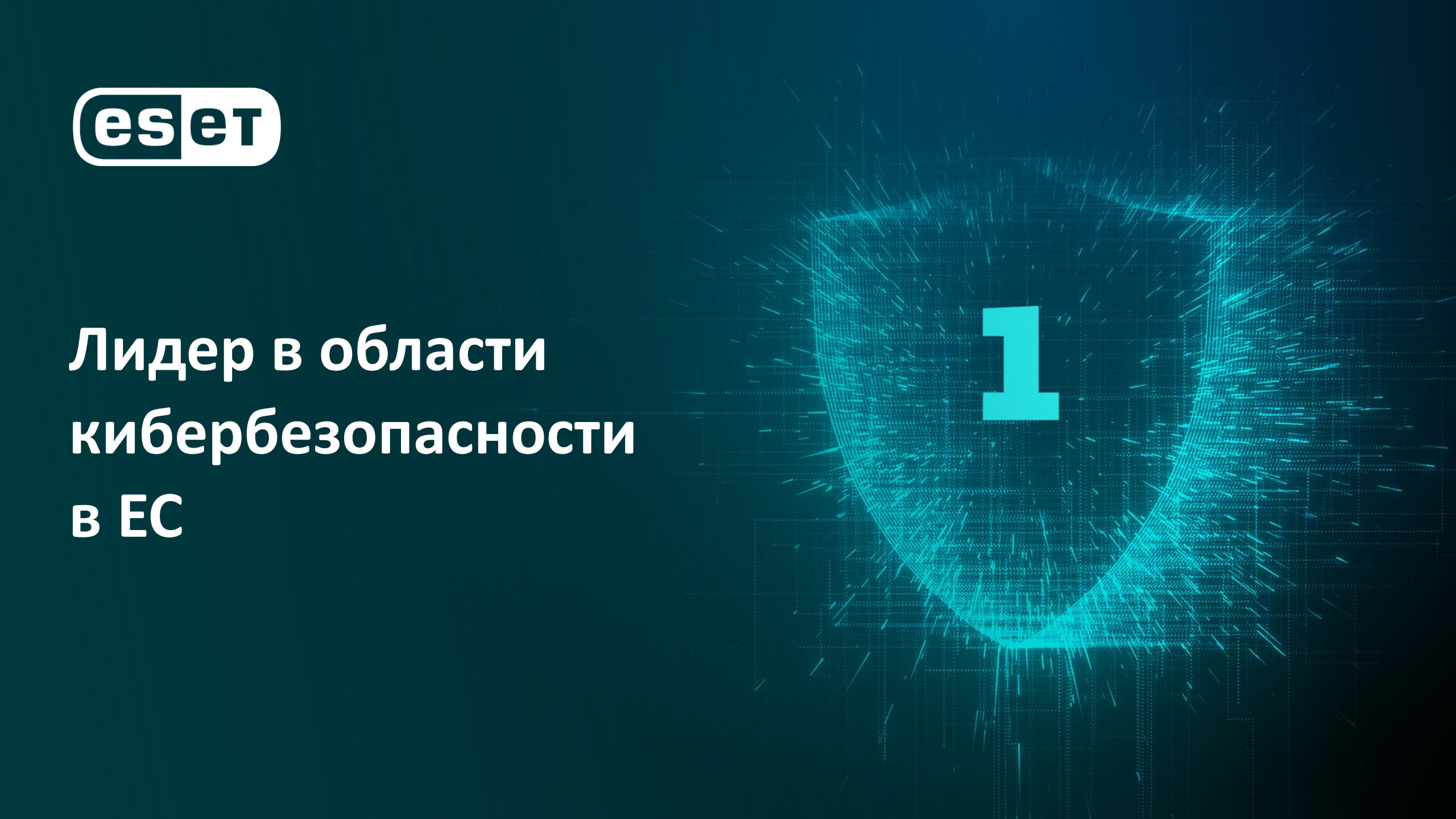

eset
SECURITY
DAYS

Антон Дмитриев

Директор по развитию бизнеса ESET
в Центральной Азии, Армении, Грузии, Молдове и Украине

anton.dmitriev@adeon.international

Лидер в области кибербезопасности в ЕС



30+ лет лидерства
на рынке
ИТ-безопасности

180+ стран, в которых
представлены
продукты

Передовые
технологии
выявления угроз

Крупнейший
поставщик
Европейского Союза

Постоянный рост
компании с момента
ее основания

В собственности
основателей с 1987 года
(произведено в Словакии)

Признание экспертов
и пользователей
в независимых оцениваниях

ESET®

Progress.
Protected.


Leader
SPRING
2023
AV
comparatives
ADVANCED+
Performance Test
APR 2023
SE Labs
AAA
Jan-Mar 2023
Enterprise Endpoint Security
EPS Protection
Gartner
Peer Insights
Customers' Choice 2023
TOP PRODUCT
AV TEST
APPROVED
CORPORATE
ENDPOINT
PROTECTION
WINDOWS
12/2022
av-test.org
TOP PRODUCT
2023
SC
AWARDS
Honoring the Best in U.S Cybersecurity
TrustRadius
Tech Cares
2023
AV
comparatives
ADVANCED+
Malware Protection
MAR 2023
Leader
WINTER
2023
canalys
CYBERSECURITY
CHAMPION
2022
APPROVED
CORPORATE
ENDPOINT
PROTECTION
TOP PRODUCT

Известные корпорации доверяют свою ИТ-безопасность ESET

MITSUBISHI MOTORS
Drive your Ambition

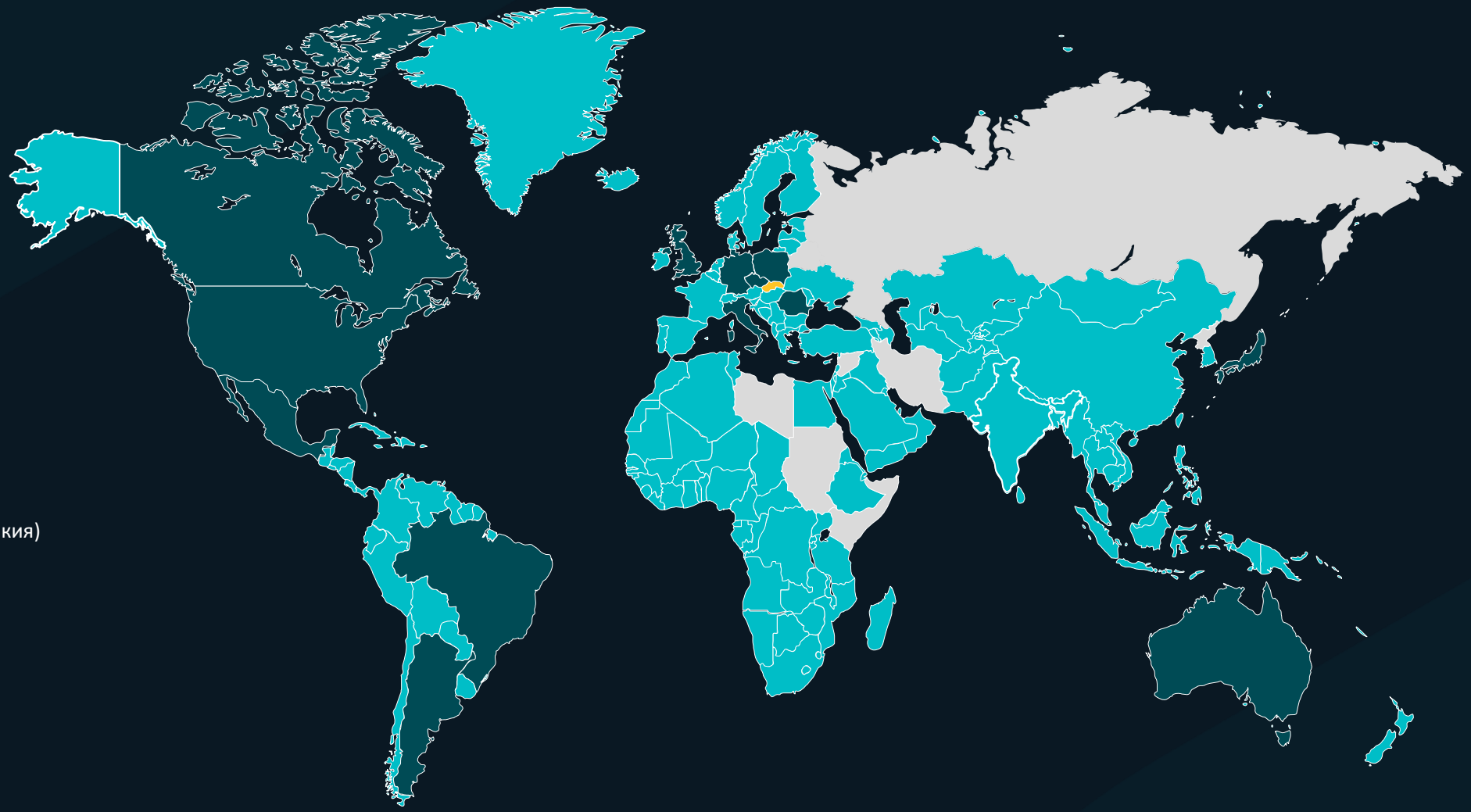
Allianz
Suisse

Canon
Canon Marketing Japan Group

T

Digital Security
Progress. Protected.

