



CYBERARK®

Stop them before they stop Your business

Securing privilege on the endpoint



The endpoint problem is a privilege problem



Follow security best practices



Put the fundamental building blocks in place



Secure privilege on the endpoint



Harden and contain attacks on the endpoint

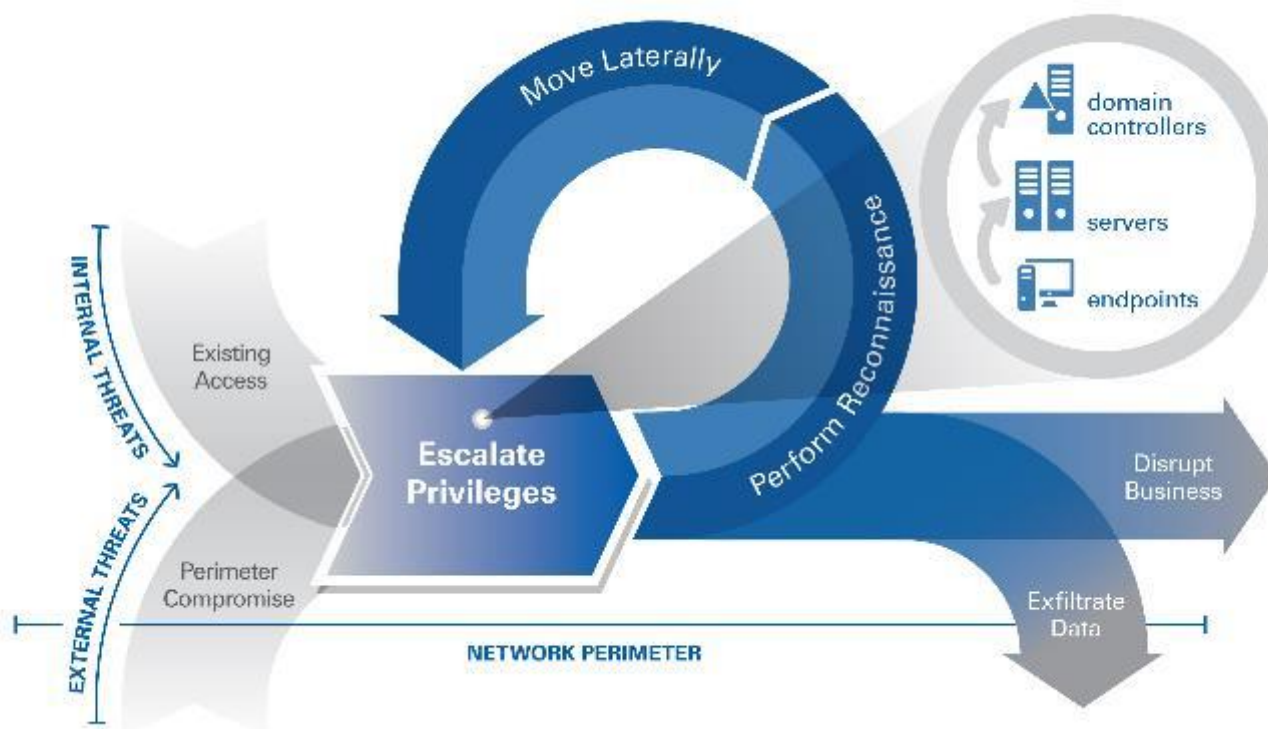


Minimize impact on users and IT support teams

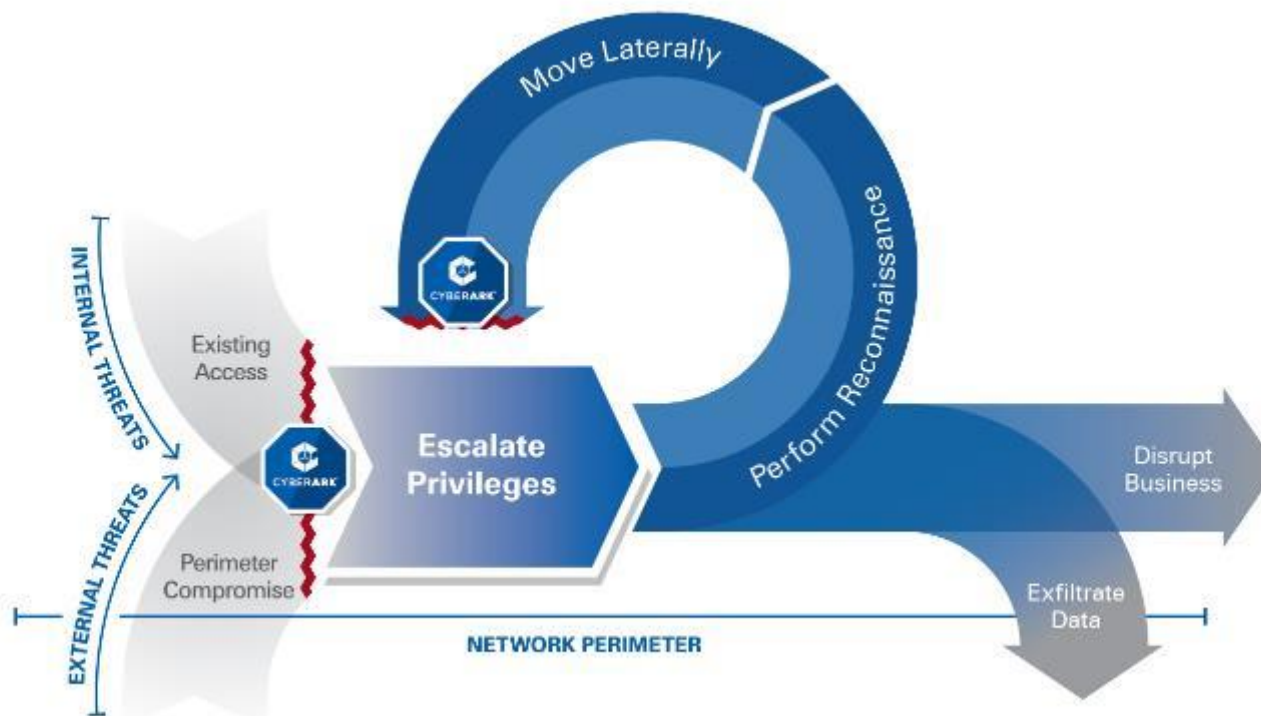


CYBERARK

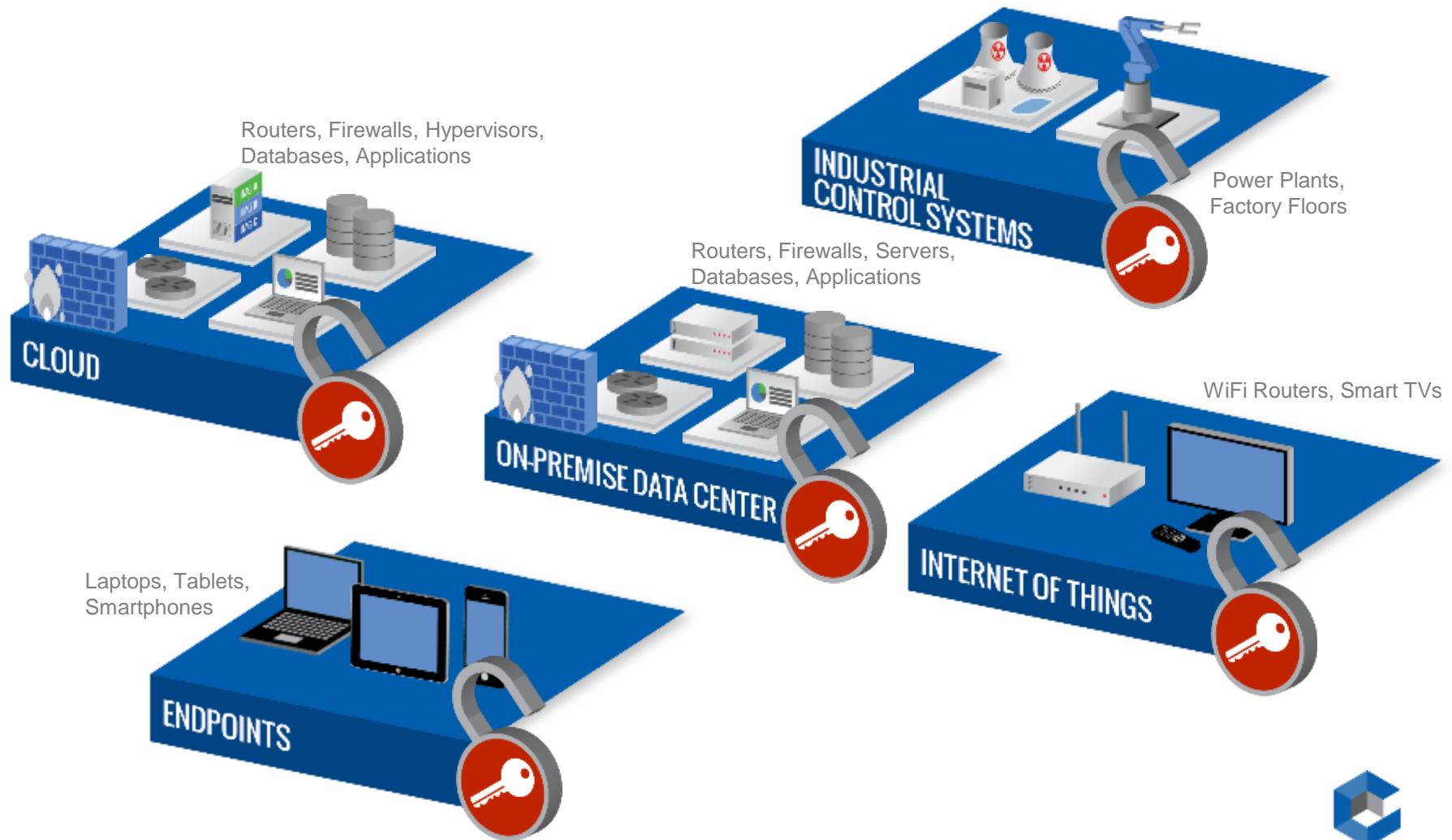
Privilege Escalation Enables Asset Escalation



CyberArk Breaks the Attack Chain



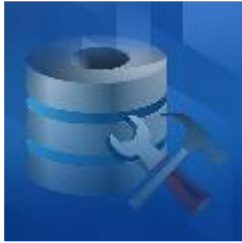
Local admin privileges create a huge attack surface



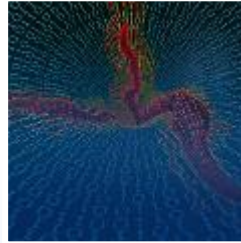
Local admin privileges create a huge attack surface



The Problem: users with admin rights can...



Change system
configurations



Install
malware



Access and change
accounts

“**62%** of organisations have not removed local admin rights”

Source: CyberArk Threat Landscape Survey, September 2016

Why not? Users without admin rights cannot...



Install device drivers like printers, display, network, etc.

