MOVE BEYOND GPO FOR NEXT-LEVEL PRIVILEGE MANAGEMENT

thycotic

MOVE BEYOND GPO FOR NEXT-LEVEL PRIVILEGE MANAGEMENT

The first stage of privilege management

Most organizations with an office full of Windows computers launch their privilege management strategy using Microsoft's Group Policy Objects (GPO). If you've been trying to get a handle on user access rights and want to manage privileges with centralized policies, GPO offers a good starting point.

GPO is free and accessible to organizations of all sizes. It includes out-of-the-box default templates you can adapt to your needs.

By configuring settings within Group Policy you can define what users in Active Directory can and can't do on their local computers, making it a helpful tool to support a least privilege policy in accordance with regulatory requirements.

GPO also allows you to set requirements for local administrator passwords such as length, complexity and frequency of changes. You can use GPO settings to require users to update their local admin passwords or be locked out.

But, you need flexibility and greater control and auditing as you grow

As your organization becomes more complex, your privilege management needs will become more diverse. The number of users and Groups in your organization will expand and may change frequently, making it difficult for you to keep up. You'll start to add on non-Window machines, non-domain endpoints, and third-party users who aren't within your Active Directory but need access to sensitive systems and data to get work done. You may have to meet compliance requirements, which all require rock-solid audit logs of exactly who is doing what, when.

Relying exclusively on GPO for privilege management can become more cumbersome, if not impossible.

Another struggle growing teams face is GPO presents "all or nothing" options for controlling privileges, without giving you the capacity to set and adjust granular policies. As a result, business users and helpdesk teams will feel the pain of increased security policies and your best laid plans can easily fail.

Let's explore what happens to a growing organization relying on GPO for privilege management, and how to fill the gaps.

WHAT HAPPENS WHEN YOU USE GPO FOR PRIVILEGE MANAGEMENT

1. No automated password creation, storage, or rotation of local privileged accounts makes password management a drain on productivity

As noted, GPO allows you to set local account password requirements. But it doesn't allow you to automatically set, retrieve, or rotate local admin credentials. Rather, it places the manual burden for creating, remembering, changing, and sharing passwords on IT and support teams. Unfortunately, most users are notoriously poor at password management. In fact, adding password rules for users can backfire, causing people to create weaker passwords, even for privileged accounts.

GPO doesn't have a password vault for local accounts that is centrally secured and managed. Therefore, administrators don't have the ability to remotely monitor sessions, or require check-out or other advanced features that lower risk of privileged credential abuse.

When people aren't able to execute applications because they don't have the proper credentials, GPO doesn't provide any help. Elevated credentials are either shared with a user or a user's account must be given privileged rights. Either way, there's no management or automation of those privileged credentials once they're out "in the wild."

2. No reporting capability makes audit compliance and incident response painful

GPO doesn't provide an easy audit trail. There are no reports you can pull to show how passwords are being used, how privileged accounts are being accessed, or how administrators have added or changed configurations.

Let's say a threat agent enters your system and gains privilege access. Chances are high that the first thing they'll do is change event logs to cover their tracks. If you were relying only on GPO to monitor privileged account access, you'd never know that a cybercriminal was inside.

