Bitdefender

# УМНЫЙ ДОМ:
## добро пожаловать или посторонним вход разрешён

# Trusted to be ahead

**Bitdefender это глобальная технологическая компания, основанная в 2001 году.**

Мы защищаем +500 миллионов устройств более чем
В 150 странах.

Bitdefender


500
MILLION USERS

# Инновации в основе бизнеса

**Команда R&D это центр Bitdefender**

Половина работников в R&D

Команда по расследованию киберпреступлений сотрудничает с основными организациями в этой сфере (NATO, Europol, Interpol и пр.)

25% годового R&D тратится на перспективные прорывные проекты

Bitdefender

# Технологическое партнерство

# Технологические партнеры

# 150+ OEM Partnerships

**Нас проверили и доверились нам**
**более 150 партнеров**

Постоянное лидерство по данным сторонних независимых сравнений.

Обеспечение защиты для: рабочих станций, мобильных устройств, шлюзов безопасности, прокси-серверов, оборудования, трафика, данных и IOT-устройств.

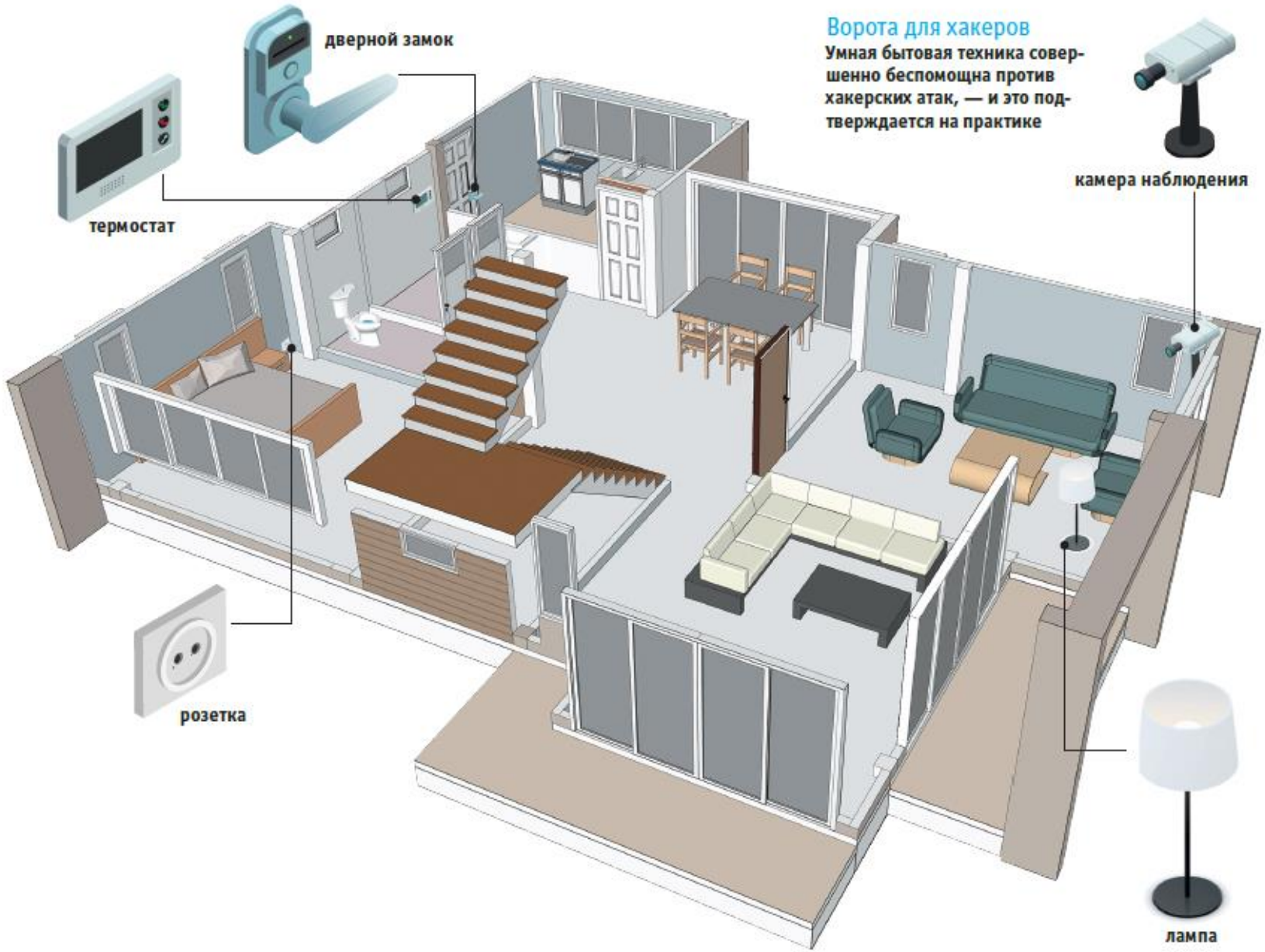
Пакеты безопасности и SDK эффективны
Удобны для использования.

Bitdefender

# Комфортно и безопасно?

## Ворота для хакеров

**Умная бытовая техника совершенно беспомощна против хакерских атак, — и это подтверждается на практике**



# Начнем с замков

«Умные замки» (Smart Locks) передают функции дверных замков смартфонам. Открываются:

- при приближении владельца с телефоном,
- дистанционно через Интернет
- командой голосом.

Когда процесс блокировки управляется с помощью Siri, если iPad или iPhone лежит достаточно близко к запертой двери, грабители легко откроют ее снаружи, просто прокричав: «Привет, Siri. Открой дверь!».

