NOVENTIQ
Global expertise, local outcomes

IT Wake UP

Microsoft 365:
Безопасность в основе бизнеса

Ташкент
30.11.2023

NOVENTIQ
Global expertise, local outcomes

MICROSOFT 365 SECURITY

Безопасность в основе бизнеса

Сергей Жуйков
Архитектор решений Microsoft
Sergey.Zhuykov@noventiq.com

30.11.2023

Международный день компьютерной безопасности 30 ноября 2023

Культура безопасности позволяет достичь большего, чем запреты

Если вы хотите создавать информационную безопасность - не напрягайте людей,
а лучше научите их быть бдительными…

Спикер

Сергей Жуйков

Sergey.Zhuykov@noventiq.com

NOVENTIQ

Global expertise, local outcomes

Noventiq — ведущий партнер Microsoft

Microsoft — крупнейший в мире поставщик стратегических технологий для цифровой трансформации предприятий. Для Noventiq, Microsoft является основой большинства наших решений.

Microsoft Partner

700+
Сертифицированных Microsoft профессионалов

Gold Microsoft Partner
Microsoft

Azure Expert MSP

Member of Microsoft Intelligent Security Association
Microsoft

Проверенный временем и успешный

25+
Лет сотрудничества

1 из 10
глобальных партнёров Microsoft по всему миру

Лучшие практики лицензирования
LSP статус в 34 странах
CSP с момента запуска (T1 and T2)
SPLA реселлер в течение 8 лет

В ряде стран мы являемся единственным поставщиком **Azure Expert Managed Service Provider**

Microsoft Partner of the Year 2020, 2021


Bulgaria


Cambodia x2


Malaysia


Vietnam x2

Microsoft Advanced Specializations:

- Windows Server and SQL Server Migration to Microsoft Azure
- Adoption and Change Management
- Kubernetes on Microsoft Azure
- Linux and Open-Source Database Migration to Azure
- Microsoft Windows Virtual Desktop
- Cloud Security
- Identity and Access Management
- Information Protection and Governance
- Threat Protection
- Azure Virtual Desktop Advance Specialization

- Security Partner of the Year 2021 Малайзия
- Modern Work Partner of The Year 2021 Малайзия
- Security Partner of the Year 2021 Камбоджа
- Security Partner of The Year 2021 Myanmar
- Security Excellence Award Филиппины
- Modern Work Partner of The Year 2021 Камбоджа
- Победитель 2021 Microsoft India's Cloud Champions programme

Как строится кибербезопасность?

- Инвестиции
- Сотрудники
- Технические решения
- Процессы
- Политики

Основные причины срыва планов:

— то одно

— то другое

Какие факторы ведут к неудачам?

