AutoElevate (PAM)

Privileged Access Management

DataComm's Privilege Management System, AutoElevate (Powered by CyberFox) allows your organization to remove administrator rights, quickly move to a more secure least privilege model, and control privileged access seamlessly.

The idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function. In an IT environment, adhering to the principle of least privilege reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.

"94% of Windows critical vulnerabilities are resolved by removing admin rights"

- 2016 Avecto Microsoft Study

How Malicious Actors Gain Access to Your Network

Attackers have a variety of methods to gain the initial foothold on a target computer. Some methods are possible with users operating with Standard privileges but often are accomplished by exploiting vulnerabilities that otherwise are only possible if the user is operating with Admin privileges.

"Privileged Accounts Are the Keys to Your Kingdom"

If a hacker can gain access to one computer that has local Admin privileges, they most likely have everything they need to "own" your whole network. Privileged accounts are the keys to the kingdom, making them the top target of any attacker seeking to gain access and move anywhere within your network.

Windows caches account credentials by default, allowing users to log in even if a network server (domain controller) isn't present to authenticate the request. Once a malicious actor gains access to a computer where a network administrator has previously logged on, using local Admin privileges they can potentially retrieve a copy of the password for highly privileged network administrator accounts. In a short amount of time, they can have a valid Network Administrator account with access to anything and everything on the network. The worst part is because they are accessing the network with a valid account, chances are slim that anyone would ever know that they were there.

Therefore, the "chaining and linking" of Admin rights through compromising other privileged accounts is a focus of attention for attackers.

Benefits

- Part of a Zero Trust Model
- Meet Security & Compliance Models
- An Essential Layer of Defense Against Malware
- Easily Create Rules for Approved Privilege Escalation
- Live Portal with Reporting
- Manage Privileges Anytime, Anywhere with Mobile App

Supports

- Microsoft Windows Endpoints

Reducing Admin Privileges is Essential

Removing Administrator privileges from everyday Windows users slows down or stops a high percentage of malware infections. This is the safest procedure to follow. By only allowing Standard privileges you'll reduce your attackers target size from the "side of a barn" to a bottlecap.

Only giving users access to what they need to do their job is a key to the success of keeping your environment secure and is the practical application of a fundamental best security practice called 'least privilege'. The principle of least privilege is a methodology in which privileges are only approved and granted when they are necessary to do a specific task or job. This makes the job for hackers much harder because it limits the chances for an attacker to compromise your entire network by targeting your typical users.

Your network security is only as strong as its weakest link. Restricting Admin accounts will enhance all your cybersecurity efforts and is one of the best ways to help stop malware and thwart attackers.

"The average time to identify and contain a security breach is 277 days, with 207 days to identify the breach and 70 days to contain it."

- 2022 IBM Data Breach Report

Why Choose DataComm?

- **Experience:** DataComm has over 20 years of experience providing security solutions to organizations of all sizes and industries. Our team of security experts has the knowledge and expertise to help you develop a customized security solution that meets your specific needs.
- **Flexibility:** DataComm understands that every organization has unique security needs. That's why we offer flexible solutions, custom-tailored to meet your institution's requirements. Whether you need a standalone PAM solution or a comprehensive security platform that includes endpoint, network, and cloud security, DataComm can help.
- **Partnership:** We are committed to building long-term partnerships with our clients. We work closely with our clients to understand their business and security needs, and we strive to provide solutions that help them achieve their goals.
- **Technical Support:** We offer comprehensive technical support and professional services to ensure successful implementation and ongoing management of our PAM Solution. Our team of certified security experts is available to provide guidance, troubleshoot issues, and help optimize your security operations.
- **Value:** Our competitive pricing allows you get the most value from your security investment. With AutoElevate, you can obtain Privileged Access Management without breaking the bank.

DataComm

800.544.4627

www.datacomm.com

sales@datacomm.com