ARGOS

— CLOUD SECURITY —

Cloud Security Assessments for Consultants and MSSPs

https://argos-security.io

Cloud Assessments in Minutes

- Spending a lot of time data gathering?
- Your trusty scripts becoming unmanageable?
- Don’t enjoy writing reports?

ARGOS brings you simplified Cloud Assessments with time-saving automated reports, increasing your project margin substantially!

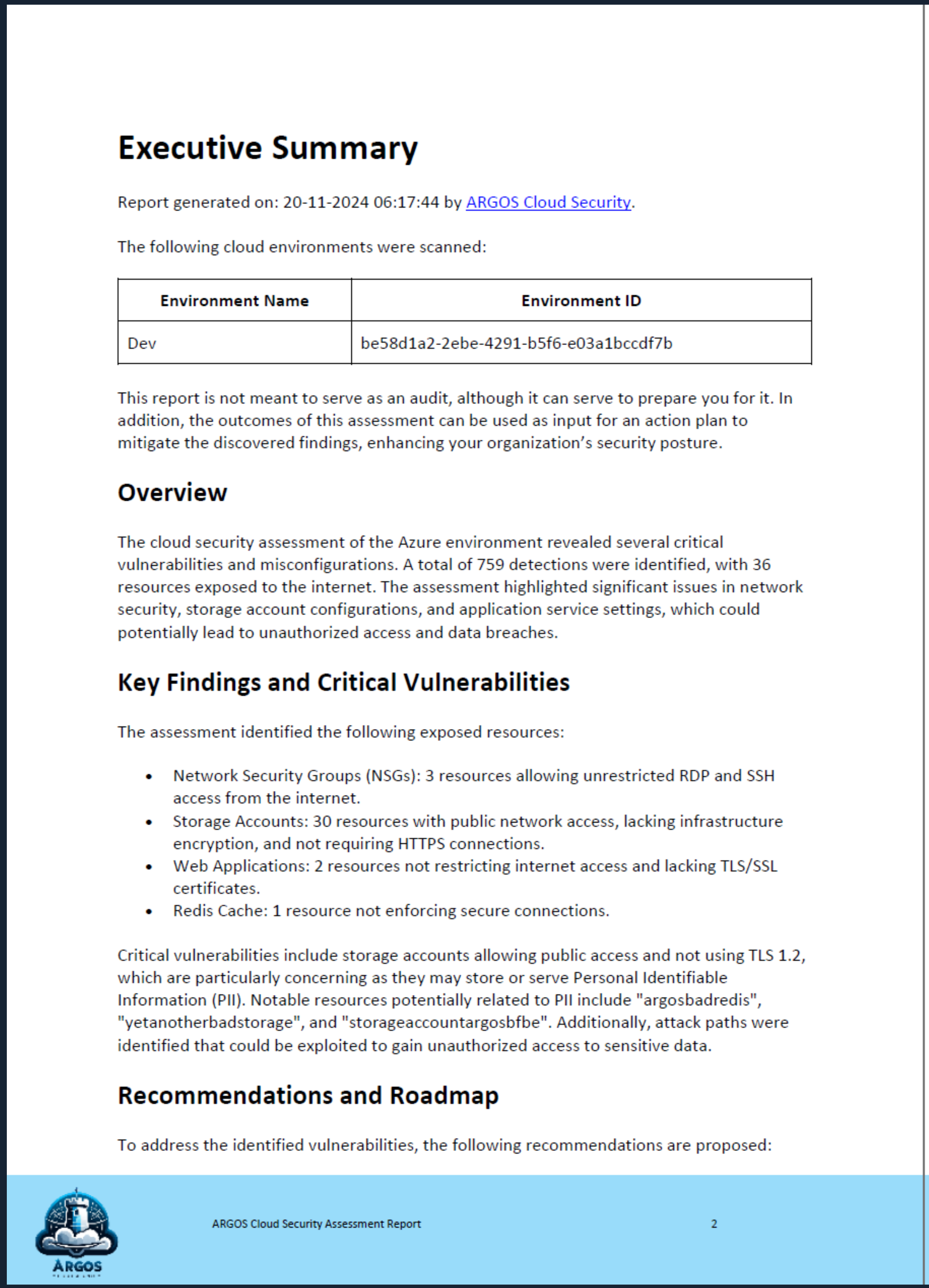
- Security, compliance, and architectural reviews completed in minutes, including customer-ready report with executive summary, roadmap, and detailed findings using architecture diagrams

ARGOS
CLOUD SECURITY

Supported Integrations

- ChatOps
  - Slack
  - Microsoft Teams
- ITSM
  - Atlassian JIRA
  - ServiceNow
- SIEM
  - Microsoft Sentinel
- All data APIs are accessible by customers using API keys supporting a wide range of custom integrations.

