Microsoft

Удачный тандем: Veeam + Azure – быстрый и надежный BackUp

Дмитрий Поляков
Генеральный директор CS IT

Содержание

- Традиционное решение Azure Backup
- Возможности Veeam Backup and Replication
- Преимущества тандема
- Архитектура решения
- Возможности приобретения

Azure Backup

простая и надежная служба архивации в облако

Хранилище резервных копий с георепликацией, доступность 99,9%

Эффективные и гибкие службы оперативной архивации, добавочное резервное копирование

Шифрование данных при передаче и на месте

Надежная целевая система автономной архивации. Возможность использования как альтернативы магнитной ленте

Veeam Backup and Replication

лучшее средство для резервирования виртуальных сред

Быстрое восстановление нужных данных удобным способом

Гарантированное восстановление каждого файла, приложения или виртуального сервера

Мониторинг в режиме реального времени и упреждающее оповещение о проблемах

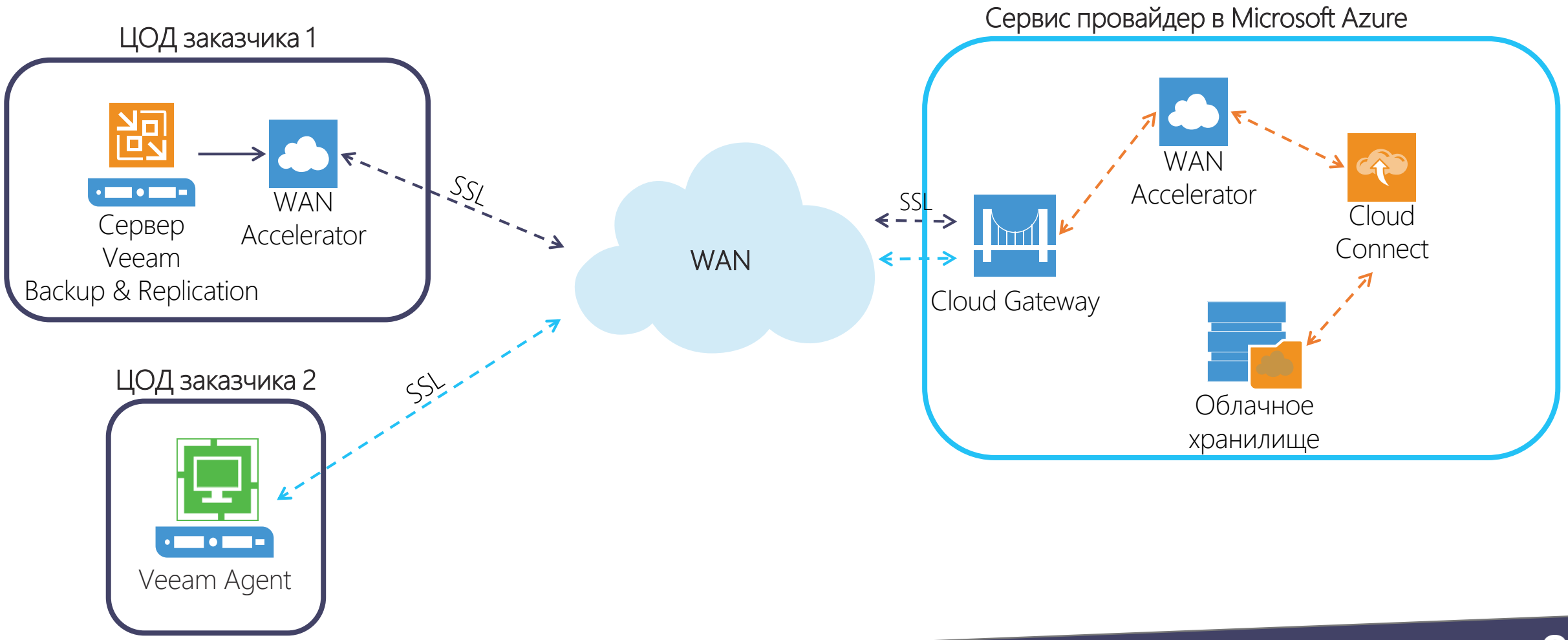
Низкие показатели целевой точки восстановления (RPO) и оптимизированное послеаварийное восстановление

Microsoft + Veeam = ?

преимущества тандема

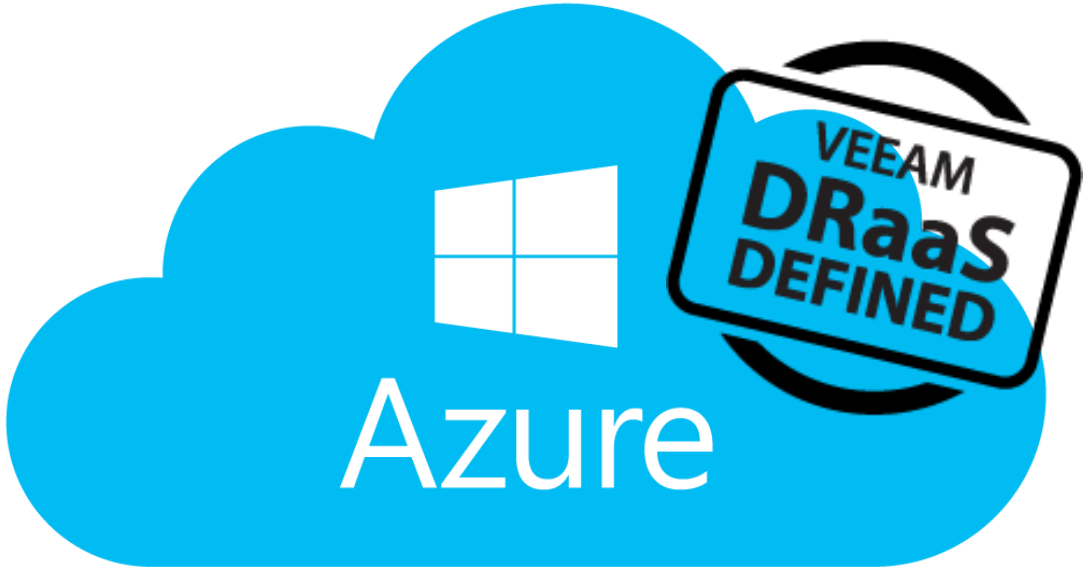
- Высокая скорость передачи данных за счет использования WAN Accelerator
- Тесная интеграция решений, поддержка на уровне вендоров
- Простая настройка со стороны заказчика
- Гибкие возможности приобретения

Архитектура общего решения



Приобретение

гибкие условия лицензирования



- Лицензирование по защищаемым виртуальным машинам
- Развертывание ресурсов по мере необходимости
- Возможность выбора между постоянными лицензиями и лицензиями на основе подписки, а так же сочетание обоих вариантов

Формула расчета:

стоимость решения = лицензии Veeam + ресурсы Azure

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дмитрий Поляков
Генеральный директор CS IT

КАК ЗАЩИТИТЬ СВОЙ БИЗНЕС С ПОМОЩЬЮ РЕШЕНИЙ MICROSOFT

- **Многофакторная идентификация** (Multi-factor authentication - MFA) – сервис, позволяющий блокировать доступ злоумышленников к чувствительным данным организации или бизнес системам, даже в случа получения логинов и паролей сотрудников вашей компании.
- **Exchange ATP (Advanced Treat Protection)** – анализирует почтовые вложения или интернет-ссылки и своевременно реагирует на выявленные атаки
- Создание белых списков приложений с помощью встроенного функционала в **Windows 10 Enterprise - Device Guard и AppLocker и др.**

Защита компьютеров финансовых работников

Многофакторная аутентификация Microsoft Azure

Зачем нужна многофакторная аутентификация?

