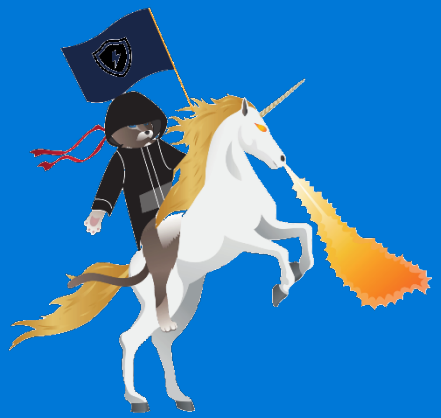
Windows Defender ATP

Улан Каражигитов,
Руководитель направления
Microsoft 365



Windows

Microsoft

Accelerate GDPR compliance with the Microsoft Cloud

Ulan Karazhigitov
Daria Brashkina

This presentation is intended to provide an overview of GDPR and is not a definitive statement of the law.

Providing clarity and consistency for the protection of personal data

The **General Data Protection Regulation** (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights

What are the key changes to address the GDPR?

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations are required to:

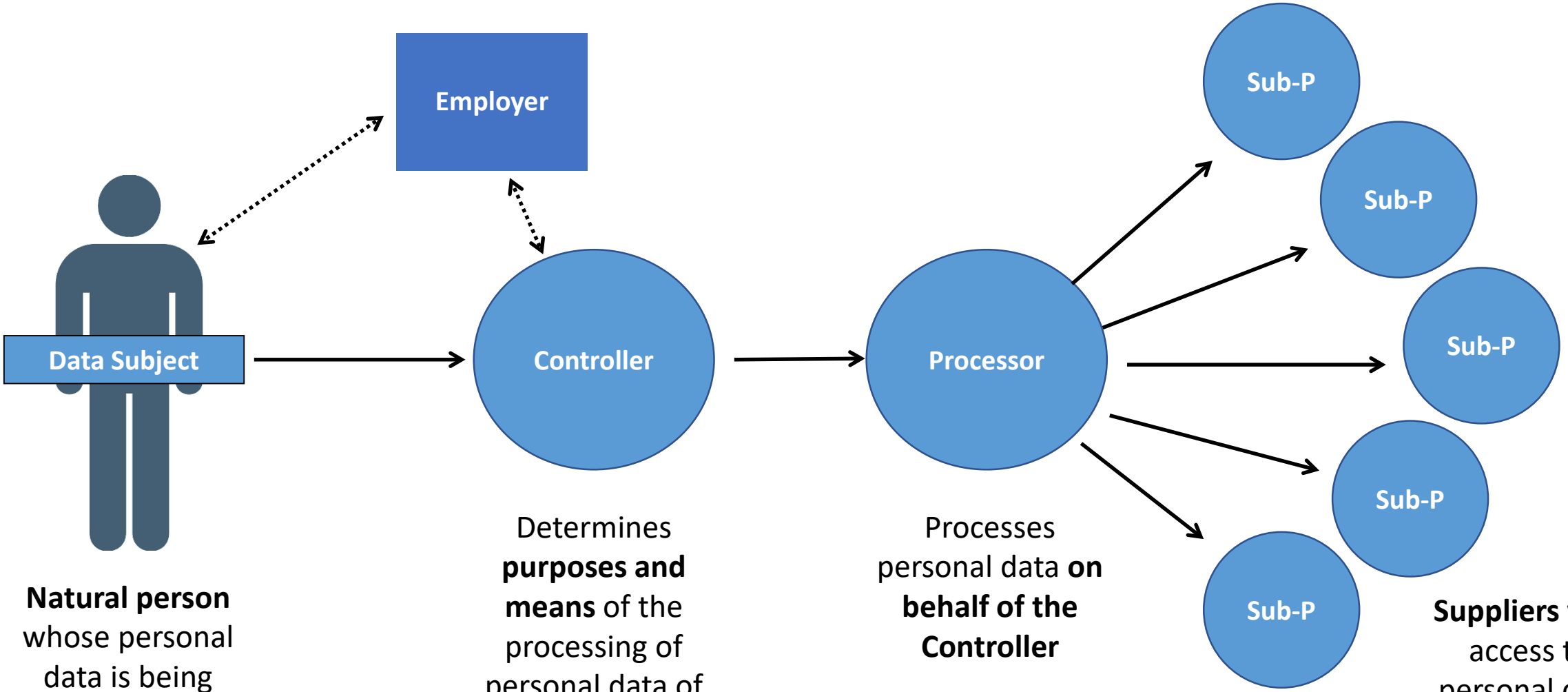
- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

Who's Who Under GDPR



Natural person whose personal data is being processed

Determines **purposes and means** of the processing of personal data of the Data Subject

Processes personal data **on behalf of the Controller**

Suppliers with access to personal data through Processor

Extraterritorial Jurisdiction

GDPR applies to processing of personal data either:

In the context of an "establishment" in the EU:

- An establishment can be a branch or subsidiary;
- Processing need not be in EU
- Minimal nexus can trigger application

In relation to either the (i) "offering of goods or services" to "data subjects" in the EU, or (ii) "monitoring" the behavior of data subjects in the EU

- Can apply even if the entity has no presence in the EU;

In case of GDPR non-compliance:

Failure to comply with GDPR may result in fines applied EU Commission :

- **10 000 000 EUR or 2%** of the total worldwide annual **turnover** of the preceding financial year (whichever is higher)
- **20 000 000 EUR or 4%** of the total worldwide annual **turnover** of the preceding financial year (whichever is higher)

Общий Регламент по защите персональных данных (GDPR)

(49) Обработка персональных данных органами государственной власти, центрами реагирования на компьютерные чрезвычайные происшествия (CERTs), центрами реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs), поставщиками сетей электронных коммуникаций и услуг, а также поставщиками технологий и услуг по обеспечению безопасности является законным интересом соответствующего контролёра данных в той мере, в какой она необходима и соразмерна а целям обеспечения сетевой и информационной безопасности, то есть способности сети или информационной системы противостоять, на заданном уровне достоверности, случайным событиям, незаконным или преднамеренным действиям, которые компрометируют доступность, подлинность, целостность и конфиденциальность сохранённых или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Такой законный интерес может включать в себя, к примеру, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространение вредоносного кода, а также пресечение сетевых атак и угроз для компьютерных и электронных систем связи.

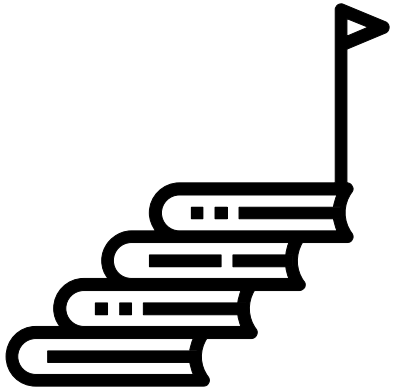
Общий Регламент по защите персональных данных (GDPR)

(83) Для того чтобы обеспечить безопасность и предотвратить обработку в нарушение настоящего Регламента, контролёр или обработчик должны оценить риски, связанные с обработкой, и использовать меры по снижению этих рисков, такие как криптографическая защита. Такие меры должны обеспечить соответствующий уровень защиты, в том числе конфиденциальности, принимая во внимание уровень развития техники и расходов на применение в отношении рисков, а также характер подлежащих защите персональных данных. При оценке риска для защиты данных необходимо уделить внимание рискам, имеющим место при обработке персональных данных, например, случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или несанкционированному доступу к пересональным данным, сохранённым или иным образом обрабатываемым данным, которые могут привести к физическому, материальным или нематериальным потерям.