**ВЗЛОМ ЧЕРЕЗ СМАРТФОН.**

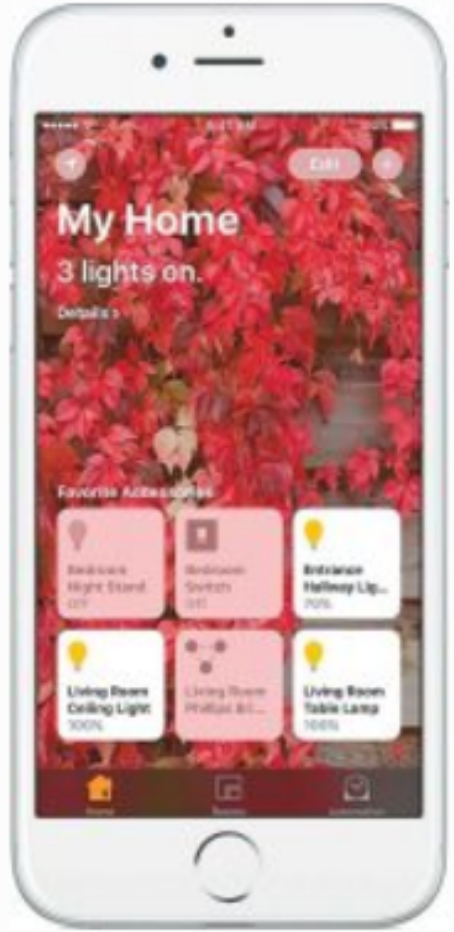
Производители современных умных замков защищают данные соединения шифрованием, но, как только производится атака на смартфон, приложение, относящееся к замку, становится небезопасным. Завладев смартфоном, хакеры владеют и входом в ваш умный дом.

**Перед использованием проверяйте, не заражен ли ваш смартфон вирусами.**

**Иначе хакеры смогут взломать дверь.**

# Плацдарм для атаки на умный дом

*Apple и Samsung для своих смартфонов и планшетов предлагают центры управления для совместимых устройств систем умного дома. Идея централизованного управления всей структурой хороша, но нынешние взломы показывают, что безопасность обеих систем пока не находится на должном уровне.*




> ***HomeKit*** *Изначально Apple хорошо защищает свою платформу. Но поскольку полный доступ к устройству с iOS можно получить с помощью джейлбрейка, то и приложение HomeKit не представляется безопасным. К тому же взломщики могут управлять важными компонентами извне через голосовые команды Siri — так, например, можно открыть входную дверь (смотри раздел «Защита дверных замков»).*

> ***Samsung SmartThings*** *Исследователи вопросов безопасности в Мичиганском университете нашли у платформы Samsung способ получения обширных прав доступа к умным устройствам с помощью приложений SmartThings. Это давало возможность так управлять дверным замком и так его блокировать, что его больше нельзя было открыть. Компания Samsung уже устранила эту брешь. Поэтому стоит следить за своевременным обновлением ПО вашей системы.*

# Начнем с замков

Исследователь Энтони Роуз (Anthony Rose) решил испытать систему поиска Bluetooth устройств.
Bluetooth-замки:

- обнаруживали себя
- активировались,
- передавали пакеты информации,
- передавали пароли в открытом виде.

Из 16 приобретенных Роузом, 12 Bluetooth-замков не соответствуют никаким нормам безопасности. В число наиболее «ущербных» попали Quicklock Doorlock, Quicklock Padloock, iBluLock Padlock и Plantraco PhantomLock.

При этом замки QuickLock позволяли без труда сменить админ-пароль, а сброс настроек можно произвести только при открытой двери. Т.е. потенциальный злоумышленник может заблокировать владельца замка в помещении так, что единственной альтернативой станет физический взлом двери.

Ряд замков оказались уязвимы к атакам путем перехвата пересылаемой информации. В результате криптозащита не имеет значения — злоумышленнику не требуется дешифровывать сообщение, он просто повторно отправляет ранее скопированный пакет информации и замок, считая его корректным, открывает дверь.

Что же делать?

1. Защищайте ПК и смартфоны от вирусов
2. Проверяйте на наличие новых прошивок ваши гаджеты
3. Используйте VPN для защиты канала связи

# IP-камеры – безопасность или опасность

Современные IP-камеры настраиваются просто: на смартфон загружается приложение и производится соединение камеры по WLAN с приложением — готово. Данные с камеры проходят через зашифрованное https-соединение.

Однако смартфон и камера часто соединяются через облачные сервисы, как было с камерой Philips. Запрос, направляемый в облако незашифрованный. В запросе идентификатор, с помощью которого и шифруется трафик. Хакер может считать идентификатор сессии и получить доступ к камере через облако. От таких взломов защитит VPN.

В некоторых камерах встречался настроенный по умолчанию и неизменяемый пароль root, одинаковый для всех моделей. Хакеры могут скачать ПО на сайте производителя, и получить этот пароль. Пользователь не может от этого защититься – подобные ошибки устраняются производителем. Поэтому нужно регулярно искать обновления ПО для систем безопасности, и относящихся к ним приложений.