Report Samples



Executive Summary

Report generated on: 20-11-2024 06:17:44 by ARGOS Cloud Security.

The following cloud environments were scanned:

Environment Name	Environment ID
Dev	be58d1a2-2ebe-4291-b5f6-e03a1bccdf7b

This report is not meant to serve as an audit, although it can serve to prepare you for it. In addition, the outcomes of this assessment can be used as input for an action plan to mitigate the discovered findings, enhancing your organization's security posture.

Overview

The cloud security assessment of the Azure environment revealed several critical vulnerabilities and misconfigurations. A total of 759 detections were identified, with 36 resources exposed to the internet. The assessment highlighted significant issues in network security, storage account configurations, and application service settings, which could potentially lead to unauthorized access and data breaches.

Key Findings and Critical Vulnerabilities

The assessment identified the following exposed resources:

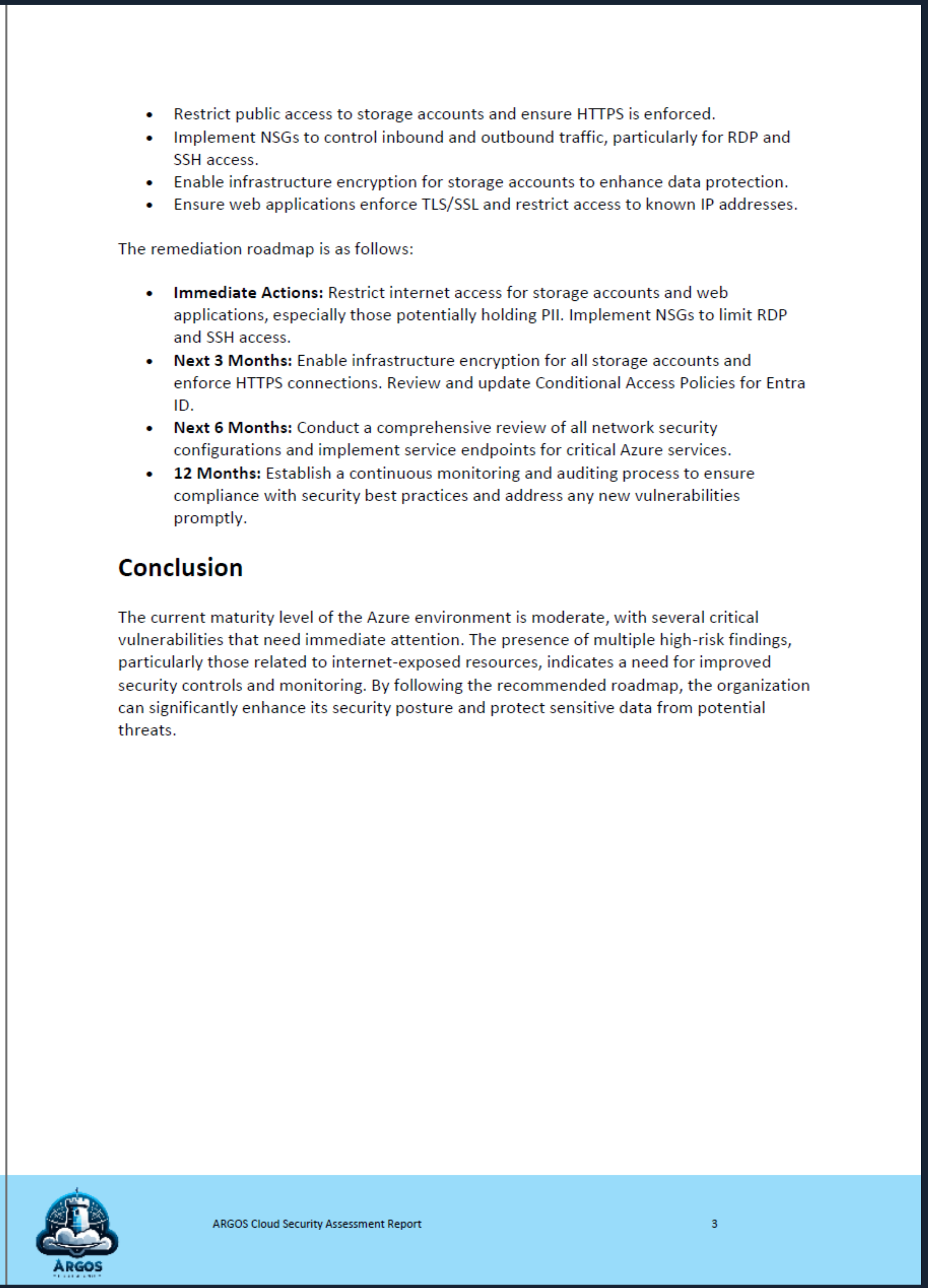
- Network Security Groups (NSGs): 3 resources allowing unrestricted RDP and SSH access from the internet.
- Storage Accounts: 30 resources with public network access, lacking infrastructure encryption, and not requiring HTTPS connections.
- Web Applications: 2 resources not restricting internet access and lacking TLS/SSL certificates.
- Redis Cache: 1 resource not enforcing secure connections.