Update and install conference and communication tools like GoToMeeting, Microsoft Lync

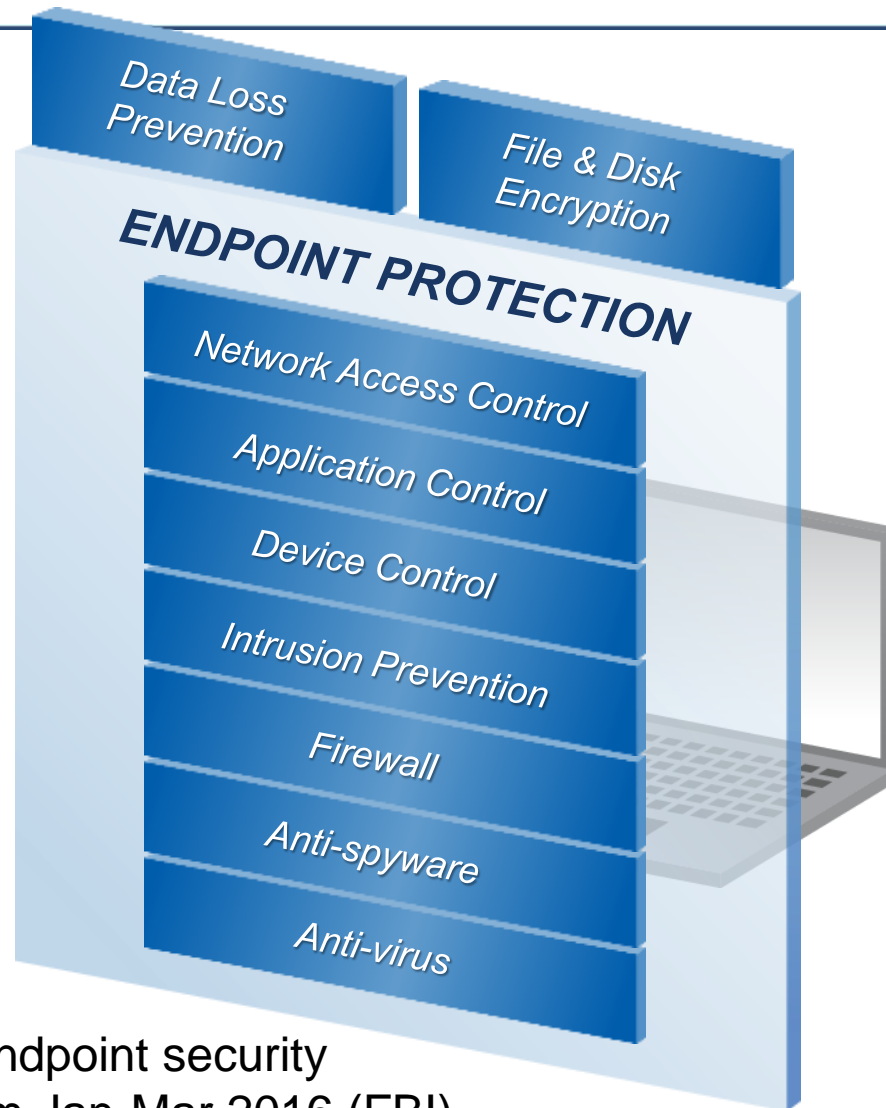
Run standard software updates including Adobe, JAVA, Apple, Citrix, etc.

Effectively use development tools such as Microsoft Visual Studio, eclipse, SQL Developer, TOAD, etc.

The dilemma – security V operational impact

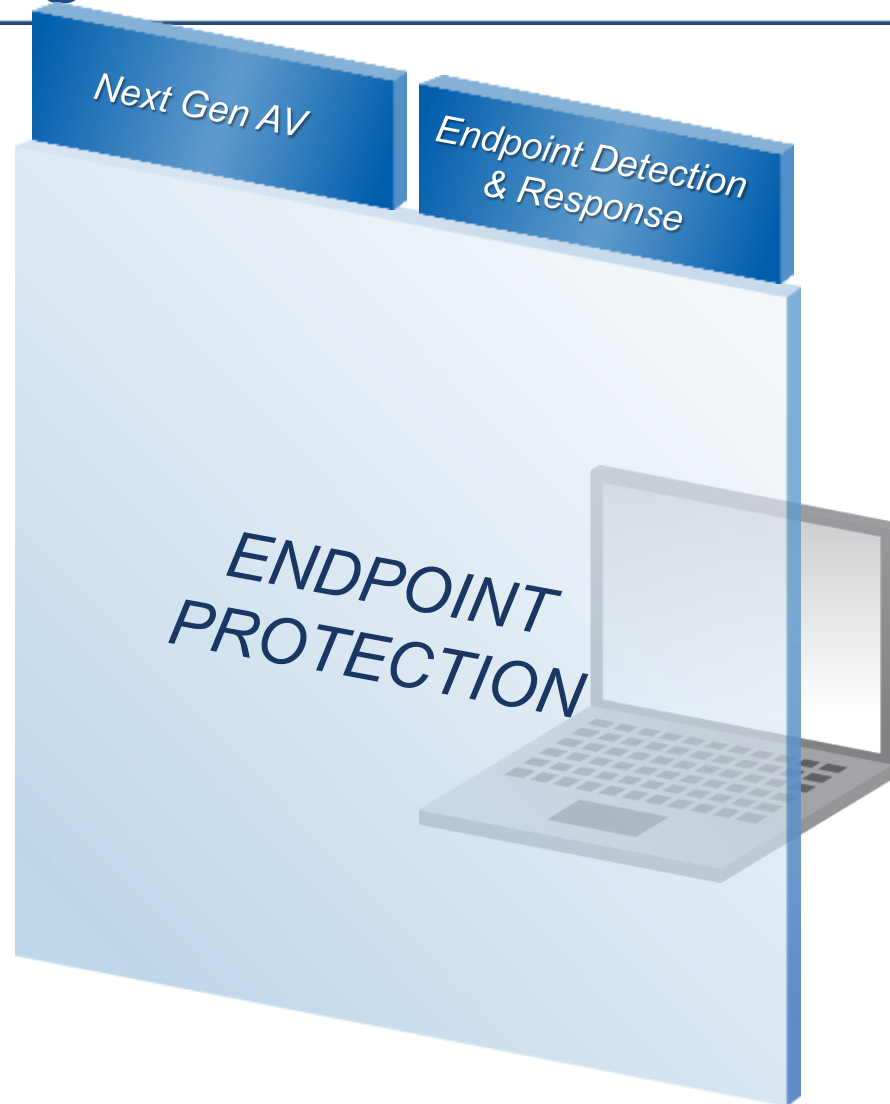
		Users have local admin rights	Local admin rights are removed
	Operations Impact	<i>Happy, productive users</i>	<i>Increased burden on the support team</i> <i>Increased calls and costs</i>
	Security Impact	<i>Increased security incidents</i>	<i>Contain attacks on the endpoint</i>