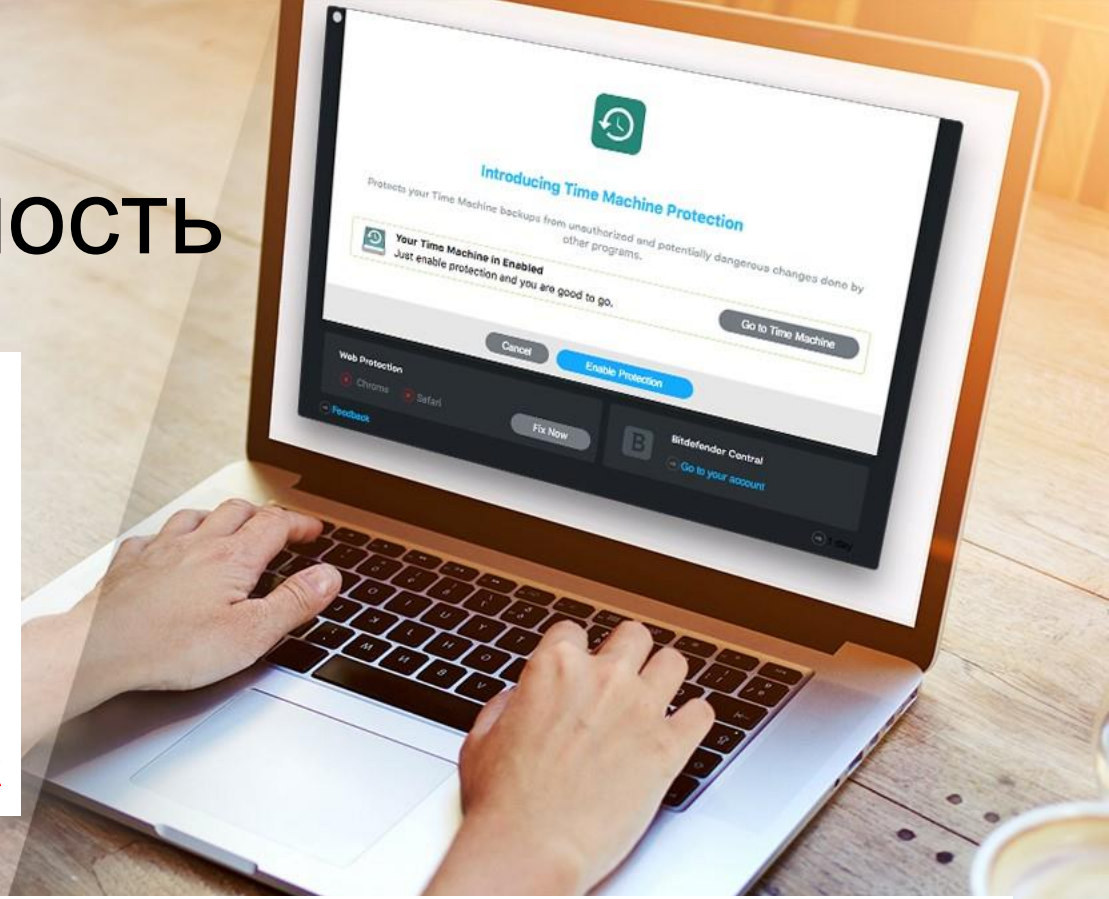
В сентябре 2016 года веб-сайт журналиста Брайана Кребса (англ. *Brian Krebs*) стал жертвой DDoS-атаки, трафик которой на пике достиг 665 Гб/с, одной из самых мощных известных DDoS-атак. Сайт пришлось на некоторое время закрыть. Атака была осуществлена ботнетом из зараженных «умных» видео-камер.

Bitdefender
Do your thing, protected

# IP-камеры – безопасность или опасность

**Зачем ломают:**

- Удаленное наблюдение за личной жизнью
- Смена ракурса камеры для проникновения
- Отключение детектора движения
- Проверка наличия хозяев дома
- Использование уязвимостей для проникновения в сеть
- Заражение камер и IoT-устройств для ботнета и DDoS-атак




**Как защититься:**

- Регулярное **обновление ПО** и прошивок
- **Смена** всех дефолтных **паролей** на более сложные
- **Анализ** сканерами **уязвимостей**
- Использование **VPN**
- Проверка **логов**
- **Антивирусная защита** управляющих ПК и смарфонов

Bitdefender

# Что еще?

# Детские товары

**11-летний Рубен Пол** осуществил **взлом «умной» игрушки**, заставив медведя светиться и записывать звук в зале. Плюшевый медведь был подключен к облачному сервису через Wi-Fi и Bluetooth. Также юный специалист просканировал устройства в зале и получил список десятков номеров смартфонов. После этого хакер подключился к одному из них и записал аудио, а затем дал послушать зрителям его через плюшевого мишку.

Плюшевые игрушки от компании Spiral Toys работают как мессенджеры: дети могут передать голосовые сообщения родителям и наоборот. Игрушки со встроенными микрофоном и динамиками подключаются по Bluetooth к смартфону. Записи разговоров хранятся в базе данных, которая не защищена даже паролем. Там можно найти аудиозаписи, личные данные о детях и родителях (всего более 800 т. записей). Злоумышленники взломали не защищённую базу данных. Нашедшие уязвимость "белые" хакеры несколько раз пытались связаться с компанией Spiral Toys, разработчики не ответили.

В Германии. запретили продавать игрушки My Friend Cayla на территории страны.
Дети могут «общаться» с игрушкой через микрофон. Когда ребёнок задаёт Кайле вопрос, игрушка передаёт аудиофайл на серверы производителя, ищет ответ на вопрос в своей базе или в Сети. После этого озвучивает найденную информацию.
Все записи могут передаваться третьим сторонам, в том числе рекламным агентствам. Мало того, хакеры могут перехватить аудиозаписи, и подменить ответы. Так злоумышленники смогут узнать у ребёнка конфиденциальные данные.

Высоко ценятся и радионяни с подключением к Интернету. Множество производителей жертвуют безопасностью ради комфорта. Доступ к детскому монитору, камера которого использует Интернет-соединение, может быть не только у членов семьи, а вообще у любого человека, который умеет пользоваться сетью.
Найти такие устройства не требует особых усилий, поисковые системы типа Shodan выводят тысячи результатов по запросу «webcam». В рамках своего исследования группа специалистов по безопасности Rapid7 обнаружила большое количество уязвимостей детских мониторов известных производителей таких, как Philips, iBaby и TrendNet.

