



# Safetica

**Защита от утечек конфиденциальных  
данных и мониторинг эффективности  
труда персонала**



АНТИВИРУСНАЯ ЗАЩИТА  
БИЗНЕС-КЛАССА



РАЗВИВАЕМ  
ТЕХНОЛОГИИ  
БЕЗОПАСНОСТИ  
УЖЕ 30 ЛЕТ



Любой бизнес так или иначе оперирует данными. Если конфиденциальная информация будет потеряна или украдена, пострадает репутация компании и ее прибыльность. Утечка данных может повлечь и юридическую ответственность.

Средний ущерб компании от утечки данных составляет **\$ 3,86 миллиона\***

**60% компаний малого бизнеса** прекращает свою деятельность в течение 6 месяцев после серьезной утечки данных\*\*

Safetica предотвращает утечки данных, упрощает соблюдение политик безопасности и защищает ваш бизнес от человеческого фактора.

Safetica – простое в использовании решение для предотвращения потери данных (DLP), доступное компаниям любого размера.

\* Международный опрос Global Cost of Data Breach Study, Ponemon Institute и IBM Security, 2020

\*\* Как утечки данных влияют на малый бизнес, withlayr.com, 2017



# Чем **Safetica** поможет вашему бизнесу?

## ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

80% компаний ежегодно сталкиваются с инцидентами информационной безопасности, включая утечки данных. Средний ущерб от утечки составляет 3,86 млн долларов, при этом до 60% малых компаний после крупного инцидента прекратит свое существование в течение полугода.

Safetica защищает от утечек ваши данные, независимо от того, где они хранятся и кто их использует:

- ✓ персональные данные
- ✓ стратегически важные документы
- ✓ базы клиентов
- ✓ платежные данные, например, реквизиты банковских карт
- ✓ интеллектуальную собственность (промышленные образцы, ноу-хау)

## ЗАЩИТА ОТ ИНСАЙДЕРОВ

Около трети сотрудников хотя бы раз в своей карьере вредили работодателям – копировали данные, чтобы использовать на новом месте работы (40%), удаленно подключались к корпоративным ресурсам после увольнения (7%), уничтожали документы (5%). Помимо этого, сотрудник может потерять интерес к текущей деятельности, активно искать новую работу, выполнять задания

других компаний или использовать оборудование и ПО работодателя в личных целях.

Safetica выявляет подозрительное и потенциально опасное поведение персонала, а также колебания производительности. Руководство получает отчеты об активности сотрудников до того, как их деятельность нанесет реальный ущерб.

## ОБУЧЕНИЕ ПЕРСОНАЛА

Сотрудники, работающие с конфиденциальными данными, не всегда обладают достаточными знаниями о правилах безопасности. Даже профессионалы совершают ошибки, критичные для бизнеса. Как следствие – только в 2019 году каждая пятая компания в России пострадала от случайных утечек данных.

С помощью Safetica вы можете обучать сотрудников тому, как правильно и безопасно работать с конфиденциальными данными.

## СОБЛЮДЕНИЕ НОРМАТИВОВ

Safetica помогает соблюдать законодательные требования и стандарты в области защиты данных, включая GDPR, ISO/IEC 27001, HIPAA, PCI DSS и др.

# Чем уникальна **Safetica**?

## КОМПЛЕКСНАЯ ЗАЩИТА ОТ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Safetica закрывает все основные каналы утечки данных и защищает от широкого спектра угроз, связанных с человеческим фактором. Решение предотвращает случайные утечки, защищает от злонамеренных действий инсайдеров и рисков BYOD, а также решает проблемы продуктивности труда персонала.

В одном решении вы получите **мониторинг, аналитику и защиту данных через несколько дней после развертывания.**

## ГЛУБОКИЙ АНАЛИЗ ПОВЕДЕНИЯ

Safetica выявляет подозрительные действия сотрудников, проводит глубокий анализ поведения и обеспечивает **понимание внутренних процессов в компании.** Вы выясните, что происходит в команде, и сможете сосредоточиться на проблемных пользователях.