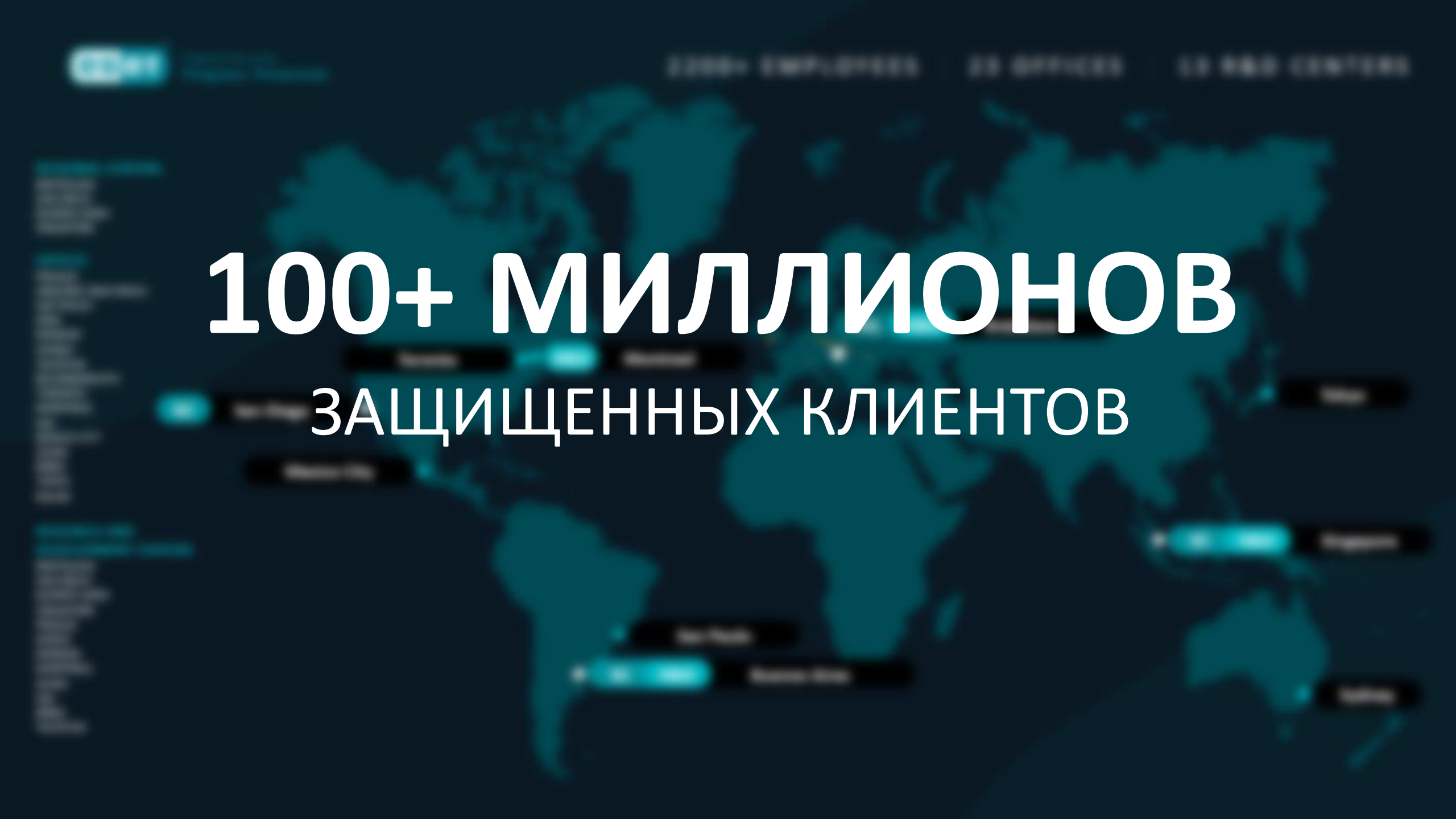
180+ СТРАН | 2200+ СОТРУДНИКОВ | 23 ОФИСА | 13 ЦЕНТРОВ ИССЛЕДОВАНИЙ



- Штаб-квартира (Братислава, Словакия)
- Офисы
- Эксклюзивные дистрибьюторы

1 МИЛЛИАРД

ЗАЩИЩЕННЫХ УСТРОЙСТВ

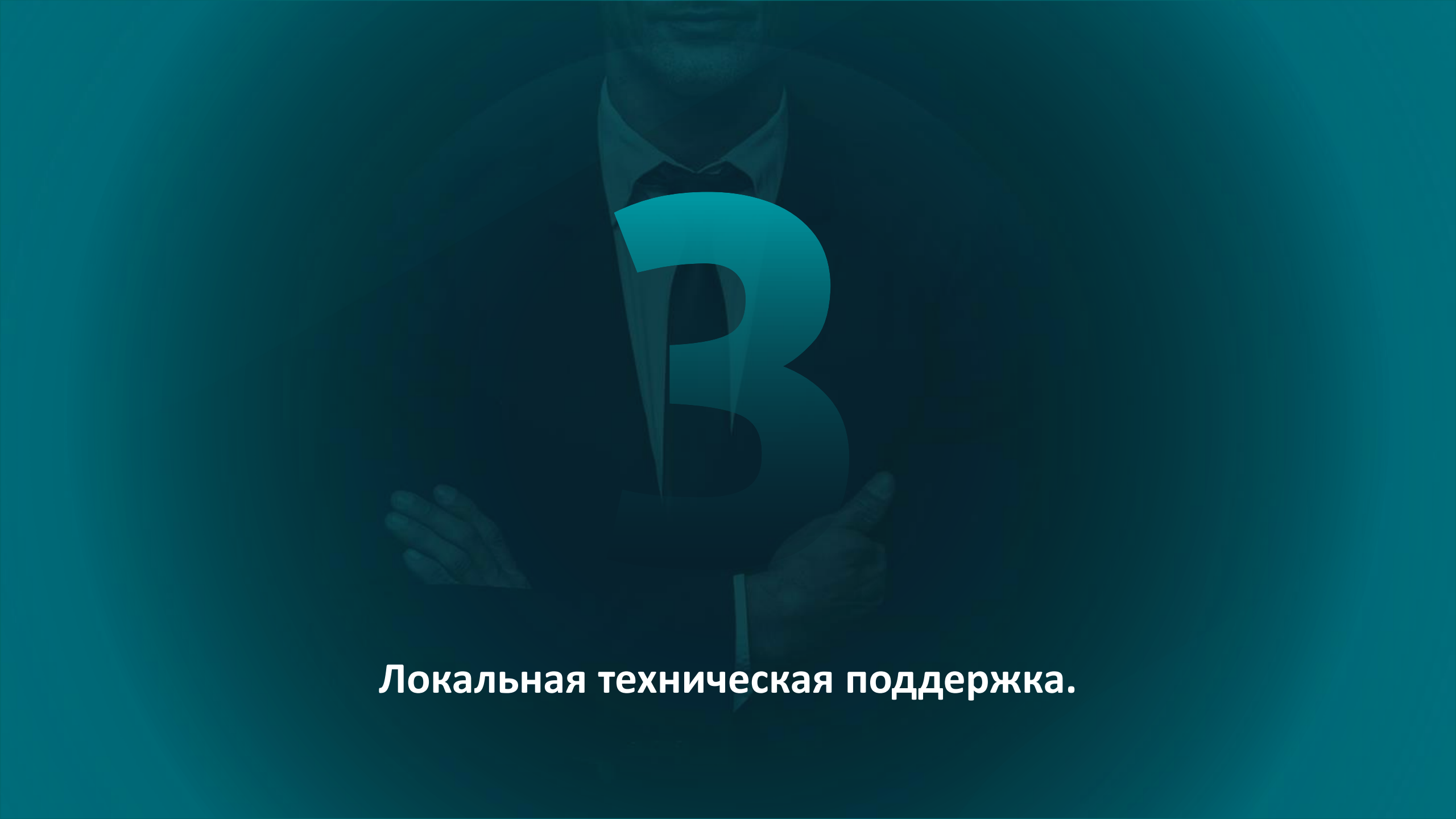

100+ МИЛЛИОНОВ
ЗАЩИЩЕННЫХ КЛИЕНТОВ

ПОЧЕМУ ПОЛЬЗОВАТЕЛИ ЦЕНЯТ ESET?

Высокий уровень обнаружения.
Отсутствие ложных срабатываний.
Минимальное влияние на работу системы.

2

Простота использования.
Защита различных популярных платформ.



Локальная техническая поддержка.

Многоуровневая защита

Уникальные технологии, превосходящие возможности традиционных антивирусов

Облачная защита

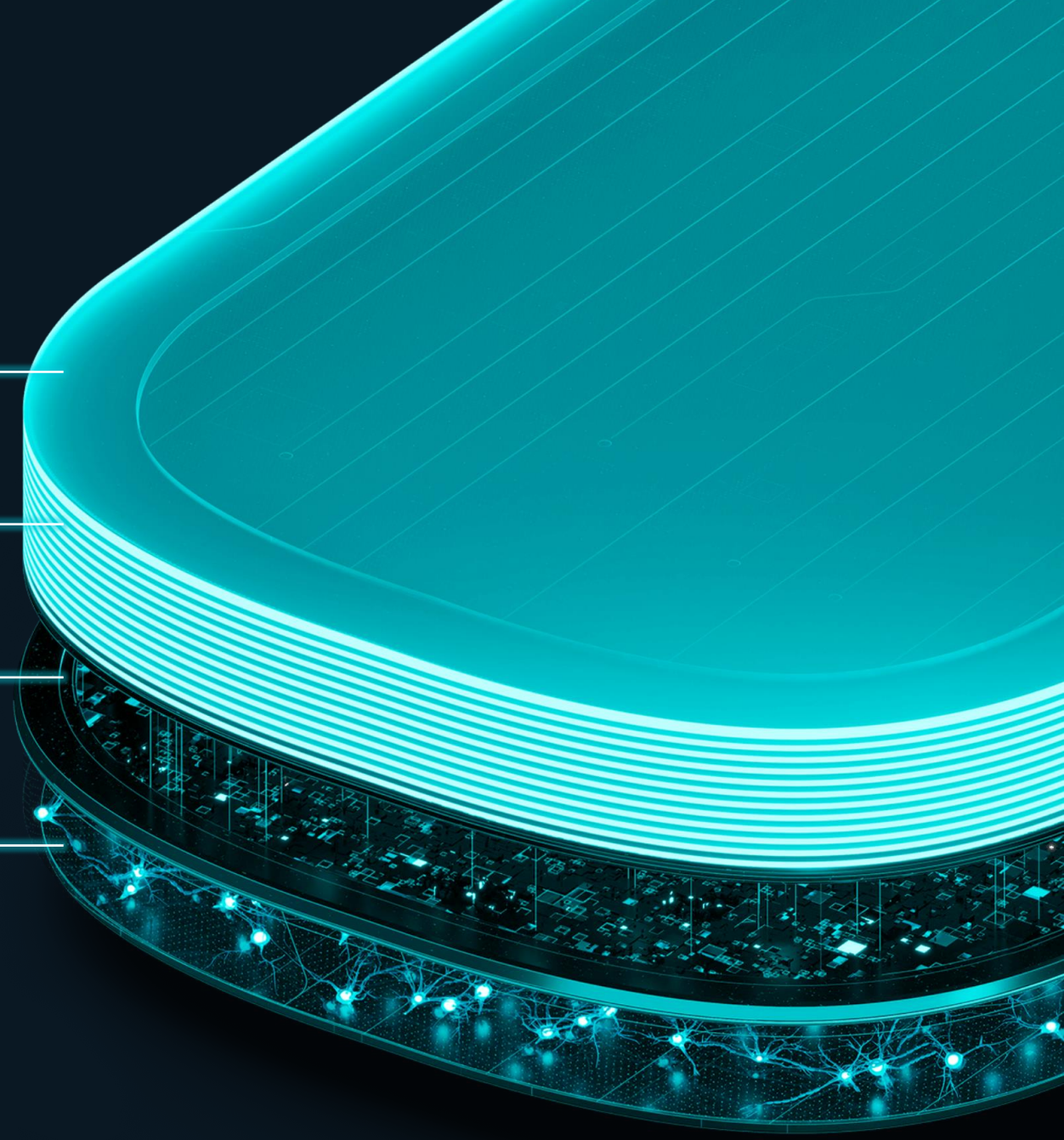
Мощные облачные технологии обнаружения угроз

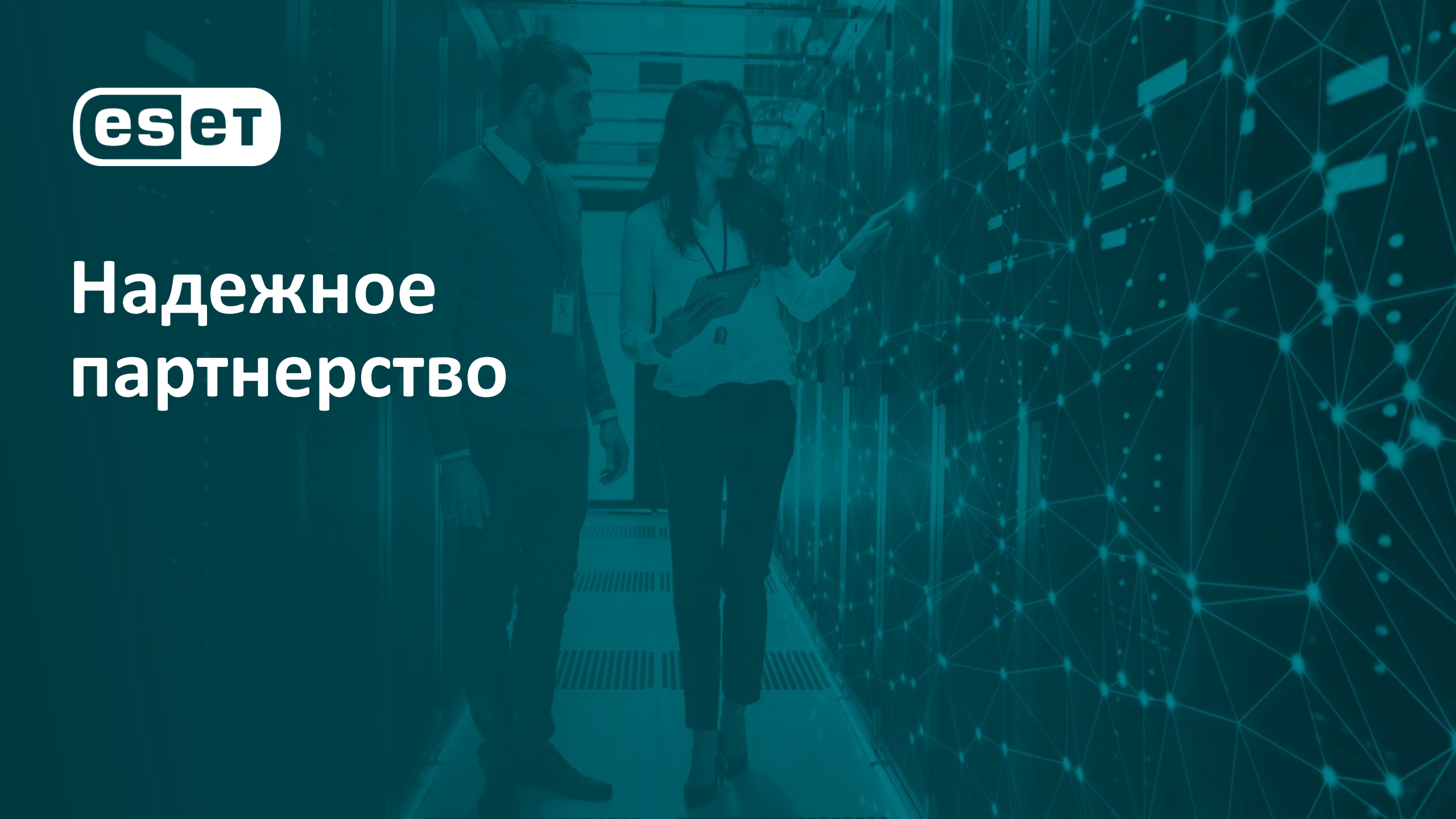
Искусственный интеллект

Продукты созданы с использованием передовых моделей искусственного интеллекта

Опыт специалистов

Разработка и внедрение новых технологий благодаря работе 13 исследовательских центров по всему миру