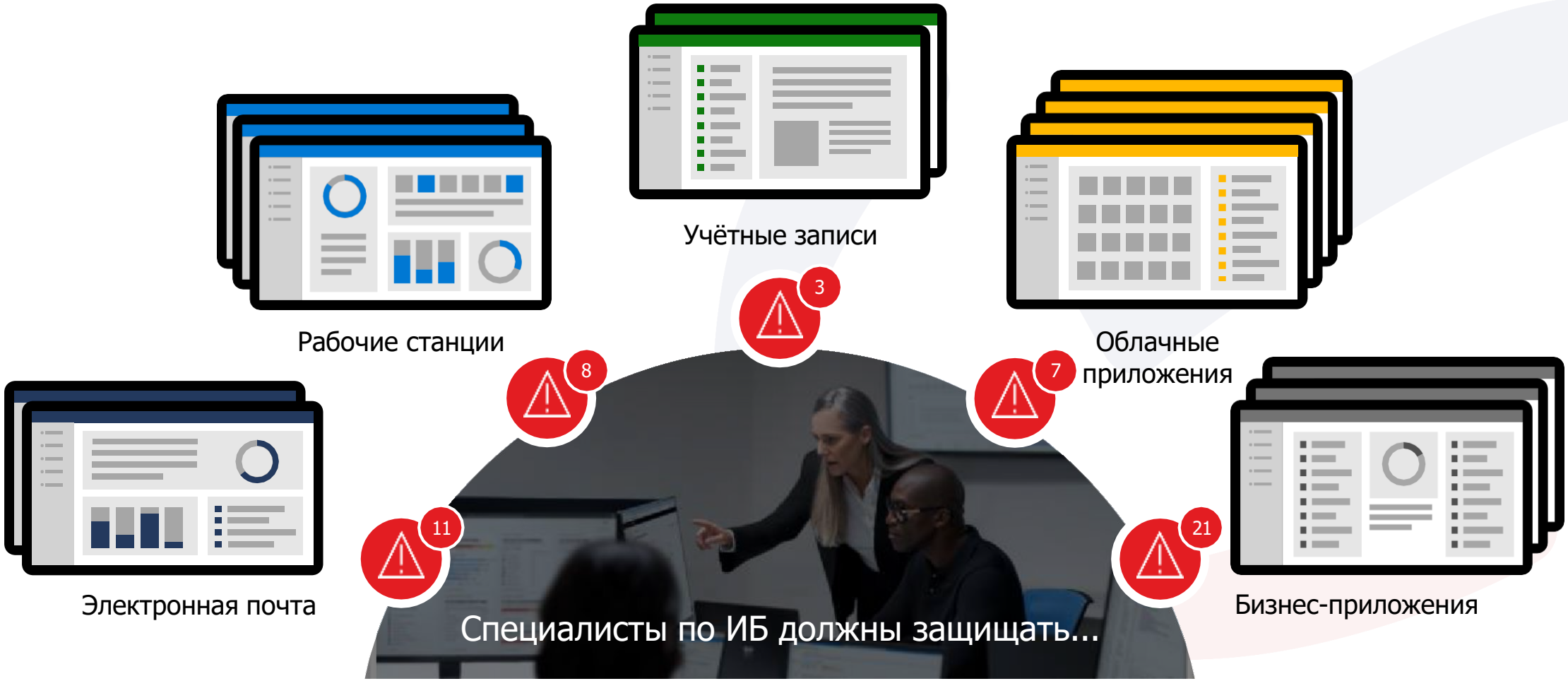
- «Языковой барьер» между ИБ и бизнесом
- Ошибки планирования (занижение оценки времени)
- Ошибки бюджетирования
- Отсутствие лидерства
- Ошибки выбора технологии
- Неверная приоритезация задач
- Устаревшие подходы / архитектура
- (НЕ) соблюдение политик
- Низкая культура кибергигиены
- Предпочтение нулевого риска (мы слишком маленькие)
- Отсутствие измеримых показателей
- Слишком много данных

