Azure Native Qumulo Scalable File Storage Service Security Practices

White Paper

November 2023

Abstract

This whitepaper provides a deep dive into our Azure Native Qumulo (ANQ) service's security architecture, the technology security features, and compliance readiness, assuring enterprises of the robustness of our solution.

Table of Contents

Introduction

Qumulo has built the first truly cloud-native, elastic, pay-only-for-what-you-use file storage offering in the public cloud complete with enterprise data services and true multi-protocol support for Windows & Mac SMB, POSIX NFS, NFSv4, and even an S3-compatible API. Our solution, built natively for Azure infrastructure with resource provider[1] level integration, is tailored for enterprises demanding a TCO comparable to their on-premises storage solutions, as well as elastic performance and uncompromised security.

[1] Azure Native Qumulo has its own resource provider and REST API operations on the official Azure API and SDK. Learn more about resource providers here.

ANQ Architecture Security Primer

The Azure Native Qumulo (ANQ) service was designed with the following security tenets in mind:

The data in a customer's environment does not share infrastructure with other Qumulo customers.

This is unique to Qumulo as compared to traditional SaaS infrastructure where customer data may have co-residency. In this respect, each customer's environment is more like an enclave or walled garden, and therefore more secure through its inherent isolation.

Secure, Seamless connectivity via Azure's VNet Injection Technology[2]

Qumulo has integrated with Microsoft's VNet Injection technology to remove the need for either VNet Peering or proxying through Azure Private Link and a network load balancer. Customers delegate a subnet for use by the Azure Native Qumulo service, provision a resource, and Azure will inject front-end cluster NICs into the customer's environment which are directly attached to the file storage service's VMs. This provides the following benefits:

1. **Seamless integration** - ANQ customers interact only with the IPs associated with their service instance, ensuring an integrated experience without backend complexity. No IP address space coordination is required.
2. **Direct, bi-directional connectivity** - Eliminates potential vulnerabilities associated with intermediate connections.
3. **Tailored performance** - Direct connections mean reduced latency and increased throughput.
4. **Leverage standardized security controls** - Apply network security groups to either the injected NICs or the entire delegated subnet to restrict traffic at the network layer to only allowed IPs, subnets, protocols, and services.

Data is only accessible via data protocols and secured APIs

Even if a cluster node's operating system is compromised, it is impossible to see the data stored by the namespace without going through a front-end file data protocol, or via the API,

[2] See Microsoft's documentation on VNet Injection

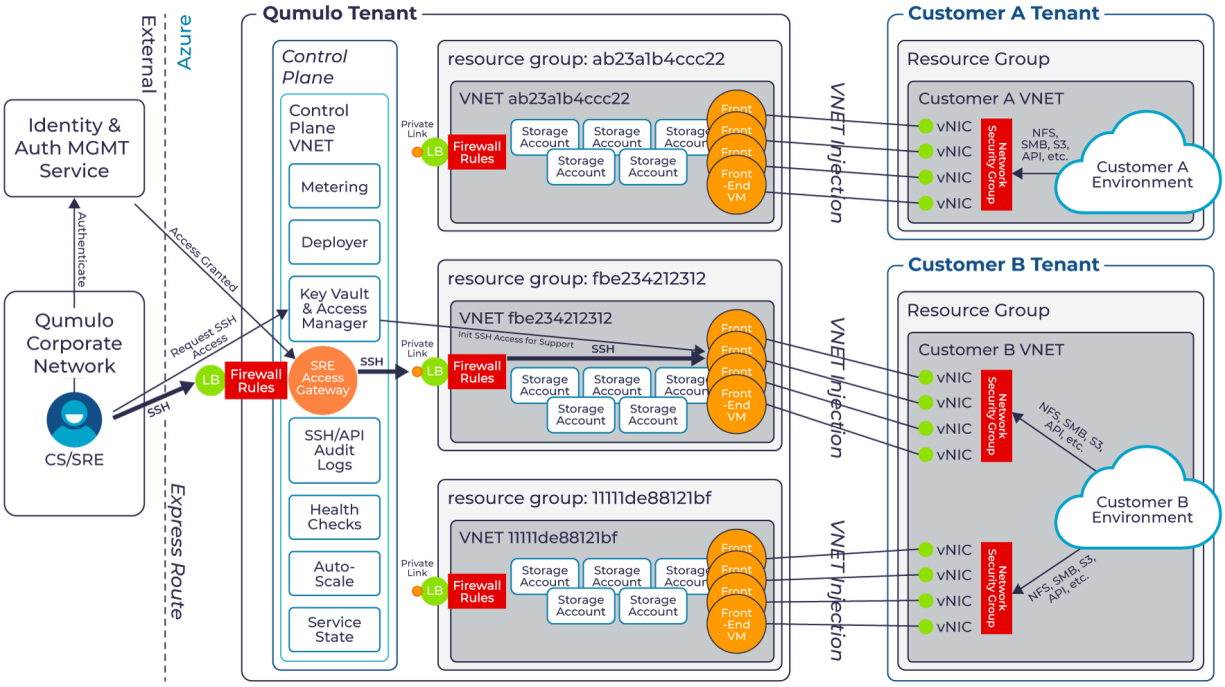
which requires authentication. Qumulo does not expose system data to the local cluster operating system.