Надежное партнерство

ОСНОВНЫЕ ЦЕННОСТИ

Эксклюзивный поставщик решений ESET и ESET Technology Alliance

Решения
по кибербезопасности
для домашних и бизнес-
пользователей любого размера

Компетентность и индивидуальный подход

Большой опыт работы в сфере
дистрибуции решений и сотни
реализованных проектов
по ИТ-безопасности
с использованием продуктов ESET

Квалифицированные специалисты

Регулярные обучения
от производителя решений
для предоставления
качественной
поддержки

Соответствие международным стандартам

Поскольку компания
зарегистрирована
в Словакии, ее деятельность
соответствует нормам,
правилам и законам ЕС

ВЫЗОВЫ И ПРОБЛЕМЫ В СФЕРЕ ИТ-БЕЗОПАСНОСТИ

Digital Security
Progress. Protected.

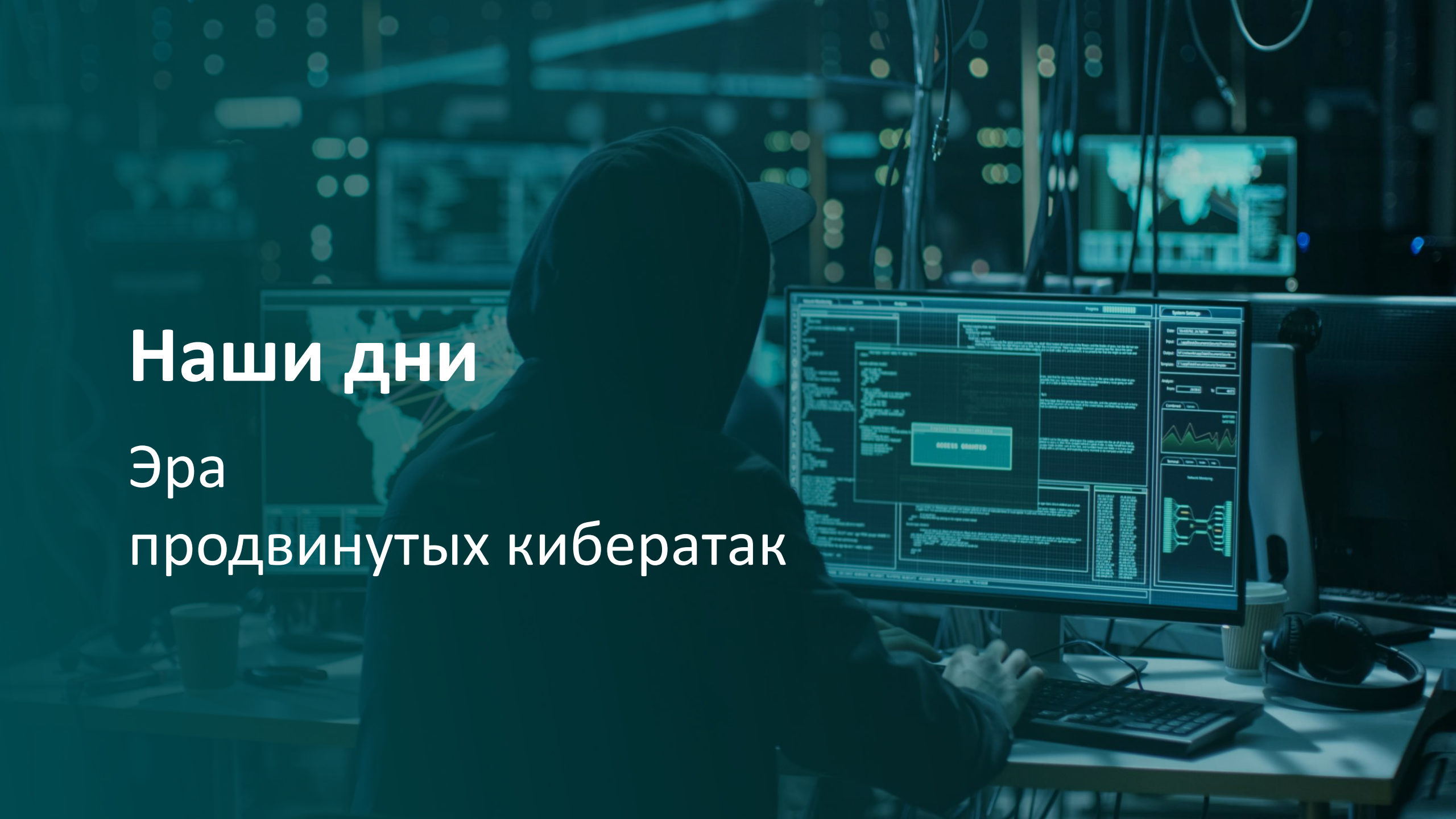
Эволюция киберугроз

1990-е

Эра компьютерных вирусов

2000-е

Эра
сетевых червей



Наши дни

Эра
продвинутых кибератак


welivesecurity BY ESET
Signed kernel dri
Unguarded gatew
Windows' core
ESET researchers look at malware that abuses vulnerabiliti
techniques against this type of exploitation
Michal Poslušný
11 Jan 2022 - 11:30AM
ulnerability:
Menu
welivesecurity BY ESET
Breaking the habit: T
bad cybersecurity ha
shed in 2022
Be alert, be proactive and break these 10 bad habits to improv
Phil Muncaster
3 Jan 2022 - 11:30AM
welivesecurity BY ESET
Menu
Prime targets: Governments shouldn't go it alone on cybersecurity
A year into the pandemic, ESET reveals new research into activities of the LuckyMouse APT group and considers how governments can rise to the cybersecurity challenges of the accelerated shift to digital
Phil Muncaster
29 Apr 2021 - 11:30AM
What are buf
attack
elivesecurity BY ESET
Cryptocurrency scams: W
to know and how to pro
yourself
it rich in the digital gold rush, make sure you k
your crypto
CES 2022 – the "anyon
make an electric car" e
But as we learned in mashing up other technologies, the security devil is in
Cameron Camp
10 Jan 2022 - 05:00PM
When the alarms go off:
10 key steps to take after
a data breach
It's often said that data breaches are no lon
should do, and avoid doing, in the case of a
welivesecurity BY ESET

Александр Иллюша

Руководитель службы технической поддержки ESET в Центральной Азии, Армении, Грузии, Молдове и Украине

oleksandr.Illiusha@adeon.international

Современные вызовы кибербезопасности

Современные вызовы кибербезопасности

Программы-вымогатели (Ransomware)

Целенаправленные атаки (APT) и взлом

Слабозащищенные инфраструктуры

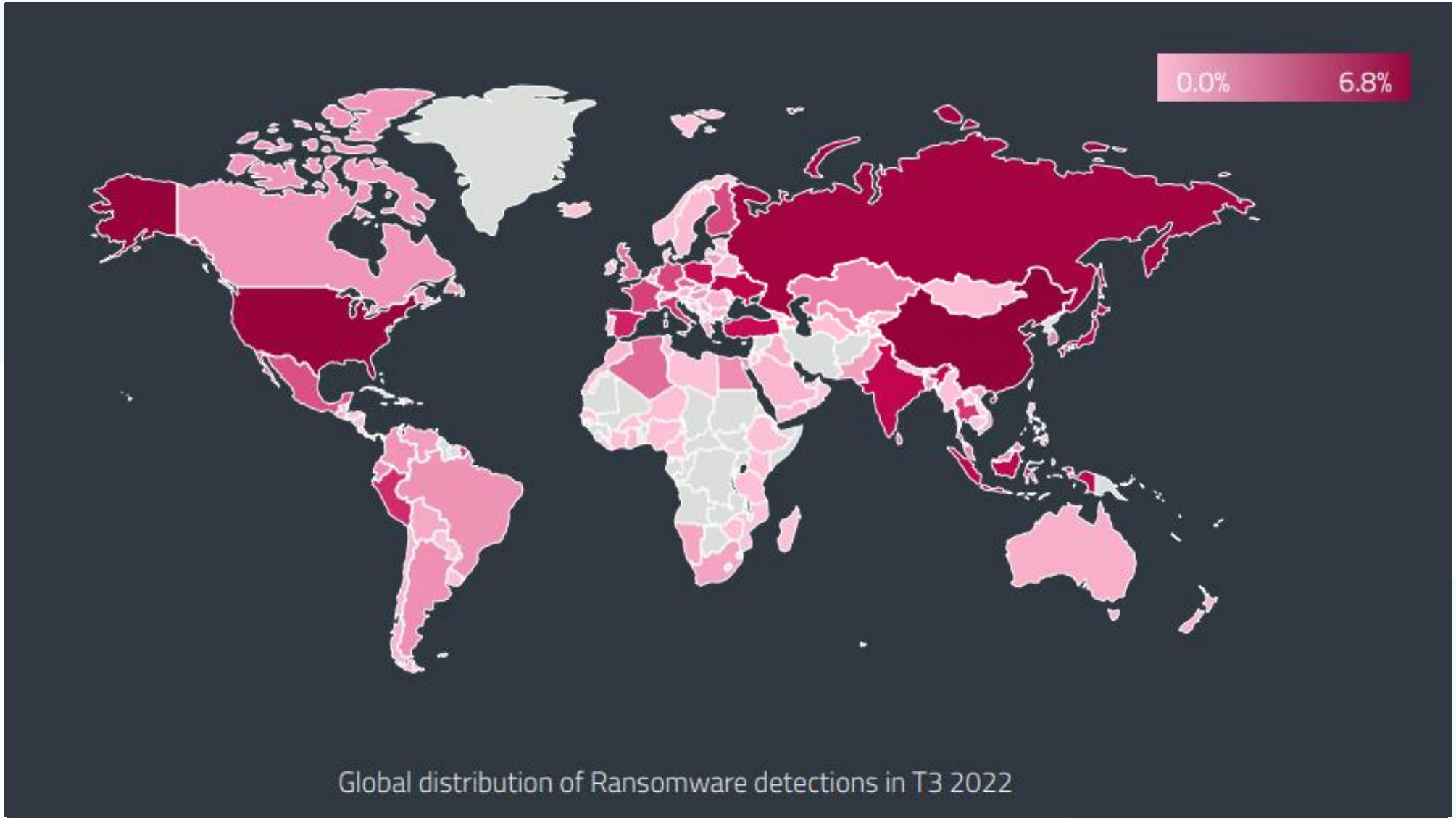
Низкая эффективность классических систем защиты

Неправомерные действия сотрудников

Отсутствие квалифицированных кадров

Программы-вымогатели (Ransomware)

Программы-вымогатели (Ransomware)



Целенаправленные атаки (APT) и взлом

Целенаправленные атаки (APT) и взлом

Цели атаки

- шпионаж
- саботаж
- компрометация
- фальсификации

Способы и методы проникновения

- социальная инженерия
- утечка учетных данных
- уязвимости ОС и ПО
- компрометация каналов связи и легального ПО
- инсайдеры *(неумышленные)*

Последствия действий атакеров

- утечка данных
- остановка бизнес-процессов
- уничтожение информации
- вывод из строя оборудования
- искажение информации

Особенности современных атак

- Атаки проводятся в несколько этапов, растянутых по времени
- Постоянные попытки проникновения через различные векторы
- Первичные модули имеют цифровую подпись и не содержат вредоносного кода
- Перехват учетных записей и повышение привилегий
- Скрытое распространение внутри взломанной инфраструктуры
- Построение защищенных каналов связи с серверами управления (C&C)
- Активная фаза атаки – без использования файлов и хранения данных