Задача

- Повышение безопасности удаленного доступа к ресурсам Компании
- Не использовать токены
- Снижение нагрузки на ИТ/Службу поддержки на обслуживание и поддержку решений по управлению доступом
- Обеспечение удаленного доступа пользователей к ресурсам компании с растущего числа различных устройств
- Обеспечение соответствия требованиям регуляторов
- Обеспечение единого механизма аутентификации для различных платформ и приложений

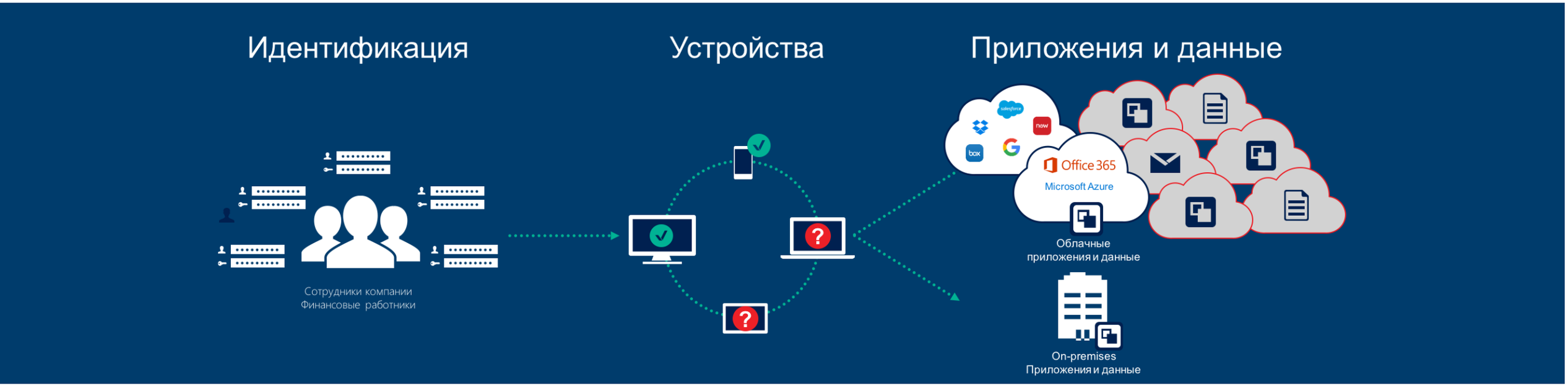
Microsoft Azure MFA

- Работает со всеми существующими телефонами, по всему миру
- Дополнительная верификация учетных данных пользователей
- Обеспечивает 100% защиту от угроз, реализуемых вредоносным ПО
- Встроенная поддержка популярных приложений
- Упрощение управления пользователями и развертыванием
- Высоко-масштабируемый сервис

Выгоды

- Минимизация рисков утечки информации
- Обеспечение регуляторных требований.
- Уменьшение времени развертывания
- Сокращение затрат на обслуживание и поддержку
- Увеличение продуктивности бизнес-пользователей
- Существенная экономия по сравнению с аппаратными средствами двухфакторной аутентификации

Варианты реализации



Варианты второго фактора

- Телефонный звонок
- Текстовое сообщение
- Мобильное приложение
- Push уведомление

Подключение

- RADIUS
- LDAP
- IIS
- RDS/VDI

Интеграция

- **Нативная интеграция**
  Функционал доступен для облачных приложений, например, O365
- **Server MFA**
  Локальное или облачное решение для обеспечения безопасного доступа для VPN или приложения, предоставляемого Microsoft или другим вендором
- **SDK**
  Добавление сервиса многофакторной аутентификации к проприетарному приложению или веб-сайту через SDK

Безопасность

Как защититься от вирусов-шифровальщиков

Расширенная защита от угроз (Advanced Threat Protection, ATP) для Exchange Server и Exchange Online

Защита от неизвестного вредоносного ПО и вирусов

- Анализ поведения при помощи машинного обучения
- Оповещения администраторов

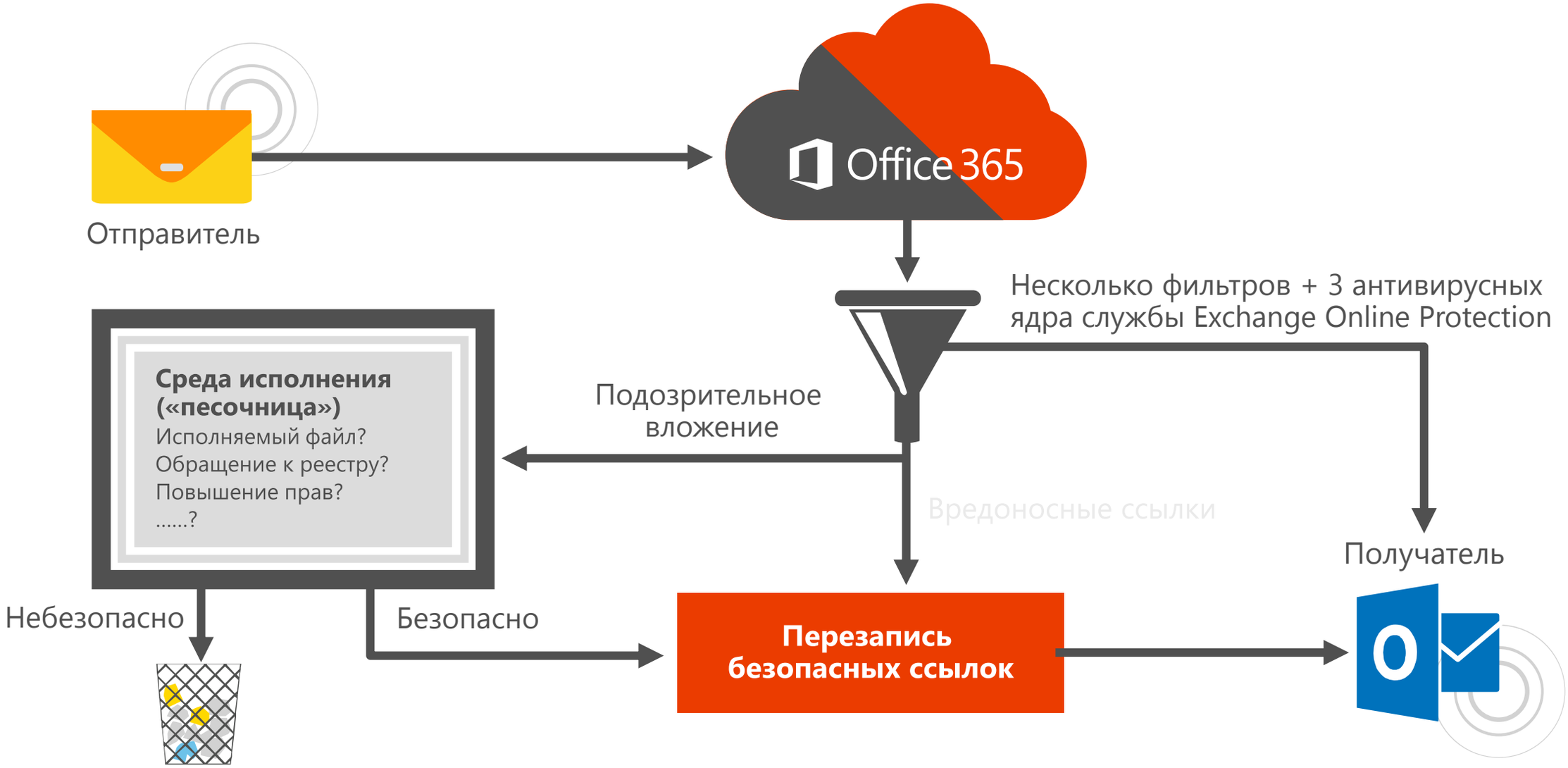
Защита во время попытки перехода по ссылкам

- Защита от вредоносных URL-адресов в режиме реального времени
- Растущая база URL-адресов