Critical vulnerabilities include storage accounts allowing public access and not using TLS 1.2, which are particularly concerning as they may store or serve Personal Identifiable Information (PII). Notable resources potentially related to PII include "argosbadredis", "yetanotherbadstorage", and "storageaccountargosbfbe". Additionally, attack paths were identified that could be exploited to gain unauthorized access to sensitive data.

Recommendations and Roadmap

To address the identified vulnerabilities, the following recommendations are proposed:

ARGOS Cloud Security Assessment Report 2



- Restrict public access to storage accounts and ensure HTTPS is enforced.
- Implement NSGs to control inbound and outbound traffic, particularly for RDP and SSH access.
- Enable infrastructure encryption for storage accounts to enhance data protection.
- Ensure web applications enforce TLS/SSL and restrict access to known IP addresses.

The remediation roadmap is as follows:

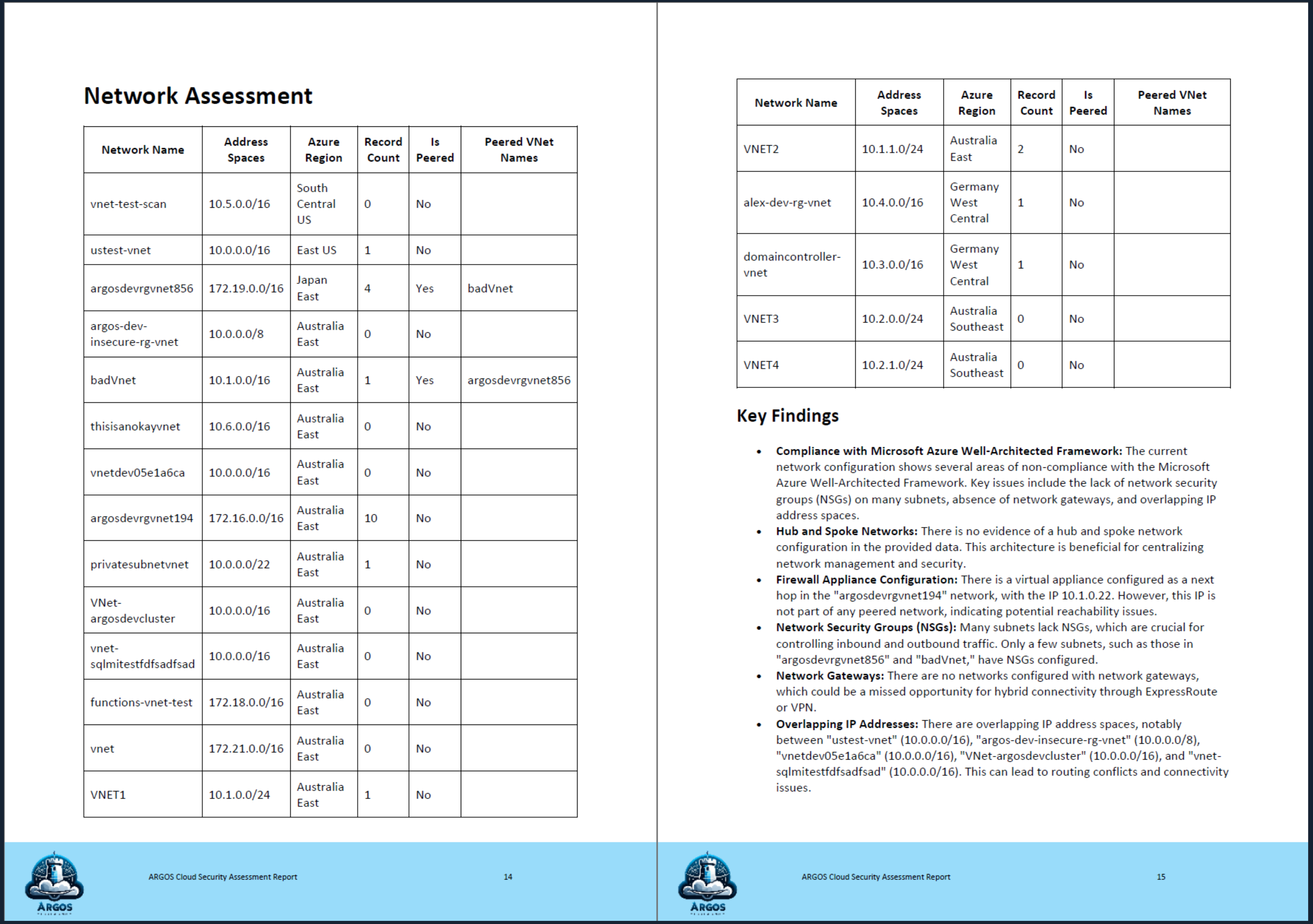
- **Immediate Actions:** Restrict internet access for storage accounts and web applications, especially those potentially holding PII. Implement NSGs to limit RDP and SSH access.
- **Next 3 Months:** Enable infrastructure encryption for all storage accounts and enforce HTTPS connections. Review and update Conditional Access Policies for Entra ID.
- **Next 6 Months:** Conduct a comprehensive review of all network security configurations and implement service endpoints for critical Azure services.
- **12 Months:** Establish a continuous monitoring and auditing process to ensure compliance with security best practices and address any new vulnerabilities promptly.

Conclusion

The current maturity level of the Azure environment is moderate, with several critical vulnerabilities that need immediate attention. The presence of multiple high-risk findings, particularly those related to internet-exposed resources, indicates a need for improved security controls and monitoring. By following the recommended roadmap, the organization can significantly enhance its security posture and protect sensitive data from potential threats.

