



Управление привилегированным доступом для Hybrid Cloud

Xceedium Xsuite® является решением по безопасности корпоративной сети, которое контролирует доступ и регламентирует действия привилегированных пользователей в комплексе серверов, коммутаторов и корпоративных систем, а также ведет мониторинг и запись всех действий администраторов и суперпользователей. Xsuite является единой точкой контроля любого типа административного доступа к защищаемой информации в организации, где внедрен принцип «нулевого доверия» - администратор имеет доступ и права только к определенному политикой списку консолей и действий на них.

Xsuite — первое и единственное в настоящее время решение по управлению привилегированным доступом (privileged identity access management, PIAM), которое защищает и «гибридные облака» — включая физические дата-центры, виртуальные инфраструктуры и общедоступные облачные среды.

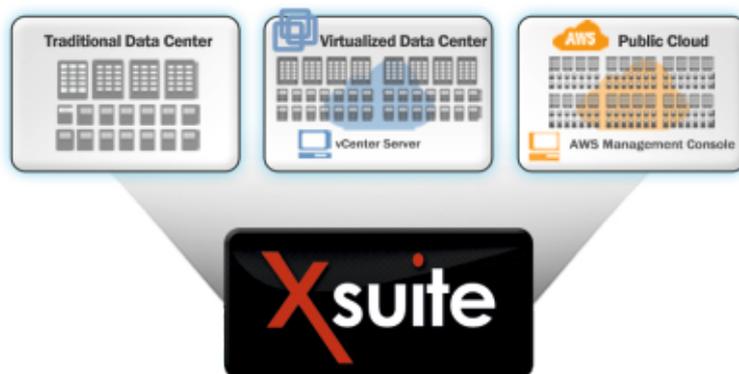
Управление | Мониторинг | Запись | Аудит

Управление учетными записями привилегированных пользователей и их правами доступа, в большинстве организаций является сложным, влекущим за собой существенные риски, процессом. Обычно крайне сложно идентифицировать, авторизовать и контролировать работу лиц, пользующихся совместно используемыми учетными записями; управлять доступом к критичным ресурсам; обеспечить соответствие государственным регулятивным нормам и требованиям по безопасности. Широкое распространение виртуализации и облачных сервисов существенно усложнили и без того непростые задачи.

Xsuite позволяет устанавливать и применять политики управления правами привилегированных пользователей во всем предприятии. Xsuite поддерживает доступ на сервера под управлением операционных систем Linux, Unix, и Windows; а также контролирует такие сетевые устройства, как маршрутизаторы; мэйнфреймы; виртуализированные системы; платформы облачных вычислений. Xsuite позволяет вам управлять паролями администраторов и суперпользователей, защищая конфиденциальные данные доступа; внедряет ролевою модель доступа; ведет протоколы активности; применяет превентивные политики безопасности — все это независимо от того, какие технологии применены в вашей инфраструктуре.

Xsuite предоставляет полную видимость по состоянию безопасности в организации, а также упрощает процесс соответствия различным законодательным требованиям.

Современная гибридная среда



Максимальная гибкость достигается за счет возможности Xsuite устанавливаться в среду как физический сервер, как виртуальная машина (OVF), или как облачный сервис Amazon Machine Instance (AMI).

Возможности Xsuite

Управление привилегированным доступом

Xsuite разделяет процесс аутентификации от процесса управления доступом. Таким образом, Xceedium разграничивает доступ, права и возможности администратора на каждом отдельном сервере на основе его ролевой модели, предотвращая leapfrogging, когда авторизация на одном сервере служит площадкой для авторизации и/или выполнения команд на другом сервере. Это унифицирует общие политики привилегированных пользователей для большого предприятия, и обеспечивает согласованный доступ к ресурсам по всем платформам. Администрирование, подготовка отчетов и аудит упрощаются с использованием централизованного управления.

