Endpoint Protection | Endpoint Protection Plus

КАКАЯ ИНФОРМАЦИЯ ОТПРАВЛЯЕТСЯ/ХРАНИТСЯ В ОБЛАКЕ

01 Какая информация отправляется / хранится в облаке?

02 Передается ли эта информация третьим лицам?

03 Информация отправляется в зашифрованном виде?

04 Насколько безопасна платформа, где размещены данные?

05 Какие сертификаты безопасности имеет платформа, где размещены данные?

06 Где расположена платформа Windows Azure?

01

Какая информация отправляется / хранится в облаке?

В данной статье описывается, какая информация отправляется в облако агентами Endpoint Protection, установленными на каждой конечной точке для защиты ноутбуков, рабочих станций и серверов Windows.

Важно отметить, что Endpoint Protection не отправляет в облако какие-либо персональные данные.

Сообщения о статусе

Сообщения о статусе содержат информацию о статусе защиты каждого управляемого компьютера. Отправляется следующая информация:

— Название компьютера.

— Рабочая группа / Active Directory Название группы.

— Операционная система.

— Service Pack.

— Группа, к которой принадлежит защищаемый компьютер.

— IP-адрес компьютера по умолчанию.

— MAC-адрес.

— IP-адреса сетевых адаптеров.

— MAC-адреса сетевых адаптеров.

— ОЗУ (МБ).

— Утилиты удаленного доступа (LogMeIn, TeamViewer, UVNC, TVNC и RVNC). В отправляемой информации указывается, установлены ли они и включены ли они на компьютере.

Сообщения об обнаружении

Следующая информация передается в сообщениях об обнаружении (включая сообщения карантина):

— Путь к файлу.

— Название файла.

— IP-адрес компьютера, где файл был обнаружен.

— Авторизованный пользователь.

— Данные сообщения, Если угроза была обнаружена в почтовом сообщении(отправитель и получатель).

Сообщения об обнаружении компьютеров

Следующая информация передается в сообщениях об обнаружении компьютеров:

— Название компьютера.

— IP-адрес компьютера без защиты Endpoint Protection.

Сообщения, отправляемые в Коллективный разум

Следующая информация включена в сообщения, отправляемые на платформу Коллективного разума для облачного анализа:

— Значение MD5 (SHA1 в случае с Android) файлов, которые должны быть проверены в облаке. MD5 - это уникальная 16-байтовая (128 бит) "сигнатура" или "хэш", которая уникально идентифицирует файл. Хэш SHA1 - то же самое, только 160 бит (20 байт).

— IP-адрес компьютера.

— Статистическая информация об объектах, обнаруженных на каждом компьютере. Эта информация помогает Коллективному разуму классифицировать больше объектов с большей точностью. Эта статистика содержит:

- MUID компьютера. MUID - это 16-байтное значение, которое используется для гарантии, что вся информация поступает с одного и того же компьютера
- ID продукта
- Версия продукта
- Дата сигнатурного файла
- ID технологии, которая обнаружила объект
- Модуль защиты, который обнаружил объект
- Версия операционной системы
- Service pack операционной системы
- Архитектура процессора (32/64 бит)
- Браузер
- Версия браузера
- Путь к обнаруженной вредоносной программе
- Общее количество обнаружений

— Файл (только исполняемые файлы), если необходимо. Только подозрительные файлы отправляются в Коллективный разум, и только исполняемые файлы классифицируются как подозрительные (файлы .exe, .dll или .com). Эти файлы не содержат конфиденциальной информации. Подозрительные файлы отправляются в Panda при условии, если они еще не были отправлены любым решением, использующим Коллективный разум.

02

Передается ли эта информация третьим лицам?

Нет, все данные хранятся исключительно на нашей платформе Windows Azure. Ни при каких обстоятельствах она не передается любым третьим лицам.

03

Информация отправляется в зашифрованном виде?

Да, вся информация отправляется в облако в зашифрованном формате (используется шифрование SSL или Blowfish).

04

Насколько безопасна платформа, где размещены данные?

Windows Azure - это платформа, где размещены Endpoint Protection и Partner Center. Она обеспечивает самый высокий уровень защиты конфиденциальных данных в хранилище.

Для получения подробной информации о средствах управления безопасностью и имеющихся в Azure политиках, смотрите белую книгу “Обзор безопасности Windows Azure”:

Обзор безопасности Windows Azure

05

Какие сертификаты безопасности имеет платформа, где размещены данные?

Как сказано в вышеупомянутом файле .PDF, Windows Azure работает в дата-центрах под управлением Microsoft Global Foundation Services (GFS): “Windows Azure работает в инфраструктуре Microsoft Global Foundation Services (GFS)”.

Для получения более подробной информации об управлении безопасностью в Global Foundation Services (GFS), смотрите...

Облачные сервисы Microsoft

Сертификаты W. Azure

Облачные сервисы Microsoft показывают сертификаты, полученные Windows Azure:

- ISO/IEC 27001:2005
- Statement on Auditing Standards No. 70 (SAS 70) Type I and II
- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA)

Сертификация ISO 27001

Для получения более подробной информации о сертификации ISO 27001, смотрите:

Windows Azure получил IS0 27001

+ Подробности о W. Azure

Наконец, стоит отметить, что...

Подробности

содержит детальный обзор, как Windows Azure удовлетворяет требованиям безопасности, определенным в Cloud Security Alliance (CSA) Cloud Control Matrix (CMM).

Приводим выдержку из этого обзора:

"Наша структура безопасности, основанная на ISO 27001, позволяет клиентам оценить, как Microsoft соответствует или превосходит требования стандартов безопасности и принципов внедрения. ISO 27001 определяет, как внедрить, контролировать, обслуживать и постоянно улучшать систему управления информационной безопасностью (ISMS). Кроме того, инфраструктура GFS проходит ежегодный аудит в рамках American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) No. 70, который будет заменен на аудит AICPA Statement on Standards for Attestation Engagements (SSAE) No. 16 и аудит International Standards for Assurance Engagements (ISAE) No. 3402 . Планирование аудита Windows Azure по SSAE 16 находится на стадии реализации".

06

Где расположена платформа Windows Azure?

Windows Azure имеет свои узлы по всему миру. Сейчас дата-центр Panda Security расположен в Дублине (Ирландия).

Справа - фотография дата-центра.


panda