THYCOTIC eBOOK

TOP 10 KEYS TO SUCCESSFUL LEAST PRIVILEGE ADOPTION VIA APPLICATION CONTROL

THIS eBOOK IS FOR YOU IF YOU ARE RESPONSIBLE FOR:

- Endpoint protection
- Desktop user support
- Application security within your organization

Endpoint security is a crowded and complicated business, full of overly complex and overlapping tools.

As expensive ransomware attacks and increasing compliance requirements raise the stakes for organizations trying to protect endpoints, knowing where to start can be difficult.

In this paper we'll explain how you can eliminate the risk of most malware attacks by implementing one of the most fundamental security strategies—the principle of least privilege. We'll also cover keys to successful least privilege adoption using application control, so you can avoid the common pitfalls that cause least privilege strategies to fail.

thycotic

DC | LONDON | SYDNEY

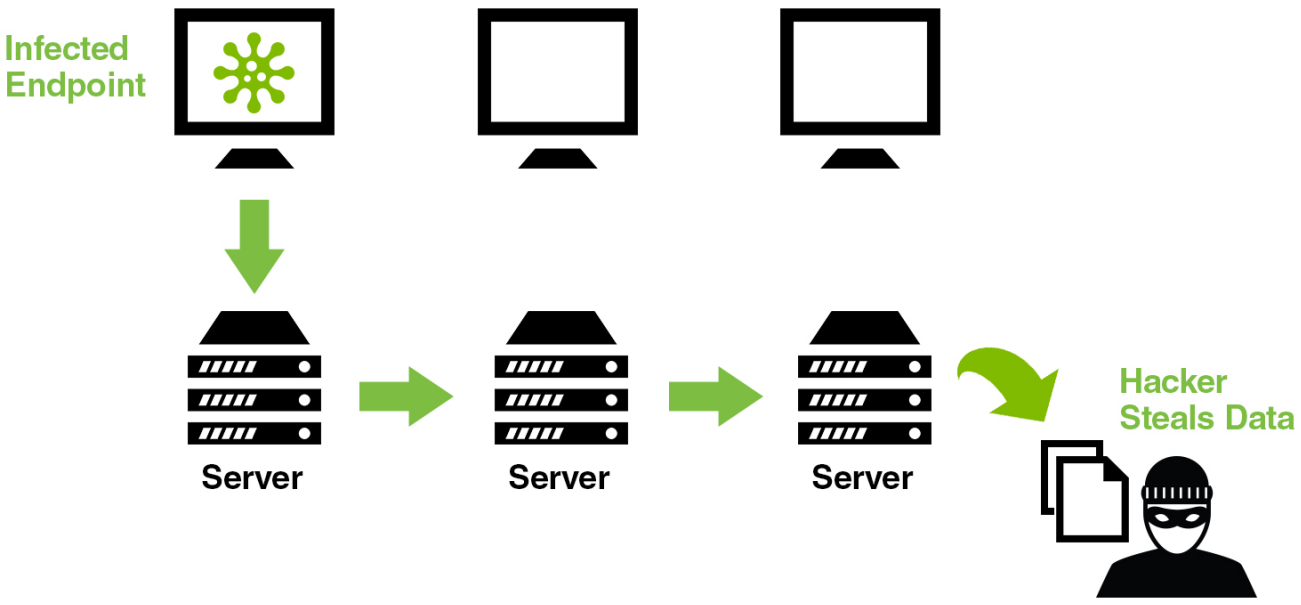
MSP@thycotic.com
+1-202-802-9399
www.thycotic.com

WHY HACKERS LOVE ENDPOINTS

John receives an email that appears to be from the CEO of the company. He clicks on the attachment. Without knowing it, John downloads malicious software onto his machine, which kicks off processes that capture his user credentials. Because John's computer contains local administrative rights, the malware has succeeded in editing the computer's registry, allowing the malware – and the hacker – to persist on John's computer. Without John realizing it, the malware has also captured the hashes of John's credentials, allowing it to traverse other areas within his organization's network. Then the malware covers its tracks by changing system logs. No one knows that the hacker is inside the network. And all of this occurred as a result of a local admin rights exploit.