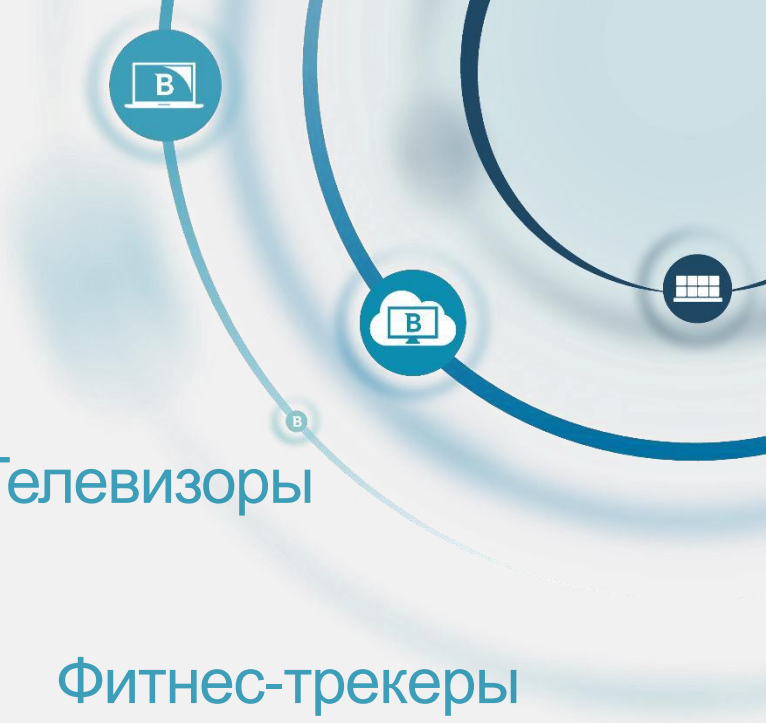
# Медицина

**Даллас, 28 мая.** Компания WhiteScope, занимающаяся информационной безопасностью, изучила *кардиостимуляторы* и *дефибрилляторы* четырех известных фирм и обнаружила в их программном коде **8000 уязвимостей**, которые могут сделать и без того больных людей жертвами хакеров.

Еще в 2013 году хакер **Барнаби Джек** заявил, что может взять под контроль *кардиостимулятор* на расстоянии до 50 метров и создать **смертельный шок** с помощью устройства. Можно удалить беспроводную функцию своего кардиостимулятора, но обновление программного обеспечения потребует хирургического вмешательства.

Прошлой осенью Johnson & Johnson была вынуждена рассказать своим клиентам, что ее *инсулиновые помпы* имели хакерскую уязвимость, которую могут использовать хакеры для назначения потенциально фатальной **передозировки** инсулина.

# Продолжаем?



Розетки

Лампочки

Телевизоры

Роутеры

Термостаты

Фитнес-трекеры

Мультиварки

Чайники

Системы кондиционирования

Термостаты

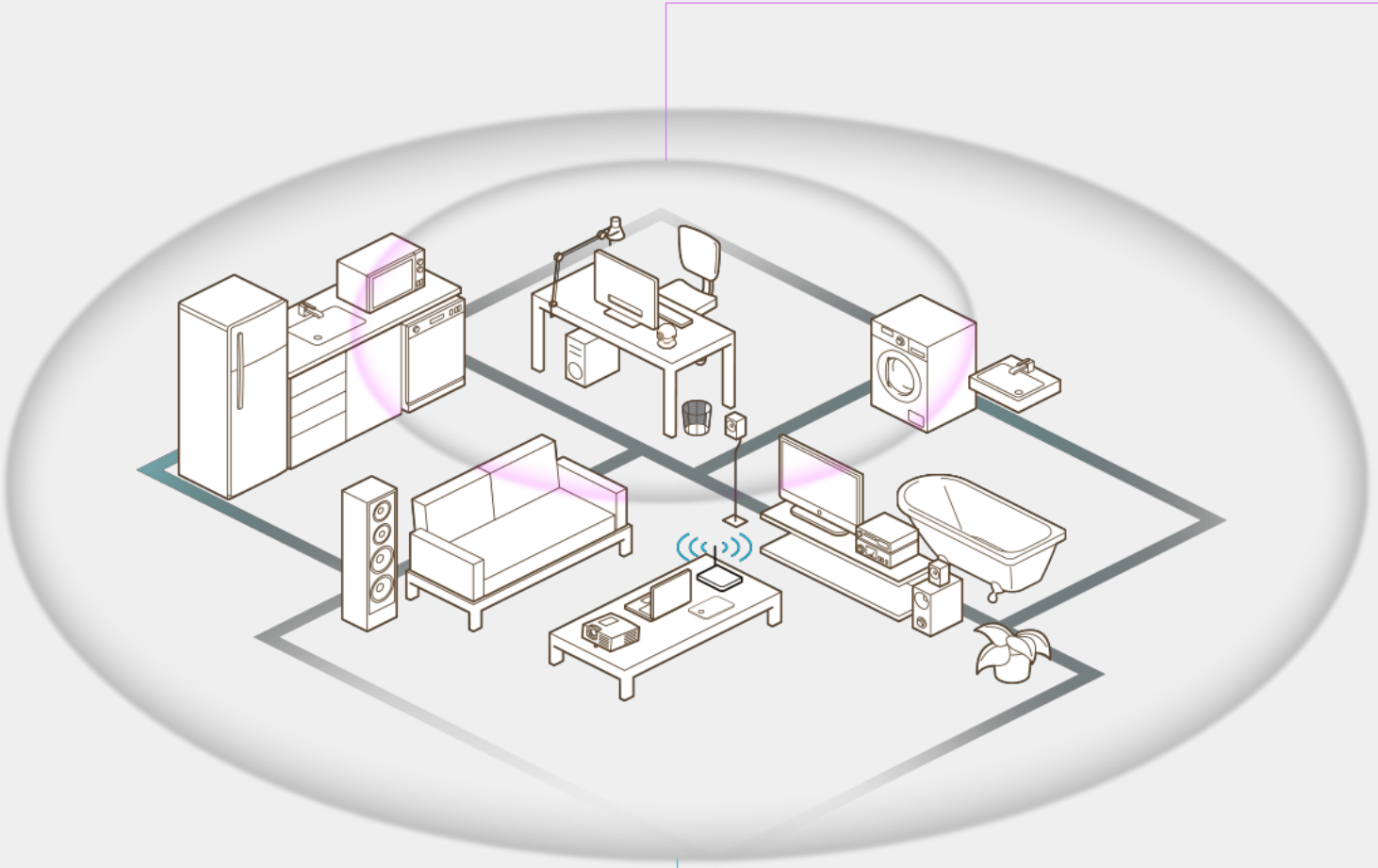
Акустика

Жалюзи

Bitdefender

# Для дома

# Решения для дома



## Bitdefender 2017

Многофункциональная кросс-платформенная защита для устройств на Windows, Mac и Android.

## Bitdefender BOX

Революционное решение интернет-безопасности, включающее в себя оборудование, облачные технологии и ПО созданное для защиты ваших близких и вашего умного дома.


