TITAN AI — AZURE Live Scan

Report ID: **AZL-20260426-132706**

Customer: **TITAN AI Live Demo**

Generated: **2026-04-26T13:27:06.4993506-05:00**

Subscription: **Pay-As-You-Go** · Resource Group: **rg-titandemo-260426-1324**

Priority Buckets

Priority	Count	SLA
P1 (24 hours)	3	Internet-facing + PHI + exploit-in-wild stacked
P2 (72 hours)	4	Two-factor risk
P3 (next sprint)	1	Lower-risk / context-only

Severity Distribution

Severity	Count
Critical	4
High	3
Medium	1
Low	0

Findings — with priority, ATT&CK;, attack path, and remediation playbook

[P2] CRITICAL — nsg_open_to_internet on nsg-titandemo-public/BAD-allow-ssh-from-internet

SSH exposed to 0.0.0.0/0

Citation	HIPAA 164.312(e)(1) Transmission Security
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > NSG nsg-titandemo-public > Subnet/NIC > Workload VM
Path length	3 hops
Recommendation	Restrict source to corporate IP ranges or remove rule entirely.

Playbook — Network/Security · 24-72 hours

1. Identify which subnet/NIC the NSG attaches to (Get-AzNetworkSecurityGroup)
2. Replace 0.0.0.0/0 source with corporate CIDR ranges or VPN gateway
3. Update Azure Firewall + Bastion if RDP/SSH access still needed
4. Re-scan to verify rule removed
5. Document change in CAB ticket

[P2] CRITICAL — nsg_open_to_internet on nsg-titandemo-public/BAD-allow-rdp-from-internet

RDP exposed to 0.0.0.0/0

Citation	HIPAA 164.312(e)(1) Transmission Security
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > NSG nsg-titandemo-public > Subnet/NIC > Workload VM
Path length	3 hops
Recommendation	Restrict source to corporate IP ranges or remove rule entirely.

Playbook — Network/Security · 24-72 hours

1. Identify which subnet/NIC the NSG attaches to (Get-AzNetworkSecurityGroup)
2. Replace 0.0.0.0/0 source with corporate CIDR ranges or VPN gateway
3. Update Azure Firewall + Bastion if RDP/SSH access still needed
4. Re-scan to verify rule removed
5. Document change in CAB ticket

[P2] CRITICAL — nsg_open_to_internet on nsg-titandemo-public/BAD-allow-sql-from-internet

SQL Server exposed to 0.0.0.0/0

Citation	HIPAA 164.312(e)(1) Transmission Security
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	Internet-facing, Business-critical
MITRE ATT&CK	T1133 - External Remote Services
Attack path	Internet > NSG nsg-titandemo-public > Subnet/NIC > Workload VM
Path length	3 hops
Recommendation	Restrict source to corporate IP ranges or remove rule entirely.

Playbook — Network/Security · 24-72 hours

1. Identify which subnet/NIC the NSG attaches to (Get-AzNetworkSecurityGroup)
2. Replace 0.0.0.0/0 source with corporate CIDR ranges or VPN gateway
3. Update Azure Firewall + Bastion if RDP/SSH access still needed
4. Re-scan to verify rule removed
5. Document change in CAB ticket

[P1] CRITICAL — storage_public_blob on satitandemo2604261324

Anonymous blob access enabled (PHI exposure risk)

Citation	HIPAA 164.502 Uses and Disclosures
Priority	P1 • Fix in 24 hours • score 75/100
Risk factors	Internet-facing, PHI-exposure, Business-critical
MITRE ATT&CK	T1530 - Data from Cloud Storage
Attack path	Internet > Public Blob Endpoint > PHI/PII Container

Path length	1 hops
Blast radius	1 storage_account
Recommendation	Set AllowBlobPublicAccess=false.

