SILVERFORT

ОБЗОР РЕШЕНИЯ

СТРОГАЯ АУТЕНТИФИКАЦИЯ И ZERO TRUST БЕЗ АГЕНТОВ И ПРОКСИ

Инновационная архитектура без агентов и прокси позволяет платформе Silverfort обеспечивать аутентификацию и применение политик доступа на основе ИИ во всех корпоративных сетях и облачных средах, включая чувствительные системы, которые ранее считались незащищаемыми

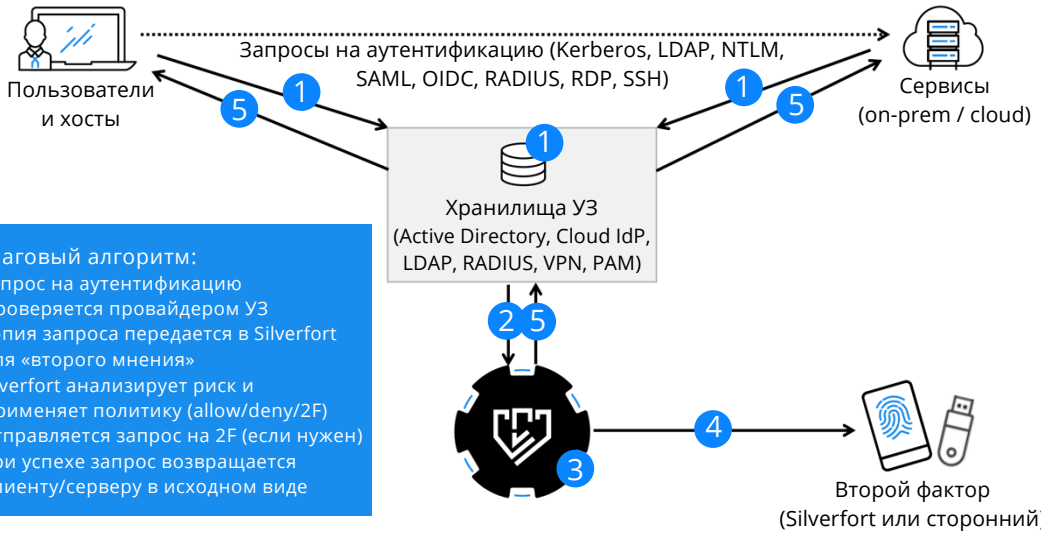
Прорывы в сфере ИТ за последние несколько лет, такие как облака, Интернет вещей (IoT) и Bring Your Own Device (BYOD), приводят к серьезным изменениям в корпоративных сетях. Новая реальность с бесчисленными устройствами и сервисами, тесно связанными между собой без каких-либо четких границ, делает критически важным подтверждение личности пользователей и контроль доступа к чувствительным ресурсам. Однако решать эти задачи сегодня гораздо сложнее, чем раньше.

Платформа аутентификации нового поколения Silverfort

Silverfort использует инновационную архитектуру и мощный механизм управления рисками на основе ИИ для отслеживания, анализа и обеспечения безопасности всех действий, связанных с аутентификацией и запросами доступа в системах компании.

Платформа не требует агентов, прокси или модификаций ПО и при этом обеспечивает многофакторную аутентификацию (МФА), аутентификацию с учетом уровня риска, применение политик Zero Trust и комплексный мониторинг для всех чувствительных систем, в том числе тех, которые ранее считались «незащищаемыми». Такие системы включают в себя приложения собственной разработки, ИТ-инфраструктуру, файловые ресурсы, устройства IoT, динамические среды IaaS, доступ при коммуникациях «машина-машина» и др.