Слабозащищенные инфраструктуры

Слабозащищенные инфраструктуры

- Несегментированная сетевая инфраструктура
- Незащищенные каналы связи
- Слабозащищенный доступ к корпоративным ресурсам
- Отсутствие актуальных обновлений ОС и ПО
- Незащищенные ОС (Linux/Unix, macOS, Android, iOS)
- Неконтролируемые удаленные рабочие станции
- Отсутствие защиты конфиденциальной информации
- Отсутствие надежных систем резервного копирования

Низкая эффективность классических систем защиты

Низкая эффективность классических систем защиты

Недостатки классических систем защиты

- Устаревшие подходы к защите инфраструктуры
- Отсутствие систем централизованного мониторинга
- Неправильная оценка критичности инцидентов
- Отсутствие решений для выявления аномальной активности
- Отсутствие инструментов для реагирования на киберинциденты
- Недостаток ИТ-ресурсов (аппаратных и человеческих)

Низкая эффективность классических систем защиты

Специфика деятельности киберпреступников

- Атакеры действуют в обход существующих систем защиты
- APT-группировки постоянно изобретают новые техники и тактики
- Регулярно выявляются новые уязвимости в ПО и ОС
- Ложные цели – множество заблокированных файлов и IP-адресов
- **Самое слабое звено в защищенной инфраструктуре – человек**

Неправомерные действия сотрудников

Неправомерные действия сотрудников

- Посещение недоверенных или опасных Интернет-ресурсов
- Использование сторонних непроверенных съемных носителей
- Несанкционированное подключение сторонних устройств
- Самовольная установка и использование непроверенного ПО
- Нарушение прочих правил политики безопасности

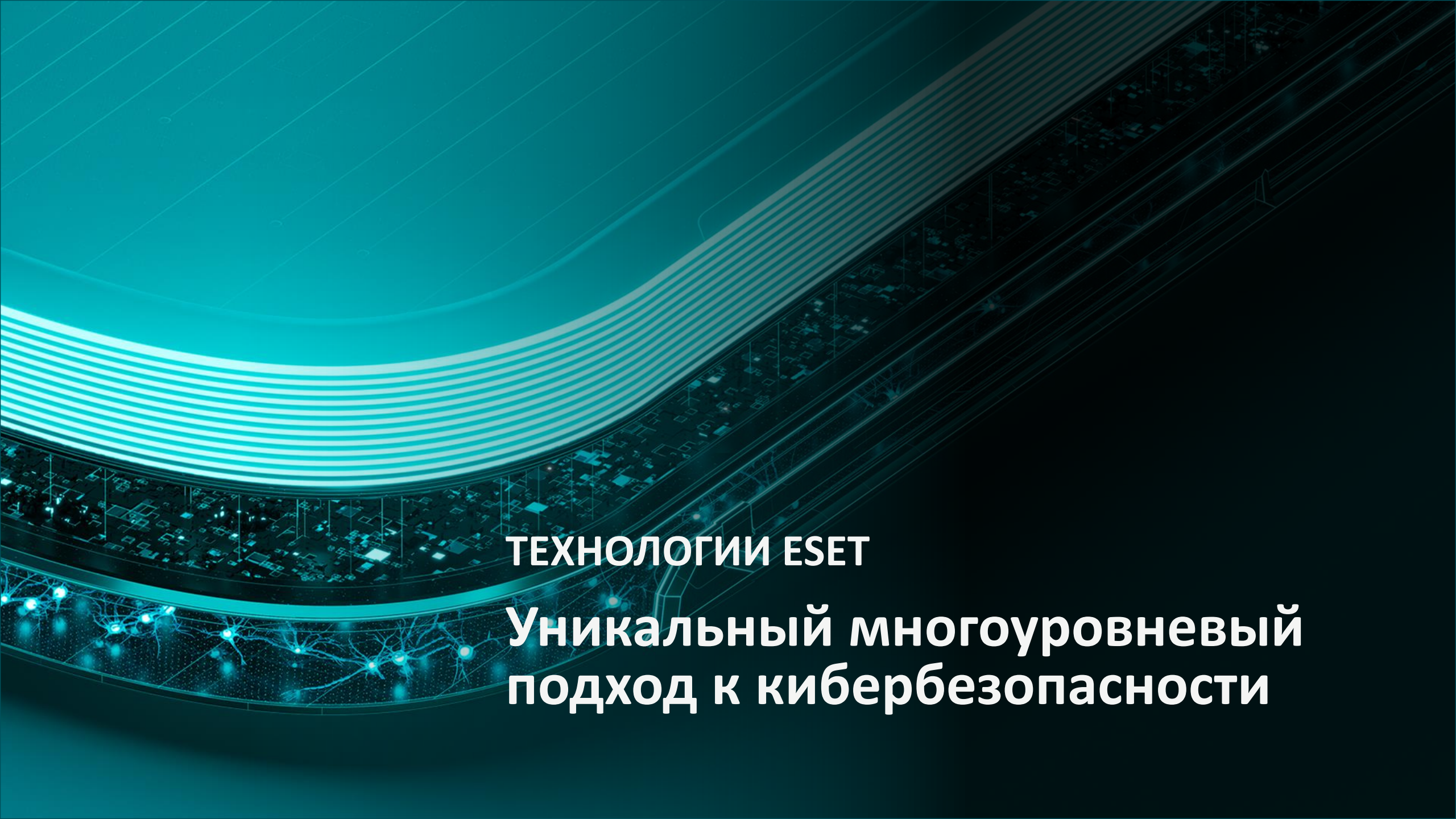
Отсутствие квалифицированных кадров

Отсутствие квалифицированных кадров

- Отсутствие подразделения ИБ как такового
- Неправильное взаимодействие между ИТ и ИБ
- Отсутствие понимания проблематики кибербезопасности
  (С чем боремся? От чего защищаемся?)
- Отсутствие четкой утвержденной политики безопасности
- Отсутствие процедуры реакции на атаку *(массовое заражение)*
- Отсутствие плана восстановления после атаки *(Disaster Recovery Plan)*

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ESET ДЛЯ МОЩНОЙ ВСЕСТОРОННЕЙ ЗАЩИТЫ

Digital Security
Progress. Protected.



ТЕХНОЛОГИИ ESET

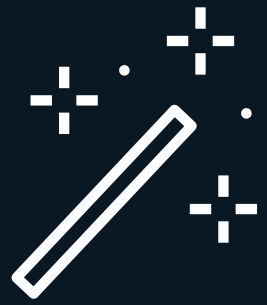
Уникальный многоуровневый подход к кибербезопасности

ОСНОВНЫЕ ПРИНЦИПЫ ТЕХНОЛОГИЙ ESET

НАДЕЖНОСТЬ

ВЫСОКИЙ УРОВЕНЬ ОБНАРУЖЕНИЯ

МИНИМАЛЬНОЕ ПОТРЕБЛЕНИЕ РЕСУРСОВ



ЛЕГКОСТЬ ИСПОЛЬЗОВАНИЯ

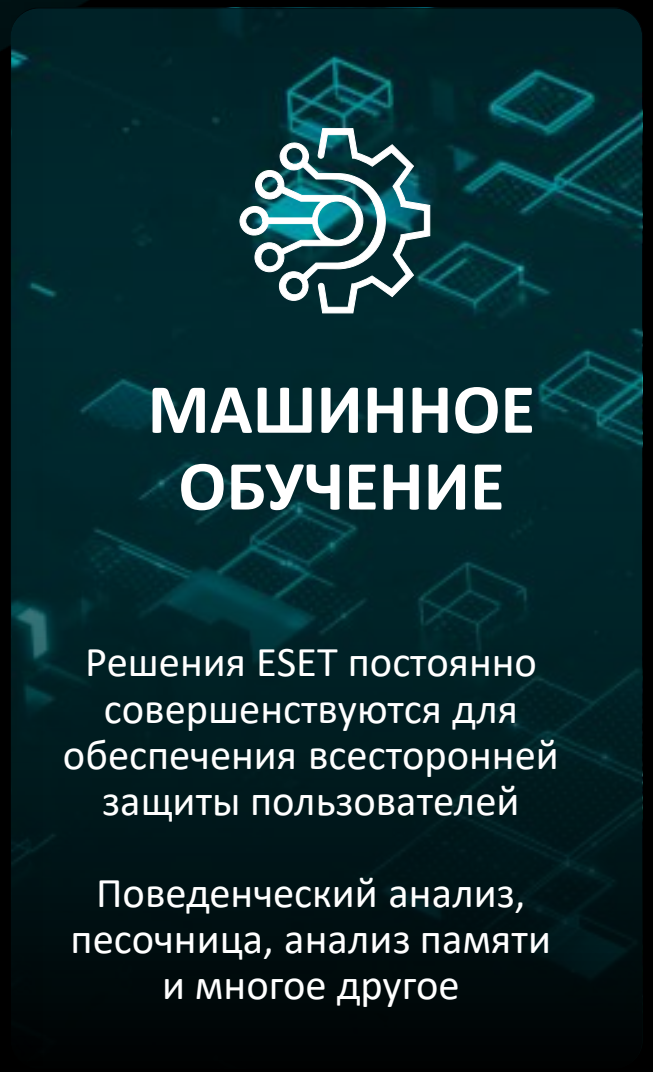
ОСНОВА КИБЕРЗАЩИТЫ ESET

ESET LIVEGRID

(Облачная репутационная система)

Информация об угрозах непрерывно актуализируется благодаря данным с устройств ESET во всем мире

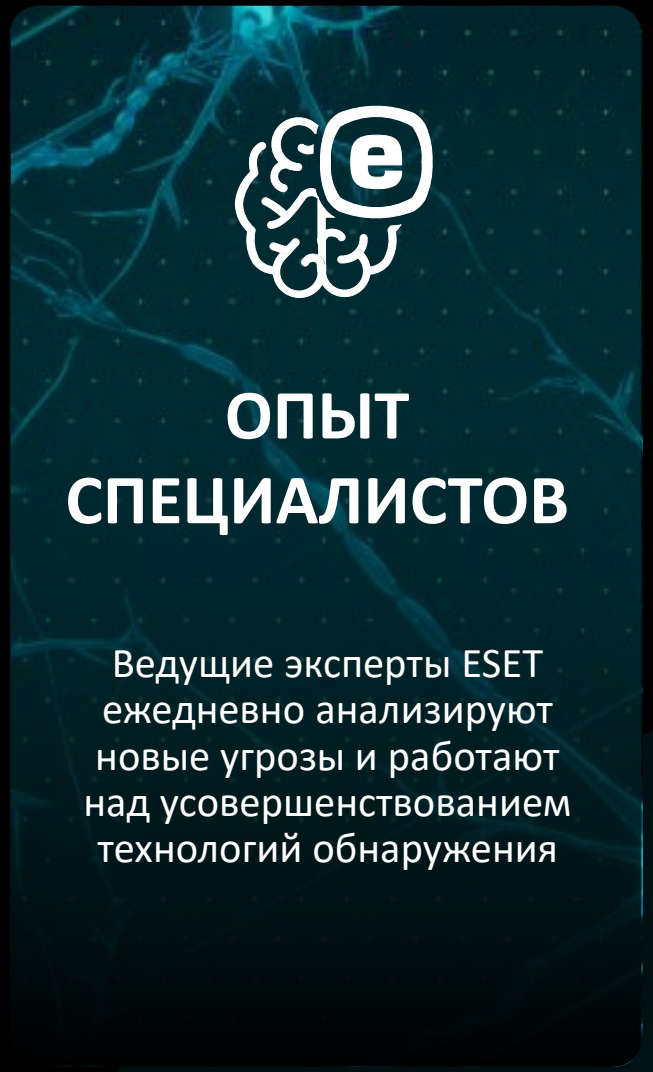
Новые угрозы мгновенно блокируются у пользователей ESET LiveGrid



МАШИННОЕ ОБУЧЕНИЕ

Решения ESET постоянно совершенствуются для обеспечения всесторонней защиты пользователей

Поведенческий анализ, песочница, анализ памяти и многое другое



ОПЫТ СПЕЦИАЛИСТОВ

Ведущие эксперты ESET ежедневно анализируют новые угрозы и работают над усовершенствованием технологий обнаружения

МНОГОУРОВНЕВАЯ ЗАЩИТА

ESET LiveGrid®
(Облачная репутационная система)

Машинное обучение

Опыт специалистов

ESET LiveSense®
Многоуровневая технология для защиты

ESET LiveSense®

В основе продуктов ESET – эффективные технологии защиты, которые могут обнаруживать и блокировать угрозы на разных этапах их активности.

