Cyber-Ark®

Security That Empowers People™

Pim 7.0

Высокий уровень безопасности защищает «Ключи от Королевства», а также проверенный детальный аудит, соответствующий нормативным требованиям.

Встроенные передовые практики определения и применения единой политики управления привилегированными записями в IT -инфраструктуре, как облачной, так и устанавливаемой локально у заказчиков.

Улучшение производительности труда с помощью одной точки доступа для обработки привилегированных записей.

Privileged Identity Management Suite - это решение корпоративного класса на основе единой базы политик, которое предоставляет возможности по обеспечению безопасности, управления, контроля и мониторинга всех действий, связанных со всеми типами привилегированных учётных записей.

ВЫЗОВ

В современном мире большинство организаций тратит существенную часть ресурсов на построение инфраструктуры защиты ценной корпоративной информации, обеспечение непрерывности своей работы и соответствия требованиям регуляторов. Типовая IT- инфраструктура организации включает в себя сотни и даже тысячи серверов, баз данных, активных сетевых устройств, контролируемых и управляемых с использованием разнообразных привилегированных и совместно используемых учётных записей, таких как Root в UNIX/Linux, Администратор/Administrator в Windows, CiscoEnable, Oraclesystem/sys, MSSQLSA и многих других. Каким бы смешным это не показалось, этими идентификаторами часто пренебрегают, никогда не меняя установленные пароли и не отслеживая сессии доступа.

Использование этих учётных записей распространено не только среди IT-сотрудников, но и среди сторонних организаций, что требует повышенного внимания к учетным записям, например, использования безопасного удаленного доступа, а также защищенную инициализацию сессии доступа, при которой учетные данные надежно защищены.

В виртуальной среде привилегированные учетные записи разрешают доступ к системе нескольким гостевым машинам, ставя таким образом организацию под удар.

Нерациональное использование «Ключей от Королевства» налагает определенные риски на организацию, вне зависимости от того, находится ли ваш data-центр в помещении, на хостинге или облаке:

- **Угрозы, связанные с действиями внутренних злоумышленников (инсайдеров)**

  Одна из актуальнейших проблем сегодняшнего дня – риски, связанные с внутренними злоумышленниками. Во многих организациях один и тот же пароль идентификатора Administrator (root) используется для доступа ко всем системам, позволяя недовольному инсайдеру «неожиданно» и единовременно обрушить большинство жизненно важных систем и украсть ритически важную информацию. В настоящее время, кроме инсайдеров, особую угрозу также представляют внешние злоумышленники, которые все чаще и чаще проникают в организацию и и наносят вред используя привилегированные учетные записи. Эти атаки становятся все более изощренными и целенаправленны-

Факты &цифры:

Cyber-Ark обслуживает 8 из 10 крупнейших банков мира

Каждая третья компания из Fortune 50 выбрала Cyber-Ark

Privileged Identity Management Suite представляет единую центральную консоль для управления, регистрации и просмотра всех форм привилегированных записей, которые осуществляют доступ к наиболее чувствительным системам в IT-инфраструктуре вашей организации, а также привилегированных команд, которые к ним относятся.

ми, что означает необходимость в изначальном превентивном подходе.

- **Утрата чувствительной информации**
  Привилегированные учётные записи обычно имеют неограниченный доступ к IT-системам организации. Компрометация таких идентификаторов может повлечь неконтролируемый доступ к данным в обход существующей системной логики, например, прямые манипуляции с таблицами счетов, выражающиеся в финансовом и репутационном ущербе для организации.

- **Накладные расходы на управление**
  При наличии сотен - тысяч устройств и систем, ручное управление их привилегированными учётными записями, включая регулярную смену паролей и полноценную отчётность, становится чрезвычайно ресурсоёмким процессом и часто приводит к ошибкам. Более того, недоступность какого-либо пароля при необходимости восстановления системы может стоить часов и суток её недоступности конечным пользователям.

- **Аудит и отчетность**
  Соглашения(например, Sarbanes Oxley, PCIи BaselII) требуют от организаций отчетности о пользователях общих записей, о том, кем, когда и какие действия были произведены, защищены и обновлены ли пароли в соответствии с политикой безопасности.

