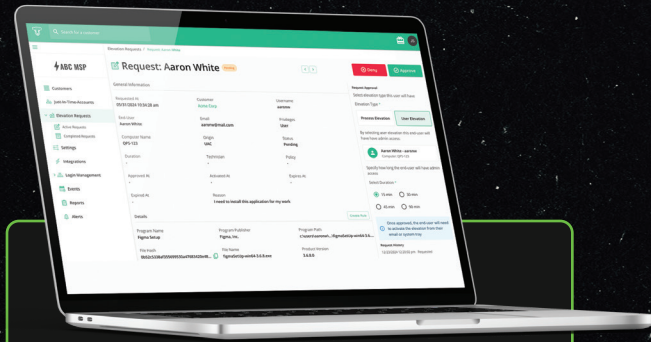


QDesk - Simplified End-User Access Management (EUAM)

Protect Identities. Control Privileges. Empower Users.

Attackers now more than ever use social engineering for IT service desk impersonation—to steal credentials and privileged access in addition to phishing and local admin abuse for malware and ransomware deployment.

QDesk enables companies to eliminate always-on local admin rights and empower end-users with just-in-time access, prevent social engineering attacks with identity verification and boost technician productivity with essential account management all in one-platform.



80% of critical Microsoft vulnerabilities last year required administrative privileges with experts reporting 94% of Microsoft's critical **vulnerabilities could be mitigated by removing admin rights.**

There has been an estimated **3,000% increase in the use of deepfakes** in the past year, with incidents **expected to rise by 50-60% in 2024.**

Why Removing Always On-Admin Rights and Verifying End-User Identities Matters



Blocks Malware and Ransomware Installation

Blocks unauthorized processes from running with admin rights, stopping malware before it can take hold or escalate.



Prevents Privilege Escalation

Ensures users operate with standard privileges by default and blocks unapproved elevation attempts.



Prevent Social Engineering & Impersonation Attacks

By confirming user identities before sensitive requests such as credential / MFA resets and privilege changes, IT service desks can ensure assistance is provided only to authorized individuals, protecting the organization from severe security breaches that target IT professionals and their privileged access.



Meet Compliance & Cyber Insurance Requirements

Compliance frameworks, including NIST 800-53, CIS V8, ISO-27001:2022, CMMC 2.0, and HIPAA, along with many cyber insurance providers, require the removal of local admin rights for end-users to enforce least privilege and to require strong access controls such as identity verification before resetting user credentials.

Feature

Outcome



Endpoint Privilege Management

Eliminate Local Admin Rights Without Sacrificing Productivity: By removing always-on local admin privileges from endpoints while allowing just-in-time, policy-controlled elevation, Endpoint Privilege Management dramatically reduces the attack surface for malware, ransomware, and insider threats, without disrupting users' ability to perform legitimate tasks.



Identity Verification

Prevent Social Engineering & Impersonation Attacks: Defend IT service desks against social engineering, impersonation, and insider threats that can lead to unauthorized access, data breaches, or privilege escalation. Empower service desk technicians with multiple options to verify end-user identities — including SMS, email, secure push notifications from a branded mobile app, or Microsoft Authenticator.



Essential Account Management with PSA Integrations

Efficient Service Desk Management: Boost technician productivity without compromising security by integrating with leading PSA platforms like ConnectWise PSA, Datto Autotask, and Halo PSA. CyberQP enables technicians to verify end-user identities and resolve essential end-user account management tickets directly within the PSA service ticket screen with a single pane of glass.



Compliance Control Mappings

Meet Compliance and Cyber Insurance Requirements: CyberQP includes mappings to many identity security controls to compliance frameworks such as NIST 800-53, CIS V8, CMMC 2.0, HIPPA, and ISO 27001. Allowing organizations to meet both compliance and Cyber Insurance requirements.



"I can sleep better at night knowing everyone who calls for support must verify who they are."

— Michael Goldstein
LAN InfoTech

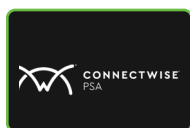
"QDesk Pro helps us deliver faster service with stronger security. It's a win-win."

— Help Desk Team Lead
CyberQP Partner

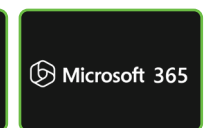
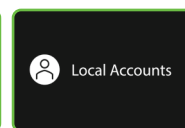
QDesk: The future of secure, efficient help desk operations starts here. Powered by CyberQP — Your SOC 2 Type 2-Certified Identity Security Partner.

[Click here to LEARN MORE](#)

Integrations



Identity Providers



CyberQP redefines Zero Trust Access Management with leading-edge Privileged Access Management (PAM) and End-User Access Management (EUAM) solutions. Our platform enables secure elevated access for both IT Professionals and end-users, along with robust self-serve and identity verification capabilities. Backed by SOC 2 Type 2 certification, we empower IT professionals to reduce or eliminate risks stemming from social engineering attacks, standing privilege, and over-privileged accounts, enforce compliance, and enhance operational efficiency. Our mission is simple: "Empowering Access, Redefining Privilege" for security-focused IT professionals around the globe. Learn more <https://www.bluechipit.com.au/cyberqp/>