ПЕРЕД ВЫПОЛНЕНИЕМ

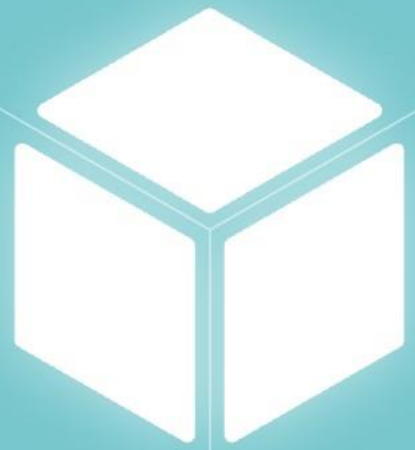
- Репутация и кэш
- Защита от сетевых атак
- Сканер UEFI
- Машинное обучение
- Защита от атак с подбором паролей
- Контроль устройств
- Родовые обнаружения
- Встроенная песочница

ВО ВРЕМЯ ВЫПОЛНЕНИЯ

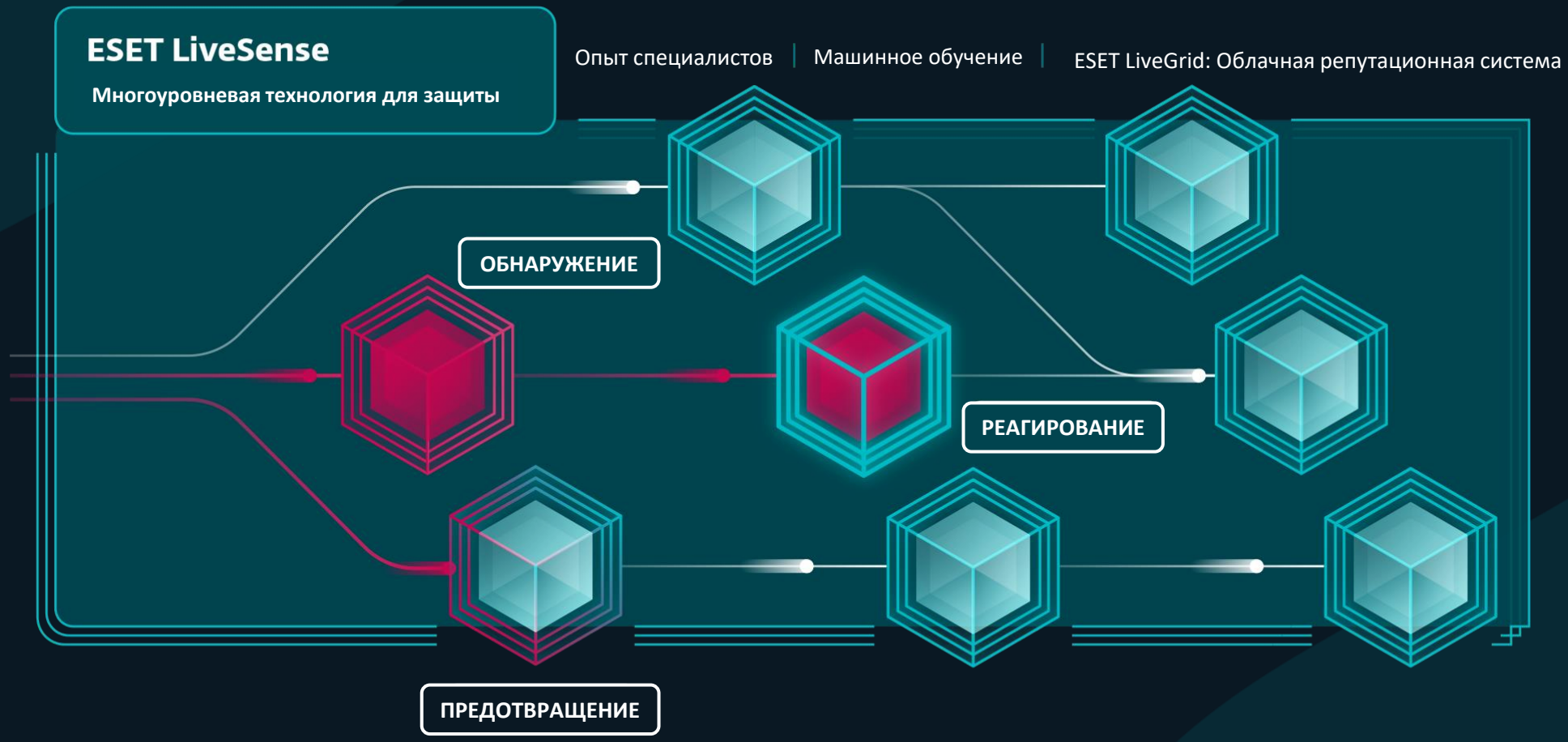
- Защита от программ-вымогателей
- Сканер скриптов и AMSI
- Расширенный сканер памяти
- Защита от эксплойтов
- Анализ поведения

ПОСЛЕ ВЫПОЛНЕНИЯ

- Технология ESET LiveGrid®
- Защита браузера
- Защита от ботнетов

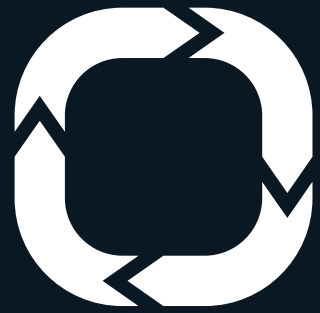


ЦЕЛОСТНЫЙ ПОДХОД ESET К БЕЗОПАСНОСТИ



ПРОГНОЗИРОВАНИЕ

ПРЕДОТВРАЩЕНИЕ



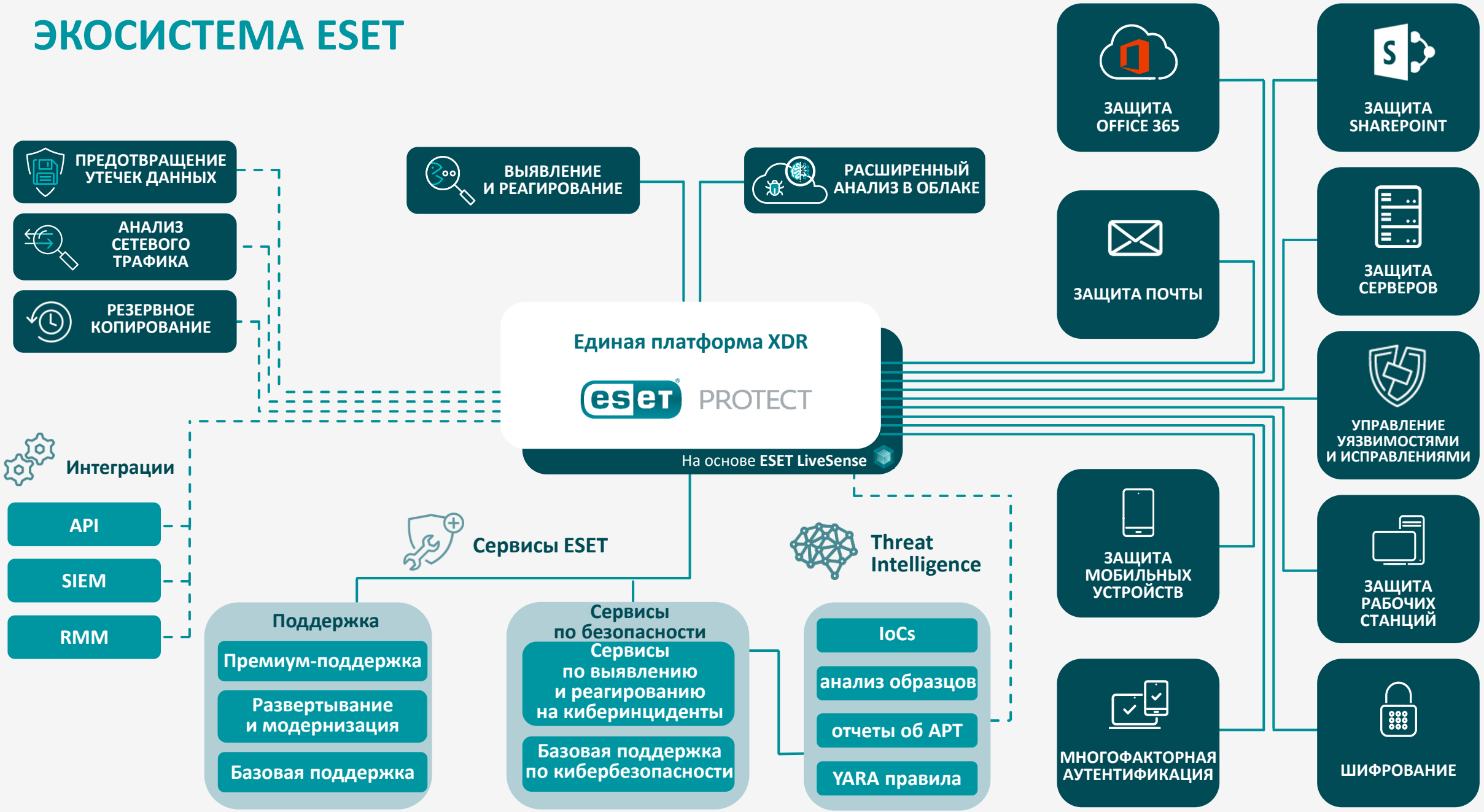
РЕАГИРОВАНИЕ

ОБНАРУЖЕНИЕ

ЭКОСИСТЕМА ESET – МНОГОУРОВНЕВАЯ КОМПЛЕКСНАЯ ЗАЩИТА

Digital Security
Progress. Protected.

ЭКОСИСТЕМА ESET

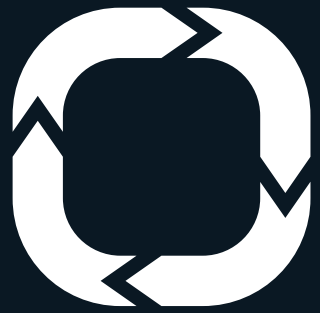


ESET Threat Intelligence
Индикаторы компрометации
Отчеты об APT Premium

ПРОГНОЗИРОВАНИЕ

ESET PROTECT
ESET Endpoint Security
ESET Secure Authentication
ESET Endpoint Encryption
Safetica – Предотвращение утечки данных

ПРЕДОТВРАЩЕНИЕ



РЕАГИРОВАНИЕ

ESET PROTECT
ESET LiveGuard Advanced
ESET Cloud Office Security
ESET Inspect
Управление уязвимостями и исправлениями
Xopero – Резервное копирование
GreyCortex – Анализ сетевого трафика

ОБНАРУЖЕНИЕ

ESET PROTECT
ESET Endpoint Security
ESET LiveGuard Advanced
ESET Cloud Office Security
Управление уязвимостями и исправлениями
Safetica – Предотвращение утечки данных
GreyCortex – Анализ сетевого трафика

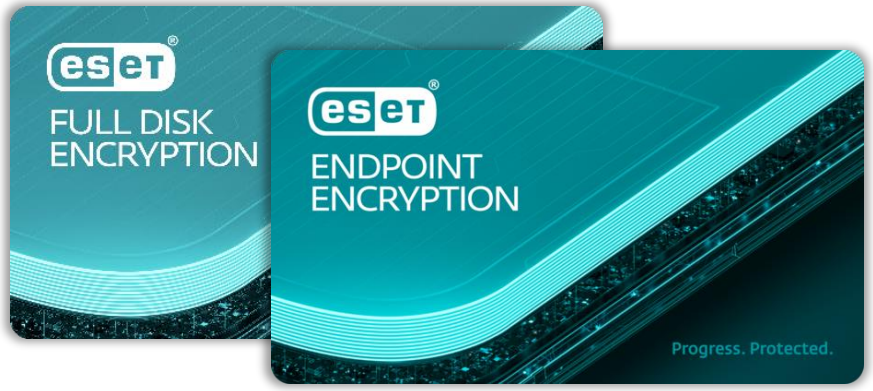
ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИЙ В УСЛОВИЯХ ПОСТОЯННЫХ КИБЕРАТАК

