VMWARE WORKSPACE ONE TRUST NETWORK

Безопасность развивающейся цифровой рабочей области

КРАТКОЕ ОПИСАНИЕ

VMware Workspace ONE™ Trust Network™ предоставляет организациям комплексный и современный подход к обеспечению безопасности сотрудников, приложений, конечных устройств и сетей в среде организации. Workspace ONE Trust Network предоставляет возможности обнаружения и устранения современных угроз, расширяя встроенные возможности обеспечения безопасности аналитической платформы Workspace ONE с помощью широкой экосистемы интегрированных партнерских решений для непрерывного мониторинга рисков и быстрого реагирования на нарушения системы безопасности в цифровой рабочей области.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Workspace ONE Trust Network упрощает обеспечение безопасности и управление с помощью платформы на базе отношений доверия и проверок. Workspace ONE Trust Network предоставляет ИТ-специалистам следующие возможности:

- Объединение разрозненных компонентов системы безопасности с помощью платформы на базе действий, которая создает единое представление и снижает сложность цифровой рабочей области
- Объединение механизмов обеспечения безопасности и администрирования доступа, устройств и приложений с аналитическими данными и средствами автоматизации для снижения рисков в экосистеме вычислительных сред конечных пользователей
- Использование открытой и доверенной экосистемы партнеров и существующих инвестиций для сокращения расходов

Безопасность — главное препятствие для внедрения современной цифровой рабочей области

Цифровая рабочая область помогает повысить эффективность работы сотрудников в пять раз[1], предоставляя удобный и безопасный доступ к приложениям и данным на любом устройстве. При движении организаций по пути к цифровой трансформации экосистема цифровой рабочей области, состоящая из сотрудников, приложений, конечных устройств и сетей, выходит за пределы традиционного периметра благодаря популярным тенденциям, таким как использование личных устройств и потребительская модель ИТ-услуг. По мере исчезновения традиционного периметра растет число сложных киберугроз, таких как атаки нулевого дня, атаки через посредника, кража конфиденциальной информации, боты и программы-вымогатели.

Для инвестиций в мобильные системы и цифровую рабочую область безопасность является главным приоритетом[2], однако существующие средства обеспечения безопасности предоставляют ИТ-специалистам лишь ограниченный уровень визуализации, в который входят только изолированные области безопасности, предоставляющие традиционные возможности. Это приводит к «латанию дыр», что повышает расходы организаций из-за сложности и необходимости в задачах, выполняемых вручную, для защиты цифровой рабочей области. Соответственно, безопасность стала главным препятствием для внедрения современной цифровой рабочей области.

Комплексная система безопасности с возможностями прогнозирования для организации без периметра

Необходимо удовлетворить новый набор требований для решения задач обеспечения безопасности без ущерба для условий работы пользователей.

1. Для получения единого представлении организациям требуется использовать платформу для установления отношений доверия между компонентами, защищающими экосистему.
2. Для непрерывного снижения рисков организациям необходима возможность извлечения аналитических данных из среды для принятия автоматизированных решений на основе прогнозов для защиты цифровой рабочей области.

Workspace ONE Trust Network предоставляет организациям комплексный и современный подход к обеспечению безопасности сотрудников, приложений, конечных устройств и сетей в среде организации. Workspace ONE Trust Network реализует набор возможностей для защиты, обнаружения и устранения угроз в меняющейся цифровой рабочей области с помощью платформы на базе отношений доверия и проверок. Результатом установления отношений доверия в цифровой рабочей области является взаимосвязанная система на базе принципа минимальных привилегий, которая расширяет возможности сотрудников и обеспечивает их безопасность в любой точке, где они работают. Для управления рисками, связанными с современными киберугрозами, Workspace ONE Trust Network объединяет возможности аналитической платформы Workspace ONE с доверенными партнерскими решениями по обеспечению безопасности для создания автоматизированной системы безопасности с возможностями прогнозирования в цифровой рабочей области.

1 Источник: https://www.vmware.com/ru/radius/impact-digital-workforce/

2 Отчет Mobile Technology Buyer Survey («Опрос покупателей мобильных технологий»), CCS Insights, декабрь 2017 г.

Защита, обнаружение и устранение угроз

В современных условиях организации, без сомнения, станут целью кибератаки, вопрос только в том, когда это произойдет. С учетом этого отделы управления ИТ-процессами и безопасности могут управлять рисками для кибербезопасности, упрощая сопоставление возможностей обеспечения безопасности, например используя определенный стандарт, такой как NIST Cybersecurity Framework, с возможностями Workspace ONE Trust Network.

- Возможности обеспечения безопасности начинаются с защиты цифровой рабочей области, в том числе предотвращения попадания вредоносного ПО с помощью самообучающихся систем, предотвращения утечки данных из корпоративных облачных приложений и микросегментации сетей для защиты от современных постоянных угроз.
- Если угроза попадет в цифровую рабочую область, ее можно будет обнаружить с помощью непрерывного и адаптивного мониторинга, что помогает отделам управления ИТ-процессами и безопасности выявлять угрозы на мобильных конечных устройствах и компьютерах, а также в приложениях.
- После обнаружения угроз Workspace ONE Trust Network может автоматизировать их устранение, используя эффективный модуль принятия решений. При выявлении атаки на основе аномального поведения можно применить автоматизированную политику для блокирования доступа к корпоративным данным.

