Quantum Access Manager (QAM)

Unified Security Management Platform

QUANTUM® NETWORKS

Overview

Quantum Access Manager (QAM) is a secure, scalable and unified platform for identity and access control across wired, wireless, VPN and cloud networks. It combines AAA services, posture validation, device profiling and policy enforcement for cloud-first, hybrid and air-gapped environments.

QAM allows smoother onboarding, compliance enforcement and access control for all users and devices, including BYOD, guests and IoT endpoints.

Unlike multi-vendor solutions that increase complexity and cost, QAM integrates the entire security stack into a single platform to reduce the total cost of ownership while delivering Zero Trust Access without operational complexity.

The QAM solution is built on the following foundations:

Network Access Control (NAC)

Enforcing secure connections for wired and wireless networks.

Identity Management

Unified control of user and device identities.

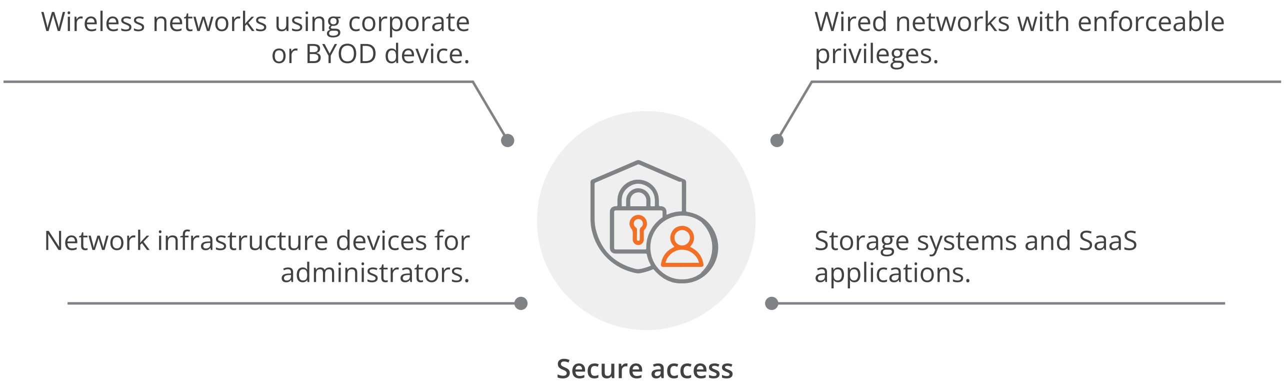
Enterprise Access Management

Centralized policies for apps, VPNs and infrastructure.

Public Key Infrastructure (PKI)

Secure certificate lifecycle management for passwordless access.

QAM resolves critical security challenges:



Wireless networks using corporate or BYOD device.

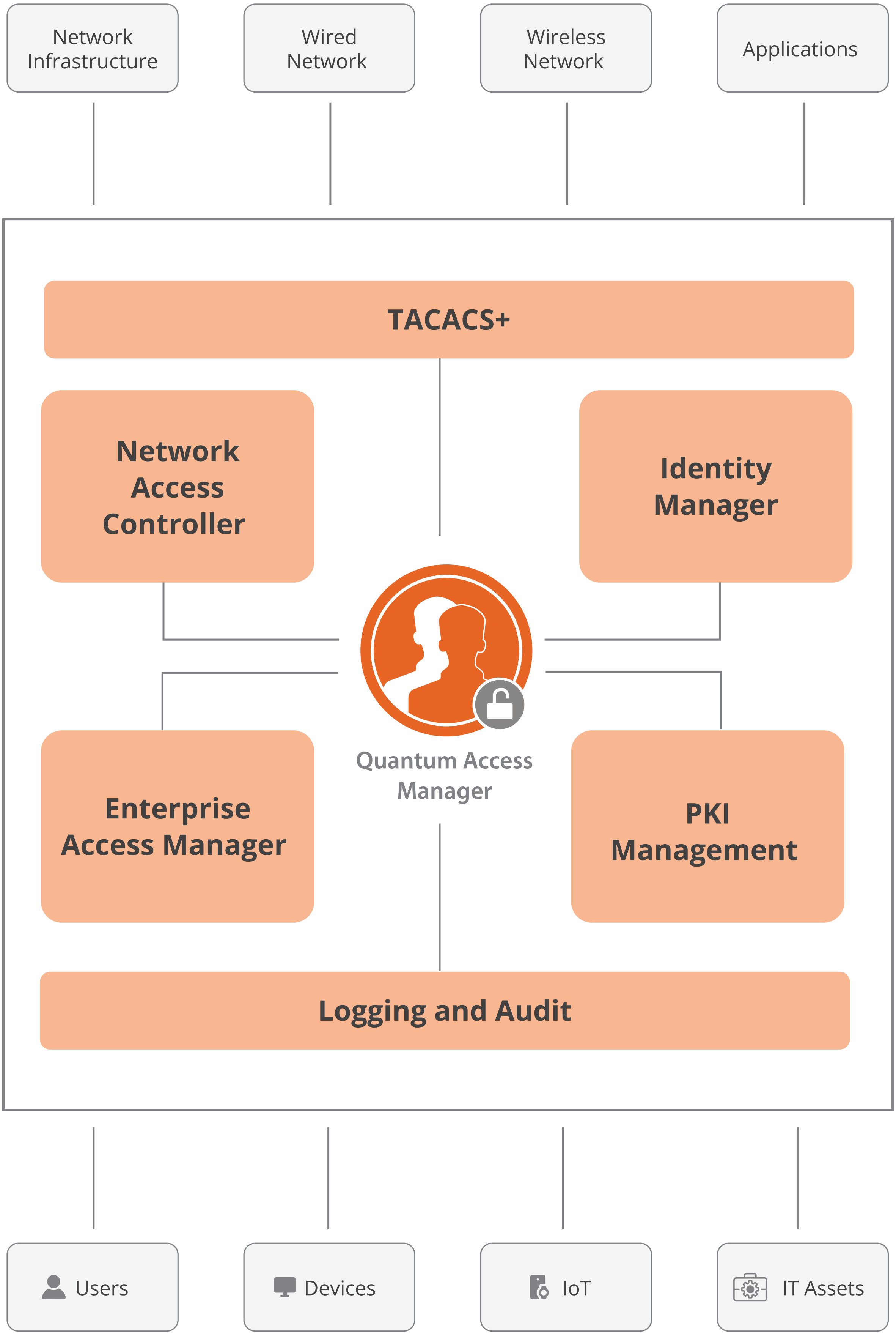
Wired networks with enforceable privileges.

