AutoElevate by CyberFOX
Privileged Access Management

AutoElevate is a privileged access management (PAM) solution that helps organizations improve security and compliance by reducing the attack surface and providing granular control over user privileges.

AutoElevate offers a number of technical capabilities that make it a powerful tool for privilege elevation management:

Real-Time UAC Interception and Routing

AutoElevate intercepts UAC prompts in real-time and automatically routes them to a central management console or mobile app for approval or denial. This allows administrators to control which applications are elevated and when, and prevent unauthorized elevation attempts. Multiple PSAs are supported.

Granular Privilege Control

Granular rules can be created and applied to individual devices, locations, companies, or globally. This helps to reduce the attack surface and prevent users from elevating applications that are not necessary or permitted.

Over-the-Shoulder Elevation

AutoElevate supports over-the-shoulder elevation, which allows administrators to elevate applications on a user's computer without requiring the user to take any action. Technician Mode allows your technical team to elevate privilege as needed when assisting/logged in as the end user.

Contextual Elevation

AutoElevate can elevate applications in the context of the currently logged-in users, or in the context of a different user account. This allows administrators to provide elevated access to applications without requiring users to enter their credentials.

AutoElevate by CyberFOX
Privileged Access Management

Scalable Integrations

Simple and scalable device deployment via a.msi, PowerShell, and integrations into a number of RMM solutions.

Centralized Management

AutoElevate provides a centralized management console for approving or denying elevation requests, viewing elevation history, managing user privileges, activating Just-in-Time Admin Login and configuring Blocker.

In addition to these technical capabilities, AutoElevate also offers a number of invaluable features that make it a pivotal tool for organizations, including:

Just-in-Time Admin

Technicians can login into Windows machines securely and having zero password knowledge using AutoElevate's mobile app with biometric security.
Just-in-Time Admin generates a temporary admin profile that automatically is purged upon logout.

Blocker

Block over 40 known native threats in Microsoft(which are may allow bad actors to circumvent WDAC) and an additional +180 other Living Off the Land (LOTL) vectors. Blocker's curated list can help mitigate false positives, helping to ensure minimal disruption to your end users and managed networks.