ARGOS Cloud Security Assessment Report 3

Report Samples



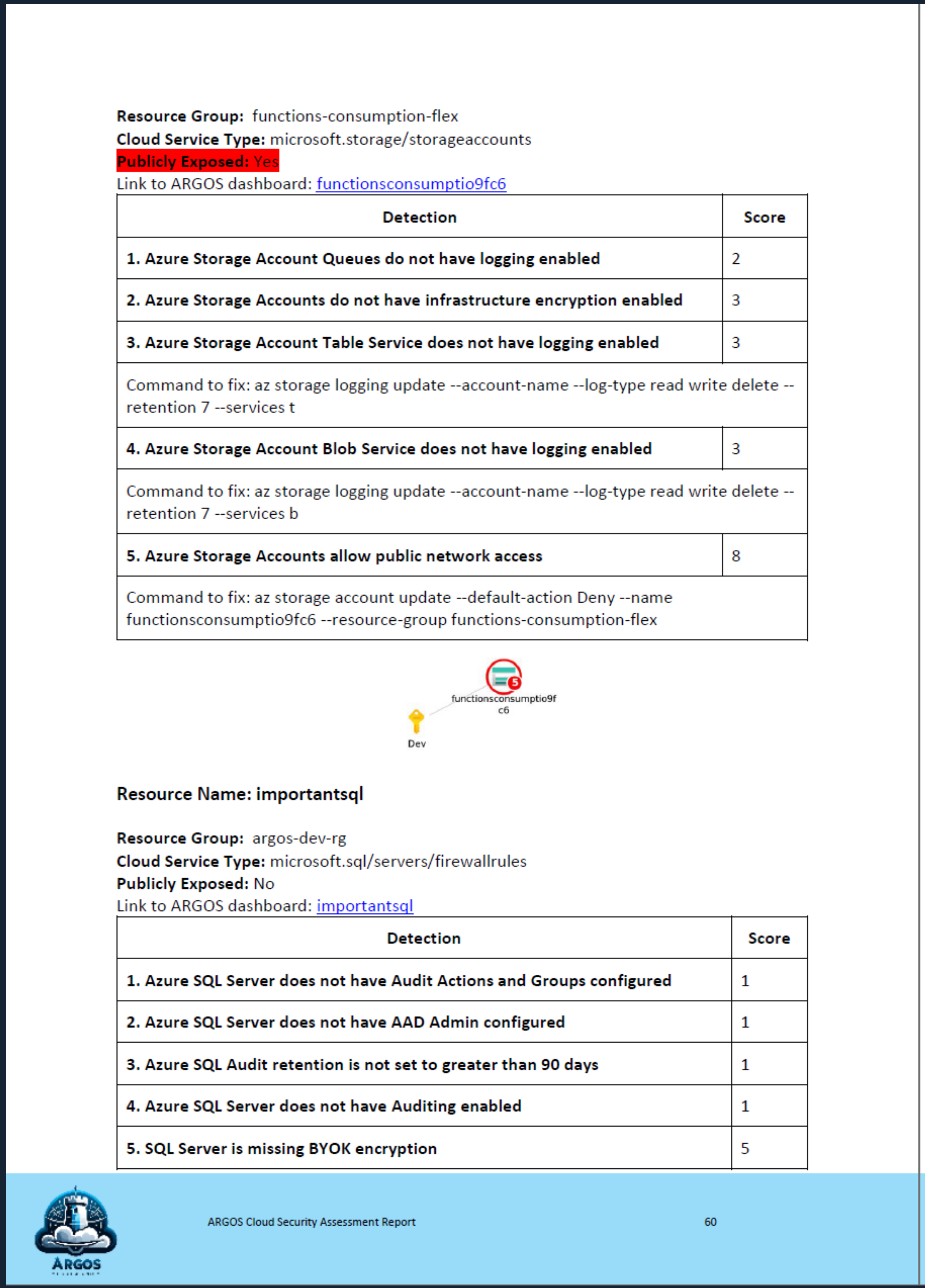
Network Assessment

Network Name	Address Spaces	Azure Region	Record Count	Is Peered	Peered VNet Names
vnet-test-scan	10.5.0.0/16	South Central US	0	No	
ustest-vnet	10.0.0.0/16	East US	1	No	
argosdevrgvnet856	172.19.0.0/16	Japan East	4	Yes	badVnet
argos-dev-insecure-rg-vnet	10.0.0.0/8	Australia East	0	No	
badVnet	10.1.0.0/16	Australia East	1	Yes	argosdevrgvnet856
thisisanokayvnet	10.6.0.0/16	Australia East	0	No	
vnetdev05e1a6ca	10.0.0.0/16	Australia East	0	No	
argosdevrgvnet194	172.16.0.0/16	Australia East	10	No	
privatesubnetvnet	10.0.0.0/22	Australia East	1	No	
VNet-argosdevcluster	10.0.0.0/16	Australia East	0	No	
vnet-sqlmitestfdfsadfsad	10.0.0.0/16	Australia East	0	No	
functions-vnet-test	172.18.0.0/16	Australia East	0	No	
vnet	172.21.0.0/16	Australia East	0	No	
VNET1	10.1.0.0/24	Australia East	1	No	
VNET2	10.1.1.0/24	Australia East	2	No	
alex-dev-rg-vnet	10.4.0.0/16	Germany West Central	1	No	
domaincontroller-vnet	10.3.0.0/16	Germany West Central	1	No	
VNET3	10.2.0.0/24	Australia Southeast	0	No	
VNET4	10.2.1.0/24	Australia Southeast	0	No	

