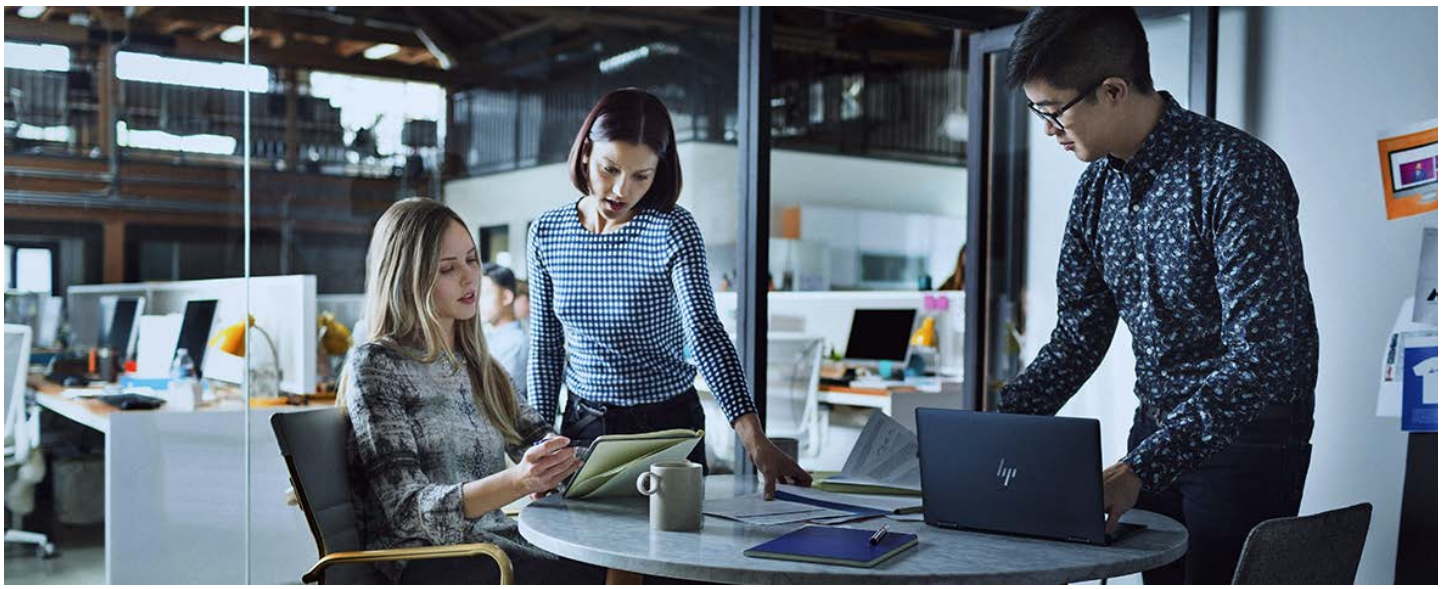
HP WOLF PRO SECURITY SERVICE

HP WOLF SECURITY



Преимущества услуги

- Предотвращение ранее неизвестных атак нулевого дня и кражи учетных данных путем усиления защиты.
- Защита конечных устройств с помощью технологии изоляции корпоративного класса.
- Защита сотрудников от киберугроз без создания барьеров, снижающих производительность их работы.

Информация об услуге

- Приоритет безопасности конечных устройств: многоуровневая система защиты в реальном времени.
- Мониторинг и управление осуществляют сертифицированные отраслевые эксперты по безопасности.
- Своевременная аналитика, практические рекомендации и отчеты

ОБЗОР УСЛУГИ

HP Wolf Pro Security помогает защитить организацию с помощью многоуровневой системы безопасности конечных устройств, ориентированной на растущие и развивающиеся компании[1]. Приоритет безопасности конечных устройств снижает риск атак и позволяет пользователям свободно работать без снижения эффективности и без увеличения нагрузки на ИТ-персонал.

Услуга HP Wolf Pro Security укрепляет защиту корпоративного класса от вредоносного ПО. В этом решении передовое антивирусное ПО нового поколения, в основе которого лежат новейшие технологии ИИ, в том числе глубокое обучение, защита от кражи персональных данных и технологии изоляции, сочетается с действенной аналитикой в реальном времени и постоянным мониторингом угроз силами экспертов по безопасности.

ОСОБЕННОСТИ И ХАРАКТЕРИСТИКИ УСЛУГИ

Защита

HP Wolf Pro Security обеспечивает многоуровневую защиту вычислительных устройств.

