FEATURE SHEET

CyberFOX AutoElevate

Least Privilege for Lean IT Teams

200+
LOTL attack vectors blocked by Blocker

0
Passwords needed for JIT Admin Login

>80%
Of elevation requests automated

1 Just-in-Time Admin Login

Get into any Windows machine directly from the lock screen — no password knowledge required, no shared credentials, no permanent admin accoutns. Open the CyberFOX AutoElevate mobile app, scan the QR code, and a temporary admin account rotates in automatically. Once you log out, it's gone — encrypted, never reused, never reshared.

2 Technician Mode

Do admin-level work without shared privileged credentials. Use a hotkey to display a QR code on any managed machine, scan it with the AutoElevate mobile app, and you're in — with full elevated access and a real-time security sidebar running application and malware checks. When you're done, turn it off and you're back to standard. Every session is logged as a UAC event so you have full visibility into each request, decision, and outcome that occurs.

3 Biometric Local Authentication

Add an extra layer of verification to the AutoElevate mobile app and control exactly where it applies. Require biometrics for JIT login, one-time approvals, rule creation, or Technician Mode — each set independently. You're not choosing between security and convenience. You're getting both.

4 AzureAD SSO

Technicians log into the AutoElevate Admin Portal using their existing AzureAD credentials. One less login to manage for your team — without giving up any control over who has access.

5 Windows Event Logs

AutoElevate writes elevation events and privileged user activity directly to each machine's Windows Event Log. If you're running a SIEM, that data is already there and ready to ingest — no manual exports, no extra steps. Full visibility into who did what, on which machine, and when.

6 Multi-Level Settings & Customization

AutoElevate gives you granular configuration control all the way down to the individual computer level. Customize dialog messages, notification timers, company branding, and agent security settings per device, location, or company — not just as a single global configuration that applies everywhere.

7 Blocklistng

Most ransomware never triggers a UAC prompt — it hijacks native Windows tools already on the machine and slips past traditional antivirus entirely. Blocker stops it by proactively blocking 40+ native Microsoft threats and 180+ LOTL attack vectors, with a built-in recommendation agent that flags risky unused tools so you can block them in one click.

CyberFOX.com/AutoElevate
(813) 578-8200

E070626

CyberFOX™ AutoElevate