Access by operators is limited, monitored, and audited

Qumulo's team of Service Reliability Engineers (SREs) can only access clusters in response to a support issue or an availability event, through a secured gateway, and all activity is recorded into an immutable audit log for later review. Authentication, multi-factor authentication, and auditing are handled via Okta Advanced Server Access (ASA) which itself meets all major compliance requirements. In addition, Okta ASA maintains 90 days of audit log records.

Please contact Qumulo Customer Success if you need to review the audit log.

Service Architecture



The Qumulo architecture separates the control plane from the data plane.

The control plane handles the automation of functions associated with a cloud service including: automated deployment and provisioning, monitoring and health checks, auto-scaling performance up and down, metering usage and submitting billing records to Azure. The service is designed to leverage cloud security best practices.

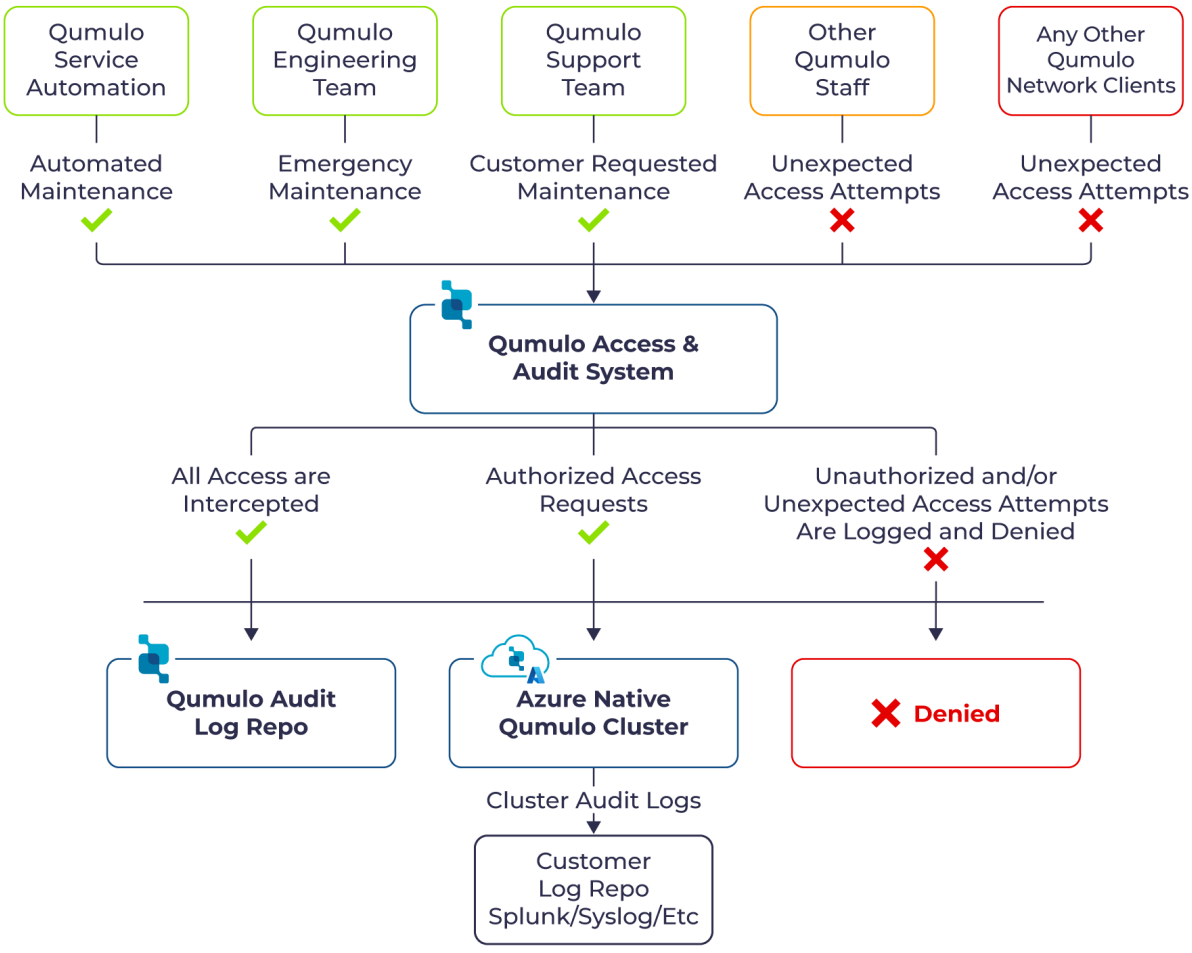
- **Restricted subscriptions following the Principle of Least Privilege (POLP)** - All Azure subscriptions hosting production Azure Native Qumulo instances are locked down to access only from authorized operators and support personnel. Operators are only permitted authority to modify subscriptions within the normal course of their assigned duties. No one outside of these individuals may view, inspect, mutate, or delete any resources living inside of these subscriptions. No one may create any unauthorized resources which were not