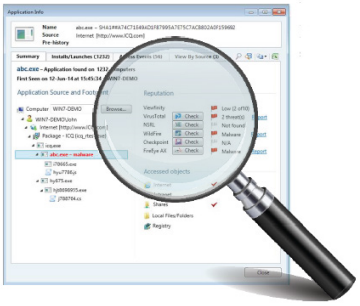
Endpoint Privilege Manager

Минимальные привилегии, контроль приложений и защита локальных учётных записей

Обеспечение безопасности привилегированных учётных записей на конечных устройствах без негативнных последствий после удаления прав локального администратора

ОПИСАНИЕ ПРОБЛЕМЫ

Когда атака обходит защиту периметра и конечной точки, остаётся полагаться только на технологии обнаружения, чтобы быстро отреагировать на инцидент и попытаться предотвратить дальнейшее распространение. Атакующие крадут учётные данные, повышают привилегии и начинают передвигаться по сети в поисках ценой информации. Обеспечение безопасности привилегий на конечной точке с целью уменьшения зоны поражения при атаке, является основной задачей любой системы безопасности. Однако недостатком является потенциальное влияние на производительность работы пользователей, возрастающая нагрузка на сеть и увеличение расходов на персонал по поддержке работы настольных компьютеров.



Просмотр всех политик привилегий, приложений и репутации приложений в одном месте.

Для уменьшения площади распространения атаки и снижения риска повреждения данных без снижения производительности необходимо установить инструменты, которые будут обеспечивать защиту привилегий на конечных точках, блокировать и сдерживать распространение атак. Данные инструменты должны применять для бизнес-пользователей и администраторов гибкие политики с наименьшими привилегиями, контролировать, каким приложениям разрешён запуск, и гарантировать, что они смогут обнаружить и заблокировать атаки, нацеленные на данные учётных записей. Без таких средств защиты организации будут сталкиваться со следующими проблемами:

- Потеря производительности

  При удалении всех привилегий, предназначенных для бизнес-пользователей, те больше не смогут выполнять задачи и использовать приложения, необходимые для их повседневной работы. Отсутствие гибких политик управления привилегиями может привести к полной остановке бизнеса.

- Большие расходы на службу поддержки

  Когда ИТ-политики не позволяют бизнес-пользователям выполнять необходимые повседневные задачи, они обычно всегда обращаются в службу поддержки для восстановления необходимых разрешений. Это может значительно увеличить расходы на ИТ и привести к перегрузке в работе персонала службы поддержки.

- Повышенный риск из-за "расплывчатых привилегий"

  Когда в организациях удаляют для бизнес-пользователей все привилегии, ИТ-специалистам иногда приходится восстанавливать привилегии для определенных задач. Однако после выполнения задач данные привилегии редко отзываются, представляя собой потенциальную уязвимость в системе безопасности, связанную с чрезмерными правами администратора.

- Повышенный риск успешных атак

  В организациях, которые минимизируют пользовательские привилегии на устройствах Windows, тем не менее, всё ещё остаются уязвимости для тех вредоносных программ, которые не требуются привилегий для распространения атак. Без дополнительных инструментов для контроля запуска приложений и защиты данных учётных записей, которые являются основной целью злоумышленников, вероятность проникновения и распространения атак внутри организации при помощи вредоносных программ будет оставаться высокой.

РЕШЕНИЕ

Endpoint Privilege Manager помогает устранить препятствия для обеспечения минимальных привилегий, позволяя организациям блокировать атаки в конечной точке, снижать риск кражи или шифрования информации с целью получения выкупа. Комбинация этих двух опций - защиты привилегий и управления приложениями - снижает риск заражения вредоносными программами. Для сдерживания угроз неизвестные приложения всегда запускаются в безопасном, ограниченном режиме, а поведенческий анализ блокирует попытки кражи учётных данных. Эти критические технологии защиты развертываются для укрепления существующей безопасности конечных точек как единый агент. Endpoint Privilege Manager также позволяет специалистам по информационной безопасности применять для ИТ-администраторов гранулярные политики минимальных привилегий, помогая тем самым эффективно распределять нагрузку на серверах Windows. Помимо управления привилегиями данный продукт обеспечивает управление приложениями, контролируя, какие приложения разрешено запускать на конечных точках и серверах.

