Achieving Protection and Productivity by **Securing Privilege on the Endpoint**

CYBERARK®

Contents

Overview 1

Challenges with Securing and Managing Users and Applications 2

Recommendations for Developing Layered Security Controls and Strengthening Endpoint Security 10

Conclusion 12

Overview

Information security professionals recognize that cyber attackers almost always look to exploit endpoint vulnerabilities, and many have taken steps to secure privilege on the endpoint as a fundamental part of their security program. For many organizations, privileged account security efforts revolve around privilege delegation. But by design, privilege delegation is often an all-or-nothing decision – meaning that users within organizations typically either have full "Administrator" rights or no administrative rights at all. As a result, business users and IT administrators often end up with far more privileges than needed, creating a large and frequently exploited attack surface. The trouble is, in the process of removing administrator privileges to reduce risks, organizations are likely to face a number of challenges. This eBook will explore these challenges and offer best practices for developing balanced, layered security controls.

Challenge 1

The threat landscape is constantly evolving

In their attempts to defeat the information security controls deployed by organizations, cyber criminals are constantly evolving their tactics. Today, there is a recognition by most information security professionals that a breach is inevitable. An attacker will evade the existing security controls and move laterally through the network, stealing credentials and elevating privileges, until he/she finds sensitive information to steal or encrypt and hold for ransom. Organizations plan for this by no longer focusing solely on prevention. Detection and response are now critical components of any security program.

Endpoint detection and response tools will help identify attacks that have evaded traditional endpoint protection. However, unless these tools can detect an attack quickly, it may be too late.

Data loss prevention technologies are designed to detect and block a successful attacker's attempts to exfiltrate sensitive information. However, they cannot help when an attacker isn't trying to steal information, but instead, simply encrypting it and holding it for ransom.

So-called next-generation endpoint protection uses new detection techniques, such as machine learning and malware behavior analysis, to try and prevent an attack. While important, this is yet another prevention technology to add to the arsenal of existing ones.

In this evolving threat landscape, a layered approach to endpoint security is required to effectively combat malware and non-malware based advanced attacks.

Challenge 2

Powerful accounts represent a large attack surface

Accounts with local administrator privileges represent a large attack surface, as they exist on every endpoint and server within the environment. And individual user accounts – on these same machines – that have administrator privileges only expand the attack surface.

Consider that users with administrative rights can intentionally or accidentally:

Change system configurations

- Install and start services
- Disable/uninstall anti-virus
- Render the machine unbootable
- Stop existing services (such as the firewall)
- Replace OS and other program files with Trojan horses

Install malware

- Kernel-mode root kits
- System-level key loggers
- Malicious ActiveX controls
- Spyware and adware
- Malware to facilitate Pass-the-Hash exploits

Access and change accounts

- Create and modify user accounts
- Reset local passwords
- Access data belonging to other users

From a security perspective, accounts with local administrator privileges are frequently targeted by advanced attackers due to the privileges they provide, and when not properly protected, these accounts can be easily exploited.

From an operations perspective, inexperienced users with administrative privileges often cause accidental harm to their machines, meaning that IT teams must spend a significant amount of on-going time and effort fixing unintentional damage and remediating incidents.

Challenge 3

It’s difficult to balance security with productivity

While it’s a security best practice to revoke administrator privileges from business users, many organizations are rightfully hesitant to make a change. Without any administrative privileges, business users may be unable to carry out certain tasks or use certain applications needed for their day-to-day roles.

For example, a user may need to use an application for work purposes that requires privileges to run. Or, a user may need to use administrative privileges to install or update an authorized, trusted application. By completely revoking administrative privileges from business users, these users are forced to call the help desk every time they need privileges to simply do their day-to-day jobs.

This results in:

Frustrated Users

Inflexible privilege policies can bring a business to a halt. This inevitably leads to frustrated users who are no longer empowered to carry out necessary tasks.

Overburdened Support Teams

When IT policies prevent business users from carrying out necessary, day-to-day tasks, users must call the help desk to restore necessary permissions. This can significantly drive up IT costs and overwhelm the support team.

Challenge 4

Too few privileges can lead to ‘privilege creep’ and increased risks

When organizations opt to revoke all administrative rights from business users, the IT team will occasionally need to re-grant privileges so that users can perform certain tasks. For example, many legacy and homegrown applications used within enterprise IT environments require privileges to run, as do many commercial off-the-shelf (COTS) applications. For business users to run these authorized and necessary applications, the IT team has to give local administrator privileges back to the users.