Multiple layers of endpoint security have failed

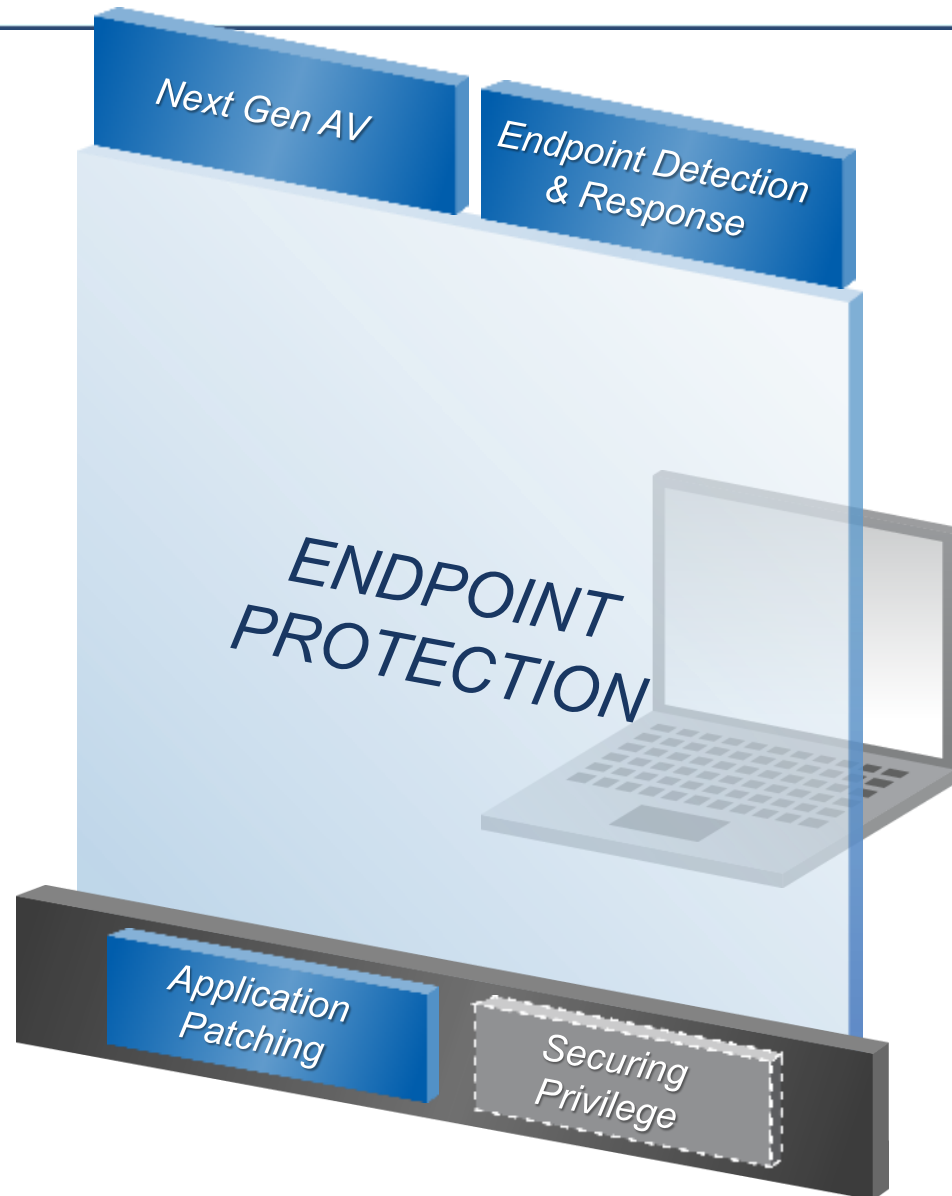


\$ Billions are spent on endpoint security
Ransomware cost \$209m Jan-Mar 2016 (FBI)

Add yet another preventative layer or try and limit the damage



A fundamental building block is missing



Gartner: The Real Value of a Non-Signature-Based Anti-Malware Solution to Your Organization

- *Key Challenges*
 - *“Endpoint hardening, including vulnerability, patch, **privilege and policy management, and application control**, is currently the **most effective form of malware defense**; however, most organizations are unwilling or unable to invest in the upfront effort required to reduce the attack surface.”*