# Bitdefender BOX

Умная защита для всех ваших устройств, подключенных к сети

PC®
PCMAG.COM
RATED
EXCELLENT

Bitdefender

# Для бизнеса

# Мы представляем трансформацию Решений по безопасности для предприятий

## Ключевые принципы

Периметр не однородный – усиливайте защиту систем

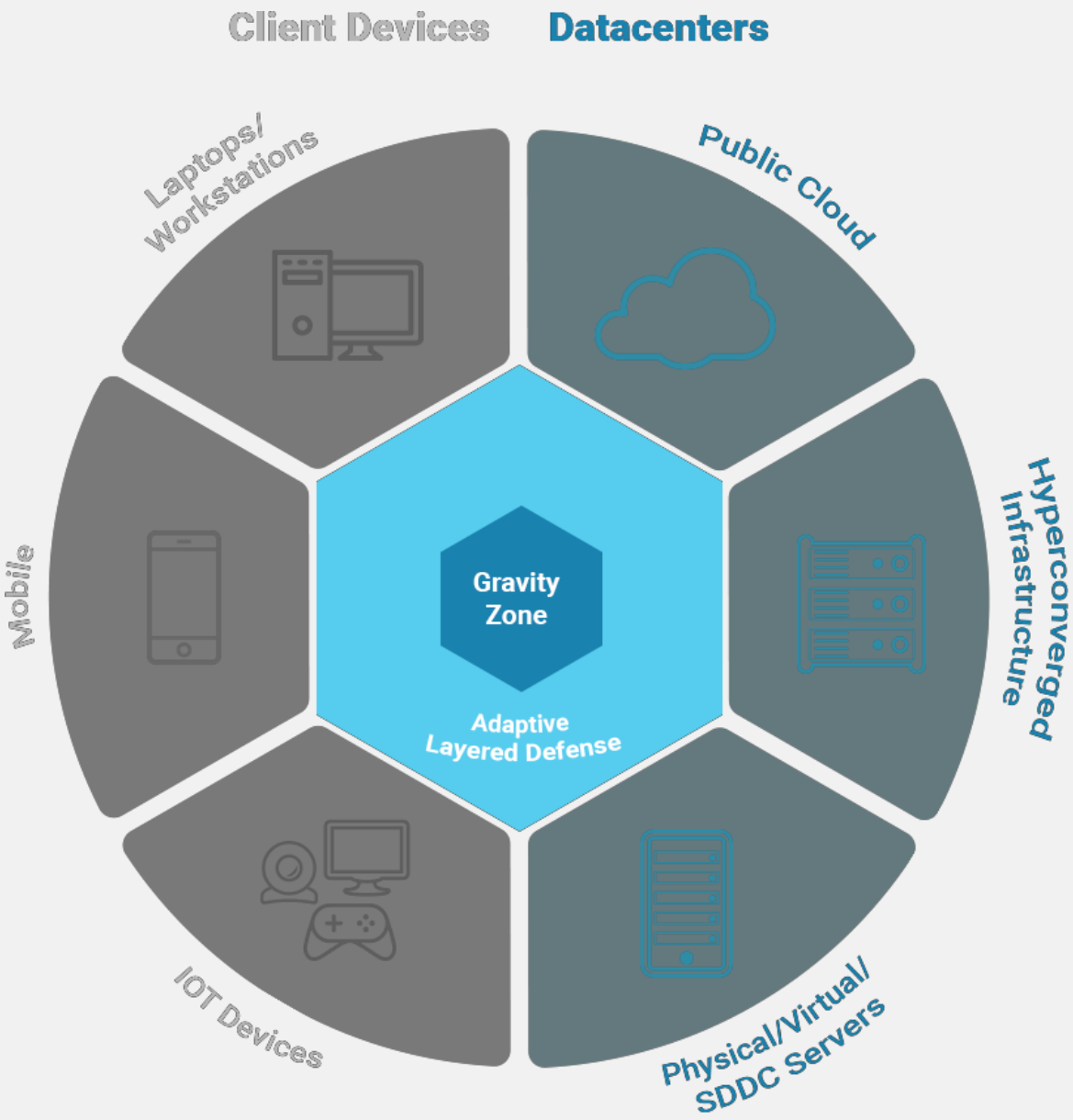
Рабочие станции и ЦОДы требуют разных подходов обеспечения безопасности

