SECURITY MATTERS

DEFENSE – IN-DEPTH

SnapAV prides itself on providing a Defense-in-Depth security platform. We do not rely on a single layer of security. Rather, we take on the philosophy of layered security.

NIST FRAMEWORK

SnapAV has adopted the NIST Framework for our security standards. This allows us to utilize the highest standard when it comes to security.

24/7 SECURITY

SnapAV utilizes a 24/7 security approach. We are always monitoring and always available.
Our Security Team is on all day and all night for your protection.

ENCRYPTION

Communications between servers are encrypted via best-practices HTTPS and Transport Layer Security (TLS) over public networks. TLS is also supported for encryption of email.

A LOOK INTO SECURITY

DATA CENTER & NETWORK SECURITY

Facilities

SnapAV servers are hosted at Tier IV or III+, SSAE-16, PCI DSS, or ISO 27001 compliant facilities. Data center facilities are powered by redundant power, each with UPS and backup generators.

On-site Security

Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, physical locks, and security breach alarms.

Monitoring

All Production Network systems, networked devices, and circuits are constantly monitored and logically administered by staff. Physical security, power, and internet connectivity beyond Azure services are monitored by the facilities providers.

Location

SnapAV leverages multiple data centers in the United States.

NETWORK SECURITY

Protection

Our network is protected by redundant firewalls, best-in-class router technology, secure HTTPS transport over public networks, regular audits, and network Intrusion Detection and/or Prevention technologies (IDS/IPS), which monitor and/or block malicious traffic and network attacks.

Vulnerability Scanning

Scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.

Third Party Penetration Test

Each year we employ third-party security experts to perform a broad penetration test across the Network.

Security Incident Response

In case of a system alert, events are escalated to our 24/7 Incident Response Team, providing Operations, Network Engineering, and Security coverage.