Once privileges are re-granted, they are rarely revoked, and over time, organizations can end up with most of their users holding local administrator rights – again. This ‘privilege creep’ reopens the security loophole associated with excessive administrative rights and makes organizations – that likely believe they are well-protected – more vulnerable to threats.

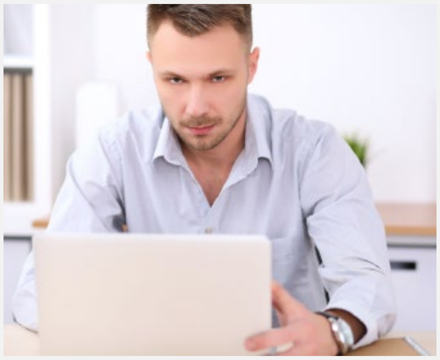
Challenge 5

Too many privileges can increase the risk of insider and advanced threats

In addition to the productivity tradeoffs associated with limiting business user privileges, many organizations are also hesitant to limit IT administrator privileges on Windows Servers. In an ideal setting, system administrators, application owners and database administrators would each have their own set of permissions on each server they are permitted to access. In practice, this segregation of duties can be difficult to implement, leaving IT administrators with far more privileges than truly needed to do their jobs.

Without role-based privilege policies in place to segregate duties for IT administrators, sensitive systems can easily be damaged by inexperienced users, exploited by malicious insiders or compromised by advanced attackers who have gained unauthorized privileged account access.

A new, inexperienced admin could accidentally damage systems by running a command in error



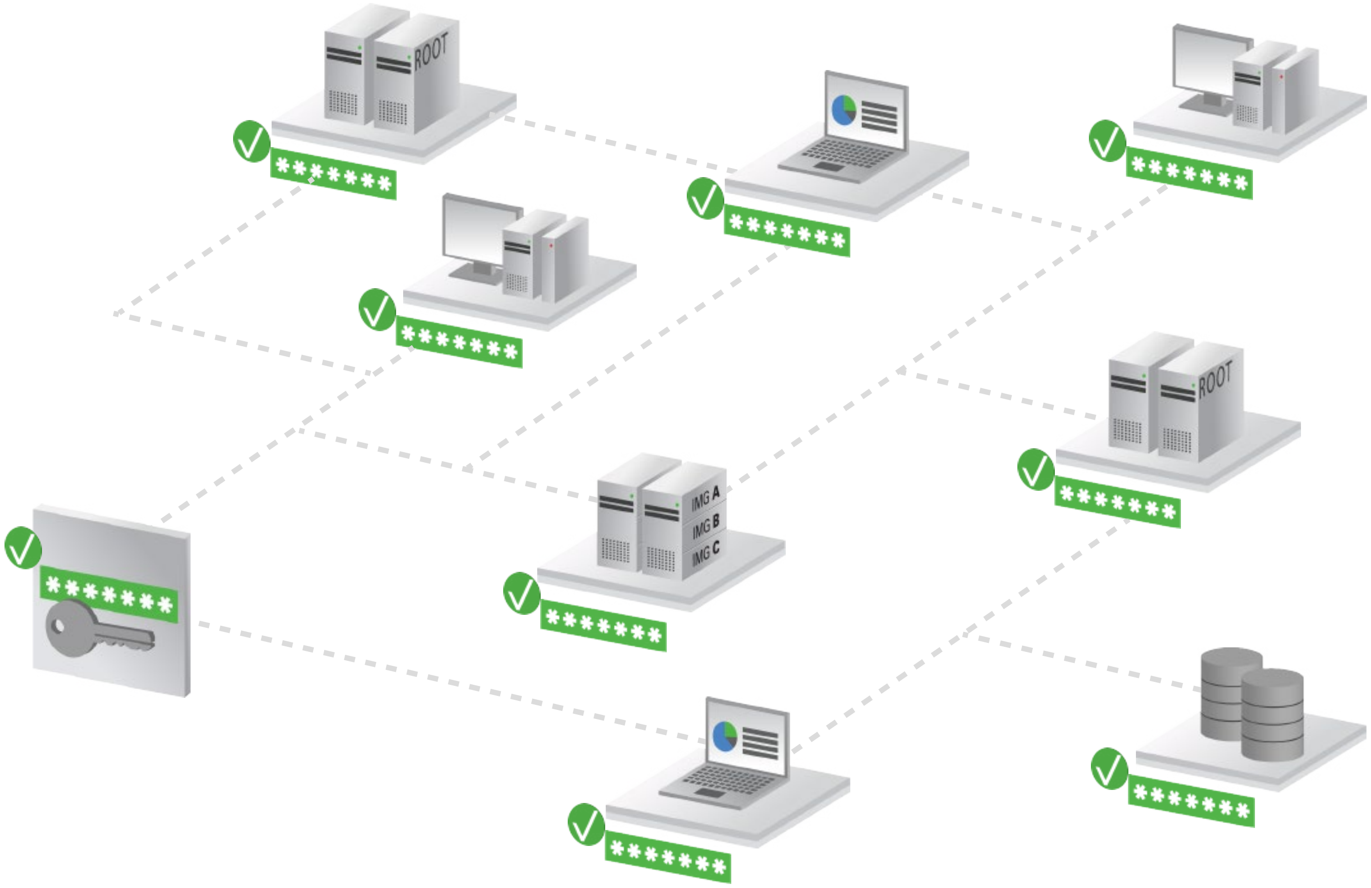
A malicious insider could use his rights to intentionally steal data or damage systems