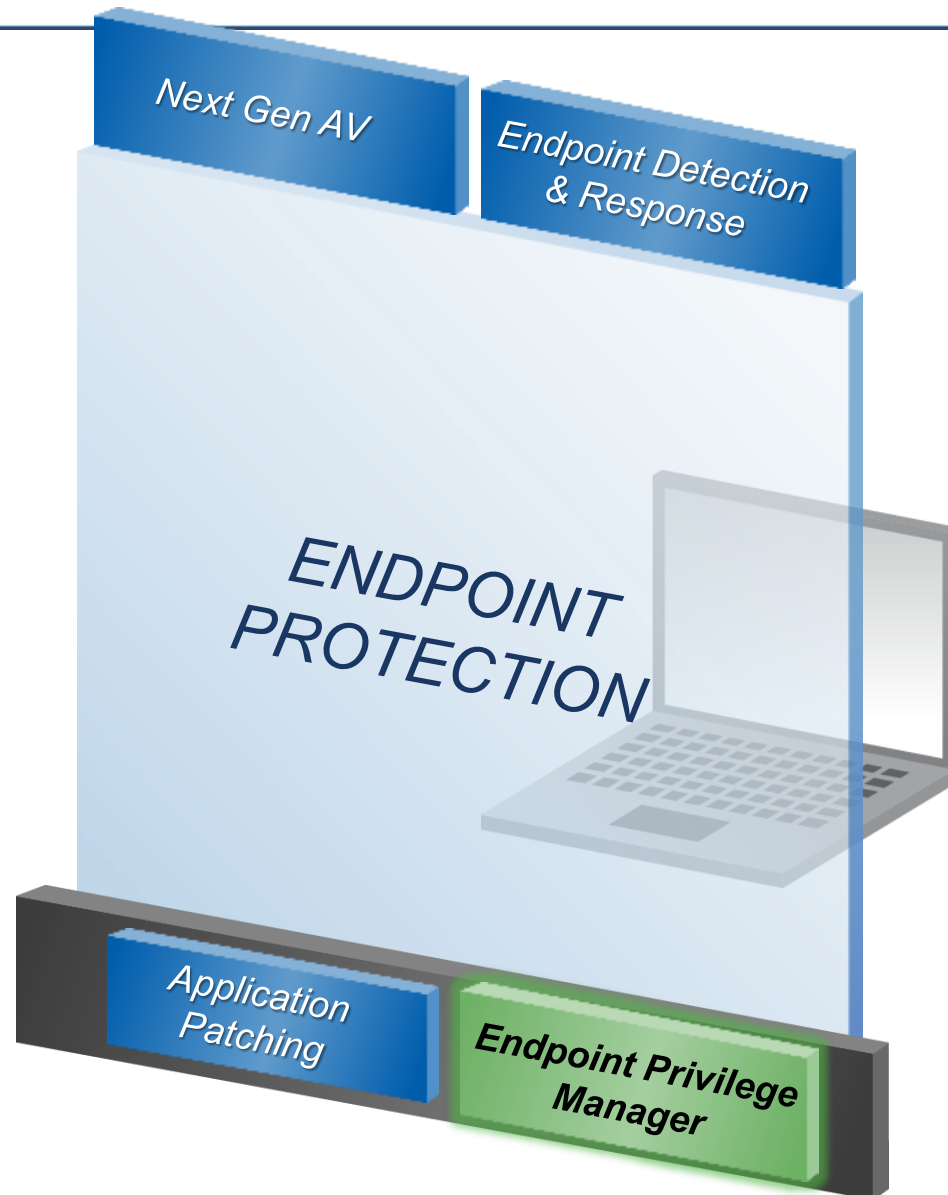
Gartner Research Note: The Real Value of a Non-Signature-Based Anti-Malware Solution to Your Organization