Despite best efforts to raise awareness and train users on secure behavior, 23% of employees will open phishing emails and 11% will click on the attachment, just as John did.[1] These types of successful social engineering attacks are one reason employee workstations are the most vulnerable part of the attack surface. All it takes is one "John" with local administrative privileges to take down an entire network.

In fact, 85% of breaches involve compromised endpoints, making them the most common entry point for threats into organizations.[2] Data breaches, changes to critical business processes, and service disruption can all be caused by a threat agent gaining local admin privileges through a single endpoint. As we saw recently, the Wannacry exploit began by gaining access to admin privileges on a single machine. In that case, malware spread beyond the initially infected endpoint through the network, eventually infecting 230k+ computers in 150 countries.



LOCAL ADMINISTRATIVE ACCOUNTS ARE PRIVILEGED ACCOUNTS

Hackers target endpoints because they are the first step to capturing the keys to your castle – privileged account credentials, which give attackers and insiders the ability to move undetected across your network. Even if local accounts have not been granted elevated privileges in the domain or the operating system, attackers can manipulate configurations of insecure applications gain the same level of access to move through your network to sensitive data.

OVER-PRIVILEGE IS RAMPANT

Overly privileged accounts are found in every type of organization, no matter their size or sophistication. According to Microsoft, "midsized directories may have dozens of accounts in the most highly privileged groups, while large installations may have hundreds or even thousands."[3]

Why does this happen? When organizations are young or rapidly growing, they may not have a mature endpoint security strategy in place. Often due to OS imaging across the organization, hidden local passwords may have been left in all workstations and are stored in local memory.

As organizations grow, the IT team often struggles to keep pace and could have made a simple mistake. For example, if you have been using Active Directory controls to change user status, it's easy to add a local user to the wrong group. Or, IT may have elevated a user to an admin status for a one-time request, but forgotten to change the user's status back.

85%

OF BREACHES INVOLVE COMPROMISED ENDPOINTS

START HERE:

LEAST PRIVILEGE FOR PROACTIVE ENDPOINT PROTECTION

Applying the core security principle of least privilege is a foundational element of your endpoint security strategy. By removing local administrative privileges on endpoints you can reduce your attack surface and block the primary attack vector, preventing the vast majority of attacks from occurring.

Least privilege adoption is the most effective way to protect your endpoints from attack, with immediate, measurable benefits.

Before you consider implementing next-generation Endpoint Protection Platforms (EPP) or complex Endpoint Discovery and Remediation solutions (EDRs), you should begin your endpoint security strategy with fundamental hygiene. Proactive protection based on least privilege means less time and resources spent detecting an infection, chasing down hackers once they have already entered your network, and remediating the damage.

REGULATORY COMPLIANCE REQUIREMENTS

In addition to the measurable impact on scarce security resources, implementing least privilege provides demonstrable evidence of your compliance with security best practices.

Compliance and regulatory mandates (including HIPAA, PCI DSS, FDDC, Government Connect, FISMA, and SOX) are putting a stronger emphasis on privileged accounts, access, and anomalous behavior. Agencies have been imposing an increasing number of fines and civil penalties for breaches that expose poor privilege hygiene. To demonstrate proper data protection and security in your next audit, you will need to address least privilege at the endpoint level.

GO INTO A LEAST PRIVILEGE MODEL WITH YOUR EYES OPEN

Organizations have learned the hard way that what works for security doesn't always work for business productivity. Many least privilege programs fail because removing local administrative rights can have negative consequences for users and IT teams.

Many processes that users run every day require administrative rights, including installing printers, updating software, and changing system preferences. Common conferencing applications like Join.me or GoToMeeting require users to download and execute applications.