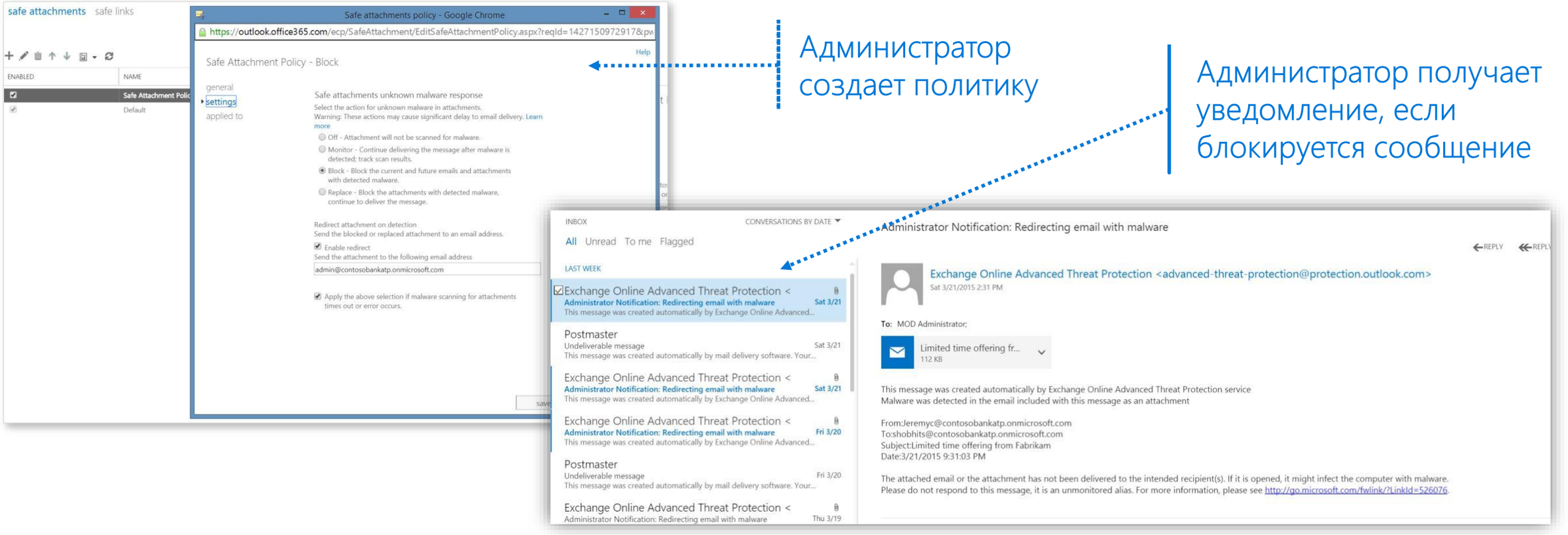
Широкие возможности создания отчетов и трассировки

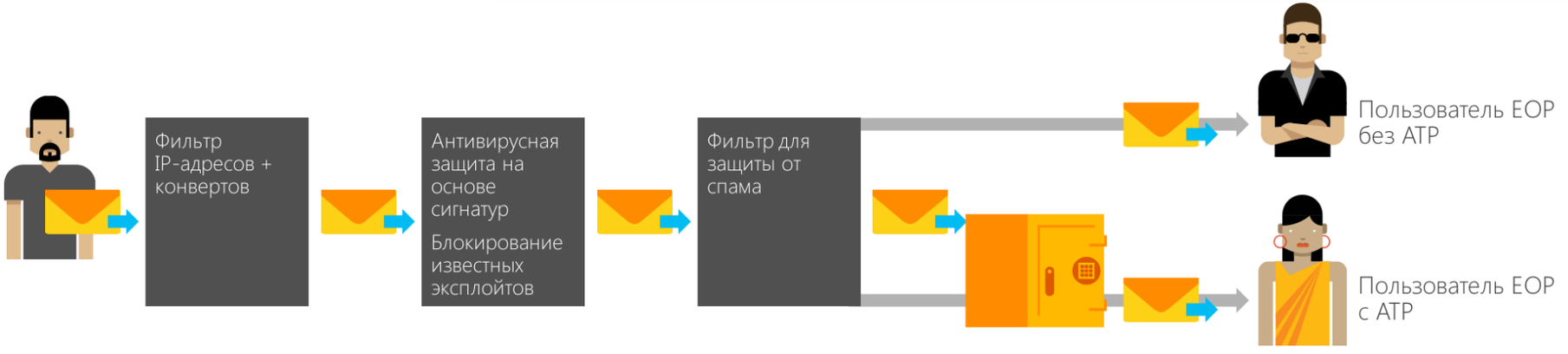
- Встроенные средства трассировки URL-адресов
- Отчеты о сложных угрозах

Архитектура службы

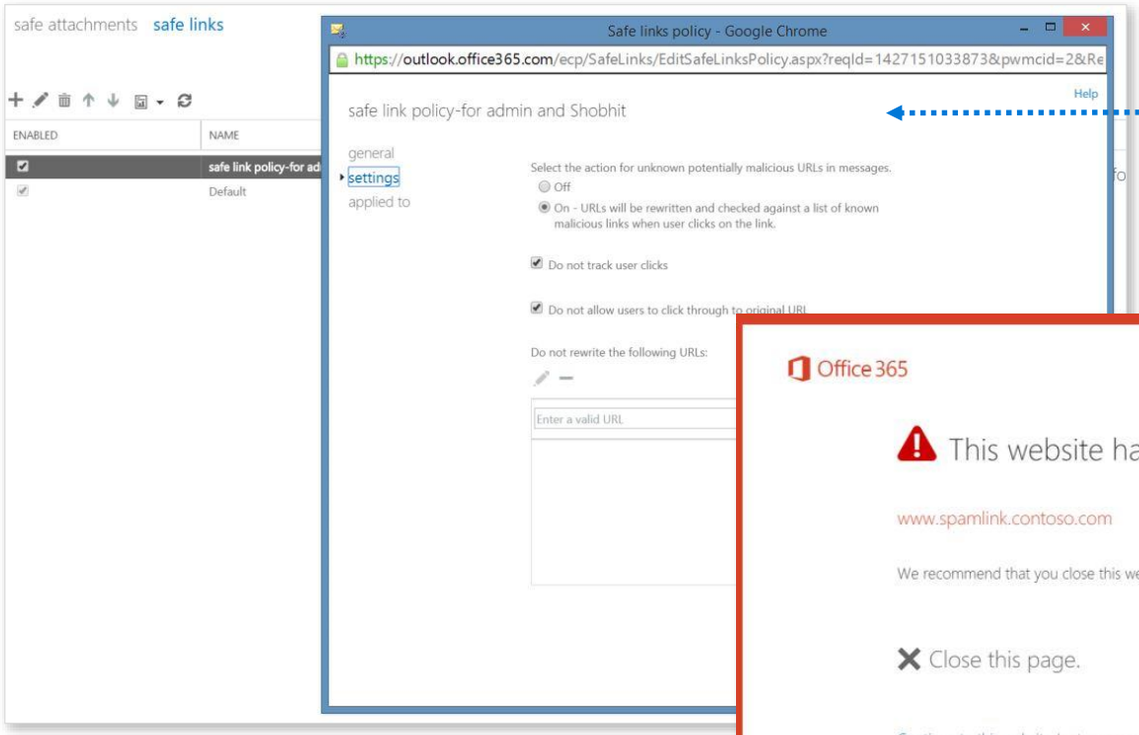


Safe Attachments (Безопасные вложения) — использование



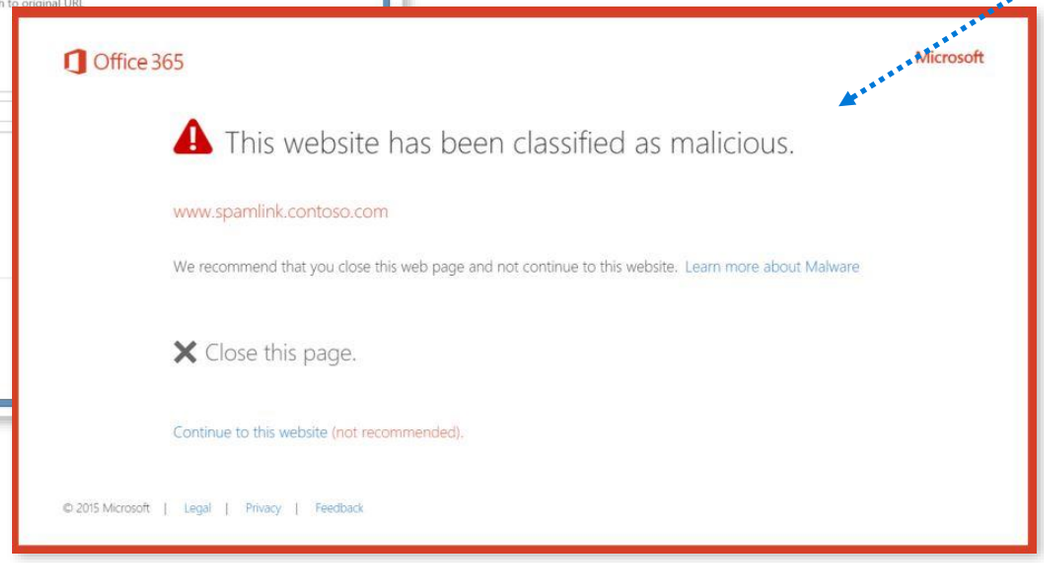


Safe Links (Безопасные ссылки) — использование



Администратор создает политику

Пользователи получают уведомление, если в электронном сообщении была нажата вредоносная ссылка