## ПРОЗРАЧНАЯ РАБОТА С ДАННЫМИ

Где, когда и каким образом используются конфиденциальные данные вашей компании? Safetica даст четкие ответы на эти вопросы и поможет выявить потенциальные проблемы. Составьте **полную картину работы с данными** и действуйте быстро и эффективно.

## ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ

Стоимость проекта внедрения равна стоимости лицензии, **без скрытых затрат и сложных технических требований.** Закупать дорогостоящее оборудование и нанимать в штат специалистов по информационной безопасности не потребуется.

## ПРОСТОЕ ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ

Safetica разработана таким образом, чтобы заказчик мог внедрить и настроить продукт силами собственного ИТ-отдела. **Развертывание занимает от нескольких часов,** первые отчеты вы получите уже через несколько дней.





# Как Safetica защищает вас?

## АУДИТ И ПРОЗРАЧНОСТЬ ПРОЦЕССОВ С SAFETICA DISCOVERY

Посмотрите, как используются данные компании, где они хранятся и куда пересылаются. Предотвратите умышленную утечку данных с помощью журналов аудита. Откройте для себя внутренние процессы и перестройте бизнес-среду.

Safetica Discovery позволяет быстро обнаружить скрытые риски и повысить прозрачность процессов в вашей организации.

## ЗАЩИТА УСТРОЙСТВ НЕЗАВИСИМО ОТ ПЛАТФОРМЫ

Safetica отслеживает использование данных как в Windows, так и в macOS. Настройте интеграцию с сетевыми устройствами Office 365 или Fortinet, чтобы получить расширенный контроль неизвестных устройств.



## ОБУЧЕНИЕ ПЕРСОНАЛА И ЗАЩИТА ДАННЫХ С SAFETICA PROTECTION

Safetica Protection создает безопасную среду для всей компании, обучает сотрудников, выявляет риски и защищает данные.

### УСТАНОВИТЕ ЧЕТКИЕ ПОЛИТИКИ ДЛЯ ВСЕХ КАНАЛОВ ДАННЫХ

Настройте политики безопасности, используя индивидуальный или групповой подход. Выберите желаемый рабочий процесс с настраиваемыми действиями, от фоновой аудита до информационных уведомлений и строгой блокировки.

### ПОСТАВЬТЕ ВСЕ ПОДКЛЮЧЕННЫЕ УСТРОЙСТВА ПОД КОНТРОЛЬ

Ограничьте использование портативных устройств или запретите несанкционированные подключения к мультимедийным ресурсам. Управляйте корпоративными мобильными устройствами и отслеживайте данные, которые покидают облако Office 365.