Published: 22 September 2016

Analyst(s): Eric Ouellet, Peter Firstbrook

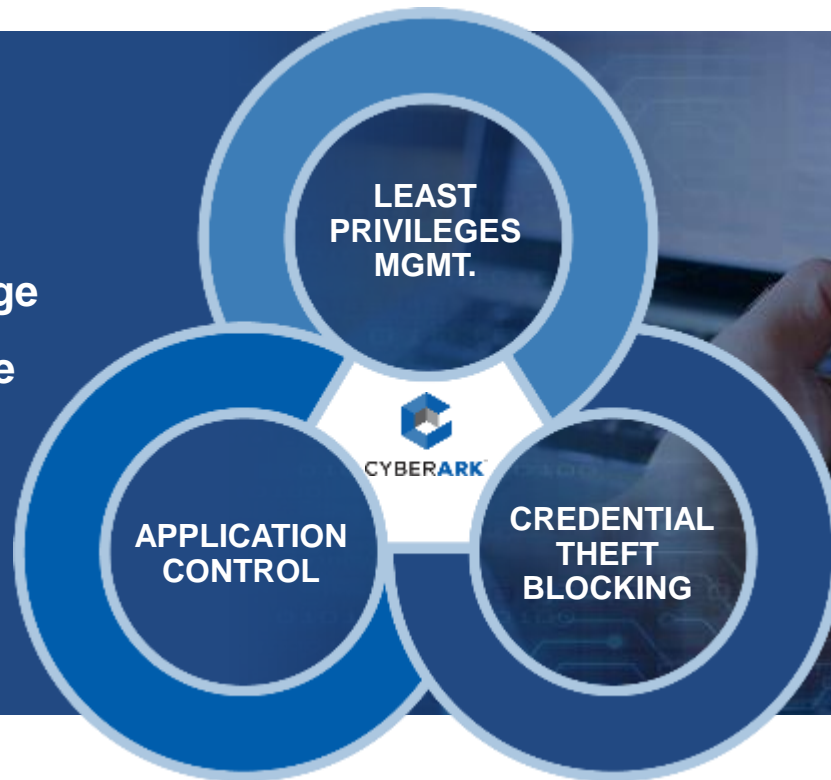
Doc ID: G00308947

Secure privilege on the endpoint



CyberArk Endpoint Privilege Manager

Enables privilege
security on the
endpoint



Enabling least privilege with application control

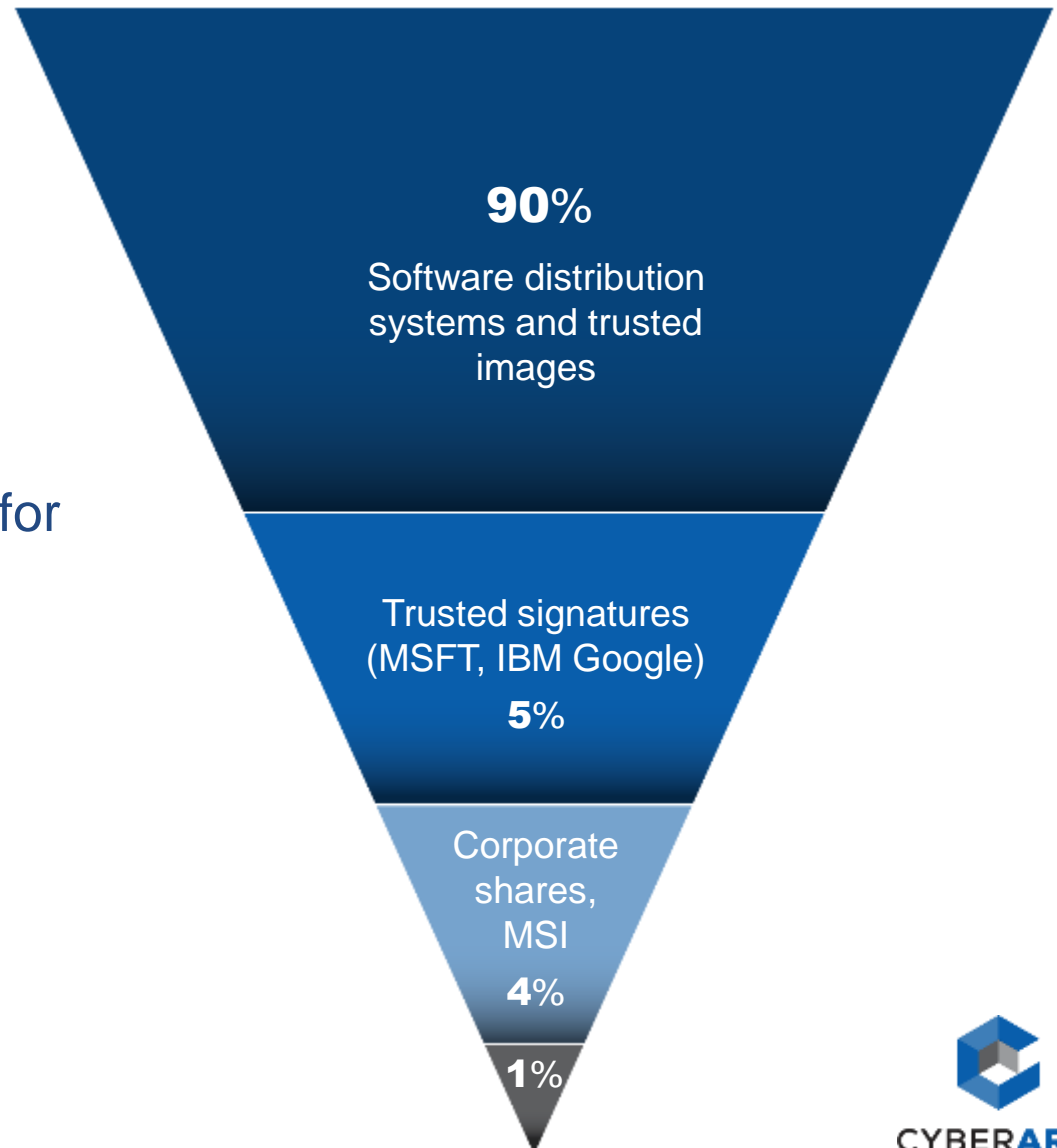
Least Privilege	Application Control
Remove and manage privileges	Only allow trusted applications
Gap: Malicious applications that don't need privileges can still get in	Gap: Applications that require privileges requires providing admin privileges to users