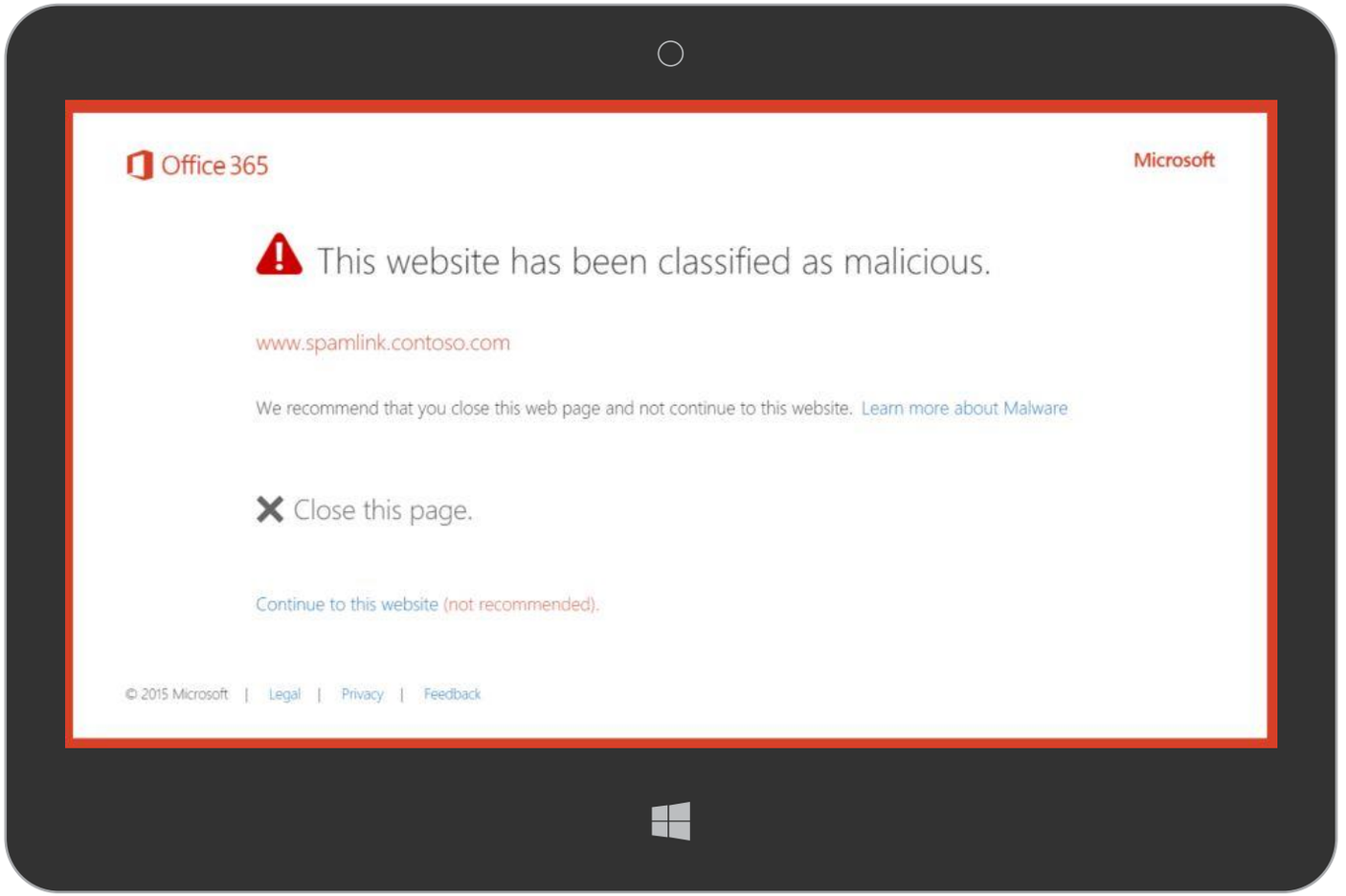
Office 365 ATP подводя итог

Защита от вредоносных URL-адресов в момент перехода по ссылке

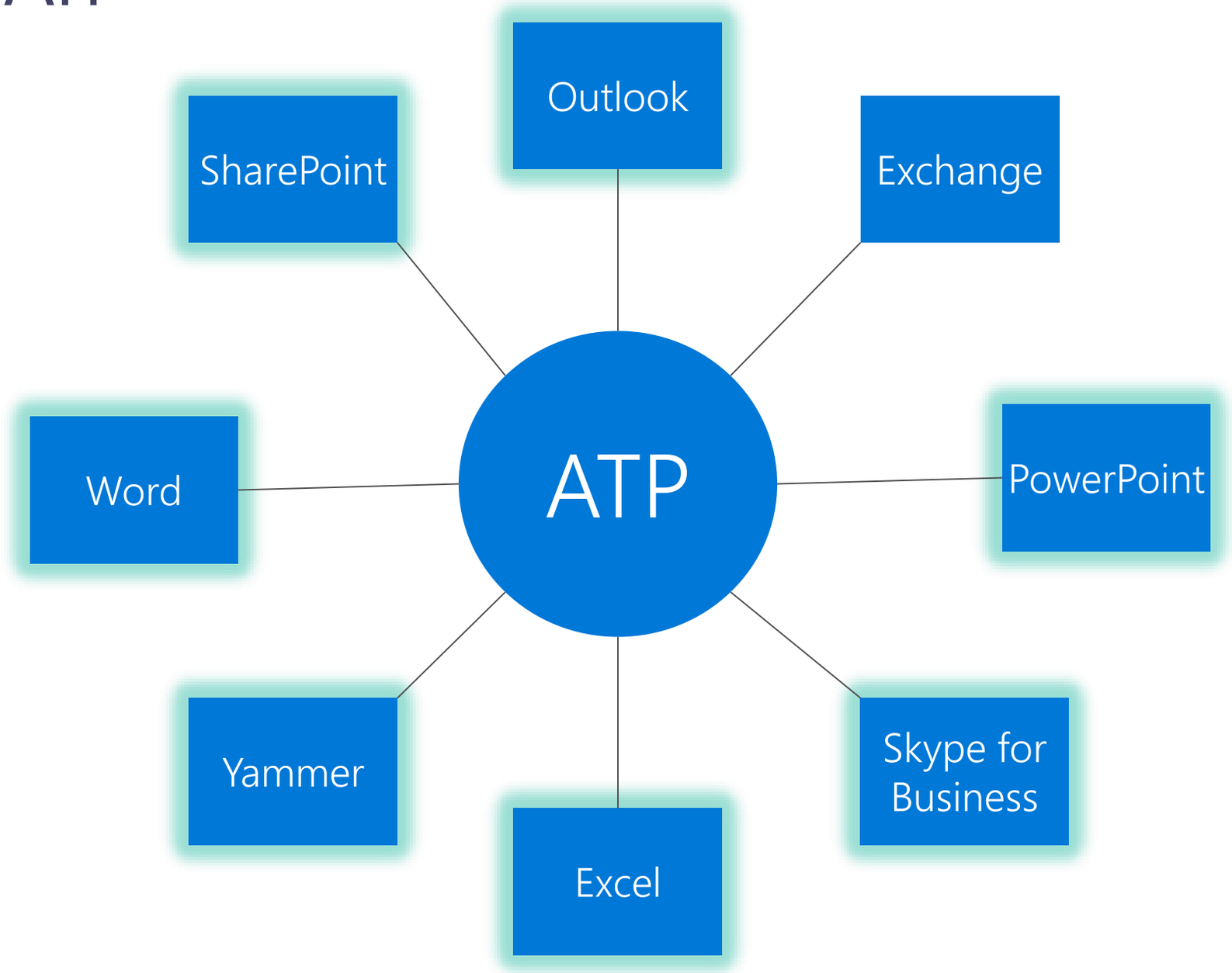
Проверка репутации URL-адресов с блокированием загрузки подозрительных вложений.