Основные способы получения доступа к конфиденциальным данным

- Компрометация учетных записей:
  - Фишинг
  - Социальная инженерия
  - Атаки методом подбора пароля
- Нарушение, несоблюдение или отсутствие бизнес-процессов в работе с конфиденциальными данными
- Человеческие ошибки
- Инсайдеры
- Отсутствие инструментов защиты конфиденциальных данных или доступа к ним

Решения ESET для защиты данных

Надежная аутентификация пользователей во время доступак корпоративным ресурсам



Шифрование конфиденциальных данных и устройств организации

ESET SECURE AUTHENTICATION

МНОГОФАКТОРНАЯ АВТЕНТИФИКАЦИЯ

ESET SECURE AUTHENTICATION

61% инцидентов несанкционированного доступа к данным связаны с учетными данными*

Продукт помогает организациям справиться с вызовами:

- Рост рисков из-за наличия персонала, работающего удаленно
- Наличие подрядчиков, имеющих доступ к сети извне
- Увеличение количества облачных сервисов
- Необходимость соблюдения требований по защите персональных данных
- Целенаправленный несанкционированный доступ к данным
- Установка простых паролей сотрудниками

* Источник: Verizon 2021 Data Breach Investigation Report

ESET SECURE AUTHENTICATION

Основные преимущества

- Работа с аппаратными ключами и смартфонами
- Отсутствие потребности в дополнительном оборудовании
- Наличие SDK и API
- Поддержка стандартного протокола (SAML2) для подключения к пользователям
- Удаленное управление
- Push-аутентификация
- Настройка за 10 минут

ESET SECURE AUTHENTICATION

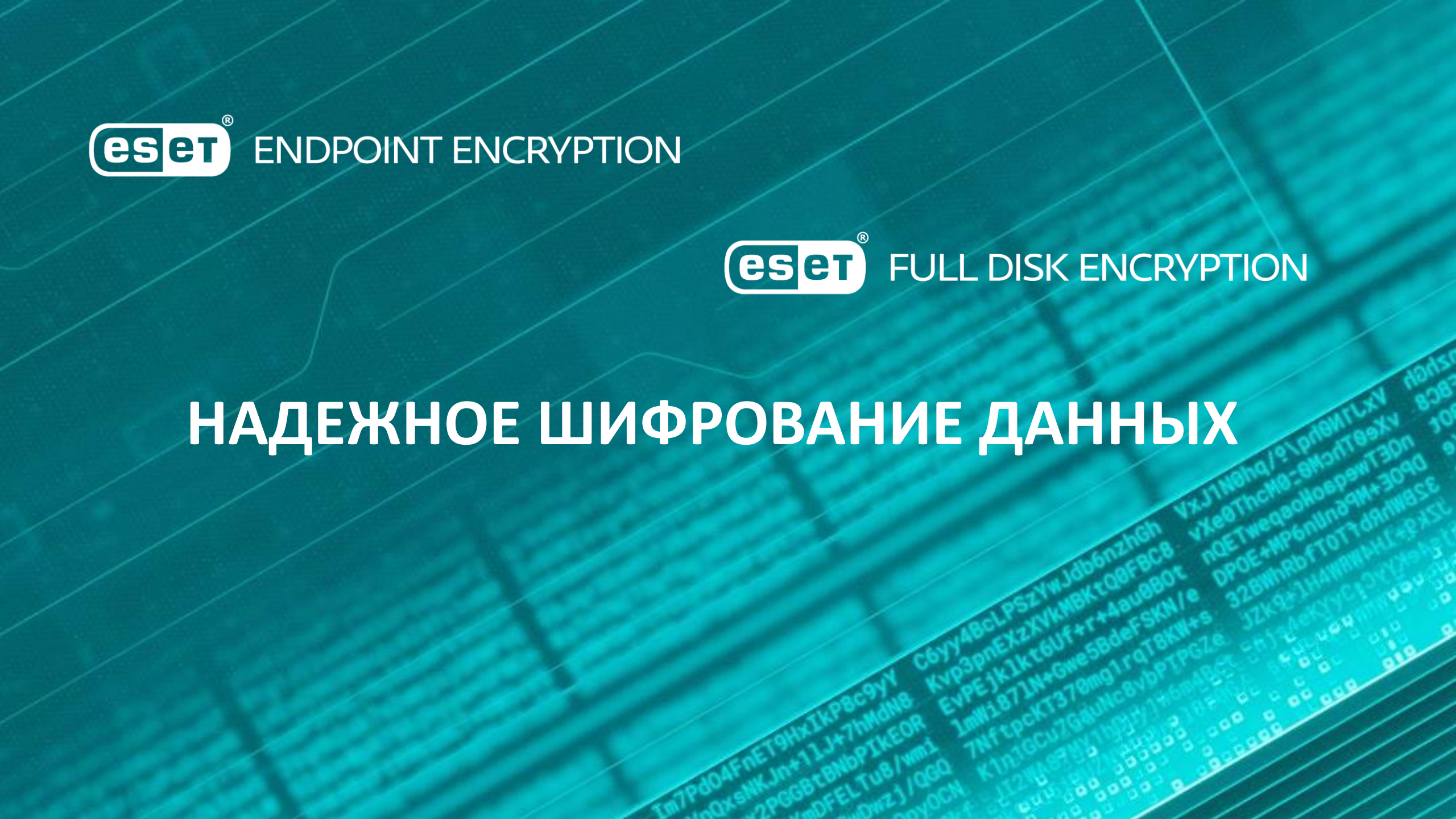
Примеры использования

- Для входа на физический локальный компьютер, виртуальный компьютер, удаленный рабочий стол
- Для входа в вебпочту, CRM и другие сервисы, доступные через браузер
- Для входа в хранилища сторонних производителей, например Dropbox
- Для VPN-соединения

ESET ENDPOINT ENCRYPTION

ESET FULL DISK ENCRYPTION

НАДЕЖНОЕ ШИФРОВАНИЕ ДАННЫХ

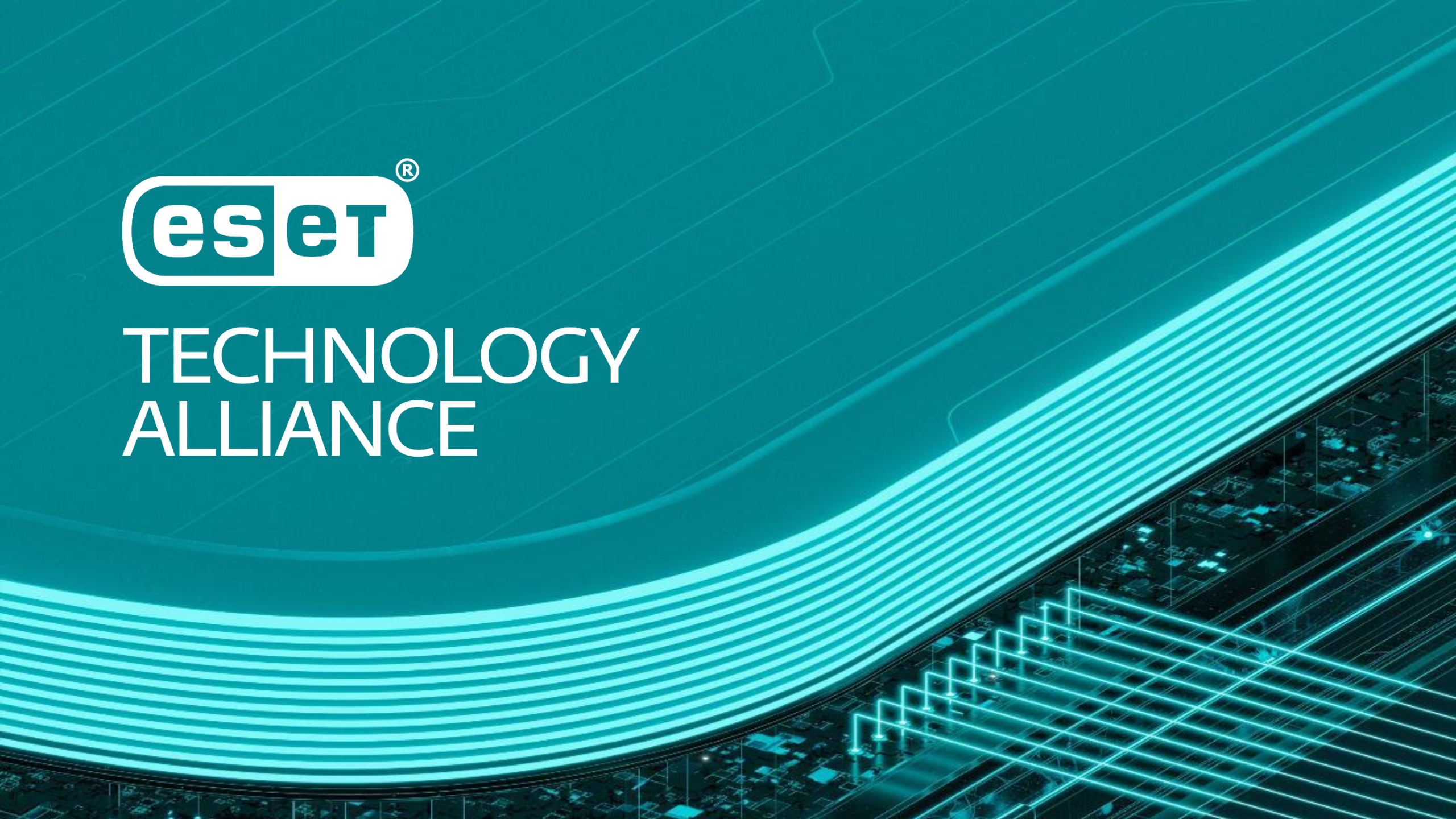


Полнодисковое шифрование	●	●
Управление шифрованием на Windows	●	●
Управление шифрованием на macOS	●	●
Шифрование сменных носителей		●
Шифрование файлов и папок		●
Плагин Outlook для сообщений электронной почты и вложений		●
Виртуальные диски и зашифрованные архивы		●

Антон Дмитриев

Директор по развитию бизнеса ESET
в Центральной Азии, Армении, Грузии, Молдове и Украине

anton.dmitriev@adeon.international


eset
TECHNOLOGY
ALLIANCE

всегда заботится о вашей безопасности

- ESET Technology Alliance был создан в **2013** году, чтобы сделать ваш бизнес еще более безопасным

- На данный момент в ESET Technology Alliance три компании: **Safetica, GREYCORTEX** и **Xopero**

ESET TECHNOLOGY ALLIANCE

OPERO Backup&Recovery

Резервное копирование и восстановление ваших бизнес-данных на месте или в облаке

safetica

Защита от внутренних угроз и защита от утечки данных (DLP – Data Leak Prevention)

GREYCORTEX

Инструмент для анализа сетевого трафика, использующий искусственный интеллект, машинное обучение и большие данные

safetica

Предотвращение потери данных и управление внутренними рисками

1 000 000+
защищенных пользователей

120+
стран

О компании

Safetica – это международная компания, предоставляющая решения для предотвращения потери данных и управления внутренними рисками для организаций всех форм и размеров.

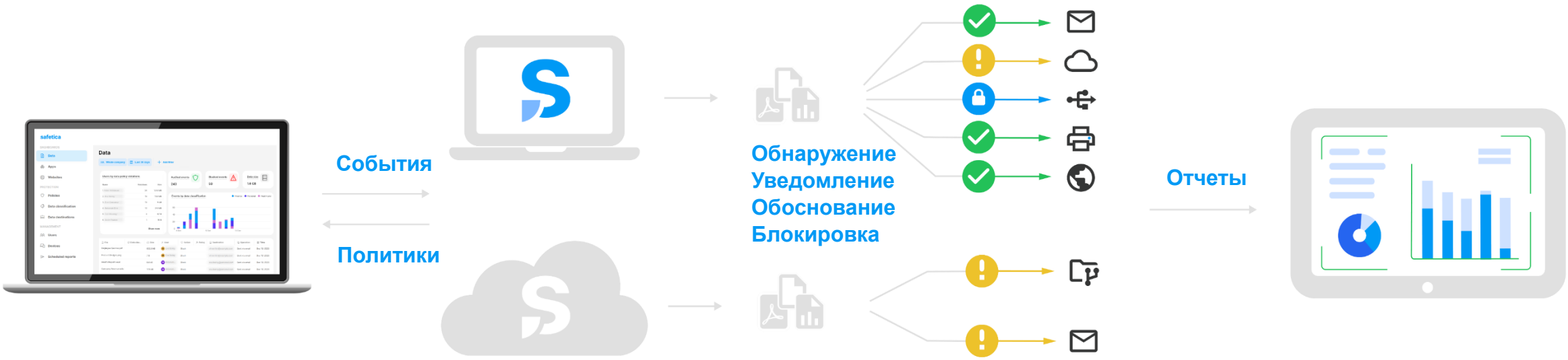
«Мы в Safetica считаем, что каждый заслуживает того, чтобы его данные были надежно защищены».