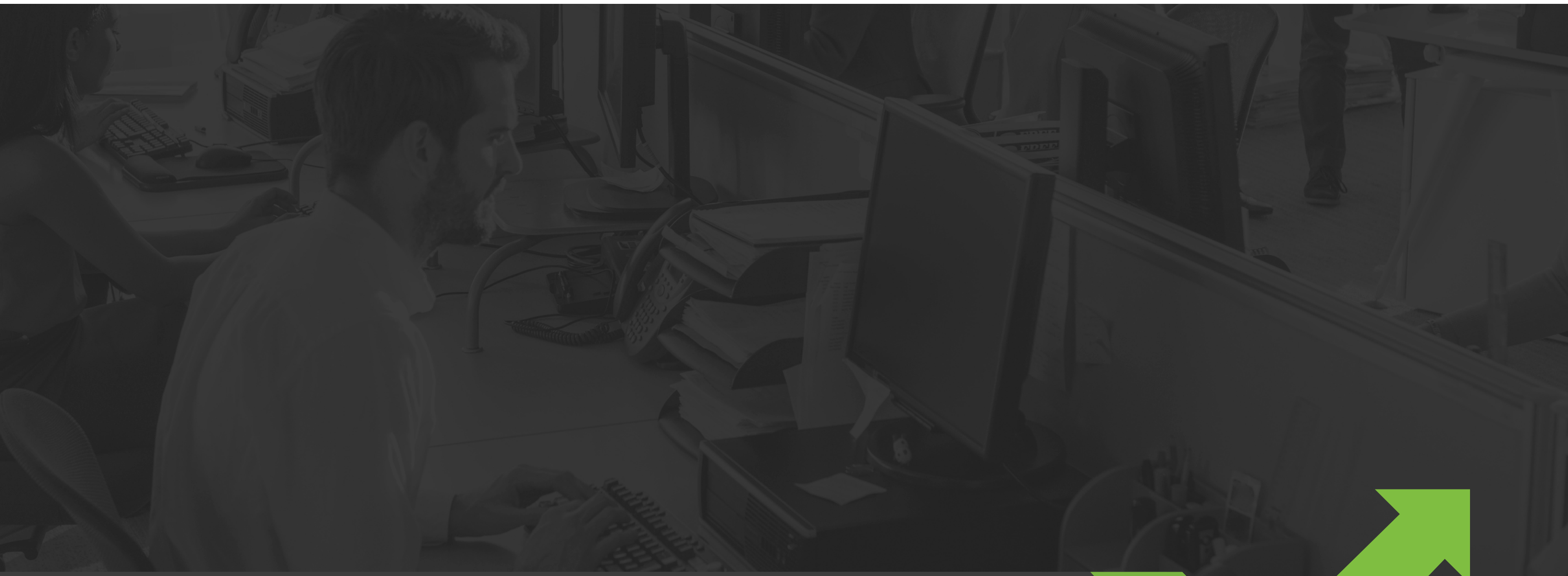
3. No discovery phase or application control, making least privilege difficult to implement and enforce

Some organizations try to use GPO to implement a least privilege policy by adding certain users into an admin group that has privileged access. However, GPO doesn't allow for a discovery phase to confirm which users require access to administrative controls and which don't before you must commit policy changes. With GPO you have no inventory of applications and programs that are currently being executed with admin rights. Without a pre-check, many users and machines can be improperly assigned excess privileges or worse, left out of the management process entirely.

Relying on GPO for a least privilege policy means you have no ability to create granular policies for application control. Therefore, every time users that are not in the admin group require access to an application to do their job, they need to ask for help – likely from an already overworked and stressed support team.

4. No privilege management for non-domain or third-parties increases your risk

GPO is intimately tied to Active Directory. But internal users on your network are not your only concern when it comes to privilege management. GPO can't manage privileges for non-domain machines, partners or contractors who need access to data, or people who are working offline.



ENTERPRISE PRIVILEGE MANAGEMENT THAT GOES BEYOND GPO

As you begin to look beyond GPO you'll have many options for privilege management solutions.

As you explore your options, make sure you keep in mind the crucial requirements for success: scalability, productivity, and control. Ask the tough questions of any privilege management vendor to make sure their solution is the right fit for your organization and will support your needs as you grow and change.

What to ask:

How does it manage local passwords?

What to expect:

Enterprise privilege management solutions should be able to create complex passwords that meet compliance requirements, store them securely in a password vault, and rotate them regularly or on-demand – all without interrupting user productivity.

Let's say you discover a cyberattack has breached one of your endpoints and you need to protect sensitive systems and data before it progresses. An effective privilege management solution allows you to automatically change all admin passwords at once, behind the scenes, and allow business to continue as usual.

What to ask:

How does application control support enforcement of a least privilege model?

What to expect:

Privilege management with application control allows you to deploy a least privilege policy that can be adopted and enforced. You can automatically audit who is using what applications, and then set your application approval policies on a granular level. This way, when your least privilege policy goes live, it does not impact your company's productivity. Applications that require administrative or root access will be silently elevated based on your policy, without having to change permissions or provide elevated credentials. Whitelisting, blacklisting,and greylisting allow for contextual polices that keep people productive.

What to ask:

How do you manage privileges for non-Windows and non-domain endpoints?

What to expect:

Enterprise privilege management tools should work with Windows and Mac devices, as well as domain-joined and non-domain-joined endpoints to give you far more visibility and control. With best-in-class privilege management solutions, privileges are secure even when employees and third parties are working remotely or off-network.

