Adaptive Defense

КАКАЯ ИНФОРМАЦИЯ ОТПРАВЛЯЕТСЯ/ХРАНИТСЯ В ОБЛАКЕ

СЕРТИФИКАТЫ AZURE

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 и хранится в облаке?

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

Новая модель защиты в Panda Adaptive Defense требует сбора информации о том, что делает каждое приложение. Непрерывный мониторинг действий, выполняемых приложениями, а также дальнейший анализ этих данных с помощью техник машинного обучения в нашем окружении Больших данных, - это то, что позволяет нам предлагать нашим пользователям гарантированную защиту.

Данные, собираемые Panda Adaptive Defense, соответствуют следующим правилам:

- Собирается только относительная информация об исполняемых файлах в Windows (файлы .exe, dll и т.д.), которые запускаются/ загружаются на машине.
- Атрибуты таких файлов отправляются в виде стандартных ссылок без специфичной для каждого пользователя информации. Например, пути файлов стандартизованы как LOCALAPPDATA\name.exe вместо c: \Users\USERS_NAME\ AppData \Local\ name.exe.
- Собираемые URL только для загружаемых исполняемых файлов. Те URL, которые пользователь сам открывает в браузере при просмотре сайтов, не собираются.
- Собираемые данные не содержат персональную информацию.
- Ни в коем случае Panda Adaptive Defense не отправляет персональную информацию в облако.

Следующая информация собирается с каждой машины:

- Название устройства.
- Операционная система.
- Service Pack.
- Группа, в которой находится защищаемый ПК.
- IP-адрес машины по умолчанию.
- MAC-адрес.
- IP-адреса, назначенные различным веб-адаптерам.
- MAC-адреса для различных веб-адаптеров.
- Память ОЗУ в МБ.

О действиях, которые приложения выполняют в системе

В качестве важной информации для поддержки новой модели защиты в Panda Adaptive Defense, в облако отправляется информация о действиях, выполняемых приложениями в системе.

Атрибут	Данные	Описание	Пример
Файл	Хэш	Хэш файла, относящегося к событию	-
URL	Url	Адрес, откуда был скачен PE-файл	http://www.malware.com/executable.exe
Путь	Путь	Стандартизованный путь, где находится файл данного события	APPDATA\
Реестр	Ключ / Значение	Ключ реестра Windows и соответствующее значение	HKEY_LOCAL_MACHINE\SOFT WARE \Panda Security\Panda Research\ Minerva\Version = 3.2.21
Операция	ID операции	ID операции выполненного события (создание/изменение/загрузка/… PE-файла, его скачивания, коммуникации и т.д.)	Тип события 0 показывает выполнение PE-файла
Коммуникация	Протокол/ Порт/Адрес	Собирает коммуникационное событие процесса (не его контент) вместе с его протоколом и адресом	Malware.exe отправляет данные UDP на порт 4865
ПО	Установленное ПО	Собирает список ПО, установленного на машине в соответствии с Windows API	Office 2007, Firefox 25, IBM Client Access 1.0

Кроме того, может потребоваться отправка исполняемых файлов на нашу платформу Коллективного разума. Чтобы снизить использование канала связи, в платформу Коллективного разума отправляются только те исполняемые файлы, которые еще не присутствуют в ней.

Отправляя любые исполняемые файлы, мы гарантируем, что в любом случае они не будут содержать конфиденциальной информации пользователя/клиента.

02

Передается эта информация третьим лицам?

Вся рабочая информация хранится исключительно на нашей облачной платформе Windows Azure.

