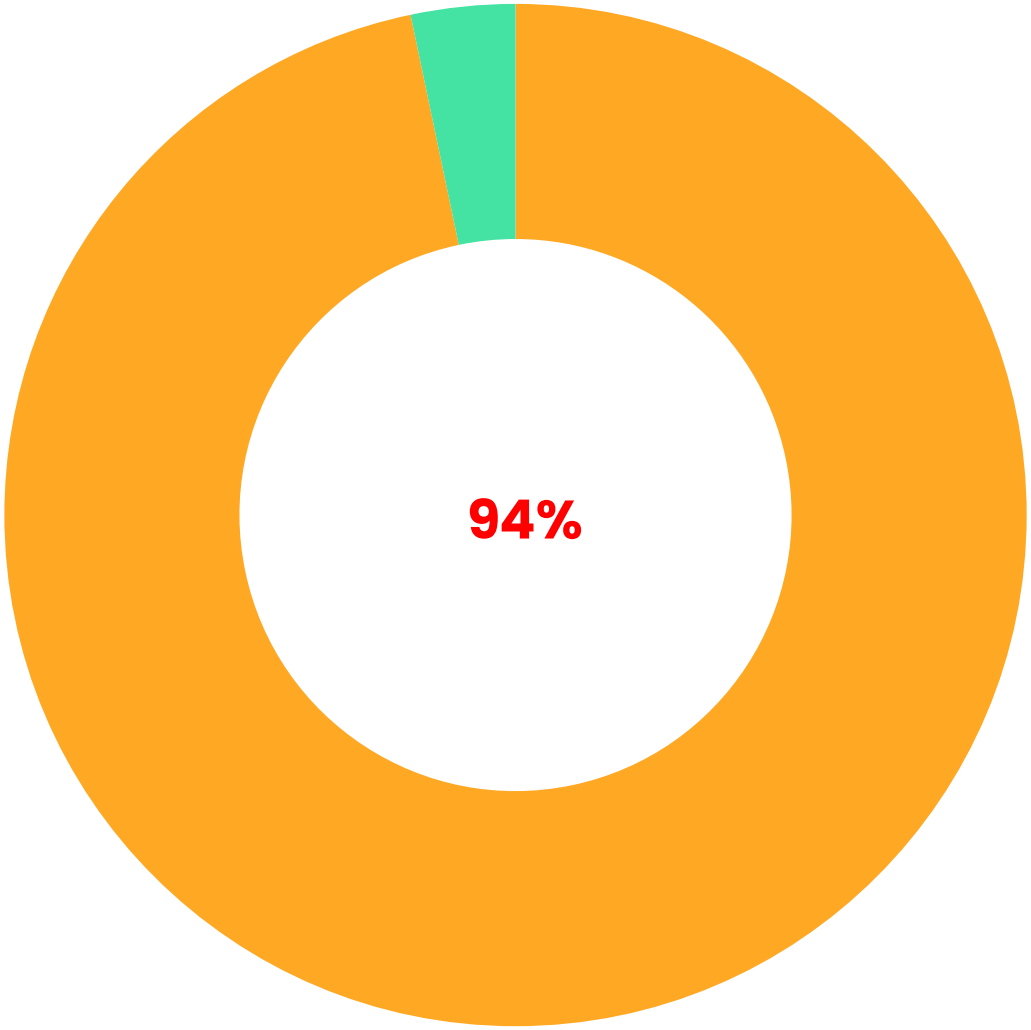
- Provide role-specific access insights and enforce compliance reporting to educate users on secure access practices.
  - Let's play the weakest link!

Let’s play… The Weakest Link

Question:

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


85%


94%

Mapping Zero Trust to NME security features

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


NerdioCon
2025
PALM SPRINGS
Q&A


NerdioCon
2025
PALM SPRINGS
Thank you...
Enjoy the rest of NerdioCon