Общий Регламент по защите персональных данных (GDPR)

(85) Утечка персональных данных, если она надлежащим образом и своевременно не была устранена, может привести к физическому, материальному или нематериальному ущербу для физических лиц, таким как утрата контроля над персональными данными или ограничение их прав, дискриминация, кража идентификационных данных или мошенничество с персональными данными, финансовые потери, несанкционированный отказ от псевдонимизации, ущерб репутации, нарушение конфиденциальности персональных данных, защищённых профессиональной тайной, или любые иные существенные экономические или социальные потери для соответствующих физических лиц. Поэтому, как только контролёру станет известно об утечке персональных данных, контролёр должен незамедлительно уведомить об утечке персональных данных надзорный орган, без неоправданной задержки и, когда это возможно, не позднее чем через 72 часа после того, как ему стало известно об этом, за исключением случаев, когда контролёр может доказать в соответствии с принципом подотчётности, что утечка персональных данных едва ли обернётся рисками для прав и свобод физических лиц. Если такое уведомление не может быть сделано в течение 72 часов, причины задержки должны быть указаны в уведомлении, а информация может предоставляться поэтапно без неоправданной дальнейшей задержки.

Preparing for the GDPR



Simplify your privacy journey

Elevate your privacy practices with our cloud

Uncover risk & take action

Use our solutions to expose areas of risk and respond with agility and confidence

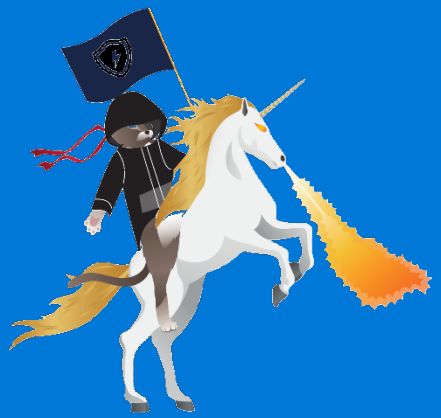
Leverage guidance from experts

Use our partner network to help you meet your privacy, security, and compliance goals


Threat Intelligence
Data Loss Prevention
Intune
Active Directory
Office
eDiscovery
Security Center
EMS
Data Log
Audit Logs
Microsoft Azure
Cloud App Security
Key Vault
SOLUTIONS TO HELP YOU
PREPARE FOR THE GDPR
Data Classification
Dynamics
Data models
Threat Detection
Advanced Threat Protection
SQL
Windows Server
Windows
Information Protection
Analytics
Windows Hello
Transparent Data Encryption
Always Encrypted

Windows Defender ATP

Улан Каражигитов,
Руководитель направления
Microsoft 365

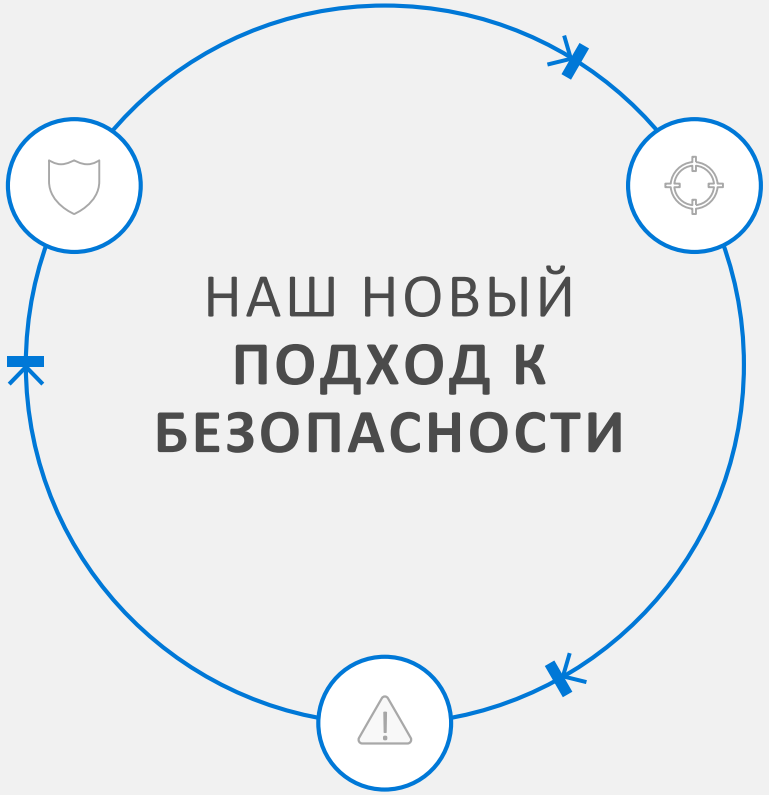


Windows

Подход Майкрософт к безопасности

ЗАЩИТА

всех конечных точек — от датчиков до центра обработки данных



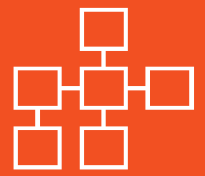
ОБНАРУЖЕНИЕ

на основе целевых событий, контроля поведения и машинного обучения

РЕАГИРОВАНИЕ

для быстрого перехода от обнаружения к действию

Уникальность положения Майкрософт на рынке



Более 1 млн компьютеров корпорации Майкрософт

Сотни лабораторий, сообществ по борьбе с вредоносным ПО

1,2 млрд устройств с Windows, отправляющих отчеты

Ежедневный анализ 1 млн файлов

11 млн корпоративных компьютеров, отправляющих отчеты

2,5 трлн индексируемых URL-адресов и 600 млн запросов репутации

Функции безопасности **Windows 7**

Защита устройств

- Центр обновления Windows
- Доверенный платформенный модуль (TPM)

Защита от угроз

- Брандмауэр Windows
- Технология SmartScreen

Защита учетных данных

Защита данных

- BitLocker Admin and Monitoring
- Технология BitLocker
- BitLocker to Go

Обнаружение нарушения безопасности: расследование и реагирование

ДО АТАКИ → ПОСЛЕ АТАКИ

Windows 10: безопасность на современных устройствах

Безопасность на основе виртуализации

Защита устройств

- Безопасная загрузка UEFI
- Доверенная загрузка Windows
- Центр обновления Windows
- Доверенный платформенный модуль (TPM)

Защита от угроз

- Device Guard
- Windows Defender Application Guard для Microsoft Edge
- Microsoft Edge
- Защитник Windows
- Брандмауэр Windows
- Технология SmartScreen

Защита учетных данных

- Credential Guard
- Устройства-компаньоны Windows Hello
- Windows Hello

Защита данных

- Шифрование устройства
- Windows Information Protection
- BitLocker Admin and Monitoring
- Технология BitLocker
- BitLocker to Go

Обнаружение нарушения безопасности: расследование и реагирование

- Управление безопасностью[2]
- Условный доступ
- Служба Advanced Threat Protection в Защитнике Windows

ДО АТАКИ → ПОСЛЕ АТАКИ

Advanced Threat Protection в Защитнике Windows

Advanced Threat Protection в Защитнике Windows

помогает корпоративным клиентам обнаруживать сложные атаки и уязвимости данных и исправлять их последствия

Динамические датчики и средства ведения журналов на стороне клиента, регистрирующие **поведение на конечных точках**, работают **совместно** с имеющимися технологиями для защиты конечных точек