An attacker could gain free reign over sensitive systems by compromising an administrator’s account

Challenge 6

There will always be an “Administrator” account on each machine

By design, all endpoints and servers contain an Administrator, root or similar level account that provides any user in possession with full administrative control over the machine. Even if you’ve removed administrator rights from individual user accounts, these powerful Administrator accounts will still exist. Poor password management policies for these Administrator accounts can result in password reuse across multiple systems, making it easy for an attacker on a compromised machine to laterally move throughout the environment – escalating privileges, stealing data and damaging systems along the way.



Challenge 7

Despite limited privileges, some malware can still get in

By limiting privileges to only those that are absolutely necessary, organizations can reduce the attack surface and block malicious applications that attempt to use privileges to install malware or damage the machine. The challenge is, not all malicious applications need privileges to execute, and as attackers become more adept in circumventing defenses, organizations are increasingly vulnerable to these types of malware.

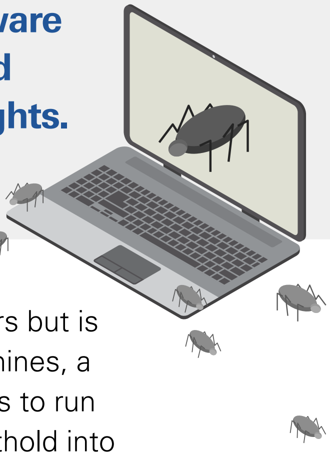
A campaign of just 10 emails will typically yield a greater than

90%

chance that at least one person will become the criminal's prey

Evidence shows that most advanced attacks start with phishing emails sent to non-privileged business users, and a campaign of just 10 emails will typically yield a greater than 90 percent chance that at least one person will become the criminal's prey.[1] These phishing attacks can include highly sophisticated malware, and once inside the network, the malware can compromise machines, steal data, capture credentials or damage systems all without using any administrative privileges.

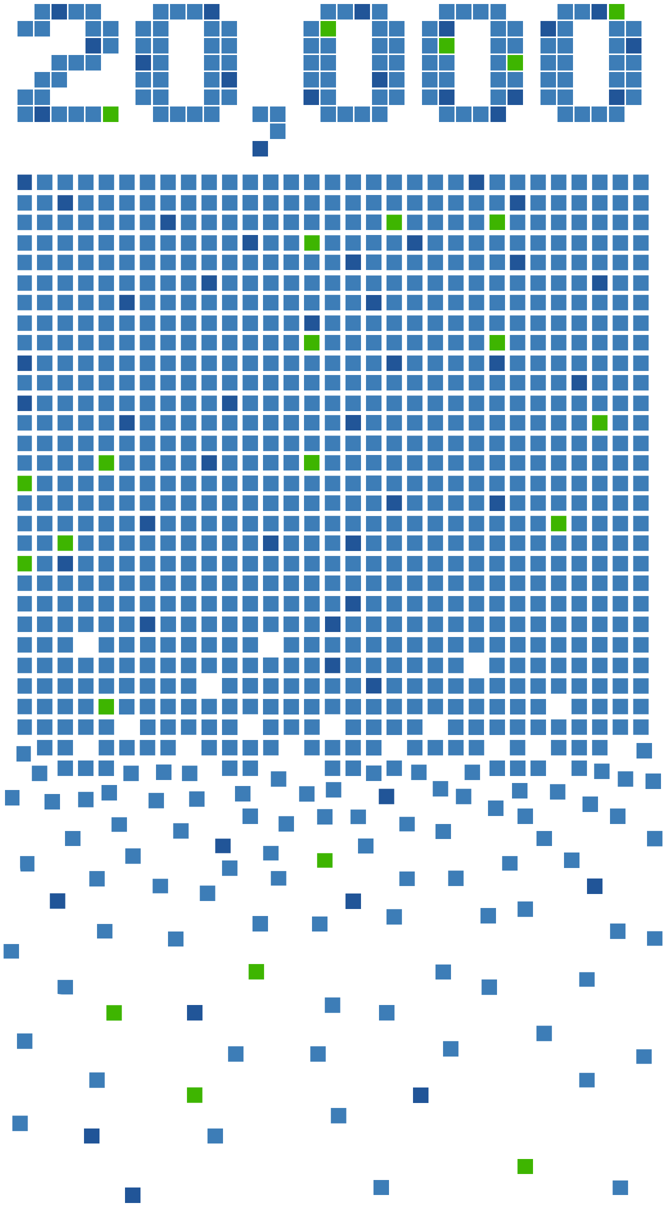
By exploiting just one vulnerability on one endpoint, malware can compromise a machine, steal sensitive information and infect other systems – all without needing administrative rights.