created via approved automation. Storage accounts are only accessible by the front-end nodes and cannot be accessed by operators directly. Furthermore, all activity by operators is logged and captured in Azure Activity logs and Azure Resource logs in the event an identity is compromised.

- **Full resource isolation, per namespace / Azure Native Qumulo Instance** - When you create an Azure Native Qumulo instance, Qumulo creates a dedicated virtual network (VNet) environment, storage accounts for data storage, and virtual machines to provide front-end file storage protocol, API, UI, and data services. VMs, storage accounts, and VNets are NOT shared between Qumulo customers or other ANQ instances. Individual ANQ instances cannot communicate directly with each other.

There is no pathway available, accidentally or nefariously, to access another ANQ instance or its underlying infrastructure from another tenant.

- **Connectivity via VNet Injection** - VNet Injection is the *only* connectivity between the customer environment, and Qumulo. VNet injection enables the customer to access the front-ends of your Azure Native Qumulo cluster without having to open access to your network. There is no requirement for proxy servers, load balancers, or VPN connection to access the ANQ environment. Network security groups can be applied to injected NICs from the front-end systems or the ANQ-delegated subnet to limit exactly what traffic is allowed to egress from the ANQ instance into your network. Restrictions can be applied to individual IP addresses, subnets, protocols, UI, and API traffic.