Облачная **аналитика с машинным обучением** обрабатывает данные с самого большого числа датчиков в мире

Ценность данных выше благодаря **сообществу** наших **«охотников на угрозы»** и **исследователей**, а также **аналитике угроз**

Встроено в Windows 10

Windows Defender Advanced Threat Protection

Выявляет и устраняет передовые кибер-атаки

Встроен в Windows 10

Не требует дополнительного развертывания
Всегда обновлен, снижает затраты

Поведенческий анализ, машинное обучение

Сигналы по известным и неизвестным угрозам
Работа с текущими и историческими данными

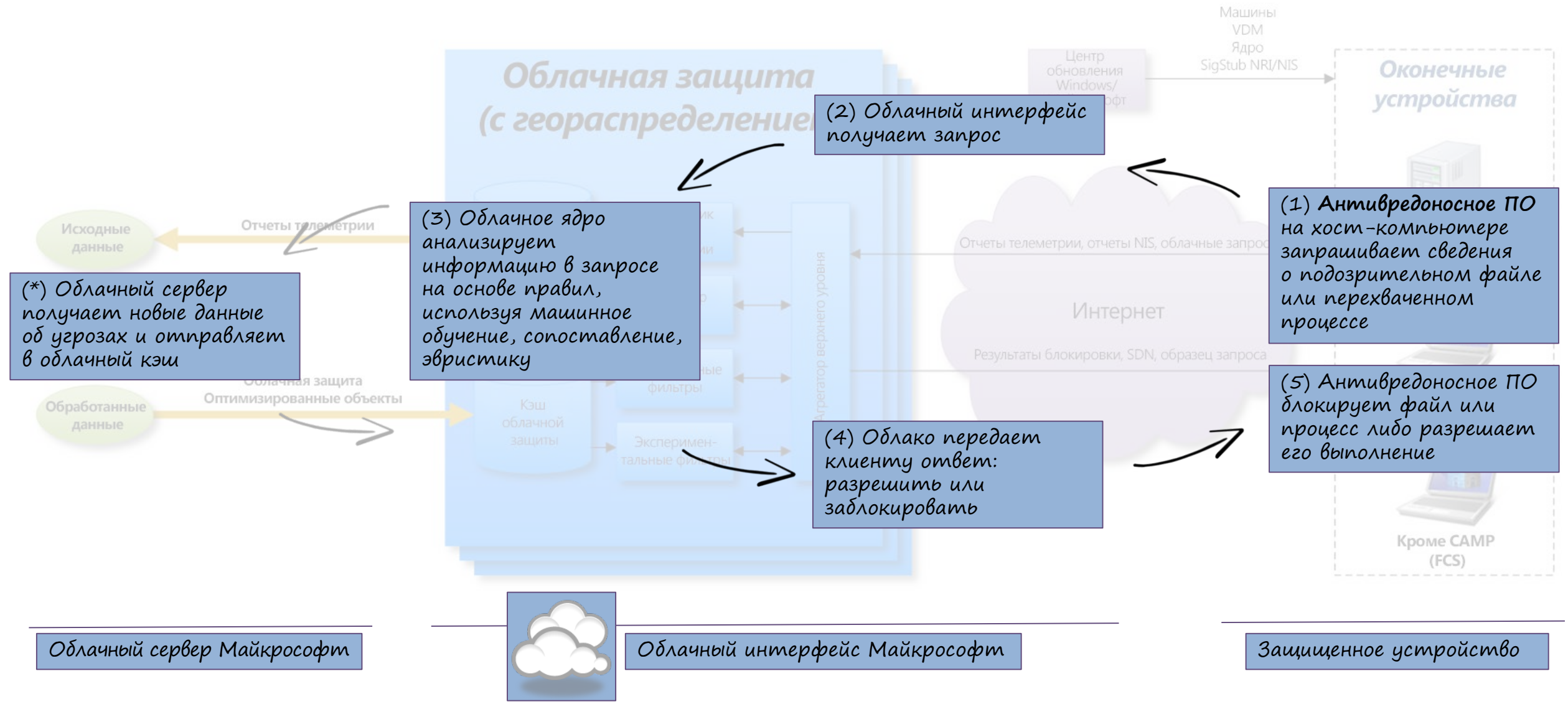
Больше времени для расследования

Легко понять масштабы нарушений. Данные собирается с конечных ПК. Глубокий анализ файлов и URL.

Уникальная база знаний кибер-угроз

Ucоставление профиля атаки с учетом данных из множества источников. Использование как собственных, так и данных от партнеров

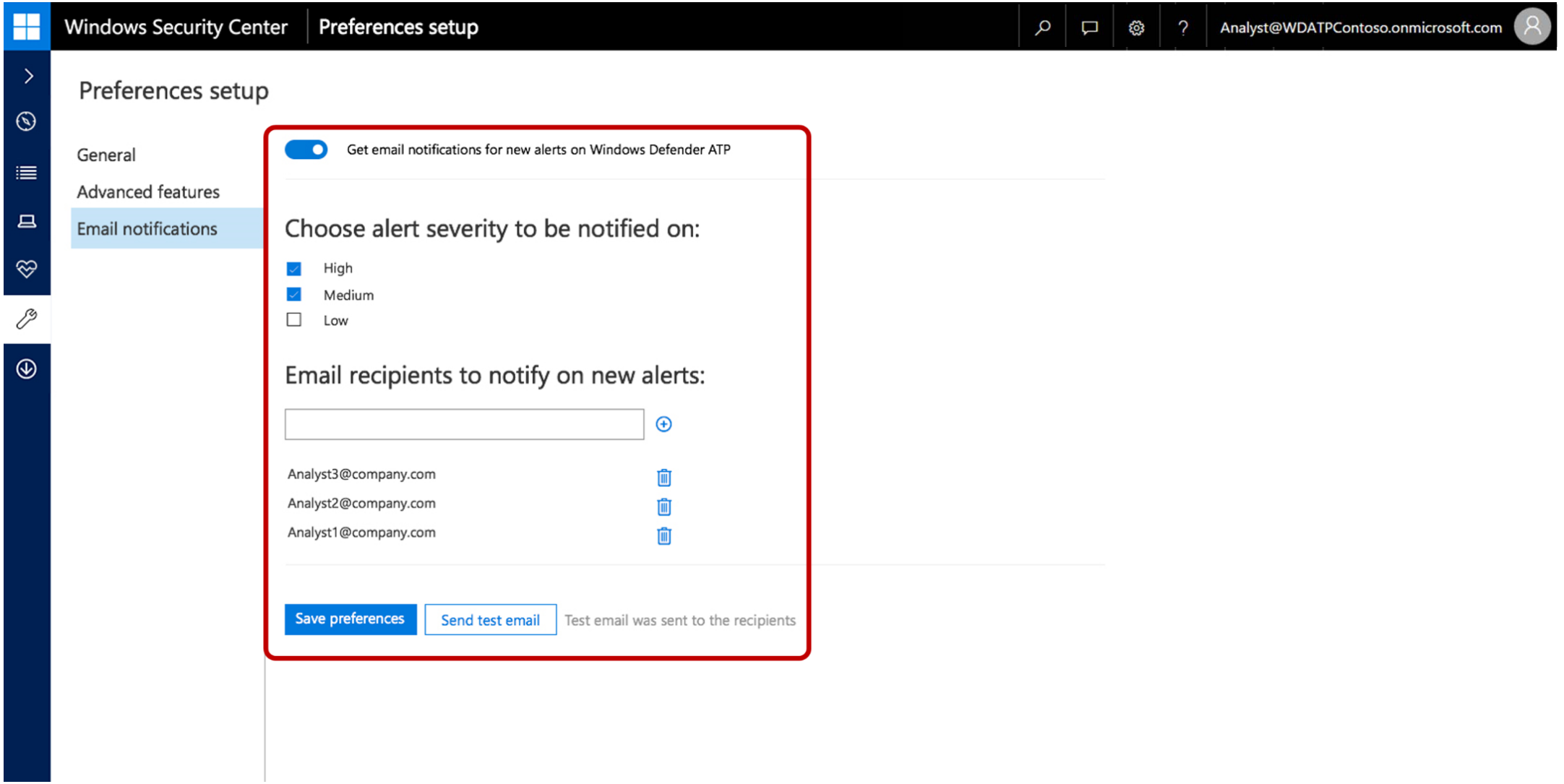
Облачная защита: расширяемая система классификации и реагирования в реальном времени