РЕШЕНИЕ

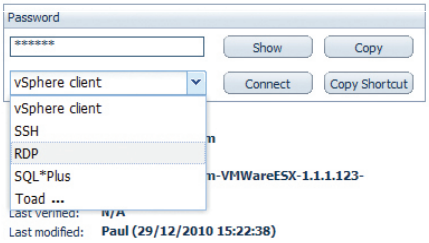
Продукт **Cyber-Ark Privileged Identity Manager Suite (PIM)** пакет управления привилегированными учётными записями, - это решение корпоративного класса на основе единой базы политик, которое предоставляет возможности по обеспечению безопасности, управления, контроля и мониторинга всех действий, связанных со всеми типами привилегированных учётных записей, а также действий, связанных с управлением data-центров, развертываемых как локально у заказчиков, так и на облаках.

PIM защищает критически важные бизнес-системы от анонимного доступа, осуществляя полный и безопасный аудит при одновременной автоматизации всех процессов, связанных с управлением прав доступа. Кроме того, PIM легко интегрируется с целым рядом систем и средств в вашей организации для более целостной отчетности и эффективности.

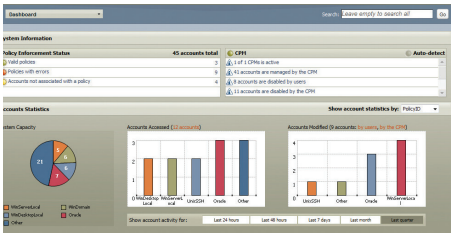
Privileged Session Management Suite - Управление Привилегированным Сессиями которое контролирует, производит мониторинг и позволяет прекращение любого доступа с использованием привилегированных учетных записей к серверам, базам данных и виртуальным средам. Обеспечивая непрерывную защиту, управление рисками и соответствие со всеми чувствительными системами, риск того, что привилегированные учетные записи могут помешать вашему бизнесу сведены к минимуму.

Пакет Cyber-Ark PIM Suite включает следующие продукты:

Enterprise Password Vault® - Корпоративное хранилище паролей (EPV). EPV позволяет организациям защищать, управлять, автоматически менять пароли и сохранять лог



Прозрачное подключение к целевым устройствам, не подвергая опасности привилегированные учетные данные



Панель PIM дает обширный обзор всех привилегированных учетных записей и их деятельности

всех действий со всеми типами привилегированных учётных записей. EPV олицетворяет передовую технологическую реализацию, развитые интеграционные возможности, масштабируемость и надежность для управления сотнями тысяч серверов, баз данных, сетевых устройств, приложений, виртуальных машин и т.д.

Application Identity Manager™ – Управление учётными записями приложений (AIM). AIM представляет собой уникальное решение для управления встроенными в приложения учётными записями и ключами шифрования. Это решение исключает необходимость хранения реквизитов в приложениях, скриптах и файлах конфигурации и позволяет хранить, управлять и проводить аудит действий с этими крайне «чувствительными» паролям с использованием запатентованной Cyber-Ark технологии Цифрового хранилища.Уникальное решение Cyber-Ark предлагает дополнительную пользу там, где только доверенные приложения имеют доступ к этим учетным записям, отсутствие простоев при замене учетных данных и защищенный локальный кэш гарантирует непрерывную доступность учетных данных, даже во время неработоспособности сети.

On-Demand Privileges Manager™ - первое единое решение для управления и мониторинга суперпользователей и привилегированные учетных записей. Использование учетных записей таких, как «root» на UNIX уже не является анонимным и теперь может контролироваться с помощью предопределенного детального контроля доступа, где регистрируются как сама команда, так и выходные данные. On-Demand Privileges Manager значительно повышает производительность и безопасность в среде Windows, путем внедрения на компьютерах и серверах «наименее привилегированной» политики. Все продукты имеют общую инфраструктуру для централизованного управления и легкого расширения.

Портал PIM - точка web-входа для доступа и управления привилегированными учетными записями во всех системах. Central Policy Manager - это революционный движок для управления привилегированными учетными записями, который автоматически управляет и реализует политику организации на локальных или удаленных сетях в рамках организации без вмешательства человека. Secure Digital Vault - уникальная запатентованная технология безопасного Цифрового хранилища(Digital Vault Technology™),защищает привилегированные учетные данные и информацию о политиках, хранит записи сессий и информацию, необходимую для проведения безопасного аудита.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

Превентивный подход против угроз

PIM управляет, защищает и контролирует доступ ко всем привилегированным учетным записям и устанавливает жестко заданные параметры доступа для приложения, скрытые от разработчиков,администраторов баз данных, третьих лиц и IT-персонала.

Обеспечить соответствия и аудит требованиям регуляторов

Пакет PIM предлагает корпоративную политику безопасности для соблюдения нормативных требований и создает простые в использовании, единые аудиторские отчеты согласно требованиям Sarbanes Oxley, PCI и многим другим.