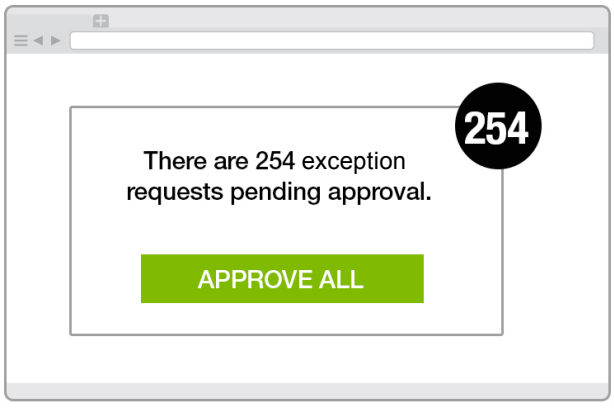
What's more, some programs, processes, ActiveX controls, and user-run scripts break if user privileges are suddenly removed.

If users are required to request exceptions from IT every time they want to run a required process or install a needed application, productivity stops. Tickets flood the desktop support queue and IT expenses increase. If the desktop team suddenly goes from managing 10 tickets each week to 100 tickets, at an average cost of $15 per ticket request, least privilege is not sustainable.[4]

Application control allows least privilege to be successful because users are able to continue using applications they need with no downtime or loss of productivity.

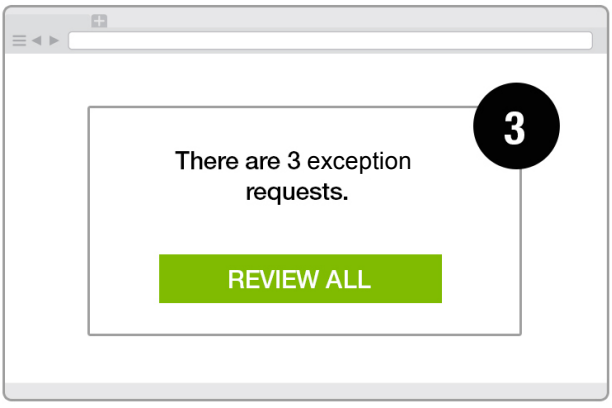
WHICH ONE WOULD YOU PREFER?

ONE-OFF MANAGEMENT
Limited choices



VS.

POLICY-BASED AUTOMATION
Contextual decision-making



Inspired by Gartner, Protecting Endpoints from Malware Using Application Whitelisting, Isolation and Privilege Management

LEAST PRIVILEGE THROUGH APPLICATION CONTROL
THE MOST SECURE & SUSTAINABLE WAY TO IMPLEMENT LEAST PRIVILEGE

There are two ways to implement least privilege so that users can continue to run the applications they need to do their jobs. Make sure you understand the differences and ask any endpoint security vendor about their approach.

CONTROL PRIVILEGE BY ELEVATING INDIVIDUAL USER ACCOUNTS

This approach briefly elevates a user to a local admin or uses a hidden admin user stored on the endpoint when rights are required for applications or processes.

This method creates vulnerabilities in your attack surface. Even having an administrative end user for a few minutes on an endpoint can lead to catastrophic data breaches if the endpoint is compromised. Although the window of opportunity is small, hackers don't need long to get inside.

OR

CONTROL PRIVILEGE BY ELEVATING APPLICATIONS

This approach elevates applications so that certain processes are allowed under certain pre-determined conditions.

By far, this method offers the strongest level of security because it ensures your users are NEVER operating as administrators.

It is also the most scalable and sustainable strategy to maintain least privilege as your organization grows, individuals change roles, and business needs dictate new types of applications and processes.

Gartner research supports application elevation as the preferred strategy to make least privilege a reality.

"By modifying application privileges, the user is able to log in as a standard user, and user permissions are untouched. **This has the following key advantages:**

- The need to provision local admin rights is reduced.
- The user is not elevated to a 'temporary' admin.
- An administrative account/password is never exposed to the user.
- The common 'pass-the-hash' attack vector is mitigated because any application security token has no validity outside of the specific instance of the running application and cannot be leveraged elsewhere." [5]

TOP 10 KEYS
TO SUCCESSFUL LEAST PRIVILEGE ADOPTION
VIA APPLICATION CONTROL

Once you decide you are ready to implement least privilege, make sure you are set up for success. A sustainable least privilege strategy is not something that can be set up overnight. It takes planning, collaboration, and the right tools to meet the needs of security, IT, desktop support, and users.