Принцип работы



Пошаговый алгоритм:

1. Запрос на аутентификацию проверяется провайдером УЗ
2. Копия запроса передается в Silverfort для «второго мнения»
3. Silverfort анализирует риск и применяет политику (allow/deny/2F)
4. Отправляется запрос на 2F (если нужен)
5. При успехе запрос возвращается клиенту/серверу в исходном виде

Уникальные преимущества

- Безопасная аутентификация и применение политик Zero Trust для любого чувствительного ресурса, включая системы, защита которых раньше считалась труднореализуемой
- Отслеживание и обеспечение безопасности действий, связанных с аутентификацией, в рамках единой платформы во всех средах и ресурсах компании, от устаревших локальных систем до облачных приложений
- Первое решение для аутентификации, не требующее агентов, прокси или модификаций ПО
- Непревзойденный алгоритм на основе ИИ, который обнаруживает угрозы в сети и автоматически усиливает аутентификацию в реальном времени
- Усиление безопасности и повышение удобства работы сотрудников за счет снижения числа МФА-запросов

Мы помогаем компаниям внедрять безопасную, комплексную и безагентную аутентификацию на основе ИИ

Безагентная МФА для «незащищаемых» ресурсов

- Приложения собственной разработки и устаревшие приложения;
- ИТ-инфраструктура (гипервизоры, контроллеры домена и др.);
- Файловые серверы и базы данных;
- Рабочие станции, виртуальные рабочие столы, серверы на Windows / Unix (включая средства удаленного администрирования);
- Интернет вещей и АСУ ТП

Архитектура Zero Trust без использования прокси

- отслеживание и контроль доступа всех пользователей и устройств в сети и облаках, а не только на шлюзе;
- реализация Zero Trust даже в больших и сложных средах, благодаря отсутствию агентов, прокси или сертификатов;
- непревзойденный механизм анализа рисков и оценки доверия с помощью ИИ для постоянного совершенствования политик доступа

Доступ при коммуникациях «машина-машина»

- автоматическое распознавание сервисных учетных записей на основе их поведения;
- обнаружение отклонений от применения по назначению;
- автоматические рекомендации по улучшению политик на основе ИИ;
- предотвращение несанкционированного доступа в реальном времени или требование одобрения администратора

Безопасная облачная миграция по стратегии Lift-and-Shift

- безопасная аутентификация и защищенный доступ для устаревших и самостоятельно разработанных систем, миграция без осложнений с точки зрения ИБ;
- нет необходимости внедрять современные методы аутентификации отдельного для каждого приложения или сервера

Безопасный привилегированный доступ

- автоматическое распознавание и отслеживание привилегированных учетных записей, включая теневые УЗ администраторов;
- МФА для PAM-решений, включая менеджер привилегированных сессий через RDP или SSH прокси (PSM RDP/SSH Proxy);
- удобство использования: без порталов и прокси, без повторного ввода одноразового пароля для каждой новой сессии;
- МФА для администраторов, в т. ч. для средств удаленного администрирования (Remote PowerShell, WinRM и др.), защиту которых не могут обеспечить традиционные МФА

Аутентификация с анализом рисков на основе ИИ

- непрерывная оценка риска и уровня доверия для всех пользователей, устройств и сервисов, как локальных, так и облачных;
- использование ИИ для анализа поведения, группирования объектов в системах, создания цифрового отпечатка людей и устройств;
- предотвращение атак с перебором паролей, латерального движения (например, Mimikatz), блокировка программ-вымогателей и сетевой разведки;
- автоматическое повышение уровня аутентификации в реальном времени при обнаружении угроз (в т. ч. при получении алертов от сторонних решений);
- уменьшение числа ложных срабатываний

Регуляторное соответствие и упражнения Red Team

- соответствие требованиям регуляторов, в том числе, PCI DSS, NY-DFS, SWIFT CSP, NIST и др.
- улучшение результатов упражнений Red Team и аудитов безопасности (с обеих сторон);
- выполнение рекомендаций проведенных аудитов, позволяющее эффективно защищать сеть от компрометации в результате атак на УЗ

Мониторинг и аудит в рамках единой платформы

- консолидированный для всех действий, связанных с получением доступа, для всех ресурсов компании;
- выявление уязвимостей аутентификации, учетных записей с высоким уровнем риска и неиспользуемых прав;
- практическая аналитика, отчеты и журнальные данные

SILVERFORT

ТАЙГЕР ОПТИКС

Gartner COOL VENDOR 2019

Тайгер Оптикс является дистрибьютором Silverfort в России и странах СНГ.
Узнайте больше о решении и закажите демонстрацию по адресу https://www.tiger-optics.ru/get-demo.