Key Findings

- **Compliance with Microsoft Azure Well-Architected Framework:** The current network configuration shows several areas of non-compliance with the Microsoft Azure Well-Architected Framework. Key issues include the lack of network security groups (NSGs) on many subnets, absence of network gateways, and overlapping IP address spaces.
- **Hub and Spoke Networks:** There is no evidence of a hub and spoke network configuration in the provided data. This architecture is beneficial for centralizing network management and security.
- **Firewall Appliance Configuration:** There is a virtual appliance configured as a next hop in the "argosdevrgvnet194" network, with the IP 10.1.0.22. However, this IP is not part of any peered network, indicating potential reachability issues.
- **Network Security Groups (NSGs):** Many subnets lack NSGs, which are crucial for controlling inbound and outbound traffic. Only a few subnets, such as those in "argosdevrgvnet856" and "badVnet," have NSGs configured.
- **Network Gateways:** There are no networks configured with network gateways, which could be a missed opportunity for hybrid connectivity through ExpressRoute or VPN.
- **Overlapping IP Addresses:** There are overlapping IP address spaces, notably between "ustest-vnet" (10.0.0.0/16), "argos-dev-insecure-rg-vnet" (10.0.0.0/8), "vnetdev05e1a6ca" (10.0.0.0/16), "VNet-argosdevcluster" (10.0.0.0/16), and "vnet-sqlmitestfdfsadfsad" (10.0.0.0/16). This can lead to routing conflicts and connectivity issues.

Report Samples



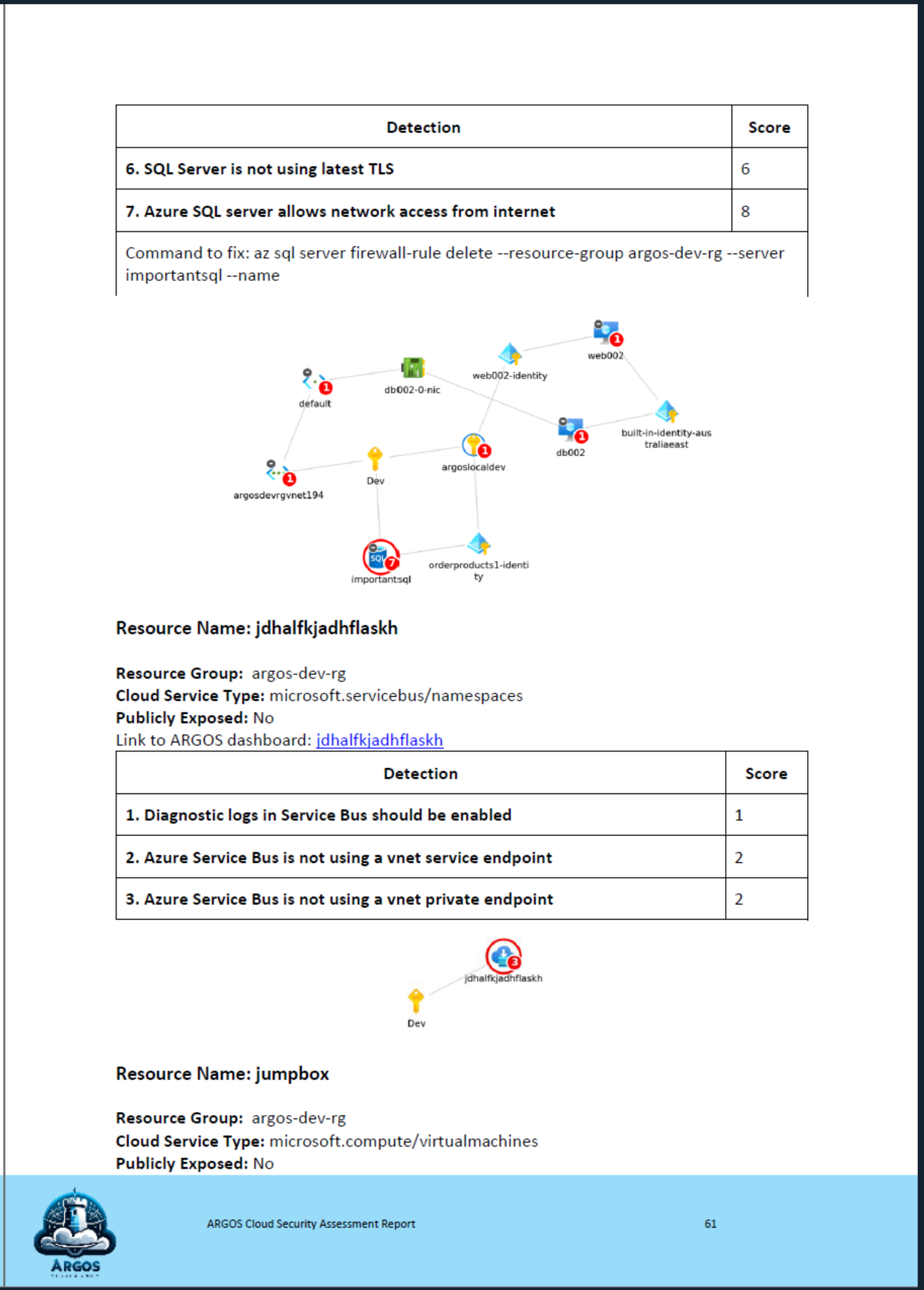
Resource Group: functions-consumption-flex
Cloud Service Type: microsoft.storage/storageaccounts
Publicly Exposed: Yes
Link to ARGOS dashboard: functionsconsumptio9fc6