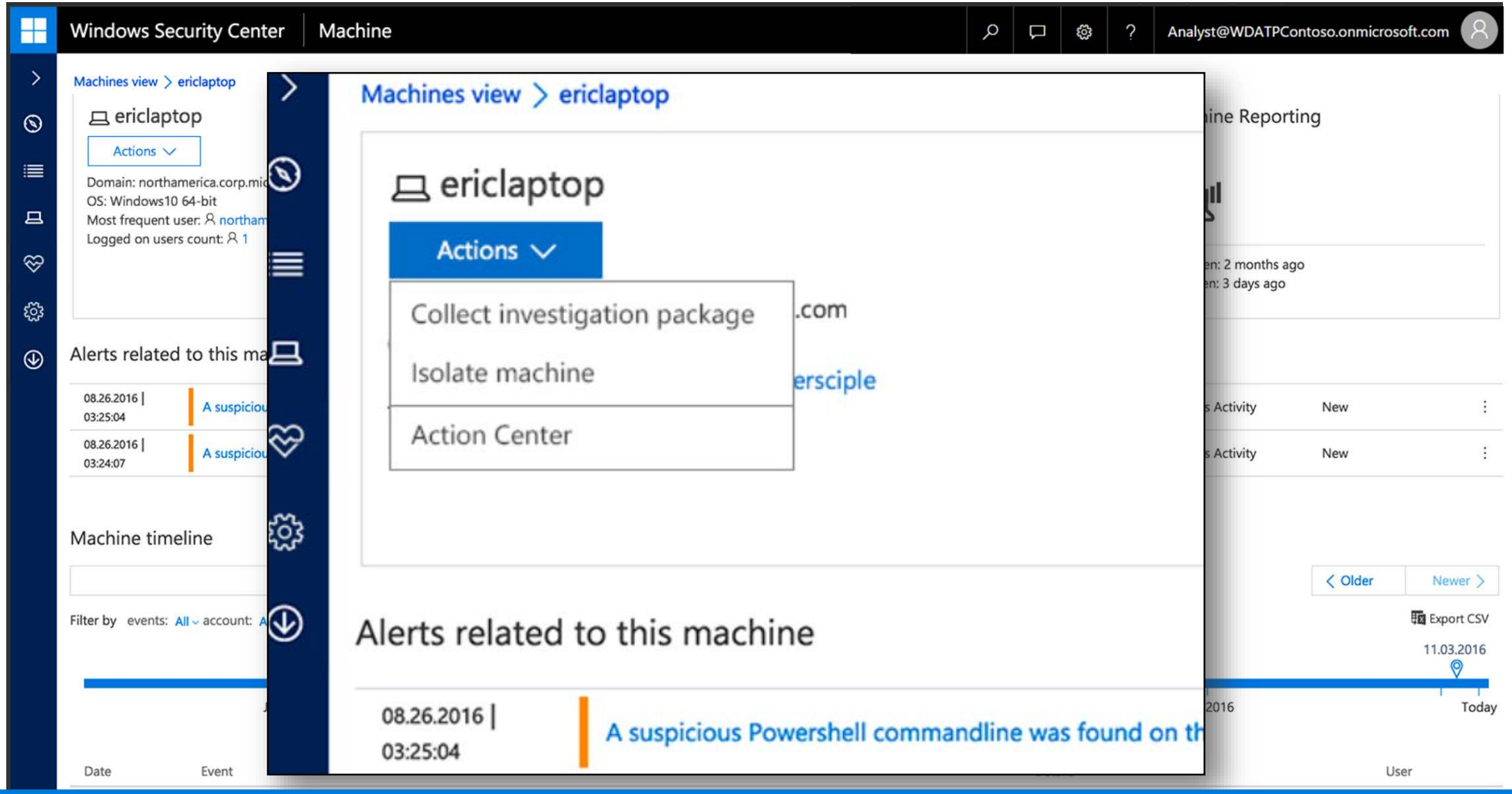
Demo screens

Windows

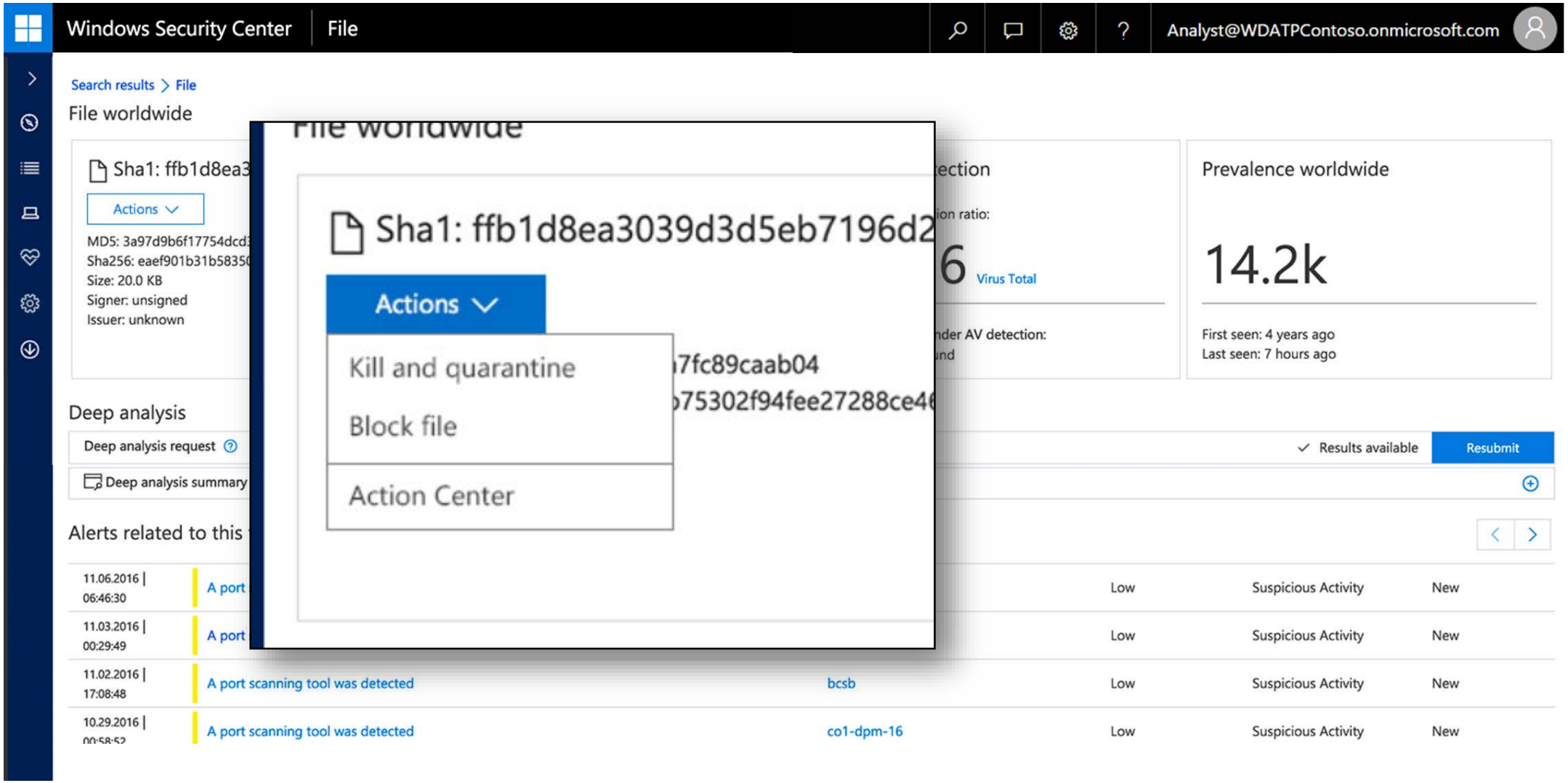
EMAIL NOTIFICATION



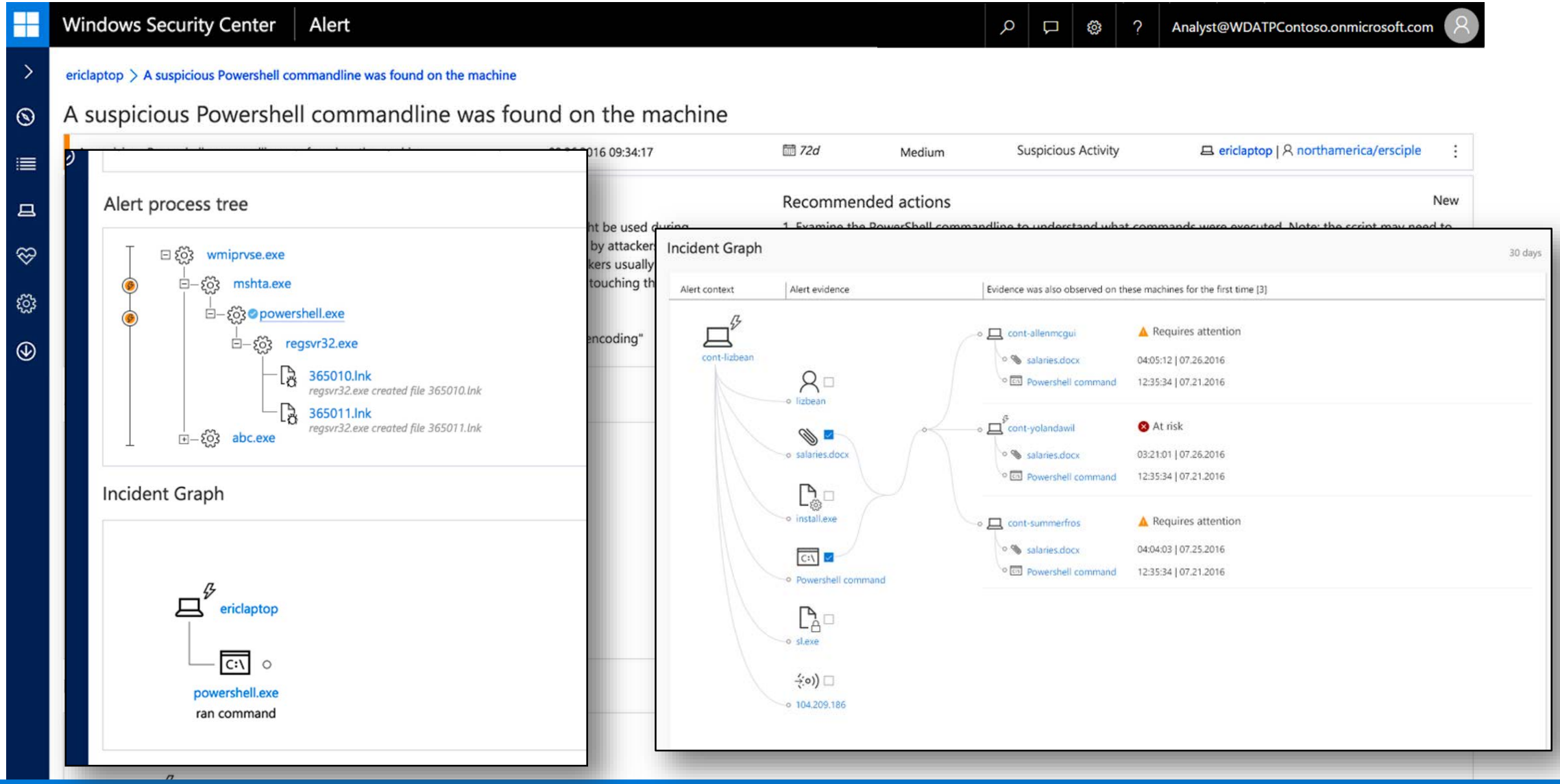
MACHINE LEVEL RESPONSE



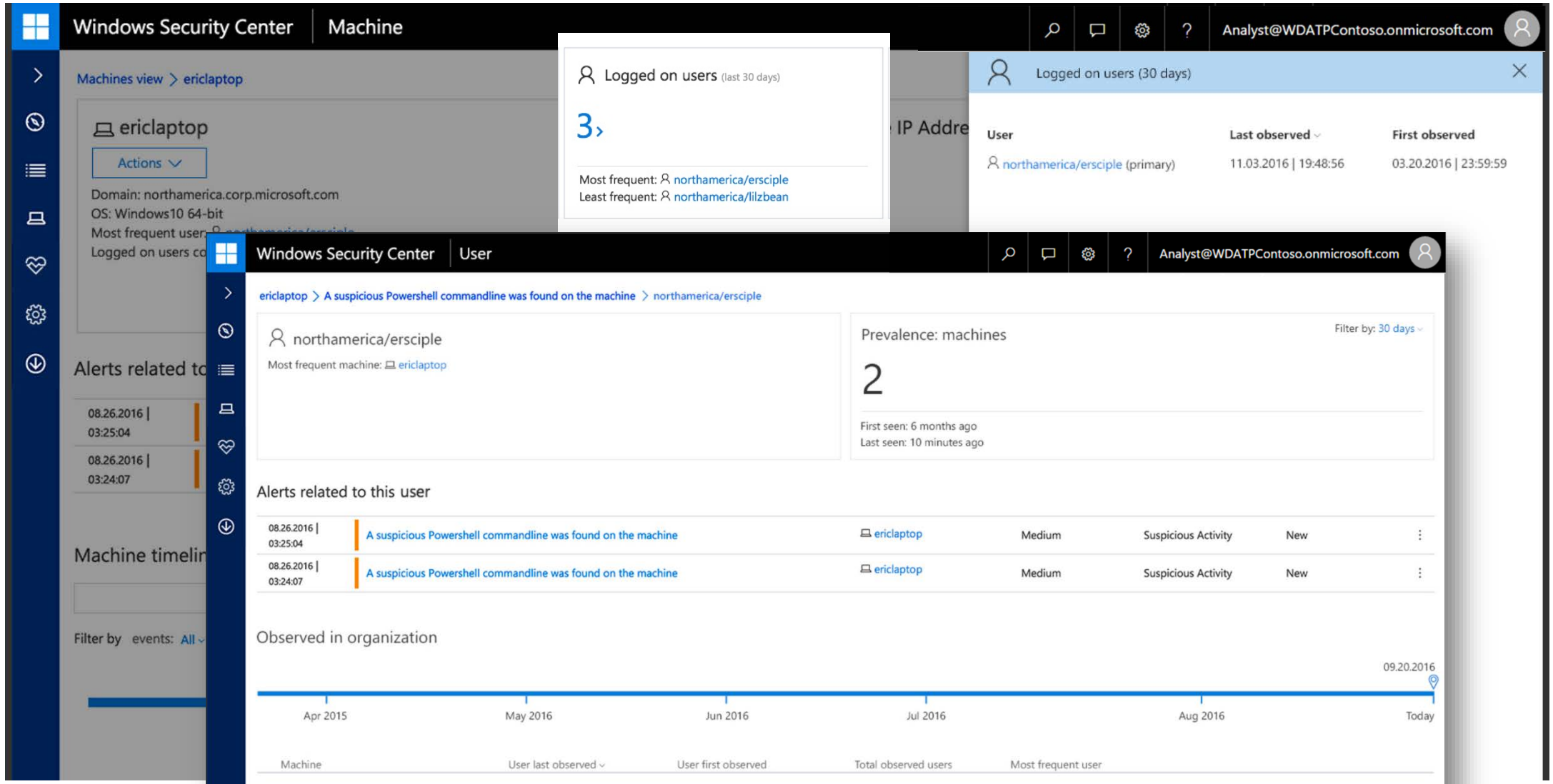
FILE LEVEL RESPONSE



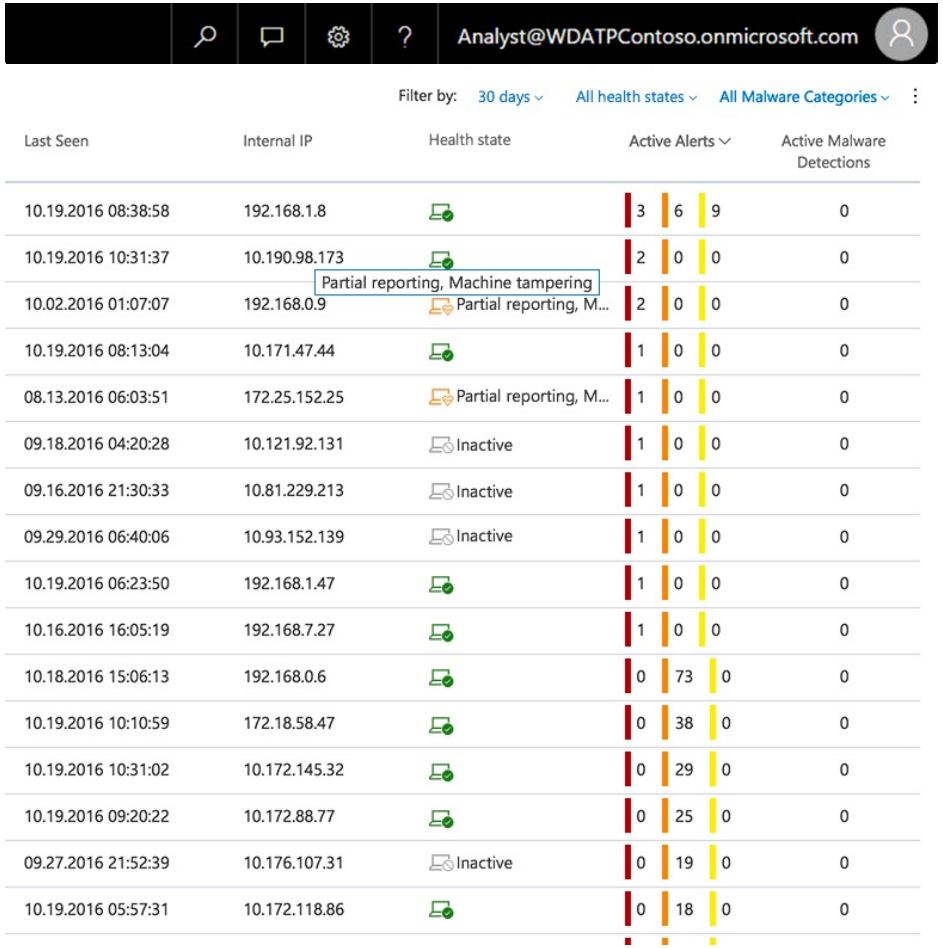
ENHANCED ALERTS VISUALIZATION

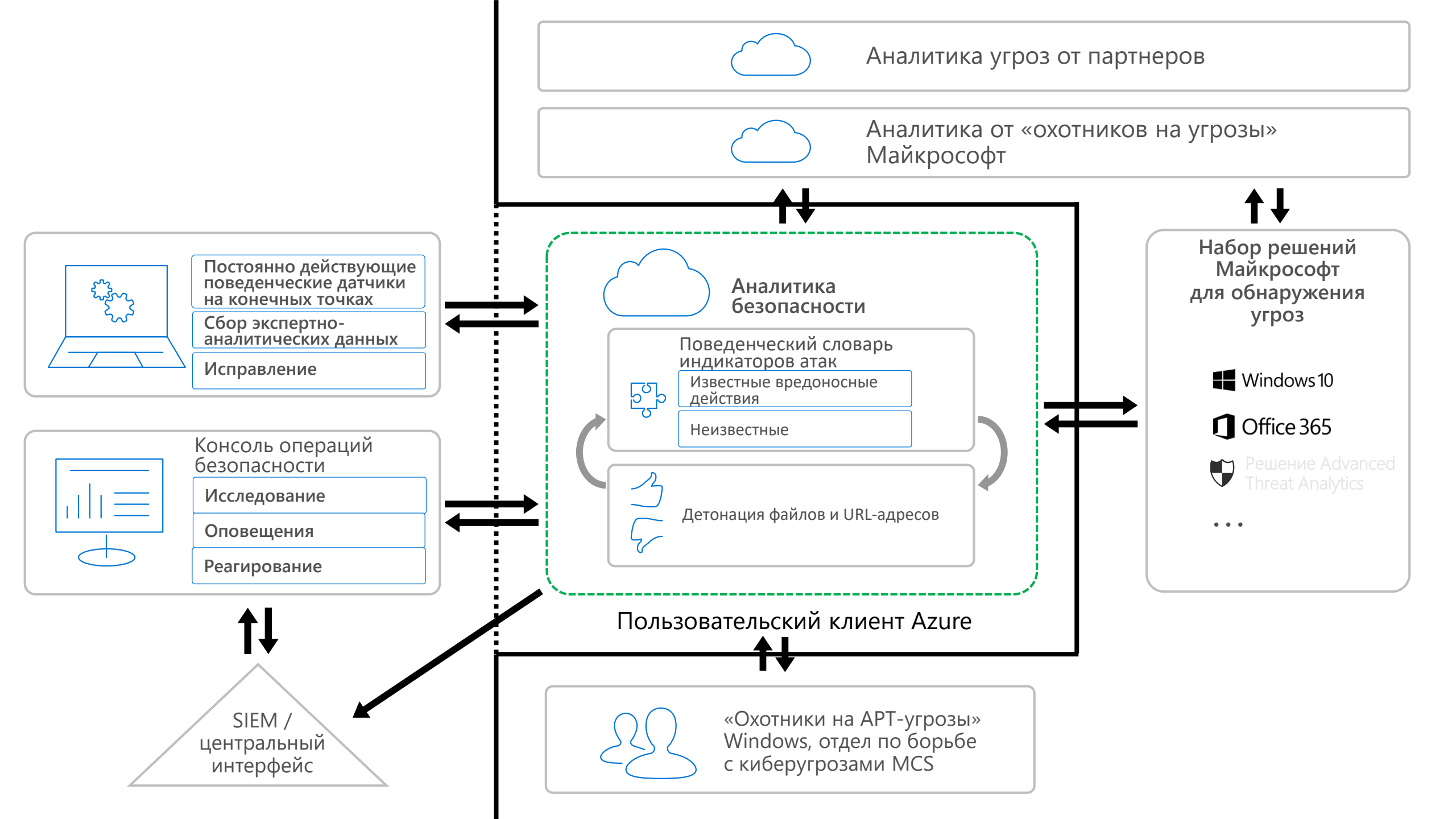


USER ENTITY


Windows Security Center
Machine
Analyst@WDATPContoso.onmicrosoft.com
Machines view > ericlaptop
ericlaptop
Actions
Domain: northamerica.corp.microsoft.com
OS: Windows10 64-bit
Most frequent user:
Logged on users co
Alerts related to
08.26.2016 | 03:25:04
08.26.2016 | 03:24:07
Machine timelin
Filter by events: All
Logged on users (last 30 days)
3
Most frequent: northamerica/ersciple
Least frequent: northamerica/lilzbean
IP Addre
Logged on users (30 days)
User
Last observed
First observed
northamerica/ersciple (primary)
11.03.2016 | 19:48:56
03.20.2016 | 23:59:59
Windows Security Center
User
Analyst@WDATPContoso.onmicrosoft.com
ericlaptop > A suspicious Powershell commandline was found on the machine > northamerica/ersciple