What to ask:

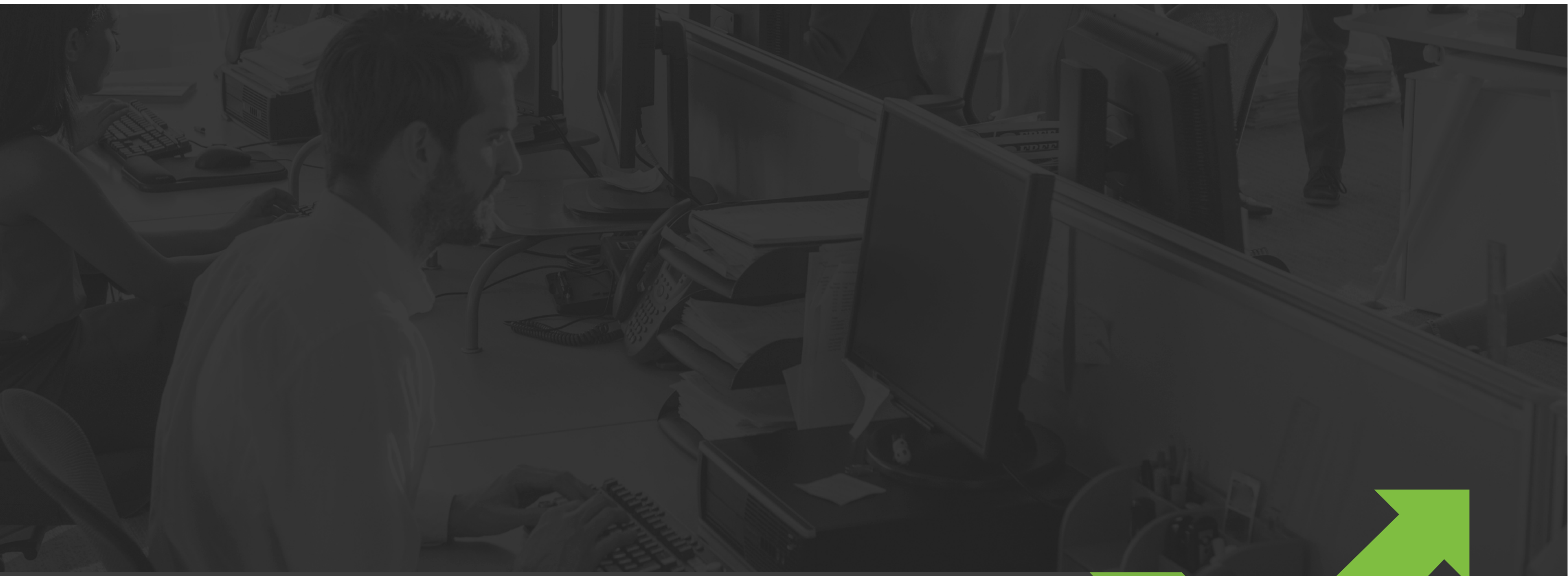
How simple and customizable are your reports?

What to expect:

Enterprise privilege management tools help you demonstrate compliance with least privilege and application control policies for your leadership team and external auditors. They should have permanent, unchangeable audit logs and come with easily configurable and sharable reports so you can see the history and usage of privileged accounts.

DON’T PAY FOR WHAT YOU DONT NEED

A word of caution: Some privilege management tools are built with an architecture that relies on GPO controls. That means they don’t have the ability to manage local accounts and they can’t protect non-domain endpoints. These tools won’t offer much, if any, upgrade from the native GPO functionality that you started with.



LET’S MAKE YOUR LIFE EASIER

As a next step, discover local admin accounts, service accounts, and applications in use on endpoints with this free Least Privilege Discovery Tool for Windows.

- Find out which endpoints and local users have admin rights
- Know what applications are in use and if they require admin rights to run
- Get a comprehensive Summary Report highlighting your risks for local and service accounts, and applications

Find out what life beyond GPO can look like

When you are ready to move beyond GPO, try Thycotic’s Privilege Manager for yourself.

With Privilege Manager you can implement least privilege best practices to control access rights and protect sensitive data and systems. Automated application controls allow people to do their jobs without requiring unneeded access or local administrative rights.

TRY PRIVILEGE MANAGE FREE FOR 30 DAYS

START MY FREE TRIAL

thycotic.com/PrivilegeManager