- **Highly Restricted Operator connectivity** - Consistent with HIPAA and GDPR compliance requirements, a restricted group of Qumulo operators are required to undergo training and follow strict rules that meet regulatory compliance standards as outlined in this document. This is augmented by quarterly internal security audits. For all operator activity, access and activity is logged and an audit record can be produced in response to any event or request from the customer. In addition, auditing records can be sent directly to the customer's logging infrastructure.



- **Strong authentication and end-to-end encryption** - All access is via audit-proxied SSH connections or API requests issued via TLS-encrypted channels to API service endpoints. All data access is gated via credentials that are verified cryptographically and signed by a certificate authority, if applicable.
- **Network security rules and Azure Private Link** - Ensure that only authorized traffic may cross between a tenant's VNet and the control plane. Azure Private Link ensures that connections may only be initiated from the control plane - no connections may be initiated from a customer's instance VNet to the control plane. The only traffic initiated by the control plane is limited to authorized support SSH traffic from the support gateway, and API calls to nodes which are required for auto-scaling, maintenance, and monitoring.
- **SSH Blocked by Default** - Customer VNets are blocked from SSH access by default, preventing any attacks via SSH from the customer side. If a customer is granted SSH access to an instance, it will only apply to the specific ANQ instance it is white-listed on, and no other instances.

Qumulo Core Security Features and Protections

In addition to service architecture and design, Qumulo Core has been designed primarily for use in highly secured enterprise storage environments. It has a multitude of security features built-in to limit unauthorized access, provide monitoring and threat detection support, and protect data from unauthorized access. Some of these features are intrinsic and on by default, some must be enabled at the discretion of the customer if they wish to harden their environment.

- **Data Protection & Security** - All data is eventually backed by Zone-redundant blob, which is triply replicated and provides 12 9's of durability. All data *written* to cache is 2x mirrored within the zone you are deployed in for our standard LRS offering. ZRS will be mirrored 3x across a region. All storage primitives (cache[3], and blob[4]) are encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

- **Software Encryption & Customer Managed Key** - Qumulo will enable software encryption and customer managed keys in future updates, scheduled for Q1 2024. We intend to support integration with Azure Key Vault, such that customers are able to see, rotate, and manage keys from their tenant environment. This includes revoking keys as an added level of protection prior to destruction of an Azure Native Qumulo instance.

- **Secured Data Transfer in-flight** - All SMB and NFSv4.1 traffic between clients running inside your environment and the Azure Native Qumulo client-facing NICs can be secured in transit. ANQ supports in-flight encryption for SMBv3 traffic, as well as the krb5p and krb5i standards for NFSv4.1 clients. This is supplemental to the built-in at-rest encryption offered by Azure at the physical layer. The Qumulo S3 and HTTPS REST API are protected by industry standard TLS/SSL v1.2 using current-generation ciphers approved for use by NIST and other governing bodies. FTP can also be secured via TLS as well.

- **Active Directory Domain Services (AD DS) and Microsoft Entra ID Integration** - Enables the Qumulo instance to leverage your domain directory as the source of truth for identities and authentication. AD DS eliminates the need to manage identities locally on the Qumulo instance. All invalid identities do not have access by default. In addition, access is removed immediately if an active identity becomes inactive; no shadow identities persist. Qumulo supports Entra ID but also can connect to an on-premise AD DS for identity services.

- **Strong Authentication** is delivered via Kerberos for NFSv4.1, SMBv2 and v3, all of which require user credentials that are cryptographically verified. In the case of HTTP

[3] Azure Managed Disk Encryption
[4] Azure Storage Account Data-At-Rest Encryption, which backs our Blob storage

API, FTP, a cryptographic hash of the user's passphrase is used. In the event the user is using Active Directory-based credentials, no passwords are persisted on the Azure Native Qumulo instance; instead they are passed to an Entra ID or Active Directory domain controller for verification over an encrypted channel. S3 is guarded by AWS SIGv4, which is currently Amazon Web Services's state-of-the-art authentication and signing protocol and meets all industry and government requirements for security.