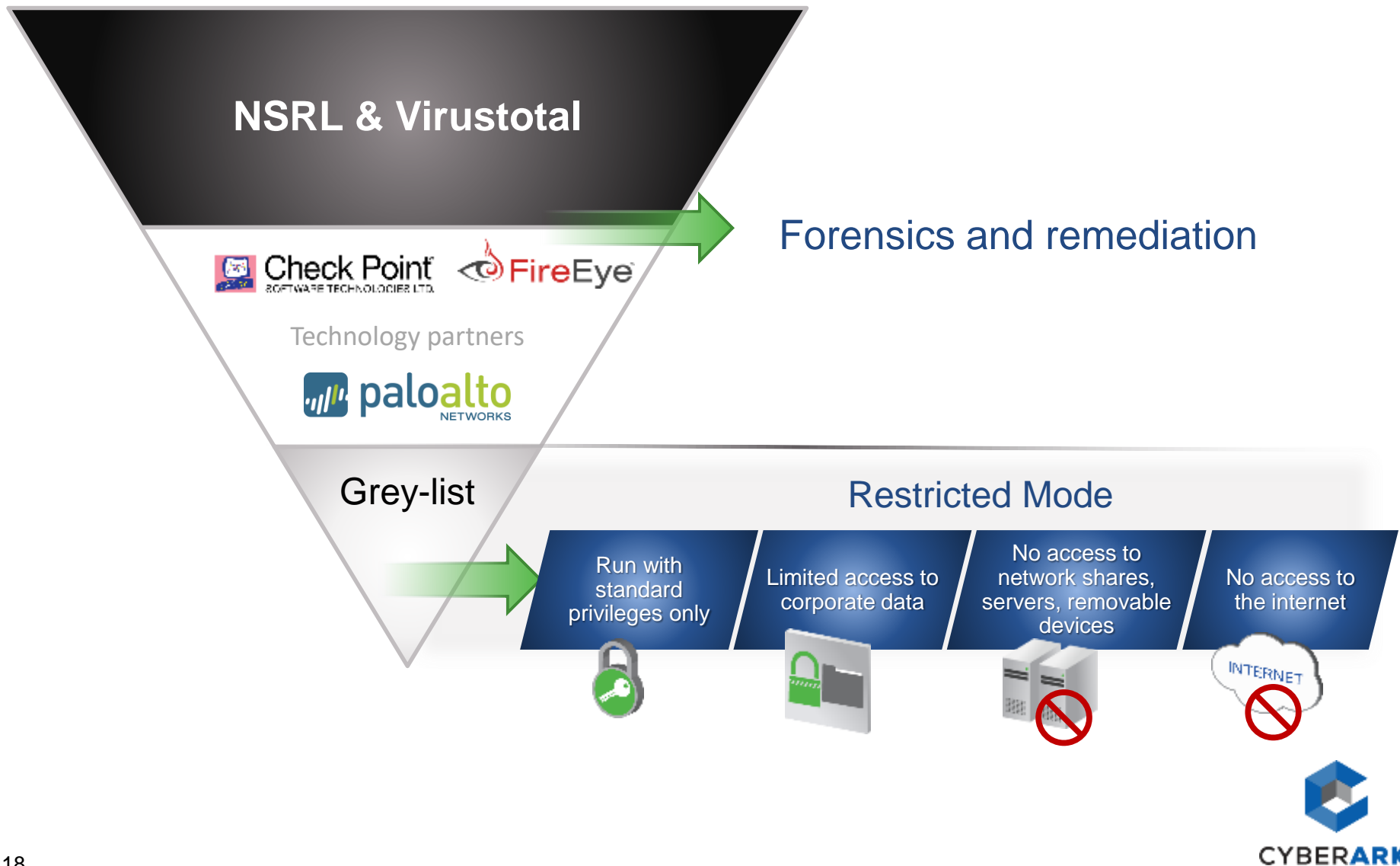
Combined, least privilege and application control enable organizations to contain malware and non-malware-based attacks

Trusted Sources removes the barriers to application control

Automates policy creation for **over 99%** of applications



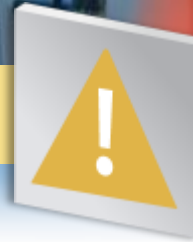
Greylisting removes the barriers to application control



Detect and block suspected credential theft

- The endpoint is the entry point for attacks
- Credentials are the main target of malware and non-malware-based attacks
- Contain the attack on the endpoint

Block



CYBERARK

Summary
Privilege Management Inbox
Application Control Inbox
Application Catalog
Policies
Threat Detection
Reports
My Computers
Threat Intelligence

Actions

Name	Action	Status	Computer	Last Modified Data
Browsers Stored Credentials Theft				
Internet Explorer Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58
Firefox Credentials Theft	Detect	Activated	All	02-Nov-16 05:45:47
Chrome Credentials Theft	Block	Activated	All	06-Nov-16 05:58:15
Remote Access Application Credentials Theft				
WinSCP Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58
VNC Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58

Secure Administrator Rights with CyberArk Endpoint Privilege Manager and Enterprise Password Vault

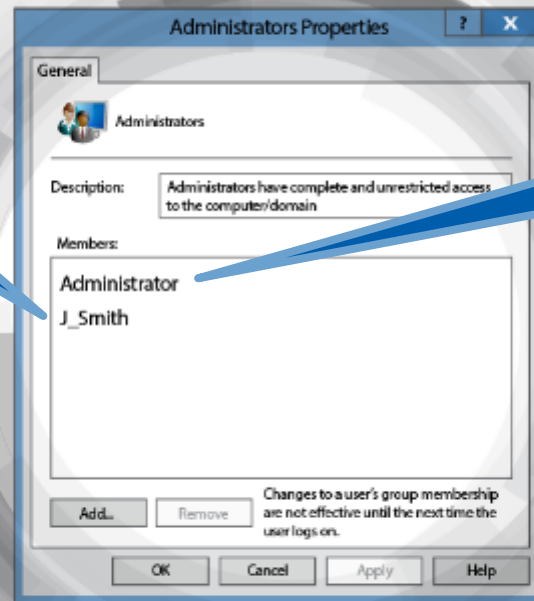
Enforce least privilege policies for business users and secure and control access to local administrator accounts