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner

Как работает Safetica



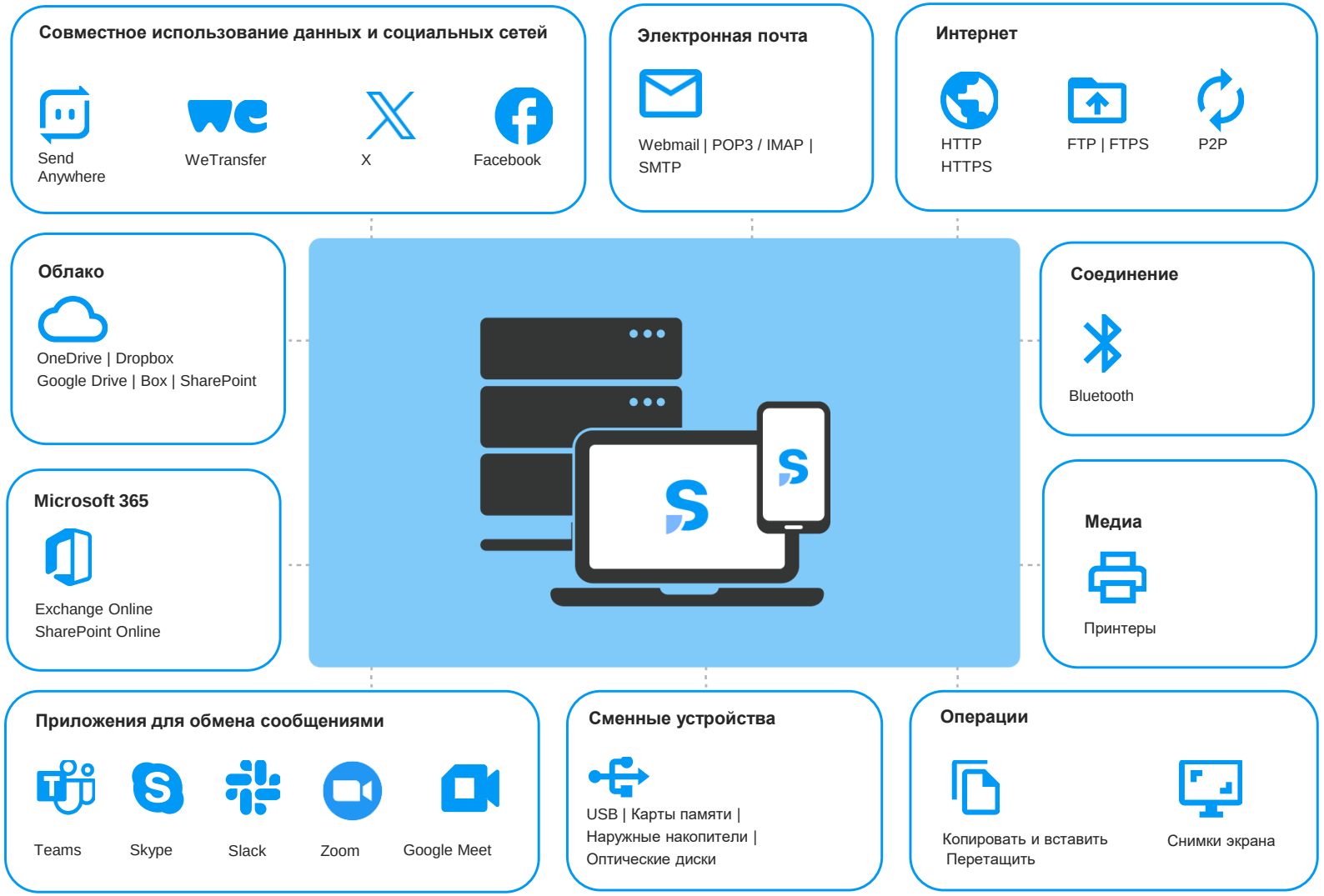
1 Обнаружение

2 Защита

3 Обучение

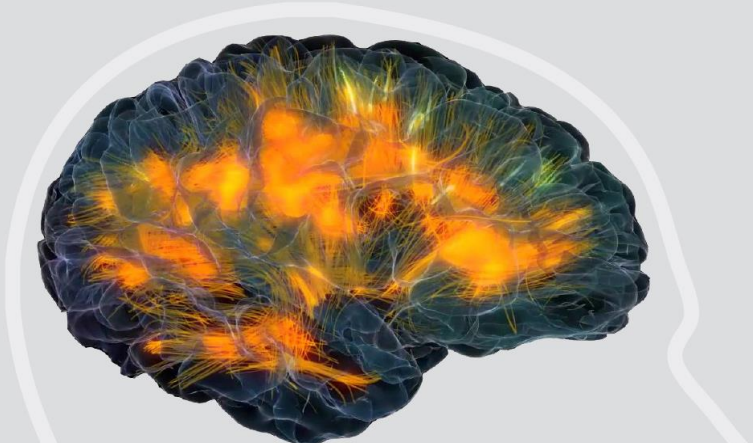
4 Расследование

Покрытие каналов передачи данных Safetica



GREYCORTEX

Мониторинг безопасности
Средних и больших ИТ-сетей



Version 2022/02

GREYCORTEX Mendel

Видимость

Все сетевые коммуникации, устройства с подробной инвентаризацией и поведением пользователей

Обнаружение

От неправильных конфигураций, проблем с производительностью или нарушений политик до необнаруженных вредоносных программ, программ-вымогателей и хакерских действий, которые могут обойти существующие инструменты безопасности

Реагирование

Быстрое реагирование на атаки, расследование и управление инцидентами

+

SCADA/ICS мониторинг

Мониторинг производительности приложений

Инвентаризация активов

KIWI.COM · Česká pošta · meopta EUROPEAN OPTICS | SINCE 1933 · Czech Republic Ministry of Transport · Sąd Apelacyjny w Warszawie · Grupa Żywiec · KB · VD

Сетевое обнаружение и реагирование / NDR

Передовой искусственный интеллект, машинное обучение, анализ данных и традиционные методы обнаружения.

GREYCORTEX

Минимальный сценарий развертывания

Развертывание одного универсального устройства

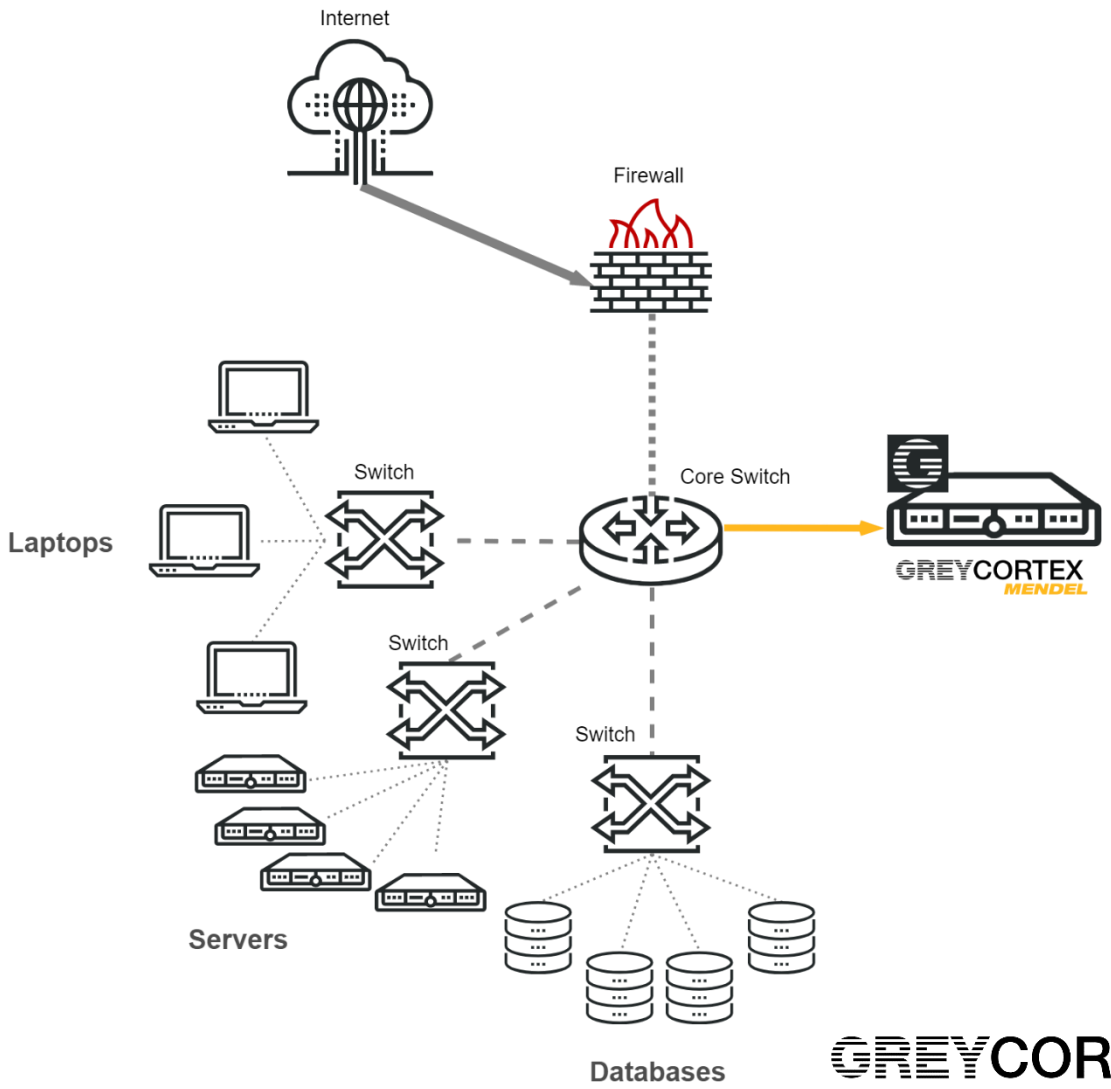
Быстрое развертывание с немедленными результатами

Модели со скоростью от 200 Мбит/с до 100 Гбит/с

Интерфейсы мониторинга 1GbE/10GbE/25GbE/100GbE

500 хостов в сети до 500.000

Поддержка VMware, KVM, AWS, Azure и GCP.