Network infrastructure devices for administrators.

Storage systems and SaaS applications.

Secure access

QAM Architecture



Key Benefits

NAC- Network Access Control

802.1X AAA Authentication

Centralized authentication, authorization and accounting for Wi-Fi, wired and VPN access using RADIUS and certificates.

Two-Factor Authentication (2FA)

Strengthen login security with OTP-based or authenticator app-based 2FA for admins, users and guests.

Policy Enforcement Engine

Dynamic VLAN Assignment

Users/devices are placed into the appropriate VLAN automatically based on identity, role or compliance posture.

Dynamic ACLs

Access Control Lists are applied dynamically to define what resources a user/device can access on the network.

Custom VSA / Attribute-based Policy

Vendor-Specific Attributes (VSAs) or other attributes can be leveraged to enforce granular access control.

Rule-based Enforcement – Policies are enforced dynamically based on:

Role-based

(employee, contractor, guest)

User-based

(individual user identity)

Attribute-based

(device type, location, time, risk score)

Device health status

(up-to-date antivirus, OS patch level, compliance check)

Endpoint Posture Checking (Device Provisioning & Profiling)

NAC Agent-Based Posture

Agentless Posture Assessment
Checks unmanaged/guest devices without installing an agent.

Device Profiling

Device Monitoring

Tracks all connected devices

App Control

Blocks unapproved applications.

Security Checks

Verifies antivirus and disk encryption.

Compliance Audit

Confirms registry and certificate settings.

Device Provisioning

USB Enable/Disable

Controls external device usage.

Firewall Enable/Disable

Enforces host firewall policy.

Idle System Lock

Locks system after inactivity.

Adaptive Authentication

Dynamically adjusts login requirements based on user context and risk factors like device, location, or behavior. It provides seamless access for trusted users while enforcing stronger checks or blocking suspicious attempts.

Enterprise Access Management

Single Sign-On (SSO)

SSO allows users to access multiple applications with one set of credentials, reducing password fatigue and improving security.

Federated Login

Federation enables authentication across different organizations or domains using trust relationships.

Supported Protocols

SAML	Auth 2.0	OpenID Connect (OIDC)	Two-Factor Authentication (2FA)

Enhances login security by adding an extra layer, such as OTP, push notification, or hardware token.

Firewall & VPN Access Control

Apply role-based permissions and compliance checks to control who can access internal or cloud applications and VPN services.

Dedicated Support

Quantum Networks provides guidance for deployment, policy setup and integration to ensure smooth operations.

Device & Guest Management

● **BYOD & IoT Control**

Enable self-service onboarding, posture checks and secure IoT isolation with identity/MAC policies.

● **Guest Access & Captive Portals**

Offer branded portals with OTP login, sponsor approval, time limits and self check-in.

PKI Management

Issue and manage certificates for passwordless access to Wi-Fi, wired and VPN networks using QAM's built-in PKI or external CAs.