- **Strong Cross-Protocol Permissions System** - All file data is annotated with permissions data which describes which identities are allowed to read, write, modify, or delete data. Qumulo stores a single, unified set of permissions that is equally enforced across all protocols, whether POSIX or ACL-based. These permissions, which are typically set by file system clients, pass through our protocol stack into the filesystem which contains a normalized, merged permission representation that enables accurate and correct permissions enforcement across all the different protocols we support on our data platform. The net of it is, if you restrict access to an identity on one protocol, that restriction will also be enforced over any other protocol that users access in Azure Native Qumulo.

- **Audit Logging** - All activity on a Qumulo system can be sent to the customer's own SIEM solution, letting you track and detect anomalous or nefarious activity. These audit logs can be sent via standard syslog protocol and are either in CSV format or JSON format.

- **NFS Export Restrictions** - Enable you to restrict access to NFS exports by IP range and/or hostname. For NFSv4 clients, you can also optionally require Kerberos authentication and either krb5i packet signing or krb5p encryption to ensure that users are always communicating with the Qumulo front-ends over a secured, authenticated, channel. NFS Export restrictions also enable you to set certain users as read-only, or squash root access to prevent a user using local sudo access to bypass permissions.

- **SMB Share Restrictions** provide the ability to restrict access at the share level to certain shares, or limit what permissions the user has to that share (i.e. read-only etc.). You can also enable *Access Based Enumeration (ABE)* to hide shares that a user does not have permission to view, so they are not even aware they are there.

- **Role Based Access Control (RBAC)** enables you to restrict what users can do on the Qumulo system, by assigning them (or a group they are a part of) to a specific role on Qumulo. For example, you can create roles which only allow access to S3 management functions, to enable users to create and delete their own access keys, but deny access to all other functions of the Azure Native Qumulo instance. By default, most users should be granted no access to API methods, and only be granted access to the filesystem, which itself has its own file permissions model, as described above.

- **Single-Sign-On support with Multi-factor Authentication (MFA)** - Leverage Microsoft Entra ID or other services that support SAML integration (Okta, OneLogin, etc.) to require that all users logging into the management interface traverse through an SSO MFA check.

- **Snapshots** - Once a snapshot is taken on a specific directory, the data contained within cannot be altered or tampered with, including metadata like file ownership or permissions. This can be used to ensure there is an immutable copy of your data present on your system at all times, even in the case of an attack by malware or a malicious actor.
- **Snapshot Locking** - Snapshots can be locked to prevent accidental or malicious premature deletion. For locked snapshots, the only way to delete them prior to their expiration date is to pass a cryptographic check using Elliptic Curve Digital Signature Algorithm (ECDSA) key pairs. For additional protection, these keys should be secured and managed in Azure Key Vault.[5]

To learn more, please see our general security white-paper.

[5] See Qumulo's documentation on ECDSA key pairs, which contains guidance on leveraging Azure Key Vault as a KMS

Compliance Readiness

Qumulo understands the criticality of regulatory compliance:

- **Global and Industry Certifications:** We adhere to internationally recognized standards like FIPS 140-2, HIPAA, GDPR, SOC2 Type 2 among others. See qumulo.com/trust for more information.
- **Transparent Documentation:** Detailed records of how we manage, protect, and process data are available, ensuring clarity and trust. Please see:
    - Our privacy policy
    - Our SaaS Terms and Conditions
    - And our Data Processing Addendum (DPA)
    - If required, contact us to receive a certificate of cybersecurity insurance
- **Continuous Improvement:** Our commitment to security and compliance doesn't wane. Regular reviews and updates keep us aligned with the ever-evolving regulatory landscape. We contract out with multiple security analyst vendors to conduct regular intrusion tests and find weak spots.