If an organization has removed users' administrative rights on endpoints and servers but is not monitoring and controlling which applications are allowed to run on these machines, a rogue application containing malware that does not require administrative privileges to run can enter the infrastructure and execute in the environment, giving attackers a foothold into the organization.

Challenge 8

It’s difficult to reliably track what applications are in my environment – and know what’s good or bad



Our study of employee endpoints reveals that it is not uncommon to find over 20,000 different applications across an enterprise[2], meaning malicious applications can easily hide in plain sight because IT teams simply don’t have the time to manually analyze everything. With that kind of scale, identifying which applications are good, bad or unknown is daunting – not to mention incredibly cost prohibitive. Making matters worse, for every obvious business application and obvious malicious application, there are dozens more that are not-so-obvious, and administrators simply do not have the time to handle the categorization process. This has resulted in traditional whitelisting technologies, included in many endpoint protection products, becoming obsolete.

Recommendations for Developing Layered Security Controls and Strengthening Endpoint Security

To address the challenges described thus far, organizations should look for flexible tools that automate the management of local administrator privileges and control of applications on endpoints and servers. This unique combination of least privilege and application control should be part of a balanced and layered security approach that helps organizations reduce the attack surface, protect against threats that have made their way inside, and alert security teams to potential in-process attacks – all without halting user productivity or overwhelming IT security teams.

To achieve this balance of security and usability, organizations should consider adopting an integrated privilege management and application control solution that includes the ability to:

1. Automatically create privilege and application control policies based on trusts.

Automatically determine what applications are trusted by the organization, identify what privileges are required by each of these applications, and create policies based on these trusts to save valuable IT time and effort.

2. Seamlessly elevate business user privileges as needed.

Remove local administrator rights from business users, but enable seamless privilege elevation, based on policy, to keep users productive without increasing the attack surface.

Recommendations for Developing Layered Security Controls and Strengthening Endpoint Security (Continued)

3. Enforce granular least privilege policies for Windows administrators.

Granularly control which commands and tasks each IT administrator is permitted to execute based on role, to effectively segregate duties and reduce the risk of insider and advanced threats.

4. Control what applications are allowed to run in the IT environment.

Enable trusted applications to seamlessly run in the environment while automatically blocking malicious applications and restricting privileges for unknown applications. Optionally enforce strict whitelist policies where needed.

5. Prevent attacker lateral movement and privilege elevation

Automatically detect and block attempts to steal credentials that would enable attackers to elevate privileges as they move through the network looking for sensitive information.

Conclusion

Today's modern business environment isn't black and white – and security tools shouldn't be either. Organizations must learn to strike a balance between security and usability to effectively reduce the attack surface while keeping users productive and minimizing the burden on IT teams.

There is now a comprehensive solution to do just that.

The CyberArk Endpoint Privilege Manager is part of the CyberArk Privileged Account Security Solution, a complete solution designed to proactively protect against advanced attacks that exploit administrative privileges to gain access to the heart of the enterprise, steal sensitive data and damage critical systems. The solution helps organizations reduce the attack surface by eliminating unnecessary local administrator privileges, preventing the progression of malware-based attacks and strengthening the security of privileged accounts. The CyberArk Privileged Account Security Solution proactively protects, isolates, controls and continuously monitors privileged accounts on endpoints, servers, physical and virtual machines, databases, applications, hypervisors, network devices, security appliances and more. Products in the solution can be managed independently, or combined for a cohesive and comprehensive privileged account security solution.

To learn more, please visit www.cyberark.com/endpoint-privilege-manager

CYBERARK®

Sources

[1] Verizon. "2015 Data Breach Investigations Report." Page 13.

[2] Viewfinity. "IT Security's 50 Shades of Grey Whitepaper." Page 2.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTALDAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Doc ID 129

CYBERARK®