Защита от угроз «нулевого дня», исходящих от вредоносных вложений

Вложения с неизвестными вирусными сигнатурами направляются в особую безопасную среду, где выполняется анализ их поведения.



Развитие ATP

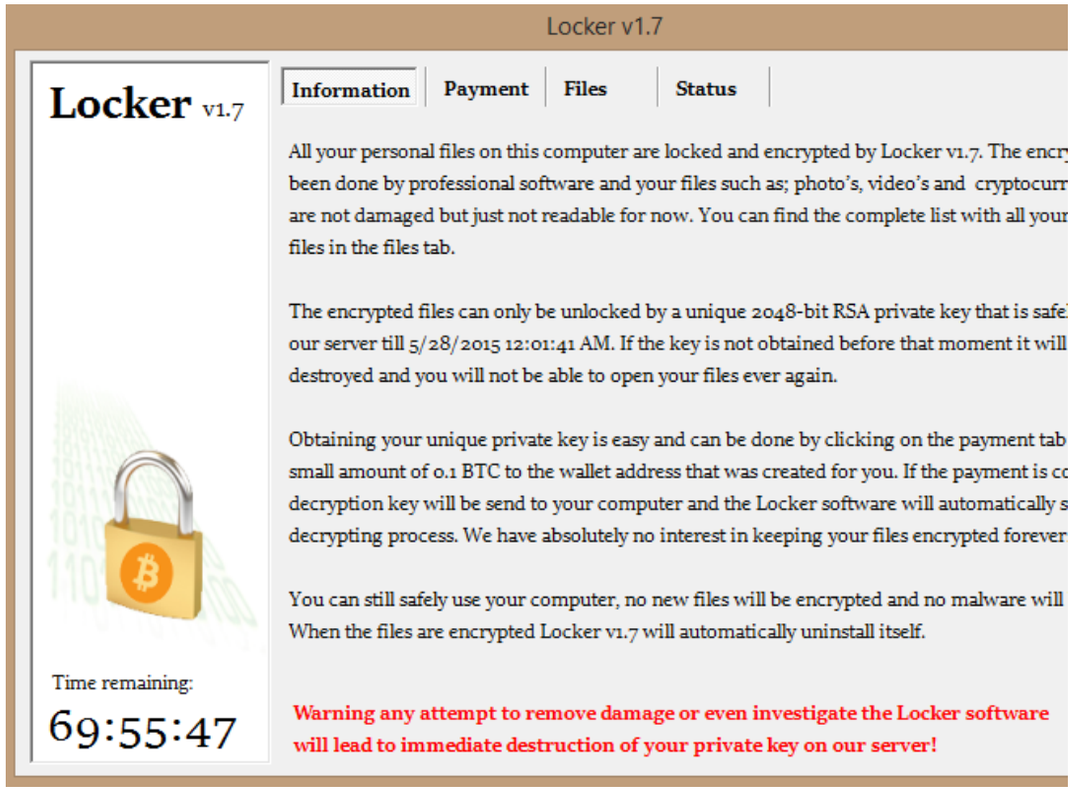


Безопасность

Как защититься от троянов-вымогателей с помощью Windows 10 Корпоративная

ТИПЫ RANSOMWARE

LOCKER RANSOMWARE



- БЛОКИРУЕТ СИСТЕМУ
- ФИШИНГОВАЯ АТАКА
- ОПЛАТА ПО ВАУЧЕРУ

CRYPTO RANSOMWARE

- ЗАШИФРОВЫВАЕТ ФАЙЛЫ
- ПОДДЕРЖИВАЕТ TOR
- ОПЛАТА БИТКОИНАМИ

КАК ЗАЩИТИТЬ СВОЙ БИЗНЕС С ПОМОЩЬЮ ВСТРОЕННЫХ СРЕДСТВ В WINDOWS 10?

- Безопасная работа в браузере MS Edge **с Smart Screen и Windows Defender Application Guard**
- Создание белых списков приложений с **Device Guard и AppLocker**
- Облачный антивирус **Windows Defender**
- Облачный сервис по выявлению сложных таргетированных угроз на клиентских ПК – **Windows Defender Advanced Threat Protection**
- Безопасность вложений на почтовых клиентах – **Office 365 ATP**

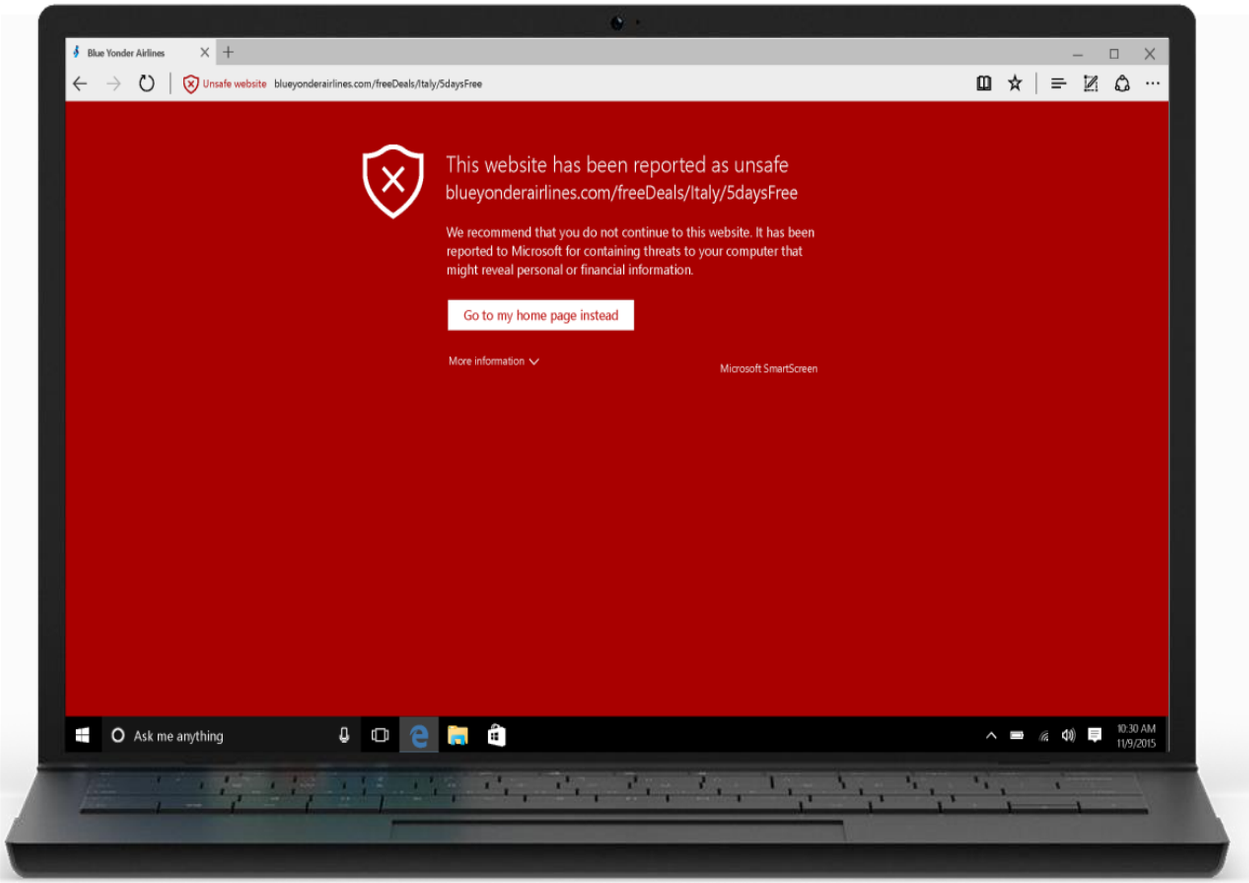
ПЕРВЫЙ ЭТАП ЗАЩИТЫ ОТ УГРОЗ

Microsoft SmartScreen – защита браузера

- Технология фильтрации вредоносного ПО для Microsoft Edge и Internet Explorer 11 в Windows 10
- Блокирует 97% атак

Защита электронной почты с Office 365 ATP

- Расширение для анализа и фильтрации вложений электронной почты
- Технология трассировки URL-адресов исследует потенциально опасные ссылки.