Централизованное обеспечение безопасности и администрирование доступа, приложений и устройств с возможностью анализа

В Workspace ONE Trust Network встроенные возможности обеспечения безопасности аналитической платформы Workspace, в том числе возможности защиты и администрирования доступа, устройств и приложений, объединены со средствами анализа для устранения разрозненных сегментов управления, которые создают решения по обеспечению безопасности. Служба Workspace ONE Intelligence предоставляет возможности анализа для платформы Workspace ONE, осуществляет объединение и сопоставление данных рабочей области и выдает рекомендации для интегрированного анализа и автоматизации. Объединяя возможности Workspace ONE Trust Network с интеллектуальной службой, организации могут обеспечить непрерывный мониторинг рисков для безопасности и ускорить реагирование на нарушения системы безопасности в современном мире без периметра.

Модуль принятия решений помогает сопоставлять информацию, например данные о корпоративных устройствах вне сети, с поведением пользователей для обнаружения угроз и автоматизации устранения нарушений с помощью политик доступа. Встроенные средства анализа угроз и детализированной визуализации состояния соответствия нормативным требованиям — это удобный способ выявления и устранения проблем безопасности в режиме реального времени, который улучшает уровень безопасности цифровой рабочей области. С помощью модуля принятия решений ИТ-специалисты могут создать правила автоматизации и оптимизации общих задач, таких как исправление уязвимых конечных устройств под управлением Windows 10 и настройка элементов управления условным доступом к приложениям и службам на уровне группы или отдельных элементов.

Использование обширной экосистемы доверенных решений партнеров

Для обеспечения комплексной безопасности в цифровой рабочей области необходимо установить отношения доверия между компонентами, которые защищают эту растущую и меняющуюся среду. Workspace ONE Trust Network предоставляет платформу на базе отношений доверия, используя PI-интерфейсы, созданные на основе Workspace ONE. Эти API-интерфейсы дают обширной экосистеме решений возможность взаимодействовать с Workspace ONE и создавать единое представление, которое помогает администраторам упростить процесс обеспечения безопасности и управление. Объединяя разрозненные решения по обеспечению безопасности, заказчики могут продолжить использовать существующие инвестиции для значительного улучшения непрерывного мониторинга, анализа рисков и сокращения времени отклика. Это помогает создать стратегию безопасности с возможностями прогнозирования на основе тенденций и закономерностей, которую можно масштабировать вместе со средой.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Подробнее о Workspace ONE Trust Network: www.vmware.com/ru/products/workspace-one/security

Бесплатное практическое занятие: https://www.vmware.com/go/workspace-hol

ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЛИ ПРИОБРЕТЕНИЯ ПРОДУКТОВ VMWARE

ОБРАЩАЙТЕСЬ ПО ТЕЛЕФОНУ
+7 (495) 212–2900,

ПОСЕТИТЕ СТРАНИЦУ
http://www.vmware.com/ru/products или найдите уполномоченного торгового посредника на сайте VMware.

Основные возможности

Организации могут реализовать преимущества этих важных возможностей Workspace ONE Trust Network для защиты, обнаружения и устранения непрерывно меняющихся киберугроз.

ВОЗМОЖНОСТЬ	ОПИСАНИЕ
Фундаментальная платформа цифровой рабочей области, объединяющая решения по обеспечению безопасности	Упрощенное обеспечение безопасности и управление с помощью платформы на базе отношений доверия, которая использует API-интерфейсы для взаимодействия между открытой экосистемой безопасности и Workspace ONE.
Управление доступом для упрощения бизнес-процессов	Расширение возможностей ИТ-отдела для инициализации приложений, реализации каталога самообслуживания, многоуровневой проверки подлинности и единого входа для всех приложений.
Оптимизированные условия работы пользователей и системы безопасности благодаря контекстным политикам	Управление проверкой подлинности с помощью политик условного доступа на основе соответствия устройств нормативным требованиям, степени защиты при проверке подлинности, степени конфиденциальности данных, местонахождения пользователя и т. д.
Политики предотвращения потери данных для защиты от утечки информации	Шифрование на уровне устройств, шифрование данных и политики безопасности оборудования. Возможность создания политик, в том числе черных списков приложений, политик связывания устройств, политик безопасности Wi-Fi и политик использования протокола TLS. Мониторинг вредоносных приложений и ПО, атак оперативной памяти и разблокированных устройств, а также автоматическое устранение угроз с помощью удаленного блокирования, очистки устройства, блокирования доступа или настраиваемых механизмов карантина устройств.
Защита приложений без ущерба для условий работы пользователей	Использование средств защиты в приложениях VMware для повышения эффективности работы: VMware Boxer™, Browser™ и Content Locker™. Обнаружение угроз и автоматическое устранение проблем для всех других приложений и облачных услуг.
Шифрование данных на хранении и данных при передаче	Проверка подлинности и шифрование трафика между приложениями на устройствах и ЦОД с помощью VMware Tunnel. Шифрование данных при хранении и передаче по стандарту AES с использованием 256-битного ключа.
Микросегментация для автоматизации обеспечения безопасности сети	Сокращение площади атаки в ЦОД благодаря возможностям микросегментации VMware NSX® для автоматизации процессов обеспечения безопасности в сети.
Интеграция и автоматизация средств анализа для реализации системы безопасности с возможностями прогнозирования	Определение и устранение проблем безопасности в режиме реального времени с помощью предоставляемых решением Workspace ONE Intelligence встроенных средств анализа угроз и детализированной визуализации состояния соответствия нормативным требованиям.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel (877) 486–9273 Fax (650) 427–5001 www.vmware.com
125284, Россия, Москва, ул. Беговая, д. 3/1. Тел.: +7 (495) 212–2900 Факс: +7 (495) 212–2901 www.vmware.com/ru