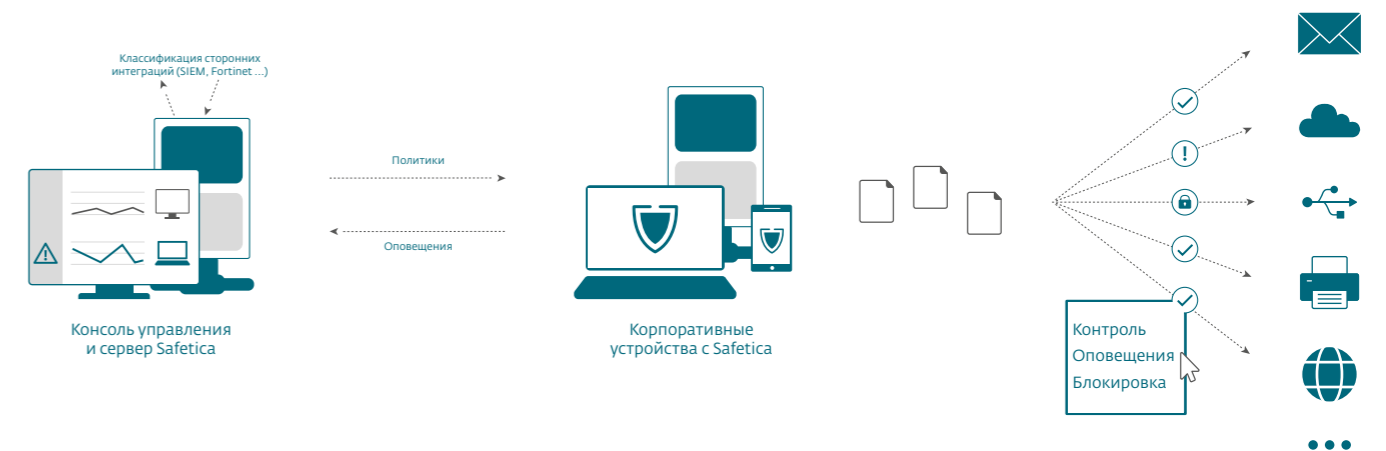
### ПОСТРОЙТЕ БЕЗОПАСНУЮ РАБОТУ С КОНФИДЕНЦИАЛЬНЫМИ ДАННЫМИ

Отображение уведомлений при потенциальном нарушении пользователем политик безопасности. Постройте безопасные процессы для работы с наиболее важными данными.

### ОБЕСПЕЧЬТЕ ПОЛНУЮ ОНЛАЙН И ОФЛАЙН-ЗАЩИТУ

Защитите данные на сетевых и офлайн-устройствах компании. Safetica остается полностью активной независимо от наличия сетевого подключения. Все собранные записи синхронизируются, как только соединение будет восстановлено.

# Как работает Safetica?



Сервер баз данных работает с журналами событий безопасности рабочих станций. Консоль Safetica Management Console позволяет пользователям управлять политиками безопасности и отображать всю собранную информацию.

Все действия записываются, и политики безопасности применяются на ПК, ноутбуках, планшетах и смартфонах с Safetica.

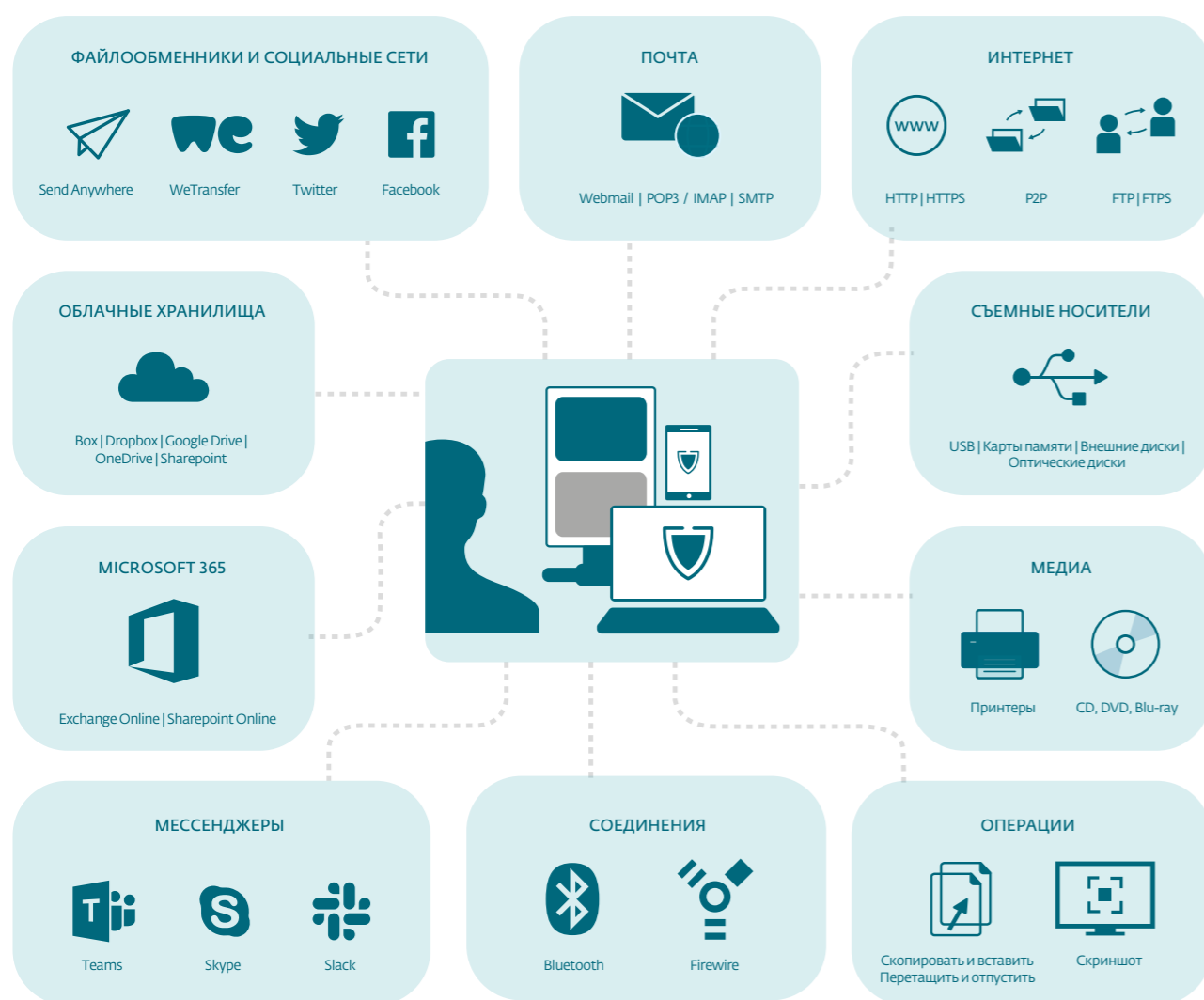
Конфиденциальные данные защищены по всем каналам.