1. PLAN FOR A DISCOVERY PHASE

From the beginning of a least privilege implementation, security and desktop teams must work together to create application control policies that match the needs of your organization.

You'll want to use an automated discovery tool to:

- Find out which endpoints and local users have admin rights.
- Know what applications are in use and if they require admin rights to run.

Although your software inventory system may have visibility into applications managed and approved by IT, users may have downloaded software or accessed SaaS tools that haven't made it onto your list. It's important to have an automated application discovery tool so your discovery phase includes a full list of applications in use by business users, and automated least privilege discovery ensures no hidden privileges are missed.

This discovery period creates shared understanding between security, IT, and business users about security concerns and application usage requirements.

2. CREATE A WHITELIST OF ACCEPTABLE APPLICATIONS AND PROCESSES

After this discovery process helps determine which applications are safe to run, you can add them to a trusted "whitelist" based on their name, signature, certificate date, or other criteria.

Once you set up an initial baseline policy, it can apply to all protected endpoints. From that point forward, instead of managing each application request one by one, most application elevation is done automatically with little work from IT and is seamless to users.

3. BLOCK KNOWN "BAD" FILES WITH A BLACKLIST

The most common security tactic to protect against malware is blacklisting, where malicious code is flagged and subsequently denied. Application control solutions will include reputational databases to guide you on what applications to blacklist, and can integrate with systems such as VirusTotal to provide the latest threat intelligence to block known threats.

4. ACCOUNT FOR THE UNKNOWN WITH A GREYLIST AND SANDBOXING

What about the threats you don't know?

Whitelisting works for a known set of applications, but your universe changes as users download new software and access new SaaS tools, often without requiring approval from IT.

The problem with blacklisting is that most malware is highly polymorphic and difficult to track. Sophisticated hackers are constantly adapting code in order to evade detection. In fact, malicious code can be unique to each affected organization, so it will not be found in a database of known threats.

You need an application control solution that provides an option for a "greylist" – a way to sandbox unknown applications so that you can investigate them before allowing users to run them, especially when they require admin rights for certain processes.

With a greylist, you can elevate an application in a limited way so that users can do their jobs, but not allow them to touch any system folders or underlying OS configurations, isolating the system from malicious behavior. For example, applications should not be able to access a system's desktop, display settings, registry, clipboard, and handles/hooks.

With sandboxing you can feel confident that even if an application should have been denied outright, any damage will be contained because there are no privileged credentials on the endpoint that would allow a threat to progress.

5. SET CONTEXTUAL POLICES

Look for application control tools that allow you to easily customize policies to match your organizational needs and detect anomalous behavior. For example, you may want to allow processes to run only on certain types of endpoints, by certain organizational groups, in certain geographic regions, or during certain times of day. If you find that there are applications attempting to run outside of the accepted conditions, you'll be able to flag potential malware attempts.

6. PLAN FOR USERS TO CHANGE

Some least privilege solutions that rely on Active Directory and Group Policies will only enforce least privilege on new accounts, or accounts that are active at the time of implementation. In these cases, it is possible for local users to be re-added to a local administrator group without the least privilege tool knowing or being able to fix the privilege creep. Instead, look for a solution that knows immediately when a local account does not meet its approved level of privilege, and can automatically fix privilege levels.

Additionally, look for a solution that makes it easy for future changes. As your business grows, you may have users who move within the company, and you may need to adjust their permissions. For some tools, making future changes to a user's privilege requires manual checks against multiple systems, which can be time consuming and easily forgotten. Make sure the solution you use can be adapted to changes in user roles and company policies.

7. DON'T RESTRICT CONTROL TO DOMAIN-CONTROLLED ENDPOINTS ONLY

Some least privilege and application control solutions only allow you to contain threats on domain-managed endpoints, but that approach only considers part of your attack surface.