Мультивендорная безопасность

Типичная команда SecOps использует **45 инструментов** от **13 вендоров**

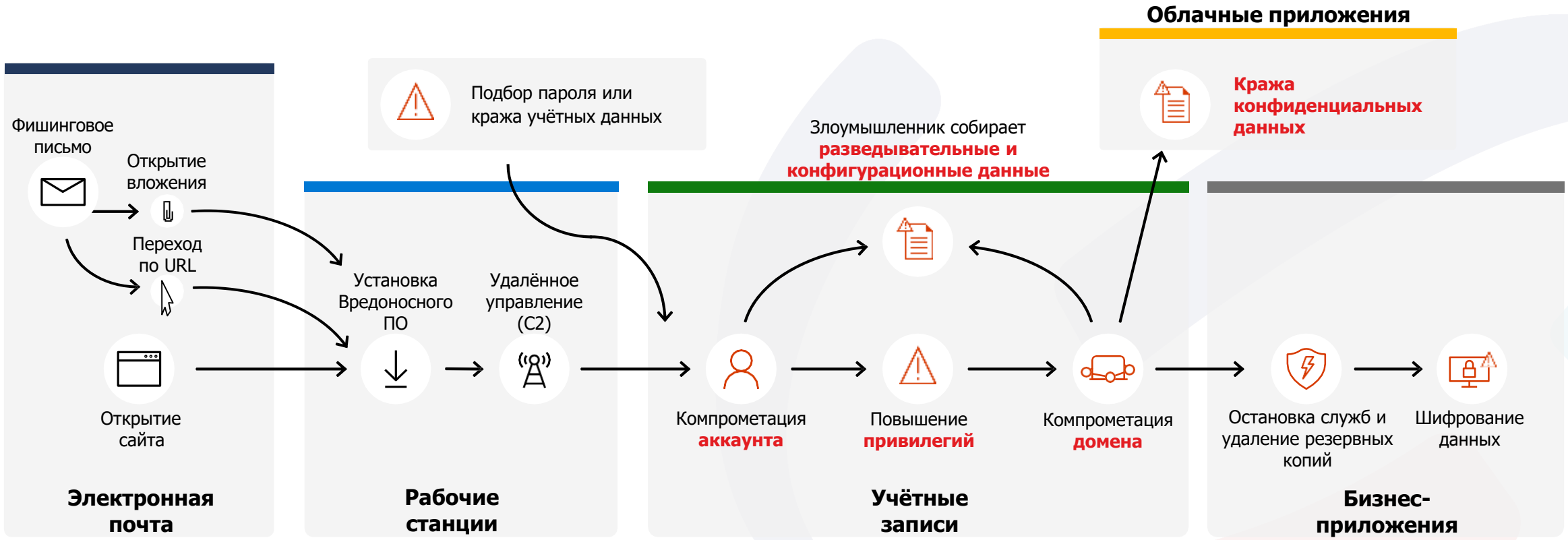
NOVENTIQ

Почему защита так сложна?