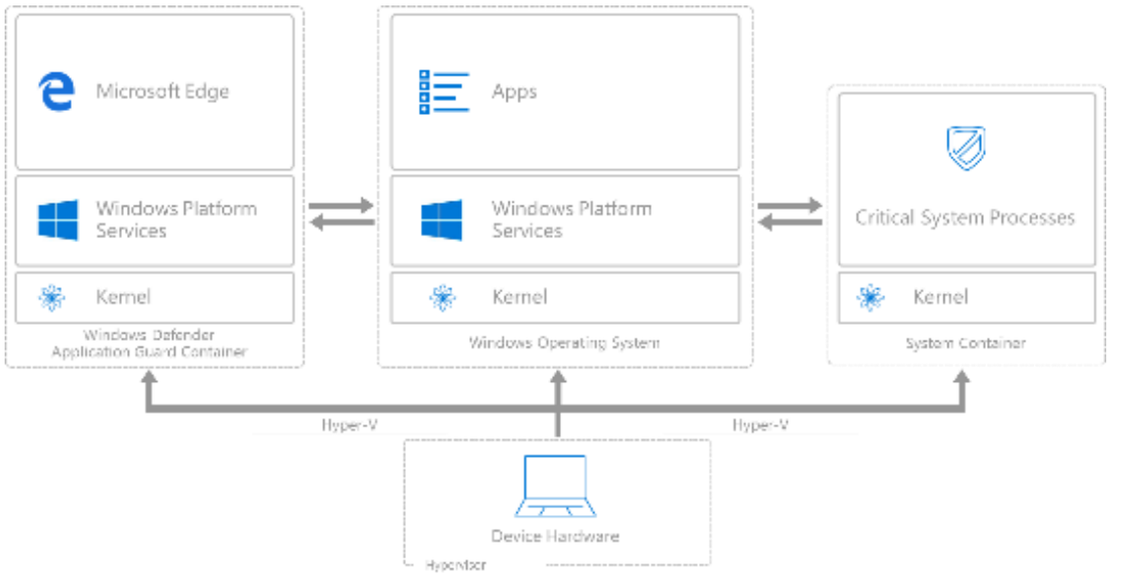


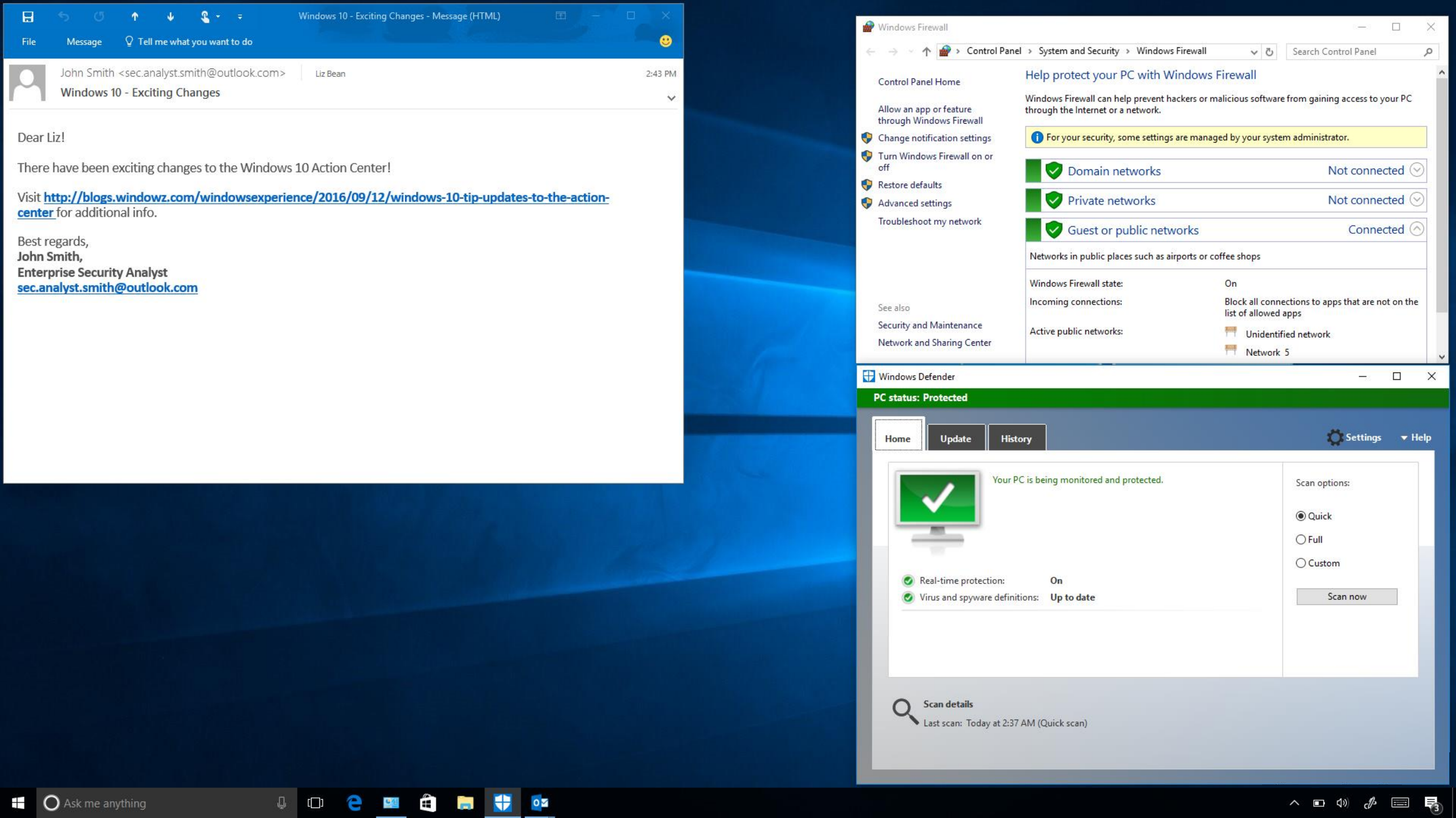
Windows Defender Application Guard

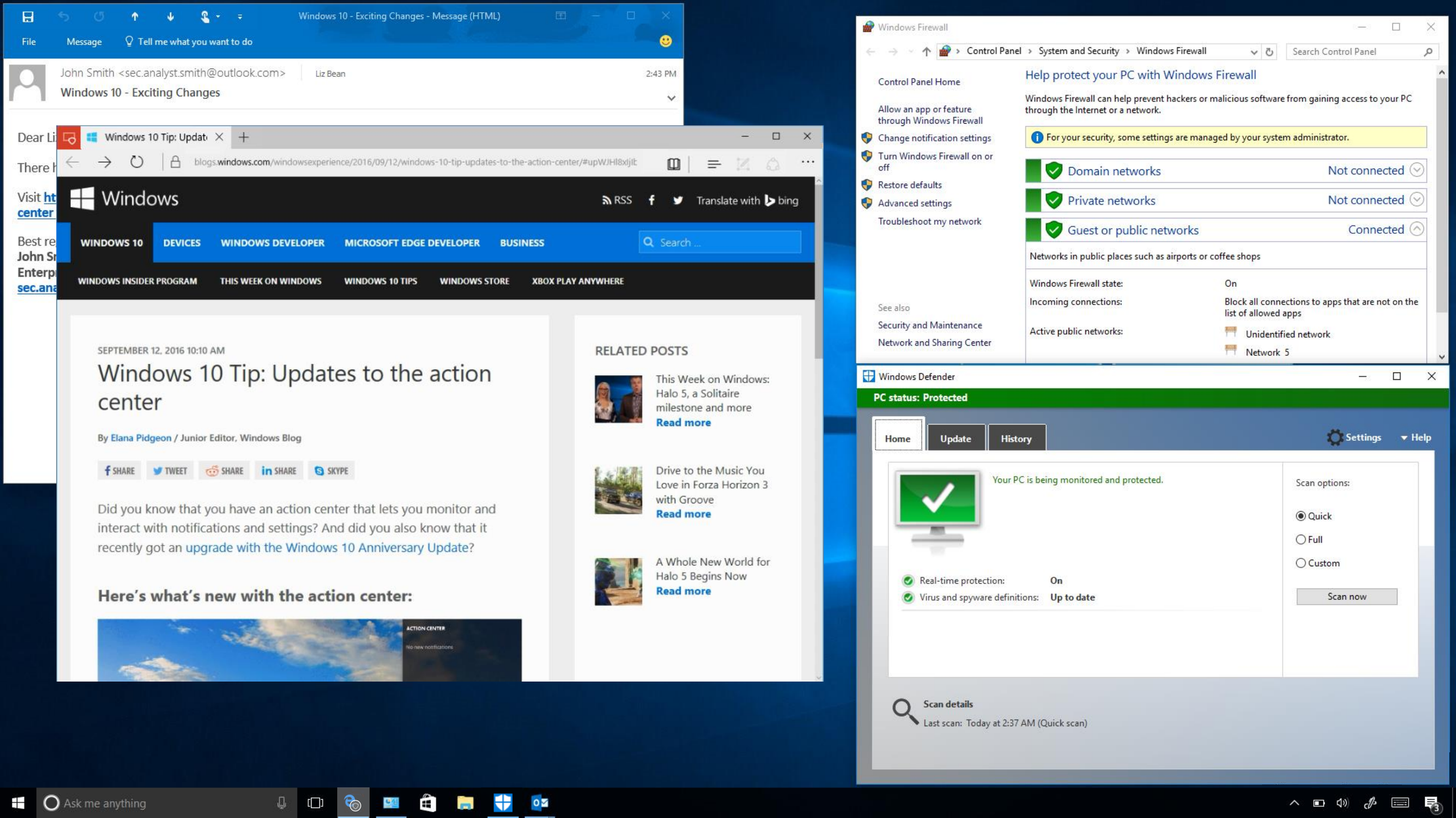
Изоляция браузера

Используется безопасность на основе виртуализации для изоляции Microsoft Edge, защищая Windows 10 от серьезных атак, вредоносных программ и использования уязвимостей, ориентированных на браузер, включая атаки «нулевого дня».

Тем самым исключая влияние на операционную систему, приложения, данные и сети




Windows 10 - Exciting Changes - Message (HTML)
File
Message
Tell me what you want to do
John Smith <sec.analyst.smith@outlook.com>
Liz Bean
2:43 PM
Windows 10 - Exciting Changes
Dear Liz!
There have been exciting changes to the Windows 10 Action Center!
Visit http://blogs.windowz.com/windowsexperience/2016/09/12/windows-10-tip-updates-to-the-action-center for additional info.
Best regards,
John Smith,
Enterprise Security Analyst
sec.analyst.smith@outlook.com
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
For your security, some settings are managed by your system administrator.
Domain networks
Not connected
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
Network 5
See also
Security and Maintenance
Network and Sharing Center
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Scan options:
Quick
Full
Custom
Real-time protection:
On
Virus and spyware definitions:
Up to date
Scan now
Scan details
Last scan: Today at 2:37 AM (Quick scan)
Ask me anything


Windows 10 - Exciting Changes - Message (HTML)
File
Message
Tell me what you want to do