## НАБОР ОСНОВНЫХ ФУНКЦИЙ

Safetica может определить, кто и когда рискует вашей конфиденциальной информацией. В зависимости от того, в каком режиме работает Safetica, возможна блокировка рискованных действий, информирование администратора или напоминание вашим сотрудникам о правилах безопасности.

# Каналы данных, защищенные Safetica

Safetica закрывает от утечек все основные каналы связи и платформы, защищая данные, где бы они ни находились и куда ни передавались.



## ВАЖНЫЕ ОТЧЕТЫ

Safetica предлагает простой для понимания обзор всех возможных угроз в едином интерфейсе управления. Вы можете в любое время и с любого устройства, даже со своего смартфона, получать полезную информацию.

Настройте доставку оповещений о подозрительном поведении по электронной почте или через SIEM, добавляйте любые данные на панель управления или экспортируйте их в XLS или PDF для дальнейшего анализа.

# Технические требования

## SAFETICA SERVER

- ✓ Четырехъядерный процессор с тактовой частотой 2,4 ГГц
- ✓ 4 ГБ ОЗУ и больше
- ✓ 100 ГБ доступного дискового пространства
- ✓ Общий или выделенный сервер, поддержка виртуальных машин и облачный хостинг
- ✓ Требуется подключение к серверу с: MS SQL 2012 и выше или Azure SQL MS Windows Server 2012 и выше

## SAFETICA CLIENT (на защищенных компьютерах)

- ✓ Двухъядерный процессор с тактовой частотой 2,4 ГГц
- ✓ 2 ГБ ОЗУ и больше
- ✓ 10 ГБ доступного дискового пространства
- ✓ MS Windows 7, 8.1, 10 (32-бит [x86] или 64-бит [x64])
- ✓ Пакет установки MSI
- ✓ .NET 4.5.2 и выше

## MS SQL (база данных сервера)

- ✓ MS SQL Server 2012 и выше, или MS SQL Express 2016 и выше, или Azure SQL
- ✓ MS SQL Express является частью универсального установщика и рекомендуется для 200 защищенных устройств
- ✓ 200 ГБ доступного дискового пространства (оптимально 500 ГБ или больше, в зависимости от диапазона хранящихся данных)
- ✓ Общий или выделенный сервер, поддержка виртуальных машин и облачный хостинг. Его можно разместить вместе с сервером Safetica

## MAC CLIENT

- ✓ Четырехъядерный процессор с тактовой частотой 2,4 ГГц
- ✓ 2 ГБ ОЗУ и больше
- ✓ 10 ГБ доступного дискового пространства
- ✓ macOS 10.10 и выше. Для полного набора функций DLP рекомендуется 10.15 и выше





# Обзор продуктов Safetica

ПРОДУКТЫ

ДОПОЛНИТЕЛЬНЫЕ  
МОДУЛИ

Safetica  
Discovery



Safetica  
Protection



Safetica  
Enterprise



Safetica UEBA



Safetica Mobile



## Продукты

### SAFETICA DISCOVERY

- ✓ Сориентируйтесь в потоке конфиденциальных данных компании. Получайте подробные отчеты о важных данных.
- ✓ Включен базовый обзор поведения пользователей компании. Аудит безопасности и аудит соответствия нормативным требованиям.
- ✓ Вы получите первые отчеты о безопасности данных в течение нескольких дней после развертывания.

