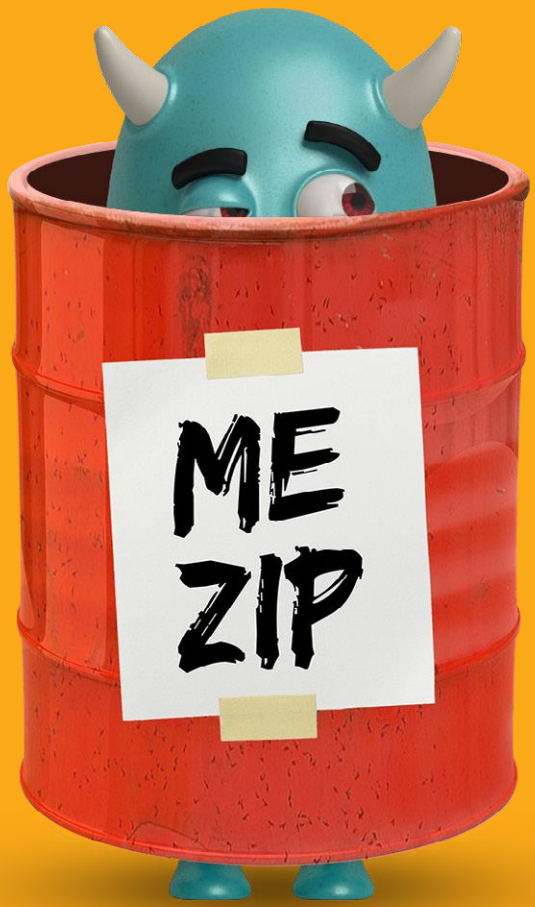
MINERVA

Minerva Anti-Evasion Platform

Блокируйте неизвестные угрозы, разработанные для обхода существующей защиты



Minerva Anti-Evasion Platform автоматически блокирует атаки, специально разработанные, чтобы обходить вашу существующую систему безопасности. Вместо попыток поиска и идентификации вредоносных программ, Minerva создаёт виртуальную реальность на конечном устройстве, вынуждающую вредоносные программы работать против себя, полностью предотвращая их угрозу. Этот уникальный подход позволяет предприятиям останавливать неизвестные, передовые вредоносные программы без привлечения дорогостоящих ресурсов для расследования инцидентов и необходимости восстановления после атак.

УСЛОЖНЁННЫЕ АТАКИ ПРЕДНАЗНАЧЕНЫ ДЛЯ УКЛОНЕНИЯ ОТ ИМЕЮЩЕЙСЯ ЗАЩИТЫ

Несмотря на постоянные инвестиции в решения безопасности, конечные точки по-прежнему заражены передовыми вредоносными программами. Разработка сложных вредоносных программ требует времени и требует значительного финансирования. Авторы вредоносных программ часто проектируют и тестируют свои творения, чтобы они оставались незамеченными для существующих средств безопасности. Такого рода вредоносное ПО позволяет избежать детонации в песочницах или специальных средах для экспертизы, скрываясь в памяти как легитимные процессы, использует сценарии, файлы и другие методы, которые позволяют обходить как традиционные меры безопасности, так и меры безопасности следующего поколения.

Для борьбы с этими угрозами предприятия продолжают полагаться на классические системы защиты и обнаружения. Хотя эти решения и реализуют различные методы защиты, их основные методы основаны на механизмах, которые пытаются идентифицировать вредоносный код на основе ранее замеченных вредоносных программ. Такие подходы, независимо от того, используют ли они сигнатуры, модели машинного обучения или поведенческий анализ, неизбежно пропускают **evasion malware** (вредоносное ПО, специально предназначенное для отклонения от ранее известных шаблонов, использующее специальные методы по уклонению от имеющейся защиты). В результате организации оказываются в погоне за ложными оповещениями и расследуют инциденты, многие из которых оказываются ложноположительными, но в итоге не в состоянии блокировать неизвестные атаки, использующие подобные методы по уклонению от стандартных средств защиты.

НЕ ТОЛЬКО ПРЕДПОЛАГАТЬ НАРУШЕНИЕ. ПРЕДОТВРАЩАТЬ ЕГО.

Понимая, что нынешних мер безопасности недостаточно для обеспечения защиты конечных точек, предприятия пытаются решить, стоит ли использовать дорогостоящий вариант по замене существующих решений для защиты от вредоносных программ более новыми, которые обещают лучшую защиту, или же добавить ещё больше продуктов для защиты, требующих дополнительных ресурсов. В том и другом случае **evasion malware** будет обнаружено только после произошедшего нарушения.

СОЗДАНИЕ ОКРУЖЕНИЯ, ГДЕ ВРЕДОНОСНОЕ ПО ОБЕЗОРУЖИВАЕТ САМО СЕБЯ

Minerva нацелена на предотвращение неизвестных угроз, которые предназначены для обхода существующих средств защиты, без попыток поиска и выявления вредоносных программ.

Этот уникальный подход к блокированию **evasion malware** позволяет избежать дублирования методов, используемых другими технологиями безопасности конечных точек, дополняя базовые решения для защиты от вредоносных программ, устраняя их недостатки, присущие любому подходу основанному на обнаружении.