You also need to consider your universe of contractors, partners, or other 3rd parties. Even though those machines are not joined to your domain, their accounts ARE connected and can be an entry point for threats. In fact, situations such as the well-publicized Target breach warn that 3rd parties often continue to have access even after they stop working with your organization.

8. DON'T FORGET CHILD PROCESSES

It is imperative that child processes do not inherit administrative privileges that would allow them to access restricted file folders or executables. An advanced application control tool will also let you decide whether to allow child processes, such as executing processes from within a PDF.

9. INTEGRATE WORKFLOW INTO EXISTING TOOLS

Although most application elevation will be pre-approved and happen behind the scenes without any intervention or justification, new applications and process requests will require some communication between users and IT.

To build awareness of the need for application review and set expectations, you can provide users who are requesting an application with a customized message that explains the requirements and time needed to evaluate their request.

So the desktop support team can view and respond quickly to application requests and track response metrics, integrate your application control process into their existing workflow. Give them the choice to consume requests however they prefer, via a web portal, mobile app, or ticketing system.

10. DEMONSTRATE SUCCESS

Imagine your CEO wants to know if your organization has been impacted by the latest malware to hit the news cycle. You should be able to pull up a report to show if your endpoints were targeted and, if so, how your policies prevented a full-blown attack.

Before you are asked, make sure you proactively demonstrate least privilege compliance with your management team as well as internal and external auditors. Gartner recommends you "maintain a thorough audit history of what applications were run, by which user and on which machine."[6] Based on the audit trail, you can create reports that demonstrate how you are protecting endpoints by following security best practices for least privilege.

For example, you could show:

- How many endpoints have been transitioned to/are in compliance with least privilege
- How many applications have gone through review and are governed by a policy for application control
- Which/how many malicious applications been blocked from executing
- Which endpoints are being targeted more than average

Compare results over time to show trends that showcase your continued progress.

NEXT STEPS

FIND OUT WHICH RISKY APPLICATIONS YOUR USERS ARE RUNNING

Get this free Endpoint Application Discovery Tool to identify which applications running in your environment may be opening the door for malware.

FIND OUT HERE:

https://thycotic.com/solutions/free-it-tools/free-endpoint-application-discovery-tool/

> "Maintain a thorough audit history of what applications were ran, by which user, and on which machine."
>
> – GARTNER

SEE HOW EASY IMPLEMENTING LEAST PRIVILEGE CAN BE

Try Thycotic Privilege Manager free for 30 days. You'll be able to create application control policies, including whitelisting, blacklisting and greylisting, and enforce least privilege without impacting productivity.

TRY IT FREE FOR 30-DAYS HERE:

https://thycotic.com/products/privilege-manager/start-a-trial/

Thycotic, a global leader in cybersecurity, is the fastest growing provider of Privileged Access Management (PAM) solutions. Thycotic enables you to minimize privileged credential risk, limit user privileges, and control applications on endpoints and servers. Thycotic's award-winning PAM solutions improve cybersecurity, increase productivity, and help demonstrate compliance for more than 7500 organizations worldwide, including Fortune 500 companies.

Thycotic Privilege Manager automatically removes administrative rights from domain and non-domain managed endpoints, including privileged credentials that are hidden or hard-coded. It uses policy-based controls to elevate applications users need to do their jobs, without requiring administrative credentials or requesting IT support. Because Privilege Manager elevates applications and not the user, it never leaves a window open for hackers, even for a moment. As your organization grows and users continually explore applications, Privilege Manager adjusts.

AUTOMATE VIRTUALLY ALL APPLICATION ELEVATION

With Thycotic Privilege Manager, the vast majority of application elevation requests are managed automatically, based on granular, contextual policies. As a result, most applications are either approved or denied without any extra work from IT, leaving only specialized or custom applications for hands-on review and approval. Your support queue is smaller and you have more time for other IT and security priorities.

