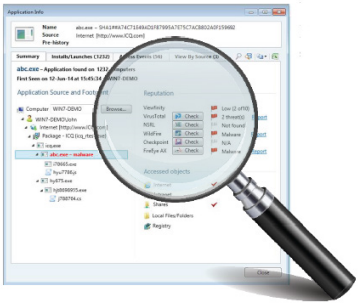
Viewfinity

Effectively minimize local administrator privileges and control applications on endpoints and servers.



View all privilege policies, applications and application reputations in a single location.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

Accounts with local administrator rights represent a large and frequently exploited attack surface, but entirely removing administrative rights from business users can result in unintended consequences. As privileges are taken away, organizations are able to reduce the attack surface, but this security benefit can come with a major productivity tradeoff if business users no longer have the rights needed to carry out day-to-day tasks. Similarly, privilege policies for IT administrators are typically treated as an all-or-nothing decision. As a result, IT administrators often maintain unnecessary, full administrative rights on servers, which can leave sensitive servers at an increased risk of compromise. Making matters worse, despite an organization's best efforts to reduce the attack surface by minimizing privileges, machines can still be vulnerable to malware that does not require privileges to execute.

To effectively reduce the attack surface and mitigate the risk of a serious data breach without impacting productivity, organizations should implement tools that enforce flexible least privilege policies for business and administrative users, as well as control what applications are allowed to run. Without such tools in place, organizations will face the following challenges:

- **Lost business productivity.** When organizations eliminate all privileges from business users, users may no longer be able to carry out certain tasks or use certain applications needed for their day-to-day roles. As a result, inflexible privilege policies can bring the business to a halt.
- **High help desk costs.** 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.
- **Increased security risks due to 'privilege creep.'** When organizations remove all privileges from business users, the IT team will occasionally need to re-grant privileges for specific tasks. However, once privileges are re-granted, they are rarely revoked. This 'privilege creep' reopens the security loophole associated with excessive administrative rights and makes the organization more vulnerable to threats.
- **Increased risk of insider and advanced threats.** When organizations treat IT administrator privileges as an all-or-nothing decision, these administrators often end up with far more privileges than needed. Without role-based privilege policies in place, sensitive systems can easily be exploited or damaged by inexperienced users, malicious insiders or advanced attackers who have gained unauthorized account access.
- **Increased risk of successful malware-based attacks.** Organizations that minimize user privileges on Windows devices can still be vulnerable to malware that does not need privileges to run. Without complementary tools in place to control which applications are permitted to run, attackers can successfully use malware-based attacks to gain a foothold into the organization.

The Solution

CyberArk Viewfinity enables organizations to enforce least privilege policies for business and administrative users, as well as control applications to reduce the attack surface without halting productivity. The solution helps organizations revoke everyday local administrator privileges from business users while seamlessly elevating privileges when required by trusted applications. CyberArk Viewfinity also enables security teams to enforce granular least privilege policies for IT administrators, helping organizations effectively segregate duties on Windows servers. Complementing these privilege controls, the solution also delivers application controls, which are designed to manage and control which applications are permitted to run on endpoints and servers and prevent malicious applications from penetrating the environment. With CyberArk Viewfinity, organizations are able to:

- **Automatically create policies based on business requirements.** CyberArk Viewfinity automatically creates application control and privilege elevation policies based on Trusted Sources such as SCCM, software distributors, updaters and more.
- **Seamlessly elevate business user privileges as needed.** Once local administrator rights are removed from business users, CyberArk Viewfinity seamlessly elevates privileges, based on policy, as required by trusted applications.
- **Quickly identify and block malicious applications.** Automatically compare unknown applications to commercially available blacklist databases, such as VirusTotal and NSRL, to quickly identify known malware and update global policies to prevent these applications from running in the environment.
- **Enable unknown applications to safely run in a restricted mode.** Unknown applications, which are neither trusted nor known to be malicious, are able to run in 'Restricted Mode.' In this state, business users may run unknown applications, but the applications are prevented from accessing corporates resources, sensitive data or the internet.
- **Leverage integrations with threat detection tools to analyze unknown applications.** CyberArk Viewfinity can send unknown applications to Check Point, FireEye and Palo Alto Networks threat detection solutions for automated file analysis. These solutions return file reputation ratings, which IT teams can then use to decide to block or permit applications in the environment.
- **Identify all instances of malware in the environment.** Using a kernel-based agent on each protected machine, the solution can immediately locate all instances of a malicious application within the environment, as well as the origin of each malicious application.

Benefits

CyberArk Viewfinity enables organizations to reduce the attack surface while keeping users productive. The solution enables organizations to:

- **Accelerate time-to-value.** Minimize time-consuming, manual IT effort by using 'Trusted Sources' to automate the creation of privilege policies for over 90 percent of applications within the organization.
- **Keep business users productive without compromising security.** Enable business users with no local administrator privileges to safely run unknown applications as needed to stay productive.
- **Reduce the risk of insider and advanced threats.** Prevent accidental and intentional damage to critical Windows Servers by segregating duties and granularly controlling administrative privileges based on role.
- **Mitigate the risk of malware-based attacks.** Proactively prevent attackers from using malware to gain a foothold into the IT environment by controlling which applications are permitted to run and which resources each application is permitted to access.
- **Leverage existing investments to quickly and accurately detect threats.** Accelerate the analysis of unknown applications by using Check Point, FireEye and Palo Alto Networks solutions to analyze and detect potential threats.
- **Accelerate the remediation of threats.** Quickly understand the severity of threats and accelerate remediation efforts by gaining clear insight into the scope and origin of malicious applications within the IT environment.

A Comprehensive Solution

CyberArk Viewfinity 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 and strengthening the security of privileged accounts. The CyberArk Privileged Account Security Solution proactively protects, isolates, controls and continuously monitors privileged accounts on 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.

Specifications

Supported Platforms:

Windows Desktop:

- Windows XP SP3
- Windows Vista SP1
- Windows 7 32-bit & 64-bit
- Windows 8 32-bit & 64-bit
- Windows 8.1 32-bit & 64-bit
- Windows 10

Windows Server:

- Windows Server 2003 SP2 32-bit & 64-bit
- Windows Server 2008 32-bit & 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2012
- Windows Server 2012 R2

Comprehensive Application Support:

- Executable
- MSI, MSU
- Administrative Tasks
- Management console snap-ins
- Scripts
- Registry settings
- ActiveX controls
- COM objects
- Web Applications

Flexible and Secure Application Rules:

- File path matching
- Command line matching
- File hashing (SHA-1)
- Product and file information
- Trusted publisher
- Trusted Source SCCM
- Trusted Software Distribution system
- Trusted Updater
- Trusted Network
- Trusted Computer image
- Trusted AD group
- Trusted product

Deployment Options:

- Microsoft Group Policy (GPO)
- On-premises server
- Software-as-a-Service

©CyberArk Software Ltd.| cyberark.com