Система на основе инструментов искусственного интеллекта, примененная в HP Wolf Pro Security, эффективно использует комбинацию машинного обучения, глубокого обучения и других методик, что дает возможность мгновенно определять даже тщательно замаскированные вредоносные файлы, а также угрозы, не связанные с файлами, по их характерным особенностям. При этом не требуются уникальные сигнатуры. Решение успешно блокирует знакомые угрозы и обнаруживает ранее неизвестные вредоносные программы нулевого дня без обновления клиента.

ОСОБЕННОСТИ И ХАРАКТЕРИСТИКИ УСЛУГИ (ПРОДОЛЖЕНИЕ)

Кроме этого, HP Wolf Pro Security защищает сотрудников от самого распространенного способа взлома: фишинговых атак с целью получения учетных данных. Защита персональных данных в HP Wolf Pro Security блокирует ввод паролей пользователями на сайтах, собирающих учетные данные, которые могли быть случайно открыты по фишинговой ссылке из письма, чата, документа PDF или другого файла.

Технология изоляции корпоративного класса в HP Wolf Pro Security служит последней линией обороны, сдерживая и обезоруживая даже невидимые угрозы, которые, возможно, сумели обойти другие инструменты защиты конечных устройств. Такая защита с изоляцией, усиленная аппаратными средствами, позволяет безопасно открывать, редактировать, распечатывать и сохранять на собственных защищенных микро виртуальных машинах вложения в электронные письма, загруженные файлы и даже содержимое с USB-носителей. Автоматический мониторинг угроз охватывает все открытые приложения. HP Wolf Security Controller предоставляет полный анализ цепочек атак для инцидентов, связанных с угрозами, помогая лучше понять характер угрозы и защититься от будущих атак.

Сочетая эти передовые технологии, HP Proactive Security обеспечивает многоуровневую проактивную защиту устройств в реальном времени.

Аналитика
HP Wolf Pro Security предоставляет клиентам действенные аналитические рекомендации через мощную платформу анализа безопасности HP Wolf Security Controller[2]. Специалисты ИТ-отделов могут контролировать статус защиты устройств, просматривать отчеты, получать уведомления о незащищенных устройствах и заблокированных действиях, используя единую облачную информационную панель.

Экспертный мониторинг и контроль[3]
В отличие от решений, основанных только на программных средствах, HP Wolf Pro Security поставляется как контролируемая услуга. Эксперты HP по безопасности внедряют и контролируют политики конфигурации и безопасности, включая управление карантином угроз от имени клиента. После регистрации устройств специалисты HP следят за статусом их защиты, проводят расследования и анализ цепочек атак, чтобы выявить ранее неизвестные угрозы нулевого дня и помочь лучше защититься в будущем.

Категория	Функциональные возможности
Защита	HP Sure Sense Pro на базе ИИ, система защиты от угроз для устройств Windows 10[4]
	HP Sure Click Pro[5], система изоляции вложений и загрузок для Windows 10
	HP Identity Protection блокирует случайное раскрытие паролей на веб-сайтах, созданных с целью кражи учетных данных
Security Analytics	Информационная панель для защиты устройств
	Данные об угрозах в HP Sure Click Pro и HP Sure Sense Pro
	Подробная информация о статусе защиты устройств
	Подробный анализ цепочки атаки с привязкой к MITRE ATT&CK™[6]
Текущее управление службами	Установка контроллера, настройка и применение политик
	Понимание и анализ угроз
	Управление карантином и исключениями
	Агент безопасности: исследование состояния
	Агент безопасности: развертывание обновления
Другие особенности	Интеграция SIEM через данные системного журнала

ОСОБЕННОСТИ ПРЕДОСТАВЛЕНИЯ УСЛУГИ

На управляемые устройства заказчиком должно быть установлено клиентское ПО систем аналитики и обеспечения безопасности. Для доступа к системам аналитики и отчетности, а также для получения обновлений политик и ПО требуется подключение к Интернету. Сами программные агенты после завершения установки не нуждаются в подключении к Интернету для обеспечения защиты. Конфиденциальная информация пользователей, включая учетные данные, файлы, материалы и персональные сведения, не собирается. Собранная информация хранится в безопасном облачном хранилище[2].

HP предоставит для HP Wolf Security Controller доступ к аналитическим данным о безопасности, включая информационную панель, отчеты и сведения об инцидентах.

Сертифицированные эксперты HP будут управлять безопасностью конечных устройств, принимая профилактические меры, в том числе настройку и применение политики безопасности; анализ инцидентов, когда обнаружена действительная угроза; управление обновлениями агента безопасности; определение причин проблем, связанных с работоспособностью агента и т. д.