Управление паролями администратора и суперпользователя

Xsuite защищает учетные записи и полномочия для всех типов ресурсов — серверов, баз данных, сетевого оборудования, и так далее — все они безопасно хранятся в зашифрованном виде. Xsuite также защищает учетные записи на Amazon Web Services (AWS). PEM-ключи безопасно хранятся и передаются напрямую из Xsuite к целевым ресурсам.

Xsuite также снижает риски того, что пароли будут встроены непосредственно в тексты скриптов и в коды приложений. Имеющийся API позволяет программно управлять полномочиями приложений и систем.

Мониторинг, реакция, и полная запись действий

Xsuite контролирует все действия привилегированных пользователей. Команды сопоставляются с действующими политиками перед их выполнением, что предотвращает неавторизованное или злонамеренное действие. События записываются для последующего анализа, генерируются сигналы, которые могут направляться ответственным лицам, или же сессии доступа могут автоматически прекращаться.

Xsuite непрерывно собирает, защищенный от возможности подделки, журнал действий администраторов, записывая сессии работы администраторов. Используя различные типы логгирования, супервайзер **Xceedium** может в точности определить и увидеть действия, выполненные с помощью RDP, VNC, и SSH сессии — в том числе и для вебприложений. Запись ведется также при совместном использовании администраторского аккаунта, так как **Xsuite** обеспечивает полную привязку действий и идентификацию конкретного лица их выполнившего.

Защита консоли Hybrid-Cloud

Развитие облачных вычислений и виртуализации расширяет поле для возможных атак и предлагает новые средства администрирования для защиты от них. **Xsuite** добавляет к этому ряд новых возможностей — ограничения на основе ролевой модели, средства единого входа (single sign-on), разделение выполняемых задач, отслеживание и аудит сессий, управление хранением паролей и ключей, и т.п. — как для AWS Management Console, так и для vCenter Server.

Поддержка многофакторной аутентификации

Xsuite обеспечивает точную аутентификацию привилегированных пользователей. **Xsuite** встраивается в существующую инфраструктуру управления пользователями и доступом через интеграцию в Active Directory, LDAP-совместимые системы, и RADIUS.

Xsuite поддерживает технологии с использованием сертификатов PKI/X.509 и токенов. Дополнительно **Xsuite** может использовать комплексную многофакторную аутентификацию для систем с высокими требованиями к безопасности, поддержкой смарткарт, токенов и аппаратных модулей безопасности.

Предотвращение Leapfrogging

Xsuite предоставляет доверенным пользователям список только тех систем, к которым они имеют права доступа. **Xsuite** также защищает от попыток извлечь информацию о сетевых ресурсах изнутри этой сети, блокируя попытки подключения к неавторизованным системам, путем поочередной установкой связи от одного разрешенного политикой сервера к другому.

Автоматическое сканирование и защита AWS и виртуальных ресурсов

Классический подход к определению и назначению политик безопасности не работает в современных системах типа hybrid cloud. Когда оператор может создать сотни новых систем простой командой, традиционные решения контроля привилегированных пользователей не работают. **Xsuite** преодолевает данные недостатки с помощью уникальной возможности автоматически определять виртуализированные и облачные ресурсы. **Xsuite** автоматически задает и применяет политики для этих динамических ресурсов. Инфраструктуре в целом ничего не угрожает, так как новые экземпляры добавляются и удаляются из портала доступа конкретного пользователя.

Xceedium обеспечивает управление правами и привилегиями доступа для инфраструктур hybrid cloud. Xceedium Xsuite снижает риски, связанные с работой привилегированных пользователей и незащищенными полномочиями доступа к системами и их данным. Xsuite обеспечивает единообразие политик, управления, мониторинга и аудита привилегированных пользователей как в традиционных дата-центрах, так и в инфраструктурах виртуализированных и общедоступных/частных облачных сред.



115114, г. Москва,
1-й Дербеневский пер., д. 5 стр. 1
Тел.: +7 (495) 66 239 66
Факс: +7 (495) 66 239 65
e-mail: info@netwell.ru
www.netwell.ru



www.xceedium.com