Detection	Score
1. Azure Storage Account Queues do not have logging enabled	2
2. Azure Storage Accounts do not have infrastructure encryption enabled	3
3. Azure Storage Account Table Service does not have logging enabled	3
Command to fix: az storage logging update --account-name --log-type read write delete --retention 7 --services t	
4. Azure Storage Account Blob Service does not have logging enabled	3
Command to fix: az storage logging update --account-name --log-type read write delete --retention 7 --services b	
5. Azure Storage Accounts allow public network access	8
Command to fix: az storage account update --default-action Deny --name functionsconsumptio9fc6 --resource-group functions-consumption-flex	

Resource Name: importantsql

Resource Group: argos-dev-rg
Cloud Service Type: microsoft.sql/servers/firewallrules
Publicly Exposed: No
Link to ARGOS dashboard: importantsql

Detection	Score
1. Azure SQL Server does not have Audit Actions and Groups configured	1
2. Azure SQL Server does not have AAD Admin configured	1
3. Azure SQL Audit retention is not set to greater than 90 days	1
4. Azure SQL Server does not have Auditing enabled	1
5. SQL Server is missing BYOK encryption	5



Detection	Score
6. SQL Server is not using latest TLS	6
7. Azure SQL server allows network access from internet	8
Command to fix: az sql server firewall-rule delete --resource-group argos-dev-rg --server importantsql --name	

Resource Name: jdhalfkjadhflaskh

Resource Group: argos-dev-rg
Cloud Service Type: microsoft.servicebus/namespaces
Publicly Exposed: No
Link to ARGOS dashboard: jdhalfkjadhflaskh

Detection	Score
1. Diagnostic logs in Service Bus should be enabled	1
2. Azure Service Bus is not using a vnet service endpoint	2
3. Azure Service Bus is not using a vnet private endpoint	2

Resource Name: jumpbox

Resource Group: argos-dev-rg
Cloud Service Type: microsoft.compute/virtualmachines
Publicly Exposed: No

How ARGOS One-Off Assessments Work

- No changes to customer environments needed! ARGOS is ready to go in minutes.
- ARGOS authenticates using the consultant’s access token
  - Azure / Entra ID JWT access token
  - AWS role assumption, supports SSO
- Recommended minimum permissions:
  - **Azure**: Reader
  - **Entra ID**: Global Reader (“Application.Read.All”, ”Directory.AccessAsUser.All”, ”Domain.Read.All”, ”openid”, ”profile”, ”User.Read.All”, ”Policy.Read.All”, ”AuditLog.Read.All”, ”EntitlementManagement.Read.All”, ”Synchronization.Read.All”)
  - **AWS**: SecurityReader
- ARGOS does not access any data layer (no files, data in databases, etc).

How ARGOS Continuous Scans Work

- ARGOS authenticates using
  - Azure / Entra ID: Entra ID App Registration
  - AWS IAM role assumption (using external ID pattern)
- Recommended minimum permissions:
  - **Azure**: Reader
  - **Entra ID**: “Application.Read.All”, ”Directory.AccessAsUser.All”, ”Domain.Read.All”, ”openid”, ”profile”, ”User.Read.All”, ”Policy.Read.All”, ”AuditLog.Read.All”, ”EntitlementManagement.Read.All”, ”Synchronization.Read.All”
  - **AWS**: SecurityReader
- ARGOS does not access any data layer (no files, data in databases, etc).

ARGOS

– CLOUD SECURITY –

https://argos-security.io

david@argos-security.io