Уменьшение IT-издержек посредством более эффективного контроля и меньшего количеством человеческих ошибок

PIM заменяет ручное администрирование надежным и непрерывным обслуживанием. Минимальные издержки администратора приводят к повышению производительности и минимальному риску ошибки человека.

Безопасность частного облака

Автоматизация управления привилегированными записями в частном облаке означает большую эффективность обнаружить, управлять и контролировать ESX гипервизоры и гостевые машины без ущерба для безопасности.

Быстрое и простое развертывание

PIM быстро развертывается и имеет проверенную репутацию в сфере улучшения IT-производительности. Наш опыт охватывает сотни корпоративных клиентов во всех вертикалях, обеспечивая немедленную окупаемость инвестиций.

Решение корпоративного класса

Благодаря ведущей в индустрии произво-

«PIM - это действительно восхитительное универсальное решение. Оно не только управляет, обеспечивает безопасность и проводит мониторинг наших привилегированных учетных записей, но и позволяет нам соответствовать требованиям, например, Sarbanes Oxley, что является для нас чрезвычайно полезным.»

Карон Дэвис, Global Security Privileged Access Manager, BT

дительности, масштабируемости и надежности, PIM может защитить и управлять сотнями тысяч привилегированных учетных записей в гетерогенных IT-средах, со сложными, распределенными сетевыми архитектурами. PIM может максимально использовать существующие инфраструктуры организации. С использованием продукта организация получает прозрачную интеграцию с имеющимися корпоративными системами.

СВОЙСТВА

От естественного управления паролями до совершенной безопасности Цифрового хранилища, все возможности, предоставляемые продуктом Privileged Identity Management Suite, основываются на взаимодополняющих свойствах системы:

Безопасность и аудит

- Высокая безопасность хранения на основе соответствующего FIPS 140-2 модуля защиты
- Централизованное управление процессом аудита как с помощью встроенной готовой аудиторской отчетности, так и с помощью запланированных отчетов, непосредственно отсылаемых в email-ящик аудитора
- Развитый и гибкий Web-портал для создания персонального доступа к привилегированным к учетным записям
- Надежное хранение такой информации, как аудиторская отчетность, сессии работы, политики и тому подобное

Управление совместно используемыми и административными учётными записями

- Автоматизация и управление гетерогенной IT-средой с более чем 70 типами сетевыми устройствами, включая большинство операционных систем, баз данных, брандмауэров и тому подобное
- Расширяемая архитектура управления устройствами, позволяющая легко добавлять новые типы устройств и систем по необходимости, в том числе уникальные плагины для управления учетными записями web-интерфейса, например, корпоративная учетная запись на Facebook, любое web-ERP / CRM приложение и т.д.
- Возможности самовосстановления целостности, такие как автоматическое согласование паролей
- Автоматическое обнаружение и выделение учетных записей гарантирует, что даже скрытые записи, запланированные задачи, пулы приложений, а также локальные группы администраторов и т.д. обнаружены и управляются в соответствии с политиками организации
- Прямой доступ к целевому устройству без раскрытия пароля конечному пользователю, а также стандартный интерфейс для прозрачного подключения к любому устройству

Привилегии по требованию

- Детальный контроль доступа для определения того, кто может запускать какие команды на индивидуальной основе
- Замена определенных SUDO решений на готовую к развертыванию беспрецедентную безопасность, централизованное легкое управление и усовершенствованные возможности аудита

Готовность к развертыванию в крупной организации

- Интеграция со всей инфраструктурой организации, включая LDAP и IAM продукты по управлению учётными данными пользователей, продуктами усиленной аутентификации (2-х факторной, RSA, Radius, PKI, LDAP и многими другими), системами управления событиями ИБ (SIEM) с использованием протокола SNMP, Syslog и SMTP, готовность к развертыванию в конфигурации высокой доступности (HA) и катастрофоустойчивости (DR)
- Полный комплект разработчика (SDK) для интеграции с заказными системами и устройствами
- Поддержка распределенной архитектуры с централизованным управлением, идеально подходящей для многосайтовых организаций с гетерогенной сетевой инфраструктурой

2010 Computing Security Awards WINNER

Cyber-Ark является победителем в номинации «Enterprise Security Solution of the Year» за его продукт Privileged Identity Management Suite, Security Awards 2010

«Пакет Cyber-Ark PIM является одним из передовых продуктов на развивающемся рынке PIM, предоставляя один из самых универсальных продуктов на рынке.»

Мартин Куппингер, Cyber-Ark Privileged Identity Management Suite (PIM) Product Report © Kuppinger Cole, IT Analysts 2010

Cyber-Ark®
Security That Empowers People™