WHITELISTING
APPROVES

Printers, drivers, conferencing, known and trusted business applications

BLACKLISTING
DENIES

Untrusted applications, suspicious files identified by threat intelligence

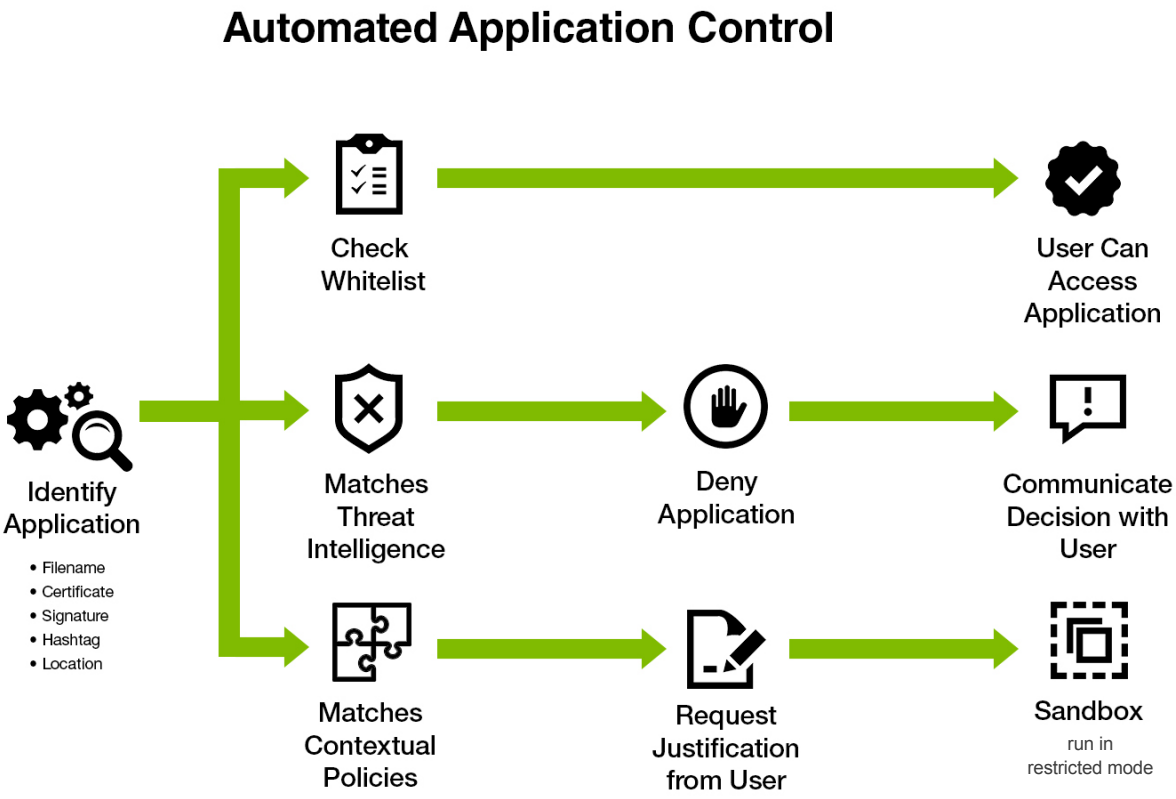
GRAYLISTING
RESTRICTS

Require approval, request user justification, quarantine file, run in sandbox/restricted mode

---

PRIVILEGE MANAGER WORKFLOW

Thycotic Privilege Manager automatically adds trusted applications to a whitelist, relies on the latest intelligence from threat databases such as VirusTotal to create blacklists, and adds unknown applications to greylists for further assessment. Sandboxing allows you to elevate applications in a limited way so they don't have access to system controls or OS configurations.



References:

1. Verizon, Data Breach Report
2. SANS, Exploits at the Endpoint
3. Microsoft, Implementing Least Privilege Administrative Models
4. Thinkhdi.com, Metric of the Month
5. Gartner, Protecting Endpoints from Malware Using Application Whitelisting, Isolation and Privilege Management

To learn more visit our website at www.thycotic.com.

MSP@thycotic.com
+1-202-802-9399
www.thycotic.com