### SAFETICA ENTERPRISE

- ✓ Продукт для защиты данных, дополняющий стек решений корпоративной ИТ-безопасности.
- ✓ Автоматическая интеграция сторонних решений и функции для расширенных вариантов использования.
- ✓ Управление рабочими процессами и поддержка мультидоменных сред.
- ✓ Персонализируйте Safetica с использованием фирменного стиля вашей компании.

### SAFETICA PROTECTION

- ✓ Универсальное решение безопасности, сочетающее аналитику и классификацию данных, а также предотвращение утечек (DLP).
- ✓ Полный контроль потоков конфиденциальных данных.
- ✓ Регулярные отчеты о безопасности и уведомления об инцидентах в режиме реального времени.
- ✓ Зонирование для упрощенной защиты данных высокого уровня.
- ✓ Простое в развертывании решение для бизнеса.

## Дополнительные модули

### SAFETICA UEBA (USER AND ENTITY BEHAVIOR ANALYTICS)

- ✓ Подробно изучайте реальную активность и поведение пользователей.
- ✓ Просматривайте детальные обзоры использования рабочего времени.
- ✓ Действуйте на основе глубокого понимания процессов вашей компании, чтобы защищать данные и соблюдать политики безопасности.

### SAFETICA MOBILE

- ✓ Защищайте данные на мобильных устройствах, например, смартфонах и планшетах.
- ✓ Получайте отчеты о состоянии мобильных устройств для выявления рисков.
- ✓ Аудит активности как в приложениях, так и на сайтах.



# Обзор функций



## Аудит безопасности

|  | Discovery | Protection | Enterprise |
|--|-----------|------------|------------|
| <b>Аудит безопасности потока данных</b><br>Аудит безопасности потока данных по всем каналам, включая внешние устройства, веб-загрузку, электронную почту, обмен мгновенными сообщениями, печать и облачные хранилища.  | ✓         | ✓          | ✓          |
| <b>Аудит файлов и электронной почты Office 365</b><br>Аудит файловых операций и исходящих электронных писем в Office 365.  | ✓         | ✓          | ✓          |
| <b>Аудит безопасности рабочих процессов</b><br>Аудит использования корпоративных устройств, приложений, сетей и печати. Обнаруживайте неиспользуемые или неправильно используемые ресурсы для поддержания эффективности рабочего процесса и сокращения затрат. | ✓         | ✓          | ✓          |
| <b>Классификация проверки содержимого</b><br>Сканируйте конфиденциальные файлы и электронные письма с помощью полной проверки содержимого – предопределенных шаблонов или настраиваемых правил и словарей.   | ✓         | ✓          | ✓          |
| <b>Обнаружение подозрительной активности</b><br>Реагируйте быстро благодаря обнаружению подозрительной активности в режиме реального времени и моментальным оповещениям по электронной почте.  | ✓         | ✓          | ✓          |
| <b>Аудит соответствия нормативным требованиям</b><br>Выявляйте нарушения наиболее распространенных правил, таких как PCI-DSS, GDPR или HIPAA во всех региональных вариациях.   | ✓         | ✓          | ✓          |

## Защита облачных данных

|   | Discovery | Protection | Enterprise |
|---|-----------|------------|------------|
| <b>Защита устройств с облачной синхронизацией</b><br>Защита данных для облачных накопителей на устройствах, например, OneDrive, Google Диск, Dropbox, Box и т.д.                    | ✗         | ✓          | ✓          |
| <b>Защита устройств с Office 365</b><br>Защита данных для Office 365 и SharePoint. Запретите совместное использование или загрузку данных, которые вы хотите хранить вне облака.    | ✗         | ✓          | ✓          |
| <b>Защита информации в Azure</b><br>Обнаружение классификаций данных в Microsoft Azure Information Protection, даже в зашифрованном виде.   | ✗         | ✓          | ✓          |
| <b>Защита Exchange Online</b><br>Унифицируйте политики электронной почты для устройств и облачных хранилищ. Управляйте и фильтруйте исходящие данные с устройств и Exchange Online. | ✗         | ✓          | ✓          |