Centralized Certificate Authority (CA) Management – Internal

An internal CA enables organizations to issue and manage certificates centrally for users, devices and applications. It strengthens security for internal communication and reduces reliance on external providers.

Root and Subordinate (Intermediate) CA Hierarchy Management

PKI uses a hierarchical trust model where the Root CA serves as the ultimate trust anchor, while subordinate (intermediate) CAs issue certificates on its behalf, creating a scalable and secure chain of trust.

External Certificate Authority Integration

External CA integration allows organizations to use trusted third-party providers for certificates on public-facing services like websites, VPNs and email, ensuring global trust and compliance with security standards.

Certificate Lifecycle Management

PKI covers the entire certificate lifecycle—generation of key pairs, issuance after identity validation, continuous validation during use and revocation if certificates are expired, compromised or no longer needed.

Centralized Management

Administrative User Management

Controls creation and privileges of admin-level accounts.

User Management

Handles adding, updating and removing user accounts.

User Role Management

Assigns roles to users based on responsibilities.

User Group Management

Organizes users into groups for easier policy application.

Role-Based Access Management (RBAC) - Grants access rights based on defined roles, not individuals.

Password Complexity Policy

Enforces strong password rules for better security.

Customization & Branding

Customize OTP emails, SMS templates, guest pages and portal themes to match your organization's identity.

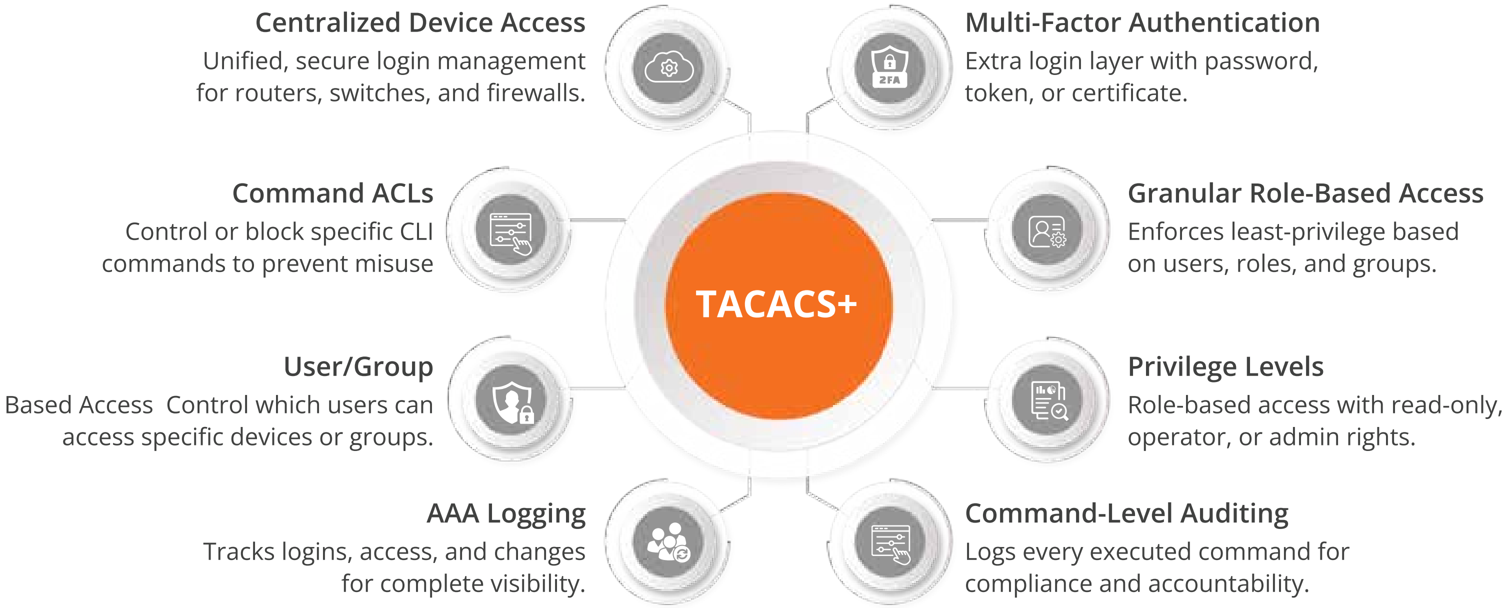
Visibility & Integration

Real-Time Analytics & Logging

Multi-Vendor Network Compatibility

Syslog, Backup & Restore

Secure Network Device Access & Control



Centralized Device Access
Unified, secure login management for routers, switches, and firewalls.

Multi-Factor Authentication
Extra login layer with password, token, or certificate.