John Smith <sec.analyst.smith@outlook.com>
Liz Bean
2:43 PM
Windows 10 - Exciting Changes
Windows 10 Tip: Updat
blogs.windows.com/windowsexperience/2016/09/12/windows-10-tip-updates-to-the-action-center/#upWJHl8xJjIt
Windows
RSS
Translate with bing
WINDOWS 10
DEVICES
WINDOWS DEVELOPER
MICROSOFT EDGE DEVELOPER
BUSINESS
Search ...
WINDOWS INSIDER PROGRAM
THIS WEEK ON WINDOWS
WINDOWS 10 TIPS
WINDOWS STORE
XBOX PLAY ANYWHERE
SEPTEMBER 12, 2016 10:10 AM
Windows 10 Tip: Updates to the action center
By Elana Pidgeon / Junior Editor, Windows Blog
SHARE
TWEET
SHARE
SHARE
SKYPE
Did you know that you have an action center that lets you monitor and interact with notifications and settings? And did you also know that it recently got an upgrade with the Windows 10 Anniversary Update?
Here's what's new with the action center:
ACTION CENTER
No new notifications
RELATED POSTS
This Week on Windows: Halo 5, a Solitaire milestone and more
Read more
Drive to the Music You Love in Forza Horizon 3 with Groove
Read more
A Whole New World for Halo 5 Begins Now
Read more
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
For your security, some settings are managed by your system administrator.
Domain networks
Not connected
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
Network 5
See also
Security and Maintenance
Network and Sharing Center
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Scan options:
Quick
Full
Custom
Real-time protection:
On
Virus and spyware definitions:
Up to date
Scan now
Scan details
Last scan: Today at 2:37 AM (Quick scan)
Ask me anything