## Защита данных

|   | Discovery | Protection | Enterprise |
|---|-----------|------------|------------|
| <b>Электронная почта и защита сети</b><br>Защита данных, которые пересылаются по электронной почте и в мессенджерах, загружаются в интернет и на сетевые ресурсы.   | ✗         | ✓          | ✓          |
| <b>Защита устройств и контроль печати</b><br>Управляйте потоком данных на внешних устройствах и предотвращайте печать конфиденциальных документов на локальных, сетевых или виртуальных принтерах.  | ✗         | ✓          | ✓          |
| <b>Защита удаленной работы</b><br>Избегайте утечек данных при подключении к удаленному рабочему столу. Поддержка широкого спектра решений для удаленного доступа.   | ✗         | ✓          | ✓          |
| <b>Расширенная классификация данных</b><br>Используйте передовые технологии для обнаружения и маркировки конфиденциальных данных на основе происхождения, контекста рабочего процесса или типа файла. Воспользуйтесь преимуществом обнаружения метаданных, чтобы использовать сторонние классификации. Разрешите пользователям классифицировать файлы самостоятельно. | ✗         | ✓          | ✓          |
| <b>Различные политики исправления</b><br>Оперативно реагируйте на обнаруженные инциденты безопасности, чтобы расширить возможности и обучить своих сотрудников. Инциденты можно логировать, блокировать или допускать / блокировать с переопределением.   | ✗         | ✓          | ✓          |
| <b>Теневая копия инцидента</b><br>Храните доказательства инцидентов, создавая теневые копии утечек данных. Теневые копии полностью зашифрованы и могут храниться на локальных компьютерах.  | ✗         | ✓          | ✓          |
| <b>Контроль рабочего пространства</b><br>Определите защищенное рабочее пространство и уменьшите периметр с помощью приложений и управления веб-сайтом. Избегайте нежелательного поведения в компании и снижайте затраты на управление безопасностью.  | ✗         | ✓          | ✓          |
| <b>Зонирование Safetica</b><br>Простое управление безопасным периметром данных с уникальными зонами Safetica, которые значительно сокращают количество политик защиты данных.   | ✗         | ✓          | ✓          |
| <b>Управление шифрованием BitLocker</b><br>Централизованное управление локальными дисками и внешними устройствами с шифрованием BitLocker.  | ✗         | ✓          | ✓          |

## Корпоративные функции

|  | Discovery | Protection | Enterprise |
|--|-----------|------------|------------|
| <b>Ребрендинг</b><br>Ребрендинг уведомлений, например, изменение логотипа.   | ✗         | ✗          | ✓          |
| <b>Контроль рабочего процесса</b><br>Политики приложений и экспертные настройки политик для согласования рабочего процесса пользователя с процессами компании. | ✗         | ✗          | ✓          |
| <b>Поддержка нескольких доменов</b><br>Поддержка нескольких доменов предприятия для Active Directory.  | ✗         | ✗          | ✓          |

## Автоматизация безопасности


|  | Discovery | Protection | Enterprise |
|--|-----------|------------|------------|
| <b>SIEM-интеграция</b><br>Автоматизированная отчетность об инцидентах в SIEM-решениях (Splunk, QRadar, LogRhythm, ArcSight и др.).                         | ✗         | ✗          | ✓          |
| <b>Интеграция с FortiGate</b><br>Автоматическая интеграция системы безопасности с сетевыми устройствами FortiGate для комплексной защиты устройств и сети. | ✗         | ✗          | ✓          |





# О SAFETICA

Safetica – чешская компания-разработчик программного обеспечения, которая создает продукты для защиты от утечек данных для компаний всех размеров и типов бизнеса. Компания входит в состав ESET Technology Alliance.