Command ACLs
Control or block specific CLI commands to prevent misuse

Granular Role-Based Access
Enforces least-privilege based on users, roles, and groups.

TACACS+

User/Group
Based Access Control which users can access specific devices or groups.

Privilege Levels
Role-based access with read-only, operator, or admin rights.

AAA Logging
Tracks logins, access, and changes for complete visibility.

Command-Level Auditing
Logs every executed command for compliance and accountability.

Device Discovery & Profiling Methods

NMAP
Scan OS, open ports and services to identify unmanaged or rogue devices.

QAM Posture Agent
Collect real-time posture data such as OS health, antivirus status and installed apps.

SNMP
Profile infrastructure devices like printers and switches using SNMP polling.

MAC OUI
Classify IoT or unmanaged devices by identifying manufacturer info via MAC address.

Customization & Support

Customization & Branding
Customize OTP emails, SMS templates, guest pages and portal themes to match your organization's identity.

Web App & VPN Access Control
Apply role-based permissions and compliance checks to control who can access internal or cloud applications and VPN services.

Dedicated Support
Quantum Networks provides guidance for deployment, policy setup and integration to ensure smooth operations.

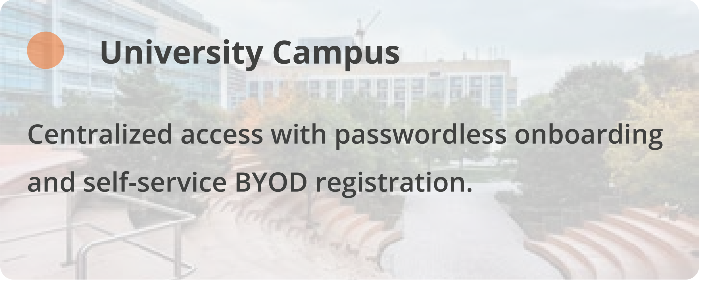
Deployment Options

Managed Cloud Controller
Fully hosted by Quantum Networks, ideal for distributed or cloud-first organizations with minimal setup.

Virtual Appliance (On-Prem)
Deployable on VMware, Hyper-V or KVM for complete data control and internal system integration.

Physical Appliances (On-Prem)
Plug-and-play hardware appliances with built-in security for regulated or air-gapped environments.

Use Cases



University Campus

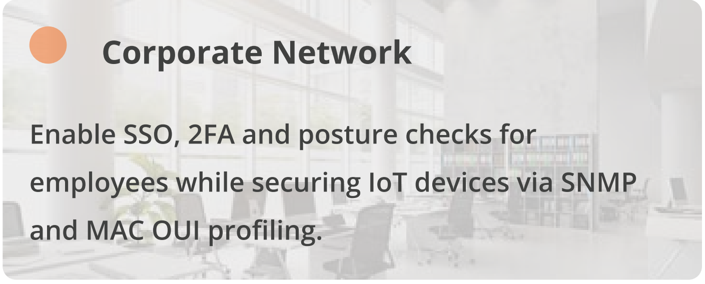
Centralized access with passwordless onboarding and self-service BYOD registration.

Technical Institute

Host QAM as a virtual appliance on-prem to meet data residency rules and integrate with Active Directory.

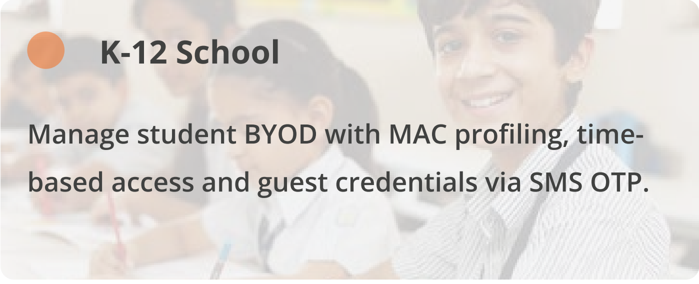
Government & Defence

Deploy hardened appliances in air-gapped environments for strict compliance and auditing.



Corporate Network

Enable SSO, 2FA and posture checks for employees while securing IoT devices via SNMP and MAC OUI profiling.



K-12 School

Manage student BYOD with MAC profiling, time-based access and guest credentials via SMS OTP.

Retail Chains

Use cloud deployment to manage Wi-Fi access across branches with role-based VLANs and centralized monitoring.

QAM as a Package

- Unified AAA, SSO and 2FA
- Support for wired, wireless and VPN networks
- Certificate-based passwordless access
- Real-time analytics and visibility
- Smart profiling using multiple techniques
- Integrates with AD, LDAP, G Suite, Okta, UEMs
- Multi-vendor network compatibility
- Cloud, virtual and hardware deployment options

CONTACT US

Quantum Networks

www.qntmnet.com | sales@qntmnet.com