Специалисты HP обеспечат поддержку клиентов первого уровня и будут работать с командами HP, включая экспертов по безопасности, для решения проблем, с которыми вы обратитесь. Специалисты HP доступны по следующему графику:

Северная Америка: поддержка на английском языке с понедельника по пятницу (исключая выходные дни HP) с 06:00 до 18:00 по горному времени США.

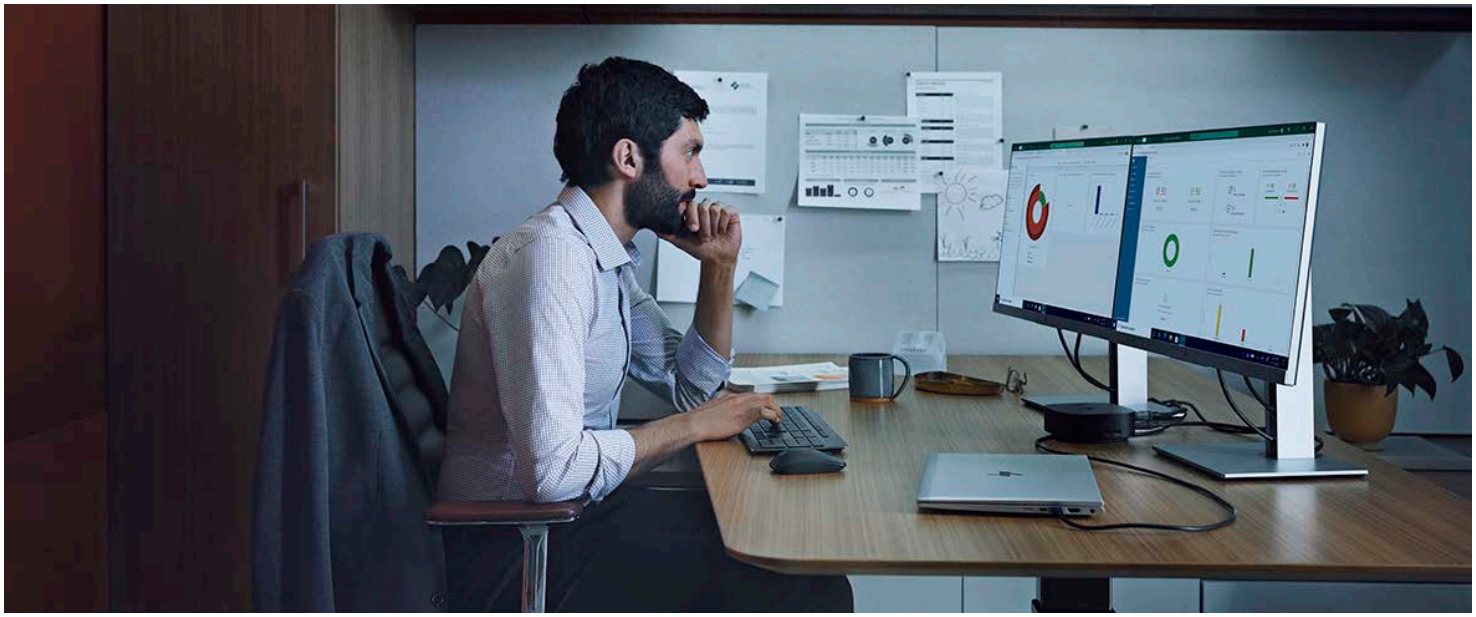
Латинская Америка: поддержка на английском и испанском языках с понедельника по пятницу (исключая выходные дни HP) с 07:00 до 18:00 GMT–5.

Европа, Ближний Восток и Африка: поддержка на английском, французском и немецком языках с понедельника по пятницу (исключая выходные дни HP) с 08:00 до 18:00 CET.

Азиатско-Тихоокеанский регион и Япония: Круглосуточная поддержка на английском языке доступна во всем регионе, поддержка на английском и японском языках доступна для Японии с 9:00 до 21:00 (японское стандартное время), 7 дней в неделю (исключая выходные дни HP).

Обязанности заказчика

- Предоставить необходимую информацию, чтобы специалисты HP могли настроить учетную запись.
- Развернуть агент Wolf Pro Security на управляемых устройствах.
- Запросить добавление в список разрешенных или удаление из него сайтов, ресурсов загрузки файлов, исключений и параметров почтовых доменов (для изоляции вложений электронной почты, защиты от вредоносного ПО на основе алгоритмов ИИ и защиты от кражи учетных данных).
- Запросить добавление или удаление диапазонов внутренних IP-адресов компании, не подлежащих изоляции.
- Запросить или одобрить выпуск или исключение файлов из карантина или блокировки.
- Войти в портал HP Wolf Security Controller для просмотра информационных панелей, отчетов и сведений об инцидентах.
- Изучать отчеты о состоянии системы безопасности и предпринимать соответствующие действия.