Endpoint Privilege Manager обеспечивает возможность:

- **Автоматически создавать политики на основе бизнес-требований**

  Политики контроля приложений и привилегий на основе надежных источников, таких как SCCM, дистрибьюторы ПО, обновления и многое другое.

- **Использовать гранулярные политики привилегий для Windows-администраторов**

  Администраторы Windows. Специалисты по ИБ полностью контролируют, какие команды и задачи может выполнять каждый ИТ-администратор на серверах Windows на основе назнаенноей ему роли.

- **Применять управление приложениями на серверах Windows с целью уменьшения зоны распространения атаки.**

  Централизованное управление и контроль над элементами управления приложениями, создание режима отказа по умолчанию для серверов 0-го уровня и постоянный контроль за установкой и выполнением приложений, которые еще не классифицированы.

- **Постепенно, по мере необходимости повышать привилеги бизнес-пользователей**

  После удаления прав локального администратора у пользователей, Endpoint Privilege Manager повышает привилегии на основе политик безопасных приложений.

- u kljhuyeylvbehdbjhlvhikgu i jbehgby

  Автоматическое сравнение неизвестных приложений с коммерческими доступными базами, содержащими чёрые списки, такими как VirusTotal и NSRL, с целью быстрого определения известных вредоносных программ, обновления глобальных политик и предотвращения запуска этих приложений.

- Hg jmblvbehdbjhlvihiuldbdjb ggvosmzkuoaibkc

  Кража данных учётных записей является основной задачей любой атаки. Поведенческий анализ помогает организации обнаруживать и блокировать распространение атаки внутри инфраструктуры, а также не допускать повышение привилегий, вовремя блокируя любую попытку кражи учё из хранилищ учётных данных Windows, ИТ-приложений, приложений удалённого доступа, а также учётных данных, хранящихся в популярных веб-браузерах.

- Ai mkdlvgbaklguijbehgby ahi kg hfjbf

  Неизвестные приложения,не входящие в списки проверенных или опасных, могут работать в режиме ограниченной функциональности, что предотвращает их доступ к корпоративным ресурсам, конфиденциальным данным или Интернету.

- Bki hevahlvbgljpbxkbgkljmfglfb hgjmgbymjhaeygebagbaklguo i jbehgbc

  Endpoint Privilege Manager может отправлять неизвестные приложения в Check Point, FireEye and Palo Alto Networks threat detection solutions for automated file analysis.

- **Identify all applications in the environment.** Using an agent on each protected machine, the solution can immediately locate all instances of an application within the environment, and the origin of each.

Benefits

- Provides an additional critical layer of protection when an attack evades traditional perimeter and endpoint security controls
- A unique combination of technologies, to protect against, block and contain attacks on the endpoint, reducing potential damage to the business
- Strengthen the protection and detection capabilities of your existing endpoint security
- Enables the desktop team to easily implement security policy, with minimal impact on the business
- Prevents users installing unsanctioned applications and causing workstation instability, resulting helpdesk calls and increased support costs
- Enables removal of local administrator rights without reduced user productivity and increased helpdesk calls
- Easy deployment with automated policy creation eases the burden on the desktop team
- ·Helps the desktop team to meet the requirements of the security / risk management team while reducing their workload
- Contains the spread of malware across the network, reducing remediation time and effort

A Comprehensive Solution

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 and strengthening the security of privileged accounts. . 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 7 32-bit & 64-bit
- Windows 8 32-bit & 64-bit
- Windows 8.1 32-bit & 64-bit
- Windows 10

Windows Server:

- 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:

- On-premises server
- Software-as-a-Service

Note: some functionality may not be available with all deployment options