northamerica/ersciple
Most frequent machine: ericlaptop
Prevalence: machines
Filter by: 30 days
2
First seen: 6 months ago
Last seen: 10 minutes ago
Alerts related to this user
08.26.2016 | 03:25:04
A suspicious Powershell commandline was found on the machine
ericlaptop
Medium
Suspicious Activity
New
08.26.2016 | 03:24:07
A suspicious Powershell commandline was found on the machine
ericlaptop
Medium
Suspicious Activity
New
Observed in organization
09.20.2016
Apr 2015
May 2016
Jun 2016
Jul 2016
Aug 2016
Today
Machine
User last observed
User first observed
Total observed users
Most frequent user
ericlaptop
11.03.2016 | 14:20:34
06.10.2016 | 19:03:15
1
northamerica/ersciple

HEALTH REPORTING



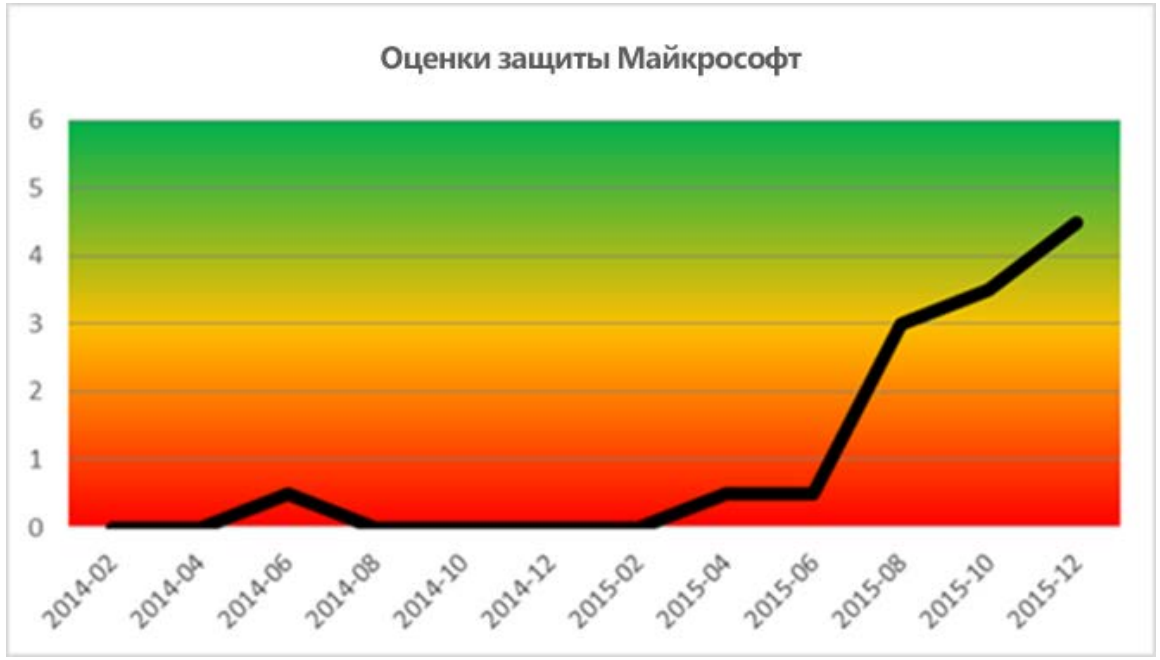

Аналитика угроз от партнеров
Аналитика от «охотников на угрозы» Майкрософт
Постоянно действующие поведенческие датчики на конечных точках
Сбор экспертно-аналитических данных
Исправление
Консоль операций безопасности
Исследование
Оповещения
Реагирование
SIEM / центральный интерфейс
Аналитика безопасности
Поведенческий словарь индикаторов атак