Remove local user accounts from Administrators group

Store local administrator accounts in the CyberArk Digital Vault

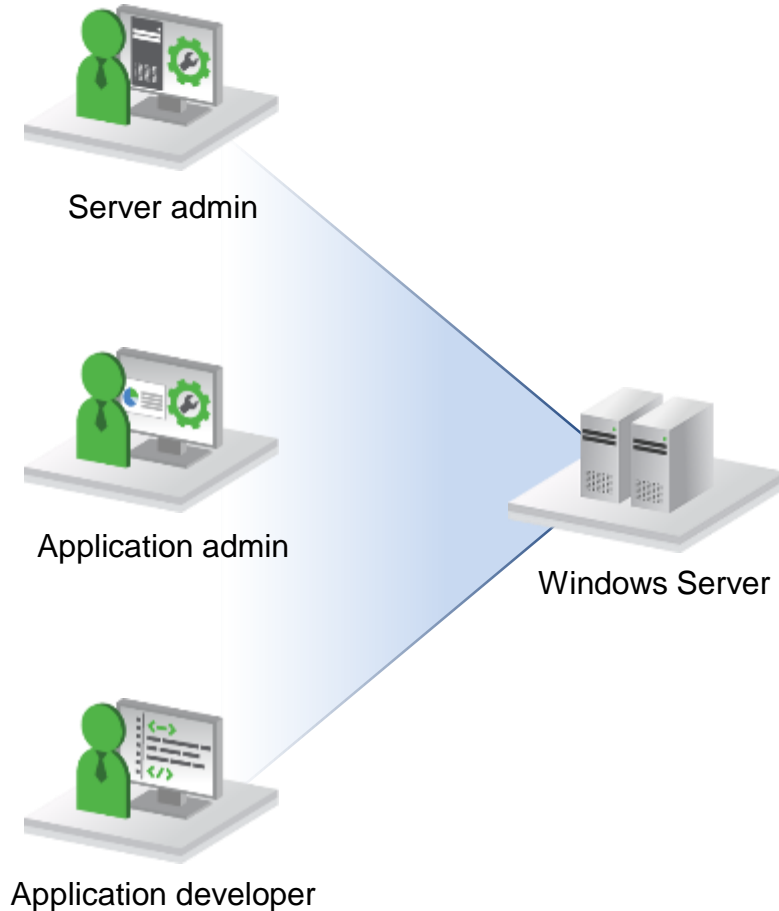
Use CyberArk Endpoint Privilege Manager to enable privilege elevation for authorized functions

Use CyberArk Enterprise Password Vault to rotate, manage and control access to local administrator accounts



CYBERARK

Control administrative privileges based on role

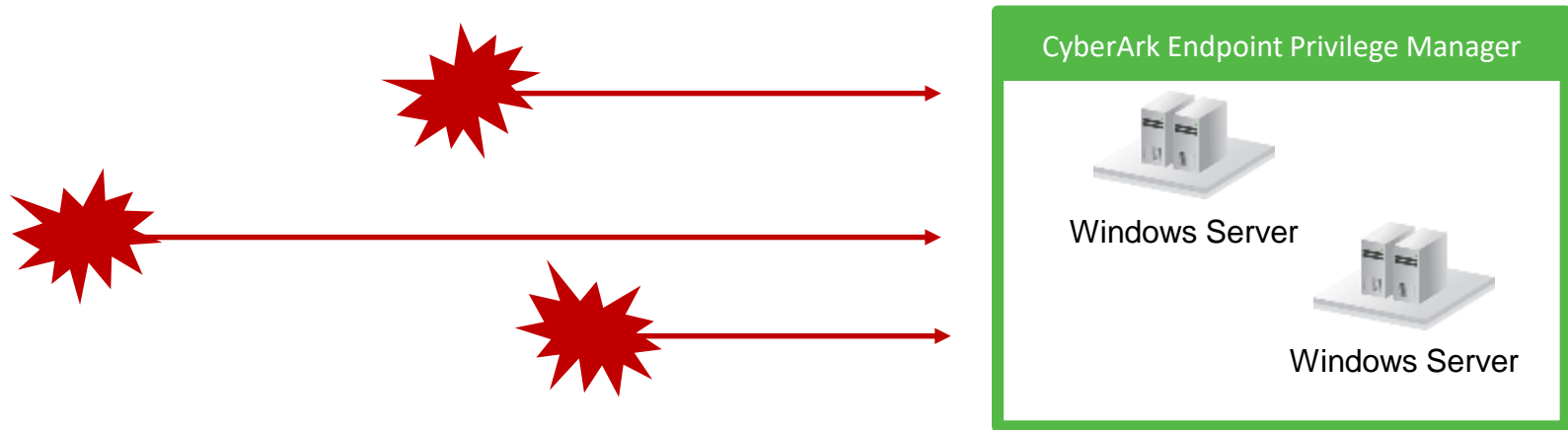


Control Windows administrator privileges based on role

- Use privilege management to segregate administrative duties
- Control the use of applications, scripts, commands and activities
- Enable privilege elevation when needed, based on policy

Control applications on Windows servers

Prevent malicious applications from executing on Windows servers



- Reduce the attack surface by centrally managing and enforcing application controls
 - Block malicious applications from reaching critical servers
 - Achieve default-deny mode for Tier 0 servers
- Continuously monitor the installation and execution of applications which are not yet classified
 - Enable unknown applications to securely run in restricted mode

IT Services Company Case Study

Challenge: As a services company with over 85% of end users having administrative rights to their machines, the company needed an automated way to enable users to be productive, but remove administrative rights to reduce the attack surface.

BEFORE CYBERARK

- Diverse IT environment running multiple Windows platforms
- Broad attack surface - majority of end users have administrative rights to their machines

REQUIRED CAPABILITIES:

- Removal of all administrative rights from business users on endpoints
- Ability to establish security policies without disruption and resistance from end users
- Ability to apply granular-level control to all policies, including the ability to define which applications are allowed to run
- Cost effective solution that provides flexibility in deployment options

“Our goal was to implement the new IT security policies with the least upset to and resistance from end users, and in the most cost effective way. We decided to go with CyberArk Endpoint Privilege Manager because we felt the pricing offered us the most functionality.”

- IT Director

After
CyberArk
Privileged
Account
Security:

- Reduced risk by removing administrative rights from business users
- Saved time and money by enabling the IT administrator to have control and visibility required to proactively tackle issues as they arise
- Enabled full audit and reporting capabilities to easily prove compliance



CYBERARK

Strengthen security while keeping users productive

BUSINESS
ISN'T
**BLACK
AND WHITE.**



SECURITY
TOOLS
SHOULDN'T BE
EITHER.

Invisibly elevate
privileges for trusted
applications

Allow users to run
“unknown” applications
in restricted mode



Enable all
applications to run
for power users – with
forensics and tracking
for follow-up

Productive, satisfied users.



CYBERARK®

Thank you