Minerva Anti-Evasion Platform основана на запатентованной версии Minerva VR™, которая контролирует как вредоносное программное обеспечение «воспринимает» окружающую среду на конечном устройстве, позволяя Minerva обманывать и нейтрализовать вредоносные программы таким образом, который резко отличается от принятого в существующей системе безопасности.

Minerva Anti-Evasion Platform

PATENTED

Minerva Anti-Evasion Platform повышает уровень защиты конечных точек клиентов от **evasion malware** с помощью нескольких модулей, которые усиливают друг друга, образуя мощное централизованно управляемое решение:

Симуляция Агрессивной Среды использует основную силу **evasion malware** против себя. Природа **evasion malware** заключается в том, чтобы запрашивать его среду, с целью проверки, что оно не будет обнаружено корпоративными системами безопасности. Ответ Minerva вводит вредоносную программу в заблуждение, в следствие чего она полагает, что на текущий момент данная среда обладает повышенным уровнем риска по обнаружению вредоносного ПО во время его выполнения. Это приводит к приостановке или прекращению работы вредоносного ПО.

Предотвращение Проникновений в Память блокирует попытки бесфайловых и других скрытых вредоносных программ спрятаться в легитимном процессе, не давая вредоносным программам закрепиться на конечной точке и делая такие методы уклонения в целом неэффективными.

Предотвращение Проникновений из Документов блокирует вредоносные действия, инициированные файлами документов, например, использующими макросы, PowerShell и другие сценарии. Minerva Anti-Evasion Platform позволяет компаниям использовать все возможности современных документов, предотвращая ущерб, который могут нанести вредоносные версии таких файлов.

Защита от Шифровальщиков перехватывает попытки разрушающего вредоносного ПО зашифровать или удалить документы и создаёт резервные копии исходных файлов на лету. Далее Minerva Anti-Evasion Platform предоставляет пользователю возможность получить исходный файл для немедленного восстановления, не полагаясь на другие решения для резервного копирования или возможности ОС, чтобы обеспечить безопасность важных файлов и избежать выплаты выкупа.

Вакцинация Конечных Точек использует типичное поведение многих вредоносных программ, которые избегают заражения одной и той же системы более одного раза. Имитируя маркёр заражения, используемый вредоносным ПО для определения того, находится ли оно уже на конечной точке, платформа Minerva Anti-Evasion блокирует атаку, заставляя вредоносное ПО прекратить попытки «повторного» заражения системы.

Защита Критических Активов блокирует вредоносные программы, исключая вмешательство в критические активы на конечном устройстве. Скрывая или ограничивая доступ к таким приложениям и их артефактам от вредоносных программ, Minerva Anti-Evasion Platform предотвращает угрозы повреждения или кражи конфиденциальных данных, таких как хранилища паролей, кэшированные учётные данные входа в систему, личная информация (PII) или другая важная информация для бизнеса.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

Блокировка Evasion Malware
Предотвращайте атаки, преодолевающие существующую защиту за счёт радикально другого подхода к повышению безопасности

Низкие Накладные Расходы
Экономьте ресурсы от необходимости сложных установок, продолжительного технического обслуживания или переустановки систем.

Без ущерба для пользователей
Усиливайте системы безопасности без замедления или причинения неудобств пользователям.

Без дорогостоящих замен
Защищайте конечные точки без рисков и затрат на проекты по их замене.

УЛУЧШЕННАЯ БЕЗОПАСНОСТЬ БЕЗ ПОВЫШЕНИЯ ОПЕРАЦИОННОЙ НАГРУЗКИ

Minerva Anti-Evasion Platform работает в пассивном режиме, не предпринимая каких-либо действий, которые могут снизить производительность системы, вызвать ложные срабатывания или помешать работе легитимных приложений, что обеспечивает чрезвычайно низкую операционную нагрузку. Развёртываемое через единый установщик, оно занимает минимальный размер на диске и не требует перезагрузок или предварительных подготовительных действий при установке.

Minerva Anti-Evasion Platform также облегчает бремя оперативной перегрузки администраторов. Больше не нужно тратить время на бессмысленные оповещения, поскольку предотвращаются только реальные события, что является следствием крайне низкого уровня ложных срабатываний.

Простая Установка
Сверхлёгкий агент. Minerva может быть установлена на тысячи машин в кратчайшие сроки и без перезагрузок конечных устройств.

Эффективно в автономном режиме
Minerva не зависит от текущих или периодических обновлений и, таким образом, остается эффективной, даже когда конечные точки отключены от сети компании.

Сокращает время на обслуживание
Minerva предотвращает повреждение от большинства типов **evasion malware** или вымогателей, блокируя их ещё до установки.

Отсутствие ложных срабатываний
Когда появляется уведомление от Minerva, вы знаете, что реальная угроза была нейтрализована и предотвращена до того, как был нанесен какой-либо ущерб.

Легковесное
Поскольку у Minerva нет тяжелого агента и не нужно выполнять активное сканирование, решение не влияет на производительность конечного устройства.

Сокращает операционные расходы
Minerva не требует постоянного обслуживания и поддержки. Для получения новых возможностей может автоматически обновляться на регулярной основе.