Известные вредоносные действия
Неизвестные
Детонация файлов и URL-адресов
Пользовательский клиент Azure
«Охотники на APT-угрозы» Windows, отдел по борьбе с киберугрозами MCS
Набор решений Майкрософт для обнаружения угроз
Windows 10
Office 365
Решение Advanced Threat Analytics
. . .

Вредоносное ПО в действии

Показатели антивирусной защиты

Windows

Мы зашли очень далеко.



- Мы смогли повысить защиту по всем фронтам
- Постоянное улучшение защиты
- Конкуренция для непрерывного совершенствования

Февраль 2015 г.

Майкрософт

Защитник Windows

В ноябре и декабре 2015 года мы непрерывно оценивали 20 домашних версий продуктов безопасности на стандартных настройках. Мы всегда использовали самые актуальные из общедоступных версий всех продуктов. Они могли обновляться в любое время и обращаться к своим облачным сервисам. Мы использовали реалистичные сценарии тестирования, предлагая справиться с реальными угрозами. Продукты должны были продемонстрировать свои возможности, используя все компоненты и уровни защиты.

	Ноябрь	Декабрь	В среднем по отрасли
Защита от атак вредоносного ПО нулевого дня, включая угрозы в Интернете и электронной почте (тестирование в реальных условиях) 140 использованных образцов	97,5 %	90,0 %	97,1 %
Обнаружение широко распространенных и преобладающих вредоносных программ, найденных за последние 4 недели (набор образцов AV-TEST) 14 658 использованных образцов	99,6 %	99,6 %	99,7 %
Оценка защиты			4.5/6.0

	Ноябрь	Декабрь	В среднем по отрасли
Сценарии использования: посещение веб-сайтов, загрузка ПО, установка и выполнение программ, копирование данных 5 использованных образцов	2 s		2s
Оценка производительности			5.0/6.0

	Ноябрь	Декабрь	В среднем по отрасли
Ложные предупреждения или блокировки при посещении веб-сайтов 500 использованных образцов	0	0	0
Ложные срабатывания на обычные программы в ходе проверки системы 1 301 224 использованных образцов	1	0	5
Ложные предупреждения об определенных действиях, выполняемых при установке и использовании обычных программ 40 использованных образцов	0		0
Ложные блокировки определенных действий, выполняемых при установке и использовании обычных программ 40 использованных образцов	0		0
Оценка удобства			6.0/6.0

Декабрь 2016 г.