Security Best-Practices

In order to ensure you are leveraging Azure Native Qumulo in the best way possible, use the following checklist as a way to guide your planning and architecture to ensure you are protected from security threats.

Item	Why	Done?
Define a network security group and rules for the vNICs or delegated subnet	Provides a network layer of defense in the extremely unlikely case that the Qumulo namespace VMs are compromised by a nefarious actor.	☐
Connect to Active Directory Domain Services	Centralized identity management and trust to a system purpose-built for large scale enterprises.	☐
Remove default shares and exports	For ease of testing and first-time use, default shares are created. They should be removed and exports and shares should be created on a case-by-case basis with prescriptive restrictions on who can access it and what they are allowed to do.	☐
Configure Audit Logging for an SIEM such as Varonis, ElasticSearch, or Splunk	Provides a trail of activity to be able to understand who did what, when. In conjunction with an SIEM that provides anomaly or ransomware detection, this can also be a way to get an early warning when an attack is in progress, as well as a way to react to that attack automatically.	☐
Set a default quota on /	Prevent either a run-away script, nefarious user, or accidental mistake from creating tons of data that drives consumption beyond desired levels.	☐
Configure RBAC	Ensure that only you and your fellow trusted admins have access to sensitive Azure Native Qumulo instance functions, and deny all other users any permission to do anything on the namespace.	☐
Set cost alerts on the Qumulo resource	Ensure that you are alerted in the event of a cost-overrun, which might be indicative of nefarious or accidental activity.	☐
Require encryption and strong authentication, everywhere.	Set all SMB shares and NFS exports to require encryption and strong authentication, when applicable. Note that NFSv4.1 will require a Kerberos environment be set up, which has additional dependencies.	☐

If NFSv3 is required, Restrict NFSv3 shares to extremely limited IP ranges or hostnames	NFSv3 is inherently insecure, but if it is required, Qumulo recommends restricting access to NFSv3 exports to as small a set of IP addresses and hostnames as possible. Ideally, restrict access to network addresses that are coming from within Azure to prevent NFSv3 traffic egressing from the Azure Availability Zone.	☐
Leave FTP and S3 off if not needed	These protocols are disabled by default, and can be left off if there is no need for them.	☐
Set up an ECDSA key pair in Azure Key Vault and add the public key to the Azure Native Qumulo instance	In order to leverage snapshot locking, an ECDSA public key must be registered with the ANQ instance to enable the use of snapshot locking to prevent malicious or premature snapshot deletion.	☐
Set up at least 1 snapshot policy	Snapshots are the break-glass-in-the-event-of-a-malicious-attack solution. Set up at least one snapshot policy at the filesystem root, occurring once a day with a 30 day retention policy,to give you at least one month's data that you can recover in the event of an attack. Qumulo recommends that this snapshot be locked as well. This should give you enough buffer to be able to recover from an attack, even if you don't notice it immediately.	☐
Create a replica in another region	In addition, you should set up another Azure Native Qumulo service instance in another region – either an archive-class instance (when available) or another standard instance – which you can use as a replication target for snapshots from your primary ANQ storage. Depending on your specific RPO and RTO requirements, you can use either snapshot replication or continuous + snapshot policy. In this case, you may wish to extend the snapshot retention period to 90 days or more, depending on workload and data ingest/change rate, to ensure that there is a golden copy of your data in the event of an attack.	☐

Conclusion

Azure Native Qumulo, underpinned by our groundbreaking elastic cloud-native architecture, provides a transformative approach to secure and scalable data storage on Microsoft Azure. Our commitment to security, data protection, and compliance ensures enterprises can confidently entrust their invaluable data assets to our care.

Disclaimer: This whitepaper aims to provide a comprehensive overview of our services and does not constitute exhaustive security advice. Enterprises should conduct their own in-depth assessments and may consult with our specialists for tailored recommendations.

For detailed technical specifications, implementation strategies, or to schedule a demo, contact azure@qumulo.com