Информация не передается третьим лицам за исключением случаев, когда наши клиенты:

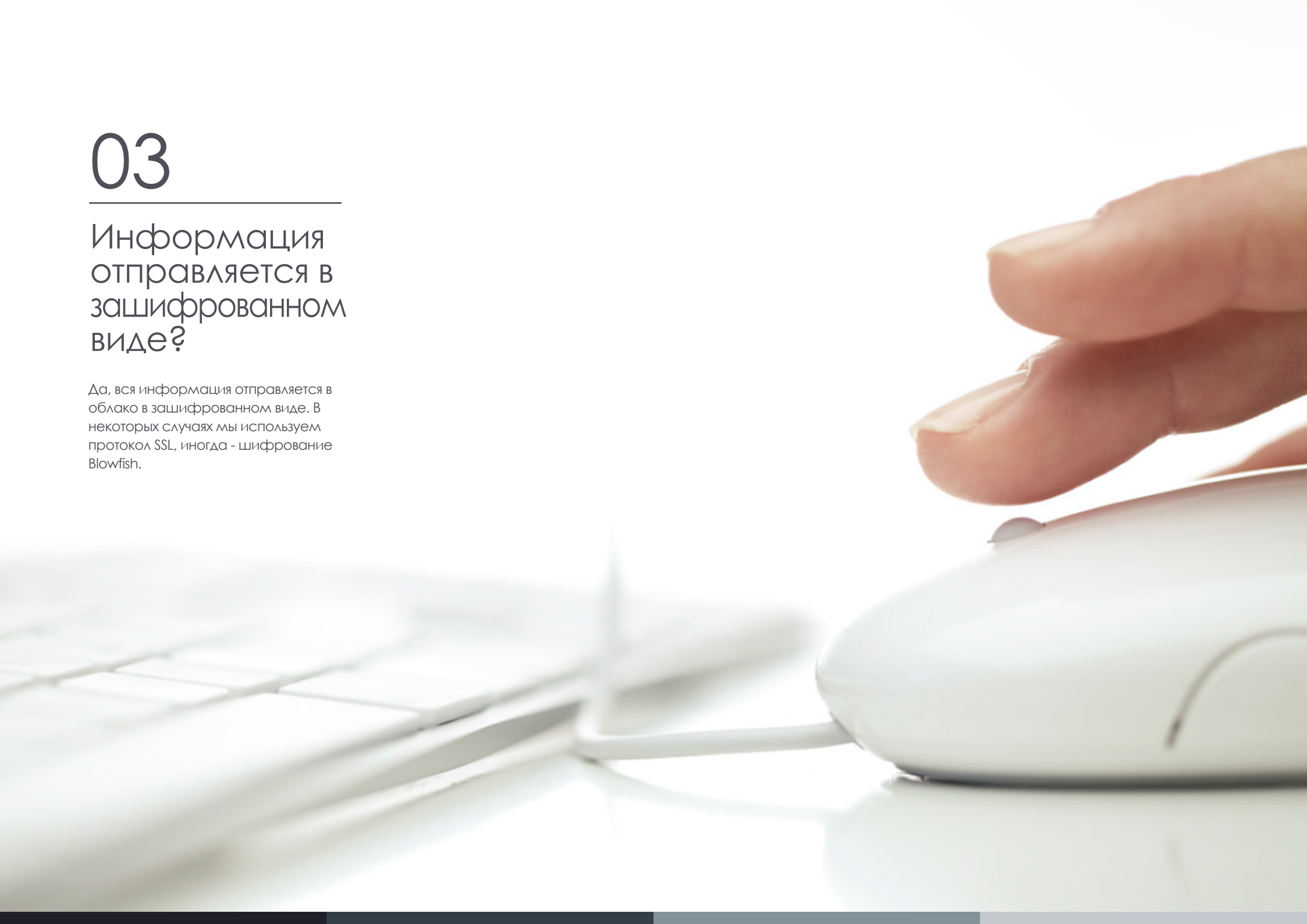
- Хотят получать информацию в свою SIEM-систему о тревогах и данных безопасности, которые собираются Panda Adaptive Defense. Информация о безопасности, собираемая Panda Adaptive Defense, будет отправляться в SIEM клиента по защищенному протоколу по согласованию с клиентом.