300 000+ защищенных устройств 

1 600+ довольных клиентов 

120+ стран 

80+ экспертов по безопасности 

## ТЕХНОЛОГИЧЕСКИЕ АЛЬЯНСЫ

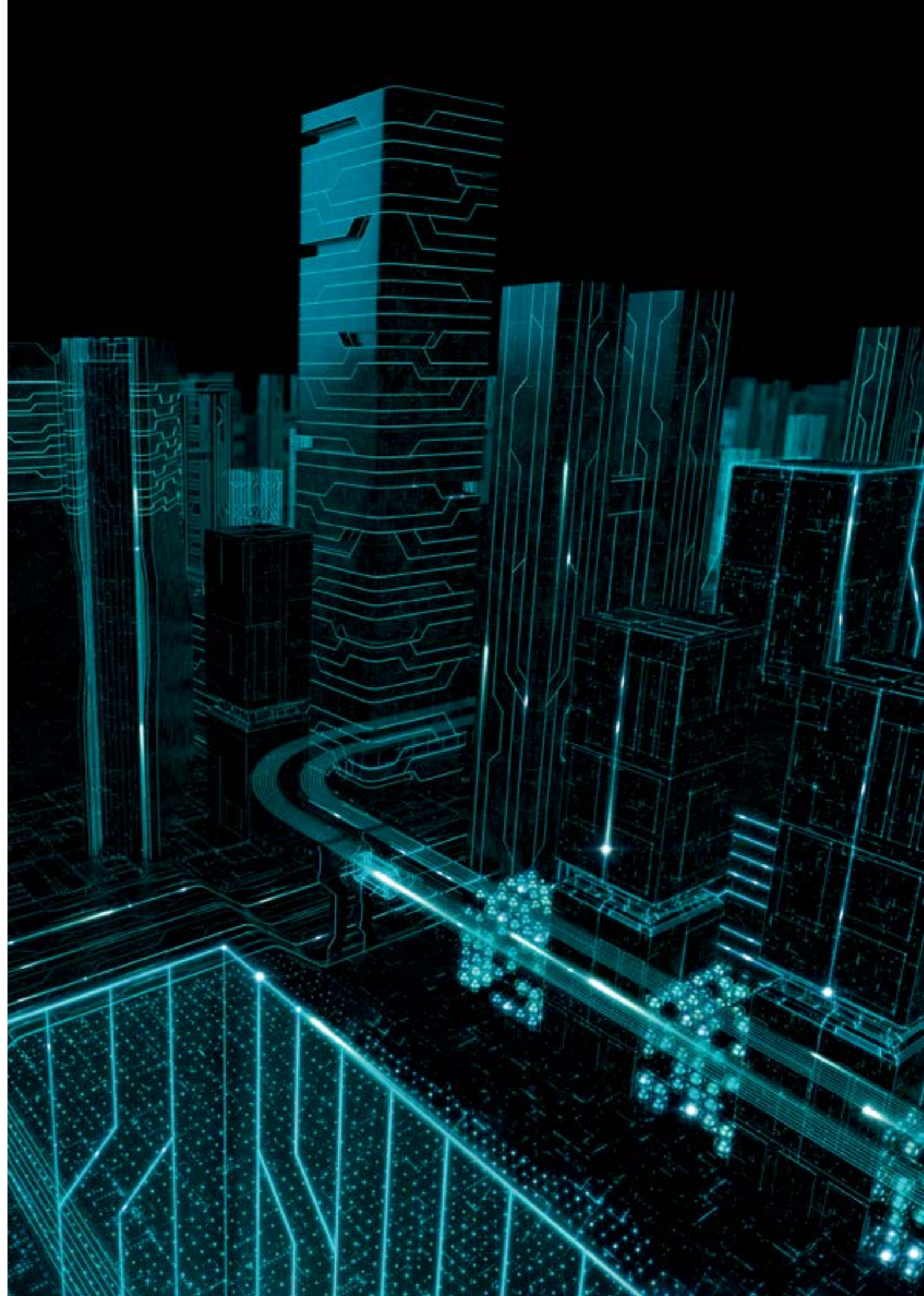


## НАГРАДЫ И ДОСТИЖЕНИЯ



FORRESTER

Gartner







АНТИВИРУСНАЯ ЗАЩИТА  
БИЗНЕС-КЛАССА