GREYCORTEX

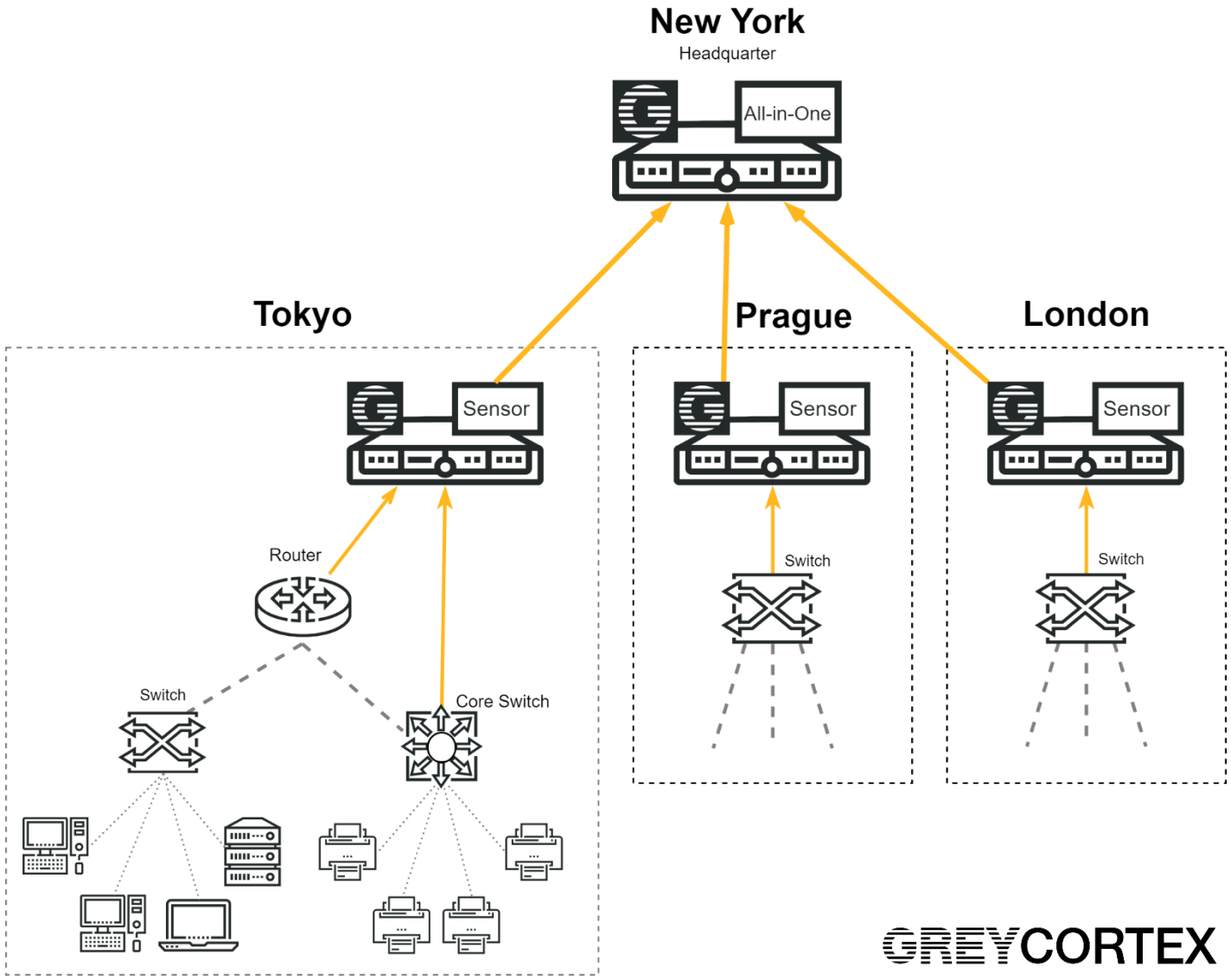
Развертывание в сложной инфраструктуре

Комплексное устройство (датчик + коллектор), развернутое в крупнейшем головном офисе

Датчики установлены в филиалах

1 коллектор может обрабатывать более 40 датчиков и 150 000 контролируемых хостов.

Несколько коллекторов можно подключить через центральное управление событиями, SIEM конечного пользователя или другую консоль управления.



GREYCORTEX


XOPERO ONE
Backup&Recovery

Безопасность на первом месте

GDPR

ISO 27001

SOC 2 Type I

SOC 2 Type II

Высокая продуктивность весна-лето 2022

5 звезд в рейтинге резервного копирования

Продукт года 2022

Продукт/сервис года 2019

Экосистема

Xopero ONE

ЛЮБАЯ ПЛАТФОРМА

Рабочие станции

Серверы

Базы данных

Виртуальные машины

Microsoft 365

DevOps

ДВЕ МОДЕЛИ РАЗВЕРТЫВАНИЯ

Локально/SaaS

Централизованное управление

ЛЮБОЕ ХРАНИЩЕ

Облако

NAS

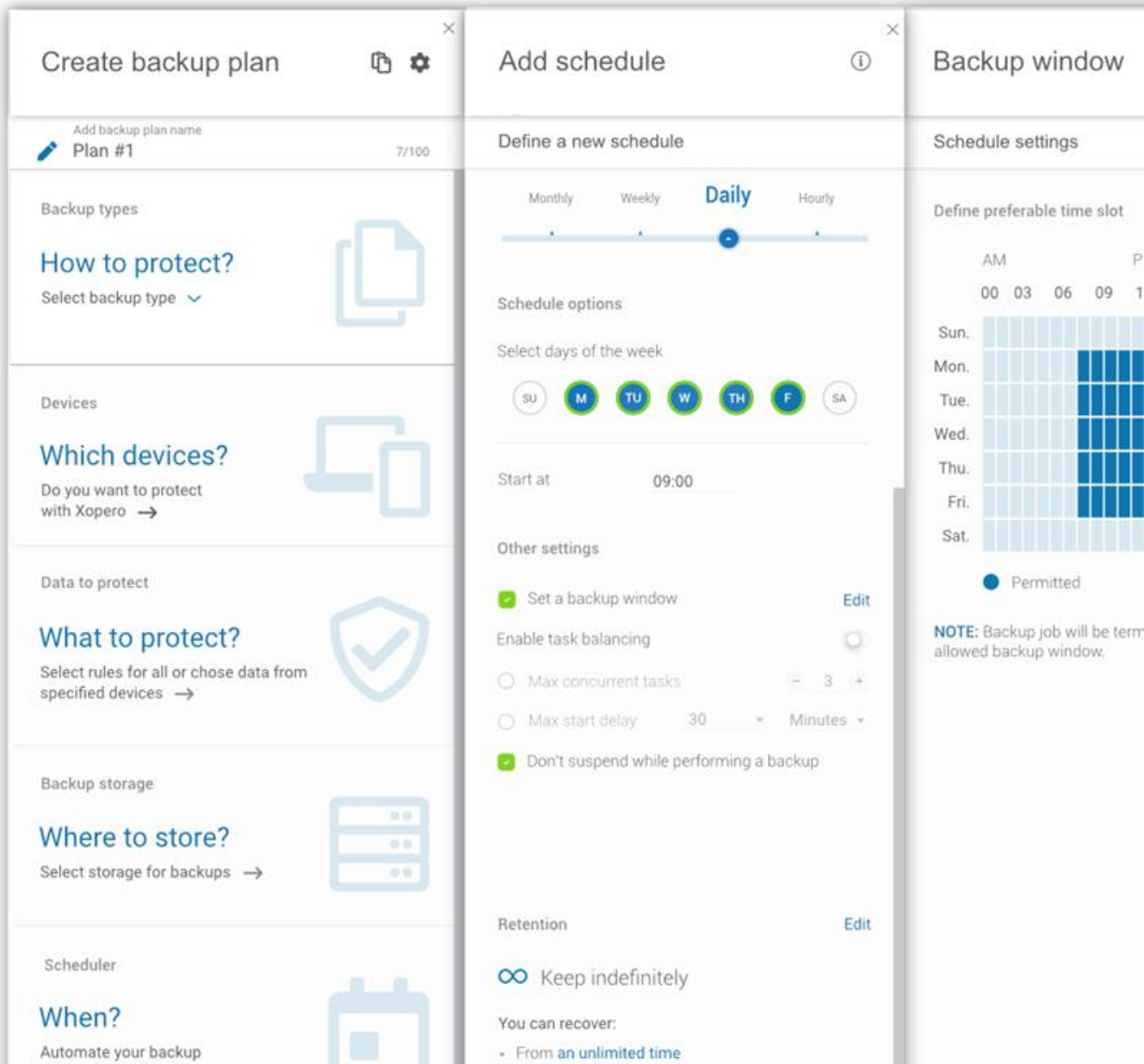
Файловая система

Local, iSCSI, SMB, CIFS, NFS

Защита от программ-вымогателей

Все лучшее собрано в Xopero ONE

- Глобальная дедупликация,
- Репликация между всеми видами хранилищ
- Возможность использования нескольких хранилищ в одной инсталяции Xopero ONE
- Моментальное восстановление
- Гибкий планировщик на основе подходов: Basic, GFS или Forever Incremental
- Расширенные настройки хранения
- Сжатие данных в источнике
- Шифрование AES налету и в состоянии покоя



Александр Иллюша

Руководитель службы технической поддержки ESET в Центральной Азии, Армении, Грузии, Молдове и Украине

oleksandr.Illiusha@adeon.international

ОПЫТ СПЕЦИАЛИСТОВ ESET: НЕСТАНДАРТНЫЕ СПОСОБЫ ОБХОДА СИСТЕМ ЗАЩИТЫ КИБЕРПРЕСТУПНИКАМИ

Digital Security
Progress. Protected.

Несанкционированный доступ в Интернет в изолированной сети

Несанкционированный доступ в Интернет в изолированной сети

Особенности

Даже когда подключение внешних модемов ЗАПРЕЩЕНО

- (**Wi-Fi** роутер) **+** (**3G** модем) **=** (источник **Internet**)
- Подключение смартфона в режиме внешней сетевой карты

Последствия

- Поочередное соединение через LAN:
  или к корпоративной сети, или к Wi-Fi роутеру с Internet
- Одновременное подключение к двум сетям:
  к корпоративной сети через LAN и к Internet через смартфон

Компрометация легальных программ и каналов связи

Компрометация легальных программ и каналов связи

Особенности

- Легальное ПО добавлено в исключение
- Адреса серверов разработчика добавлены в белые списки
- Интеграторы имеют доступ через VPN

Последствия

- Компрометация исходного кода и модулей обновления ПО
- Использование расположения ПО в системе
- Управление атакой через скомпрометированные серверы
- Проникновение в инфраструктуру через VPN-доступы интегратора

«Подписанная» компрометация

«Подписанная» компрометация

Особенности

- Разработка программных модулей под конкретную жертву
- Отсутствие вредоносного кода в первичных модулях
- Использование украденных сертификатов для цифровой подписи
- Маскировка зашифрованных скриптов под системные библиотеки

Последствия

- Беспрепятственная доставка и хранение в ОС
- Проведение разведки и сбор информации
- Использование для дальнейших этапов атаки

Получение привилегированных прав

Получение привилегированных прав

Особенности

- Использование украденных учетных данных
- Перехват учетных данных
- Повышение привилегий для простых учетных записей

Последствия

- Почти безграничные возможности для дальнейших этапов
- Действия злоумышленников незаметны для систем защиты

Защищенные каналы передачи данных для связи с серверами C&C

Защищенные каналы передачи данных для связи с серверами C&C

Особенности

- Первичная компрометация – уязвимость веб-сервера
- Развертывание легального ПО на серверах Linux *(VPN, Proxy)*
- Построение каналов связи с управляющими серверами *(C&C)*

Последствия

- Управление атакой через защищенные каналы связи
- Невозможность обнаружения системами защиты на периметре

Бесфайловая активная фаза атаки

Бесфайловая активная фаза атаки

Особенности

- Злонамеренный код не хранится на жестком диске
- Команды и сценарии расшифровываются в оперативной памяти
- Выполняются штатными средствами ОС *(powershell, wscript и т.д.)*

Последствия

- Базовые системы защиты не способны блокировать такую активность
- Нехватка информации для систем мониторинга и реагирования
- Классические инструменты реверс-инжиниринга неэффективны

Флуд киберинцидентов

Флуд киберинцидентов

Особенности

- Генерация фейковых инцидентов
- Большое количество ложных целей
- Одновременная активность на нескольких направлениях (векторах)

Последствия

- Сложности оценки критичности и определения приоритетов
- Офицеры по безопасности не успевают прорабатывать инциденты
- Некоторые системы ограничены количеством или объемом инцидентов

Перехват инициативы в ходе расследования

Перехват инициативы в ходе расследования

Особенности

- Контроль изменений в инфраструктуре жертвы
- Контроль корпоративных каналов коммуникации
- Мониторинг действий администраторов и офицеров безопасности

Последствия

- Своевременное информирование злоумышленников о ходе расследования
- Возможность злоумышленников действовать на опережение
- Использование полученной информации против «защитников»

Полная остановка инфраструктуры

Полная остановка инфраструктуры

Особенности

- Наличие прав администратора домена
- Недостатки в настройках систем защиты
- Несколько каналов для управления атакой

Последствия

- Удаление всех виртуальных машин и уничтожение гипервизора
- Удаление всех резервных копий и уничтожение сервера бекапов
- Запуск сценария уничтожения информации на всех ПК
- Сбойная перепрошивка сетевого оборудования

Возникли вопросы?

Помощь по вопросам
установки и настройки
продуктов ESET:
support@esetofficial.uz

Консультации
по выбору продуктов
и партнерстве:
sales@esetofficial.uz

https://eset.com

Digital Security
Progress. Protected.

support@esetofficial.uz

Подписывайтесь
на Facebook-страницу!


eset
SECURITY
DAYS