СИСТЕМНЫЕ ТРЕБОВАНИЯ

HP Wolf Pro Security поддерживает системы с ОС Windows 10, работающие на поддерживаемых процессорах Intel® или AMD. Актуальная версия системных требований доступна на сайте https://www.hpdaas.com/requirements

Требования к сети
Для связи между управляемым устройством и службой управления облаком требуется подключение к Интернету.

Предварительные требования
Чтобы воспользоваться услугой, ее необходимо зарегистрировать после покупки, следуя инструкциям HP. В процессе регистрации вам потребуется предоставить информацию, необходимую для настройки учетных записей и политик безопасности.

ОГРАНИЧЕНИЯ ОБСЛУЖИВАНИЯ

HP Wolf Pro Security не является постоянной службой мониторинга в реальном времени. HP Sure Sense Pro и HP Sure Click Pro автоматически блокируют или изолируют ненадежный или вредоносный контент, обеспечивая защиту ваших устройств. В HP Wolf Pro Security не включены службы корректировки или смягчения последствий на случай нарушения безопасности. Службы корректировки или смягчения последствий доступны отдельно, у партнеров HP.

УСЛОВИЯ

Условия обслуживания HP Care Pack могут применяться, если услуга приобретена как HP Care Pack. К этой услуге применимы Условия обслуживания HP TechPulse, уведомление HP о правах на персональные данные и заявление HP о защите конфиденциальности.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Обратитесь к местному коммерческому представителю или торговому партнеру HP или изучите информацию по ссылке https://www8.hp.com/us/en/services/pro-security-service.html

1 Услуги HP регулируются действующими условиями договора о предоставлении услуг HP, с которыми заказчик знакомится в момент приобретения. Клиент может обладать дополнительными законными правами в соответствии с действующим местным законодательством. Эти права не будут зависеть от условий обслуживания HP или ограниченной гарантии HP, предоставляемой вместе с продуктом HP. Полный список системных требований доступен на https://www.hpdaas.com/requirements.

2 HP не отслеживает то, какие URL-адреса посетил пользователь. Отчетность фокусируется на идентификации угроз и их источника в HP Wolf Security Controller. HP Wolf Security Controller отвечает требованиям GDPR и ISO 27001. HP Wolf Security Controller недоступен как автономный продукт и требует наличия HP Wolf Pro Security Service. Полный перечень системных требований доступен на http://www.hpdaas.com/ requirements. Предоставление услуг HP регулируется действующими условиями HP, которые клиент получает или с которыми знакомится в момент приобретения. Клиент может обладать дополнительными законными правами в соответствии с действующим местным законодательством. Эти права не будут зависеть от условий обслуживания HP или ограниченной гарантии HP, предоставляемой вместе с продуктом HP.

3 Анализ угроз экспертами HP по безопасности — это процесс расследования, который становится доступен после блокировки или изоляции вредоносного события программным агентом HP Wolf Pro Security. Это решение не является круглосуточной службой мониторинга в реальном времени. Дополнительную информацию об этой сервисной функции см. в документе «HP Wolf Pro Security Service Definition». Агент HP Wolf Pro Security автоматически изолирует ненадежный или вредоносный контент, обеспечивая защиту до проведения анализа. Также ни один план не включает услуги по исправлению или смягчению последствий в случае нарушения безопасности.

4 Полный список поддерживаемых версий Windows 10 доступен на https://www.hpdaas.com/requirements. Обратите внимание на то, что HP Wolf Pro Security не поддерживает Windows 7 и 8.1.

5 Технология HP Sure Click Pro входит в HP Wolf Pro Security и требует наличия ОС Windows 10 Pro или Enterprise. Поддерживаются браузеры Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox и новый Edge. В качестве вложений поддерживаются файлы Microsoft Office (Word, Excel, PowerPoint) и файлы PDF, если установлены приложения Microsoft Office или Adobe Acrobat. Дополнительные сведения доступны на https://www.hpdaas.com/requirements.

6 MITRE не утверждает, что ATT&CK включает все возможные типы действий и поведения, зафиксированные в модели злоумышленника и комплексе методов работы решения. Использование информации из базы данных ATT&CK с учетом всех категорий методов не гарантирует полную защиту, поскольку некоторые методы или их варианты могут быть еще не выявлены или не описаны в ATT&CK.

Подпишитесь на новости

hp.com/go/getupdated

Отправить коллегам

Оценить этот документ

4AA7-4656RUE, май 2021 г., ред. 5

HP WOLF SECURITY