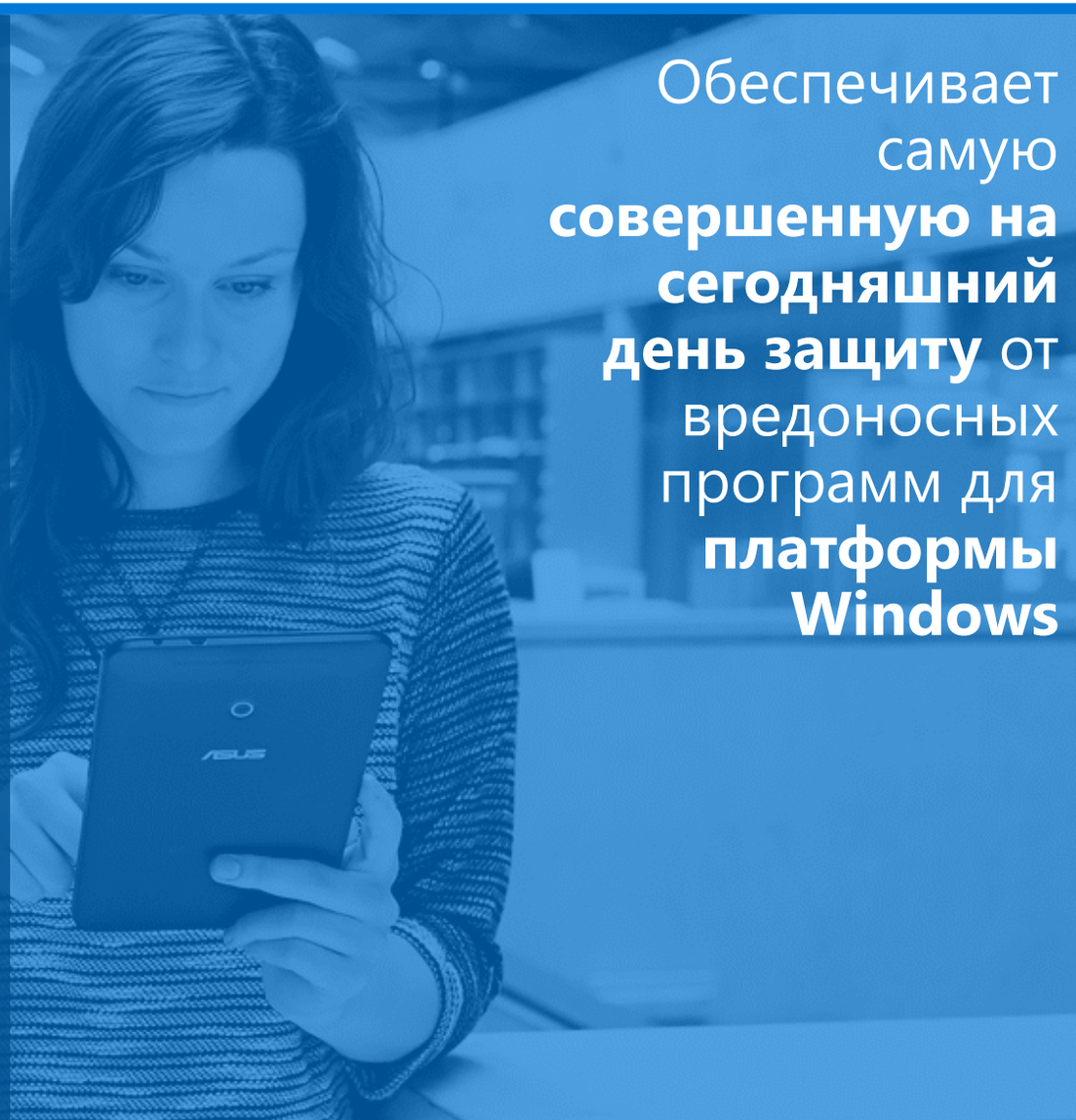
DEVICE GUARD

Аппаратный контроль приложений

Программно-аппаратный комплекс, который позволяет на настольном ПК с Windows запуск только доверенных приложений, т.е. они должны быть подписаны Microsoft

Недоверенные приложения и исполняемые файлы, включая вредоносное ПО, не будут запускаться даже под правами локального администратора

Device Guard позволяет ИТ-отделу определять надежных поставщиков ПО и приложения в своей среде. ИТ-отдел может установить в качестве доверенного подходящий набор приложений для организации, включив в него внутрикорпоративные бизнес-приложения, приложения Магазина Windows или программы конкретных поставщиков.



Обеспечивает самую **совершенную на сегодняшний день защиту** от вредоносных программ для **платформы Windows**

ЗАЩИТНИК WINDOWS - WINDOWS DEFENDER

АНТИВИРУСНАЯ ЗАЩИТА

Защита, превосходящая аналоги
Доля обнаружения 98,1 % (тест AV Comparatives: сравнение с главными конкурентами, март 2016 г.).

Обнаружение вредоносного ПО на основе анализа поведения с использованием облачных возможностей
Позволяет обнаруживать быстро меняющиеся разновидности вредоносного ПО с помощью мониторинга поведения и облачной защиты, ускоряющей доставку сигнатур

Защита от взлома
Доверенная загрузка Windows и изоляция платформы позволяют обезопасить Защитника Windows и обеспечивают самовосстановление

Встроенная в Windows
Не требуется дополнительное развертывание и изменение инфраструктуры — защита обновляется автоматически, что снижает затраты

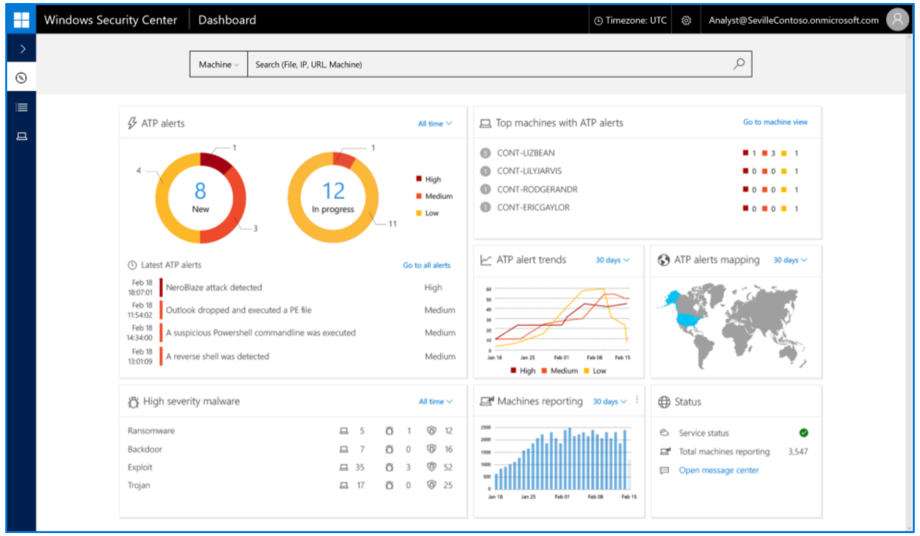
WINDOWS DEFENDER ADVANCED THREAT PROTECTION

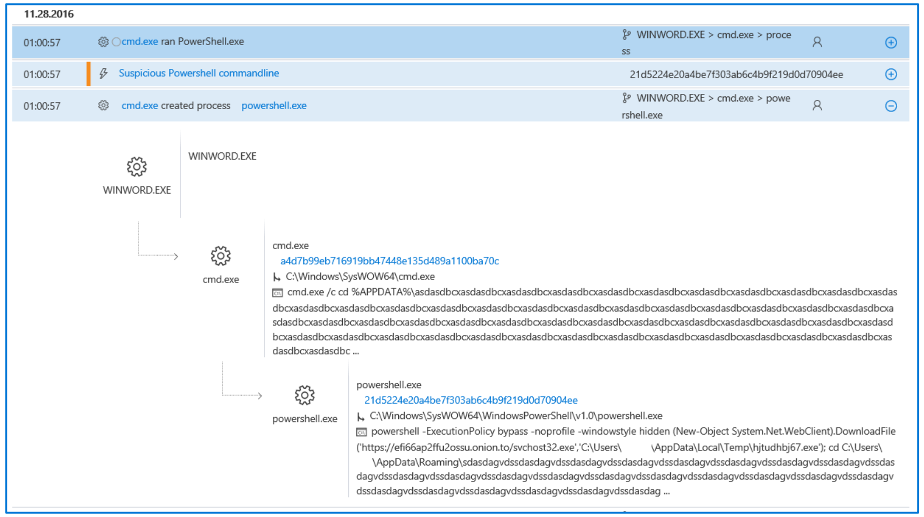
Агент встроен в Windows 10 1607
Не требуется дополнительное развертывание и изменение инфраструктуры.

Облачное обнаружение уязвимостей на основе анализа поведения
Оповещения об известных и неизвестных угрозах, соотнесенные с различными факторами. Оперативные и исторические данные.

Расследование на большом временном отрезке
Наглядное представление о масштабе уязвимости.
Сводки данных по различным конечным точкам.
Подробная аналитика файлов и URL-адресов.

Уникальная база знаний аналитики угроз
Отслеживание угроз для получения сведений о злоумышленниках.
Собственные и сторонние аналитические данные по угрозам.





РЕЗЮМИРУЯ

КАК ЗАЩИТИТЬ СВОЙ БИЗНЕС

- **Многофакторная идентификация** (Multi-factor authentication - MFA) – сервис, позволяющий блокировать доступ злоумышленников к чувствительным данным организации или бизнес системам, даже в случае получения логинов и паролей сотрудников вашей компании.
- **Exchange ATP (Advanced Treat Protection)** – анализирует почтовые вложения или интернет-ссылки и своевременно реагирует на выявленные атаки
- Использование встроенного функционала безопасности в **Windows 10 Enterprise**
    - Безопасная работа в браузере MS Edge **с Smart Screen и Windows Defender Application Guard**
    - Создание белых списков приложений с **Device Guard и AppLocker**
    - Облачный антивирус **Windows Defender**
    - Облачный сервис по выявлению сложных таргетированных угроз на клиентских ПК – **Windows Defender Advanced Threat Protection**

Microsoft

Ваши вопросы?

cs
iT