Безопасность должна быть адаптивной и многоуровневой

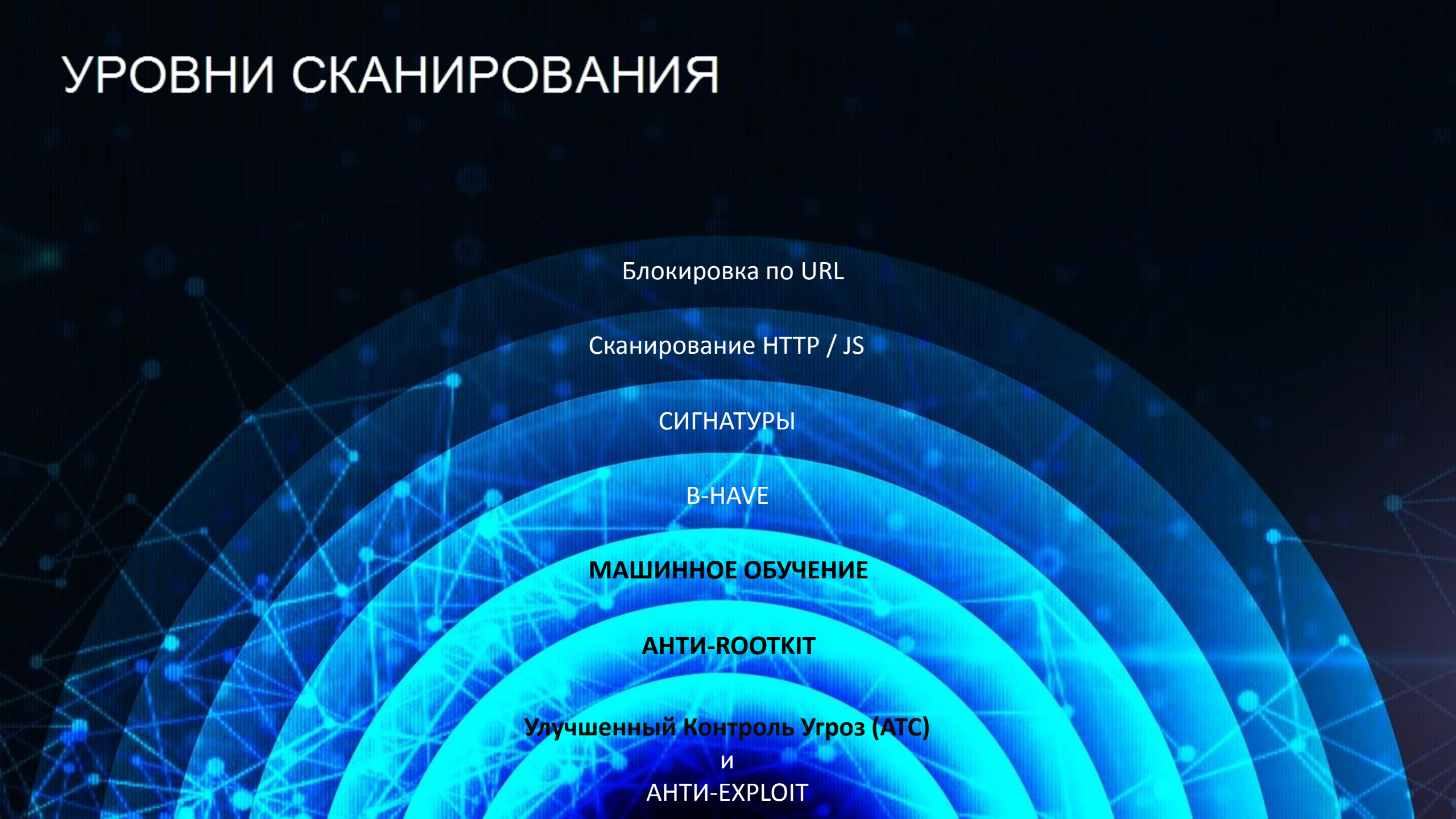
Мы должны не сменять а трансформировать

Мы созданы для производительности и управляемости

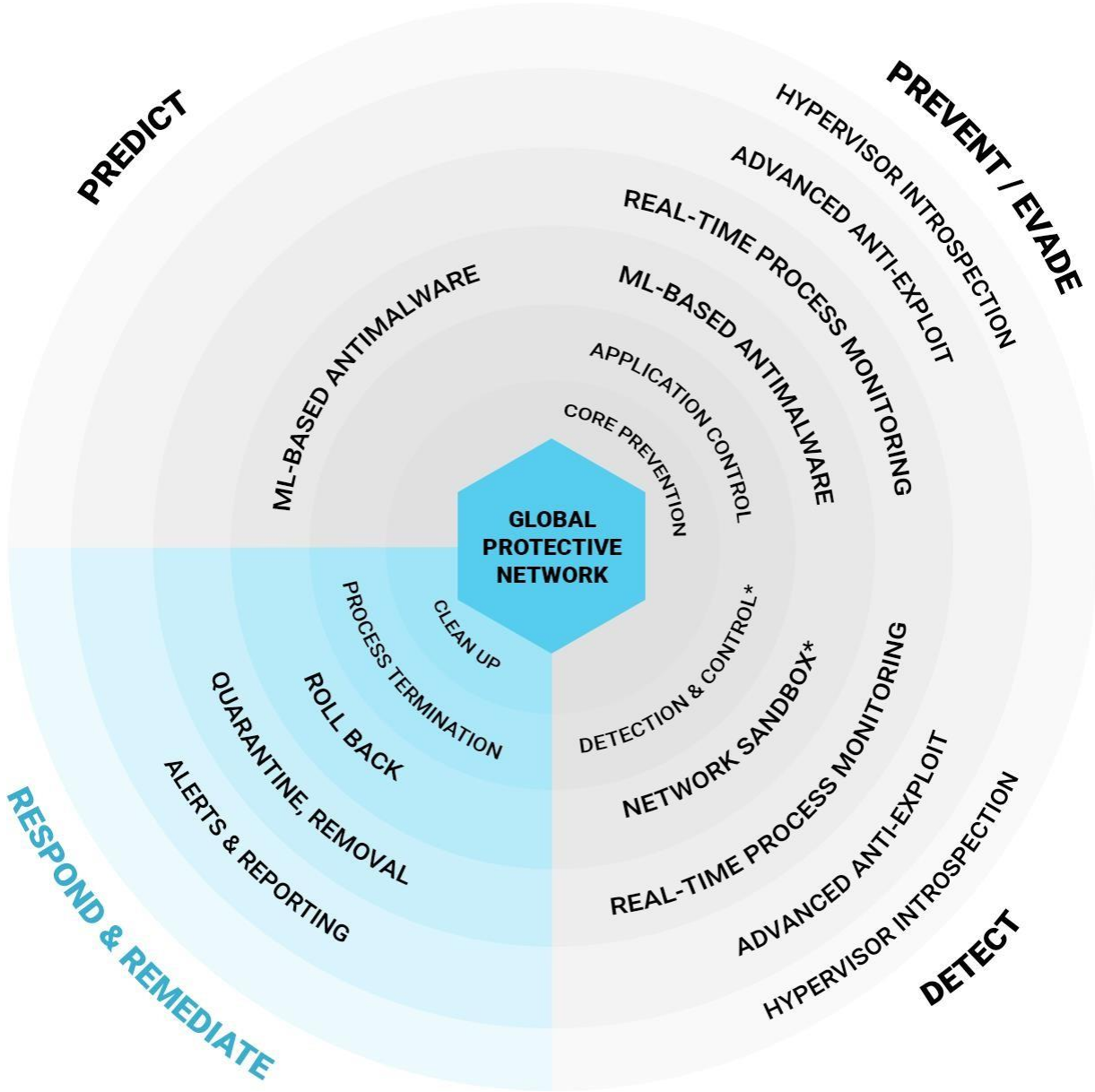
Будущее за гетерогенностью



# УРОВНИ СКАНИРОВАНИЯ



# Адаптивная и Многоуровневая защита



Bitdefender

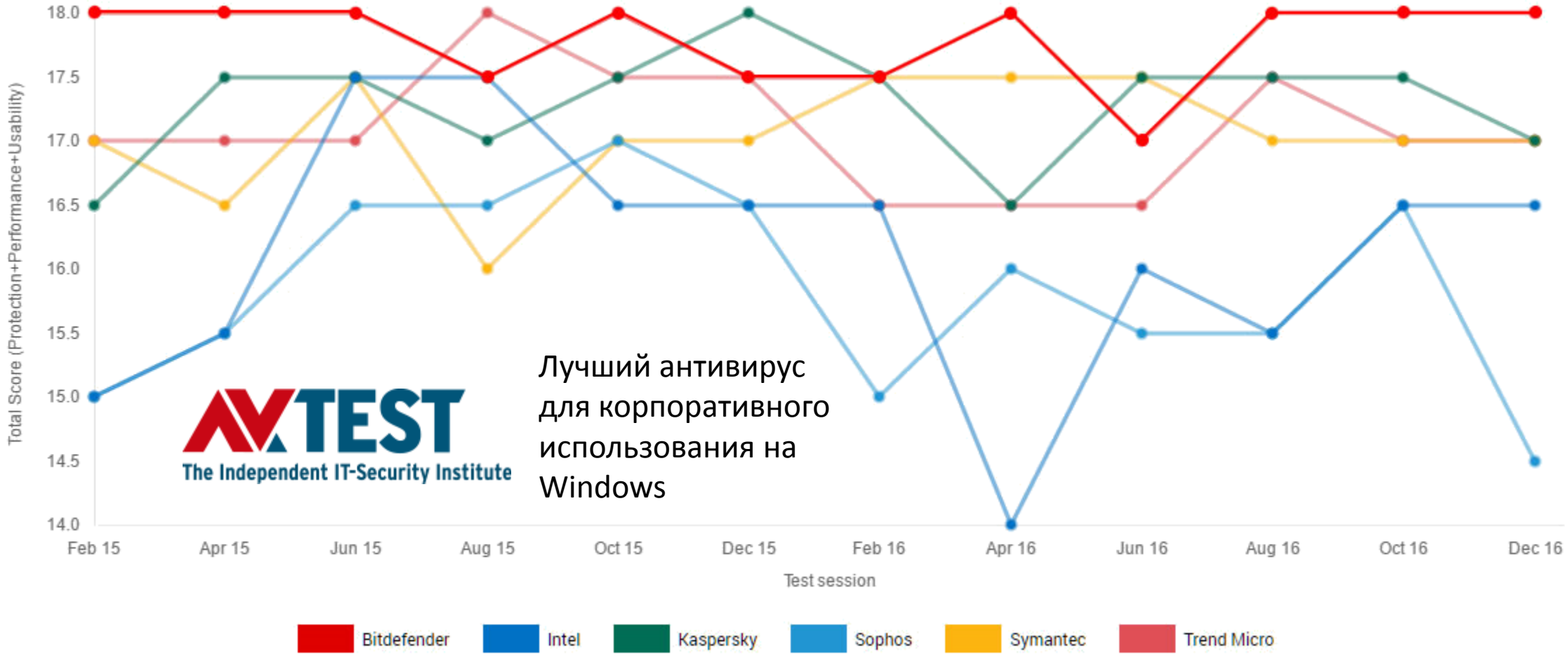
# Награды & признание

# Лучшая защита. Лучшая производительность.


**Best Protection Against Infections** (on a scale of 0 to 6 and 6 being the highest protection)
Overall Score. January 2011 – Feb 2016. AV TEST.


**Lowest Impact on Performance** (on a scale of 0 to 6 and 6 being the lowest impact)
Overall Score. January 2013 – Feb 2016. AV TEST.