- Используют платформу Logtrust, SIEM-улититу, которая интегрирована в Panda Adaptive Defense по умолчанию. Logtrust - это облачная платформа Больших данных, которая в реальном времени хранит информацию о собранных параметрах со всех машин, защищенных Panda Adaptive Defense. Информация отправляется в Logtrust через HTTPS и хранится в Logtrust CPD.

03

Информация отправляется в зашифрованном виде?

Да, вся информация отправляется в облако в зашифрованном виде. В некоторых случаях мы используем протокол SSL, иногда - шифрование Blowfish.



04

Насколько безопасна платформа, где хранятся данные?

Windows Azure - это платформа, где размещен Panda Adaptive Defense. Она предоставляет максимальную защиту и конфиденциальность хранящихся данных. Политики безопасности и контроля, установленные в Azure, описаны в Белой книге "Обзор безопасности Windows Azure"

Обзор безопасности Windows Azure

КАКУЮ БЕЗОПАСНОСТЬ ПРЕДОСТАВЛЯЕТ ПЛАТФОРМА, ГДЕ РАЗМЕЩЕН LOGTRUST?

Logtrust использует Amazon Web Services, предоставляя все преимущества мер физической и информационной безопасности дата-центров Amazon.

Для получения более подробной информации смотрите следующий документ:

Соответствие облака AWS нормативным требованиям

Доступ к системам Logtrust всегда фильтруется файерволом и защищается с помощью проверки подлинности на основе сертификатов. Кроме этого, все системы, сервисы и приложения, которые составляют облачную инфраструктуру, передают свои логи для целей аудита и безопасности.

05

Какие имеет сертификаты безопасности платформа, где размещены данные?

Как сказано в PDF в предыдущем разделе, Windows Azure работает в инфраструктуре Microsoft Global Foundation Services (GFS).

В следующем документе содержатся сведения об управлении безопасностью в Global Foundation Services (GFS) - облачной инфраструктуре Microsoft, где работает Windows Azure:

Облачные сервисы Microsoft

Сертификаты 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)

Для получения более подробной информации о сертификате 27001:

Windows Azure получил IS0 27001

Наконец, отметим, что в:

Подробности

содержится Белая книга, которая описывает, как Windows Azure соответствует требованиям безопасности, которые определены Cloud Security Alliance, Cloud Control Matrix. Параграф из этой книги:

"Наши рамки безопасности основаны на ISO 27001, что позволяет пользователям оценить, как Microsoft соответствует или превосходит стандарты безопасности и принципы их применения. ISO 27001 определяет порядок внедрения, мониторинга, поддержания и постоянного улучшения системы управления информационной безопасностью (ISMS). Кроме этого, инфраструктура GFS ежегодно проходит аудиты American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) No. 70, которые будут заменены аудитами AICPA Statement on Standards for Attestation Engagements (SSAE) No. 16 и International Standards for Assurance Engagements (ISAE) No. 3402. Также планируется аудит Windows Azure в рамках SSAE 16 audit".

СЕРТИФИКАТЫ БЕЗОПАСНОСТИ ПЛАТФОРМЫ, ГДЕ РАЗМЕЩЕНЫ ДАННЫЕ LOGTRUST

Те клиенты, которые намерены использовать сервис Logtrust, должны знать, что они могут рассчитывать на меры физической безопасности Amazon CPD.

Соответствие облака AWS нормативным требованиям

Как Вы можете видеть подробнее в предыдущей ссылке, Amazon имеет все основные сертификаты:

- ISO/IEC 27001
- SOC 1/SSAE 16/ISAE 3402 (ранее - SAS70)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA)

06

Где расположена платформа Windows Azure?

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

Ниже - фотография дата-центра в Ирландии.

ГДЕ РАСПОЛОЖЕНА ПЛАТФОРМА AMAZON LOGTRUST?

Logtrust работает в режиме высокой доступности на своей платформе Amazon, расположенной в собственном дата-центре в Ирландии.


panda