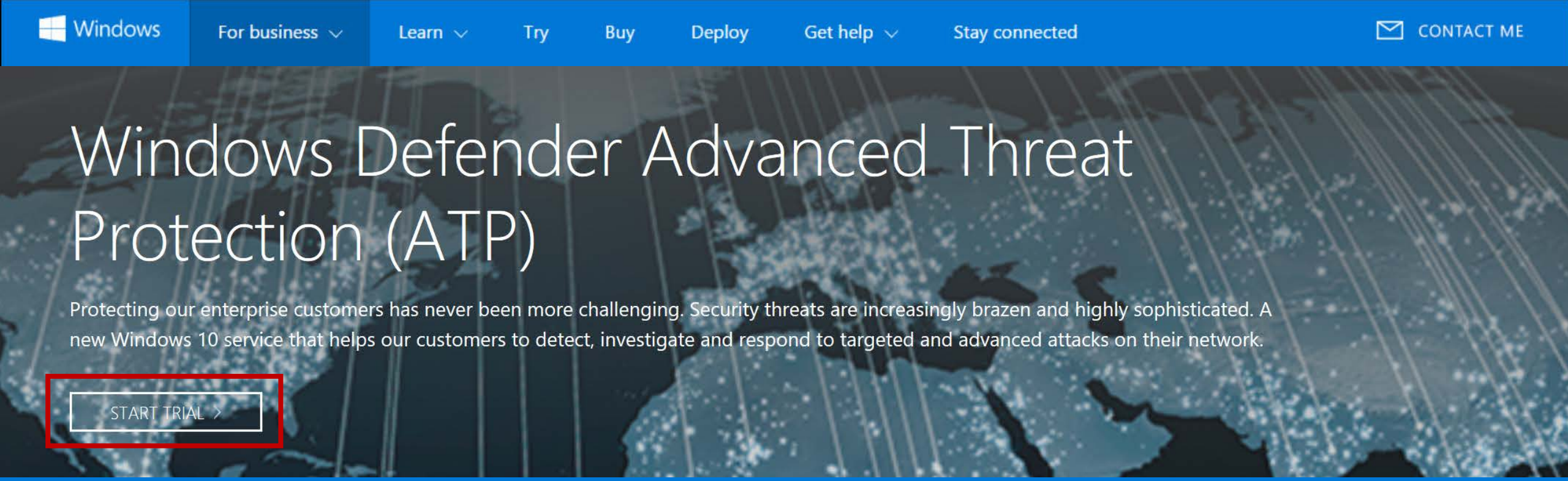
Настроения меняются.

- Публикации:
- [Показатели антивируса Майкрософт взлетели вверх (Microsoft's Antivirus Scores Soar)]
- [Майкрософт с блеском прошла тест антивирусов (Microsoft Aces Antivirus Test)]
- [Майкрософт больше нельзя назвать легкой добычей для хакеров (Microsoft Sheds Reputation as an Easy Mark for Hackers)]
- [Доказано: антивирус Защитник Windows от Майкрософт стал намного лучше]

- Dennis Labs
  - *Публичные заявления Dennis Technology Labs*
    - Исправления работают: регулярная установка обновлений Windows значительно повышает уровень защиты. **Продукт Майкрософт для защиты от вредоносного ПО вместе с обновлениями Windows обеспечивают защиту на уровне 99 процентов.**
    - **Пользователи Microsoft Security Essentials, установившие на момент тестирования все обновления и исправления**, получают уровень защиты, способный **поспорить с лучшими платными антивирусами**.

Но в последние годы Майкрософт взялась за ум: ей удалось впечатлить даже такого гуру безопасности, как Микко Хиппонена (Mikko Hypponen), ведущего исследователя F-Secure, финской компании — эксперта по безопасности, — прежде он скептически относился к попыткам Майкрософт утвердиться в этой сфере.

«Они были последними, а стали лучшими, — сказал г-н Хиппонен. — Изменения налицо: они всерьез взялись за безопасность».

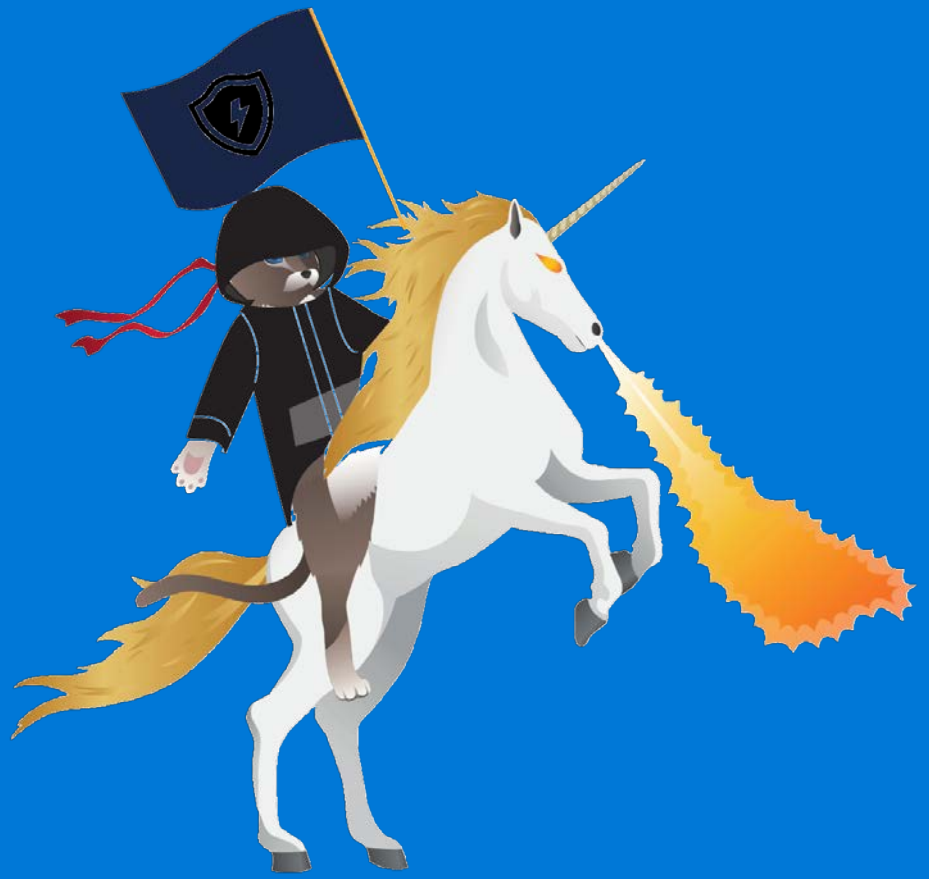


Попробуйте бесплатно @ **https://aka.ms/wdatp**

TechNet - https://aka.ms/technet-wdatp

Рахмет!

Улан КАРАЖИГИТОВ
ulkarazh@microsoft.com



Windows