Playbook — Storage Owner + Privacy · 1-2 days

1. Set-AzStorageAccount -AllowBlobPublicAccess $false on the storage account
2. Audit storage diagnostic logs (last 90 days) for any anonymous reads
3. If access detected on PHI containers: trigger HIPAA breach assessment within 60 days
4. Enable Azure Defender for Storage (continuous threat detection)
5. Configure Storage Firewall: PublicNetworkAccess=Disabled, allowlist VNet subnets

[P2] HIGH — storage_http_allowed on satitandemo2604261324

HTTP traffic allowed - PHI in transit not encrypted

Citation	HIPAA 164.312(e)(2)(ii) Encryption
Priority	P2 • Fix in 72 hours • score 50/100
Risk factors	PHI-exposure, Business-critical
MITRE ATT&CK	T1040 - Network Sniffing
Attack path	Internet > Public Blob Endpoint > PHI/PII Container
Path length	1 hops
Blast radius	1 storage_account
Recommendation	Set EnableHttpsTrafficOnly=true.

Playbook — Storage Owner · Same day

1. Set-AzStorageAccount -EnableHttpsTrafficOnly $true
2. Verify clients support TLS 1.2+ (legacy SDKs may break)
3. Re-scan to confirm
4. Update IaC template (Bicep/Terraform) so it doesn't drift back
5. Document change

[P1] HIGH — storage_public_network on satitandemo2604261324

Storage exposed to all networks (no firewall)

Citation	HIPAA 164.312(c)(1) Integrity Controls
Priority	P1 • Fix in 24 hours • score 75/100
Risk factors	Internet-facing, PHI-exposure, Business-critical
MITRE ATT&CK	T1530 - Data from Cloud Storage
Attack path	Internet > Public Blob Endpoint > PHI/PII Container
Path length	1 hops
Blast radius	1 storage_account
Recommendation	Set PublicNetworkAccess=Disabled or configure NetworkRuleSet.

Playbook — Storage Owner + Network · 1-3 days

1. Identify all consumers of this storage account (find downstream apps/services)

2. Configure NetworkRuleSet with VNet allowlist + IP allowlist for build agents
3. Set PublicNetworkAccess=Disabled
4. Use Private Endpoints for service-to-service traffic
5. Re-scan + verify clients still connect via private path

[P1] HIGH — keyvault_public_network on kv-titandemo-260426-1324

Key Vault exposed to public network

Citation	HIPAA 164.312(a)(1) Access Control
Priority	P1 • Fix in 24 hours • score 75/100
Risk factors	Internet-facing, PHI-exposure, Business-critical
MITRE ATT&CK	T1528 - Steal Application Access Token
Attack path	Internet > Key Vault Public Endpoint > Secrets/Keys/Certs
Path length	1 hops
Blast radius	1 key_vault
Recommendation	Set PublicNetworkAccess=Disabled and use private endpoint.

Playbook — Security + App Owner · 1-2 days

1. Inventory which apps/Functions reference secrets in this Key Vault
2. Set PublicNetworkAccess=Disabled and configure Private Endpoint
3. Update consumer apps to use Private Endpoint DNS
4. Test secret retrieval from each consumer
5. Re-scan

[P3] MEDIUM — keyvault_no_purge_protection on kv-titandemo-260426-1324

Purge protection disabled - keys can be permanently deleted

Citation	HIPAA 164.308(a)(7) Contingency Plan
Priority	P3 • Fix in next sprint (2 weeks) • score 25/100
Risk factors	Business-critical
MITRE ATT&CK	T1485 - Data Destruction
Attack path	Internet > Key Vault Public Endpoint > Secrets/Keys/Certs
Path length	1 hops
Blast radius	1 key_vault
Recommendation	Enable purge protection.

Playbook — Security · 30 minutes

1. Enable purge protection: Update-AzKeyVault -EnablePurgeProtection
2. Confirm soft-delete is also on (cannot disable once purge protection is set)
3. Document the irreversibility for ops team
4. Re-scan