# Защита. Производительность. Удобство.




AV-TEST
The Independent IT-Security Institute

Лучший антивирус для корпоративного использования на Windows

Source: AV-Test, Business Windows Client Trials

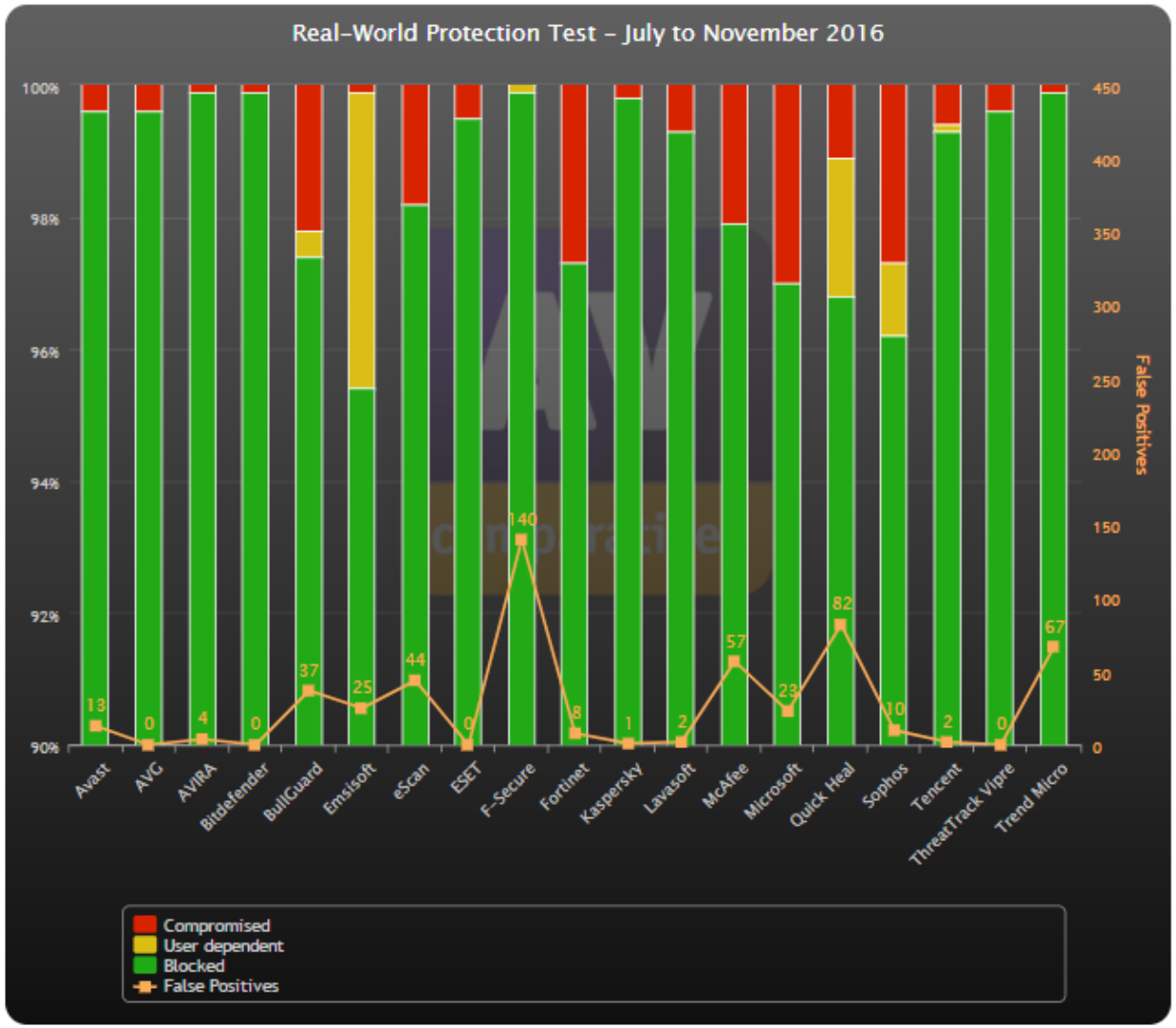

AV comparatives

OUTSTANDING SECURITY PRODUCT 2016

***“Bitdefender это выдающийся продукт 2016 года, добившийся наивысших итоговых оценок”***

**AV-Comparatives | Январь 2017**

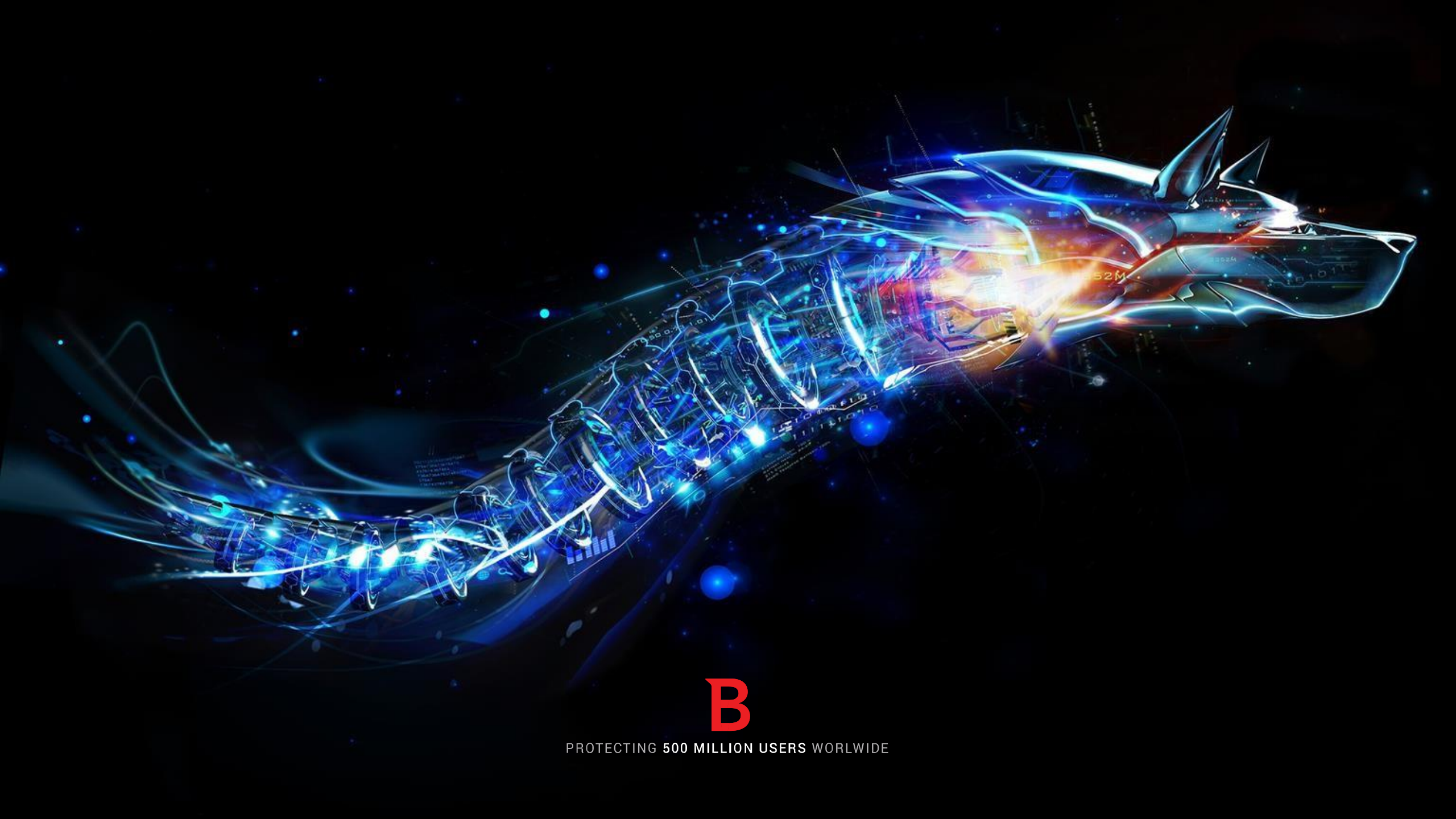
Test: Real-World Protection Test ▼ Year: 2016 ▼ Month: Jul to Nov ▼ Sort: by vendor ▼ Zoom: 90 - 100% ▼



PC 25 TIME WINNER
PCMAG.COM

*“Мало кому удавалось превзойти Norton, но Bitdefender смог!”*

PC Mag


B
PROTECTING 500 MILLION USERS WORLWIDE