BUSINESS COMMUNICATION SOLUTIONS | www.bcs-ip.com | 512-257-1433

PRIVILEGE MANAGEMENT

TAKE AWAY ADMIN RIGHTS, NOT PRODUCTIVITY.

When employees log in as administrators, one bad click can give malware control of the whole computer. AutoElevate removes those rights, and BCS approves legitimate requests in real time.

40%

of Microsoft vulnerabilities disclosed in 2025 were elevation-of-privilege flaws.
Attackers want admin rights. Take them away and many attacks hit a wall.
BeyondTrust 2026 Microsoft Vulnerabilities Report

HOW IT WORKS

Employees ask. BCS approves. Malware gets nothing.

1. An employee needs to install an app or update.
2. AutoElevate sends the request to BCS instantly.
3. A BCS tech reviews and approves it, even from a phone.
4. The app installs. Suspicious files stay blocked.

WHY BUSINESSES CHOOSE AUTOELEVATE

NO ADMIN, NO HASSLE
Employees keep working without waiting on a callback for every install.

RULES THAT LEARN
Trusted apps can be approved automatically. Risky ones are blocked.

FULL AUDIT TRAIL
Every request is logged: who asked, which computer, and the outcome.

INSURANCE-READY
Helps meet cyber insurance and CIS Controls requirements for admin rights.

FREE CYBERSECURITY ASSESSMENT

Find out who in your office has admin rights today.

(512) 257-1433
austin@bcs-ip.com
bcs-ip.com

Source: BeyondTrust 2026 Microsoft Vulnerabilities Report (509 of 1,273 Microsoft vulnerabilities disclosed in 2025 were elevation of privilege).