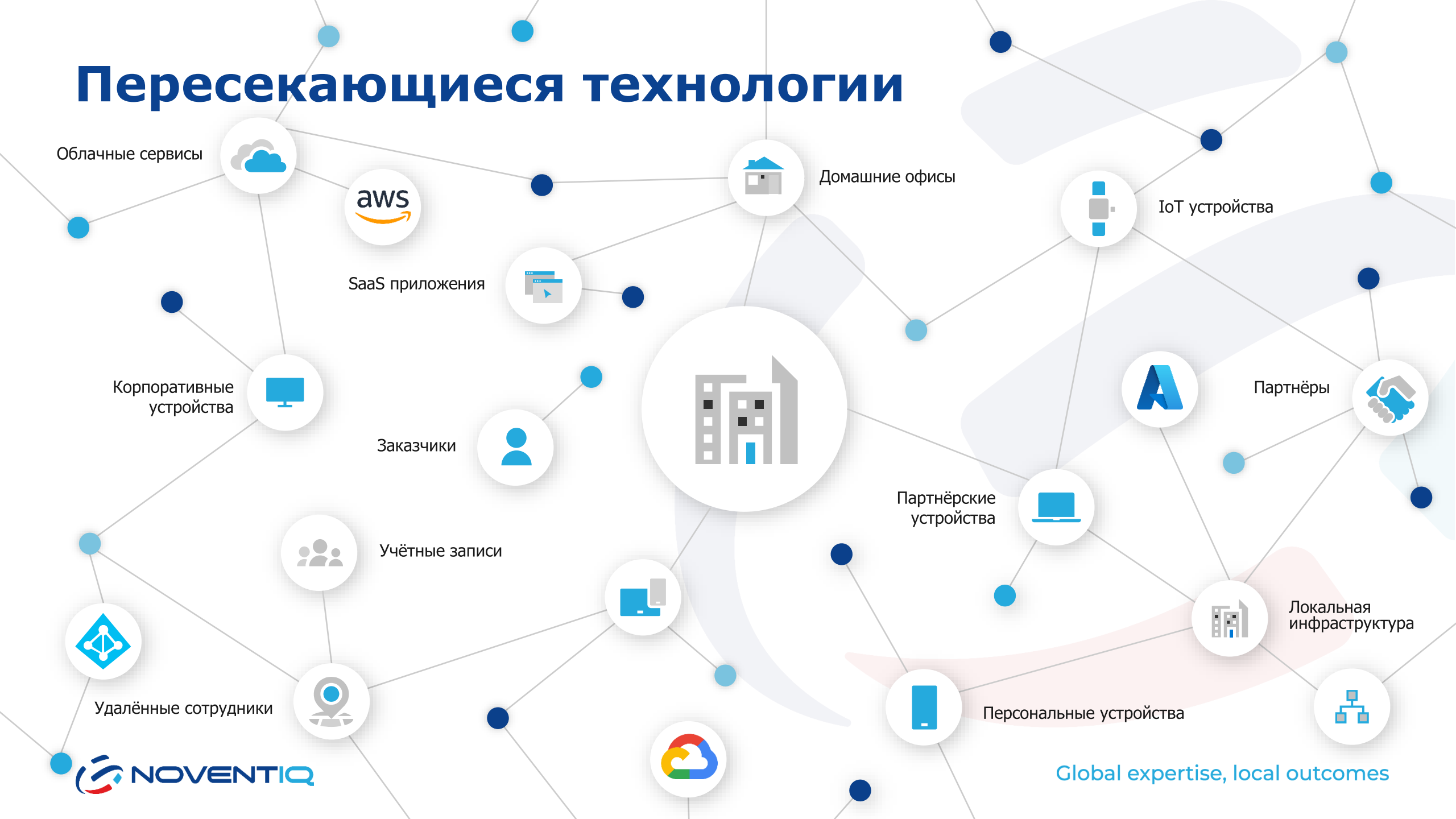


Атака охватывает сразу несколько областей

Типичная атака вымогателя, управляемая человеком



Пересекающиеся технологии

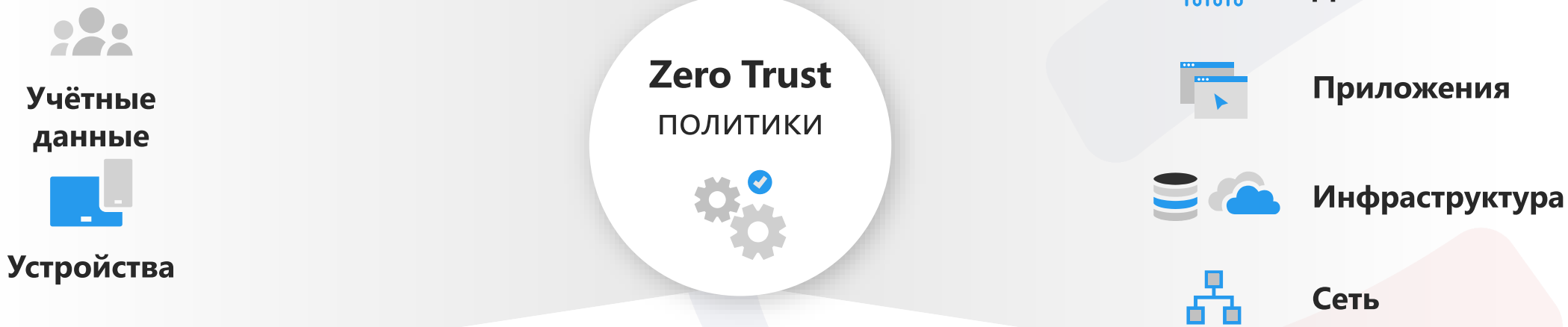


NOVENTIQ

Global expertise, local outcomes

Методология Zero Trust

Явная проверка | **Наименьшие** привилегии | Предположение **нарушения**



Методология Zero Trust

Явная проверка | **Наименьшие** привилегии | Предположение **нарушения**

Всегда проводите аутентификацию и авторизацию на основе всех доступных данных.

Ограничьте доступ пользователей с помощью функций Just-In-Time и Just-Enough-Access (JIT/JEA), адаптивных политик, основанных на оценке рисков, и защиты данных.

Минимизируйте радиуса поражения и сегментируйте доступа. Проверьте сквозное шифрование и используйте аналитику для обеспечения наглядности, обнаружения угроз и повышения эффективности защиты.

Microsoft Security

Защитить
всё

Упростить
сложное

Обнаружить
то, что упускают другие

Развивать
ваше будущее

Подход Microsoft

Управление учётными данными и доступом
Защита учётных данных пользователей и контроль доступа к ценным ресурсам на основе уровня риска пользователя

Защита от угроз
Защита от современных угроз и быстрое восстановление после атак

Защита информации
Будьте уверены, что документы и электронные письма видят только уполномоченные лица

Управление безопасностью
Наглядность и контроль над инструментами безопасности

Управление безопасностью

НАГЛЯДНОСТЬ

Понимание состояния безопасности и рисков по всем ресурсам

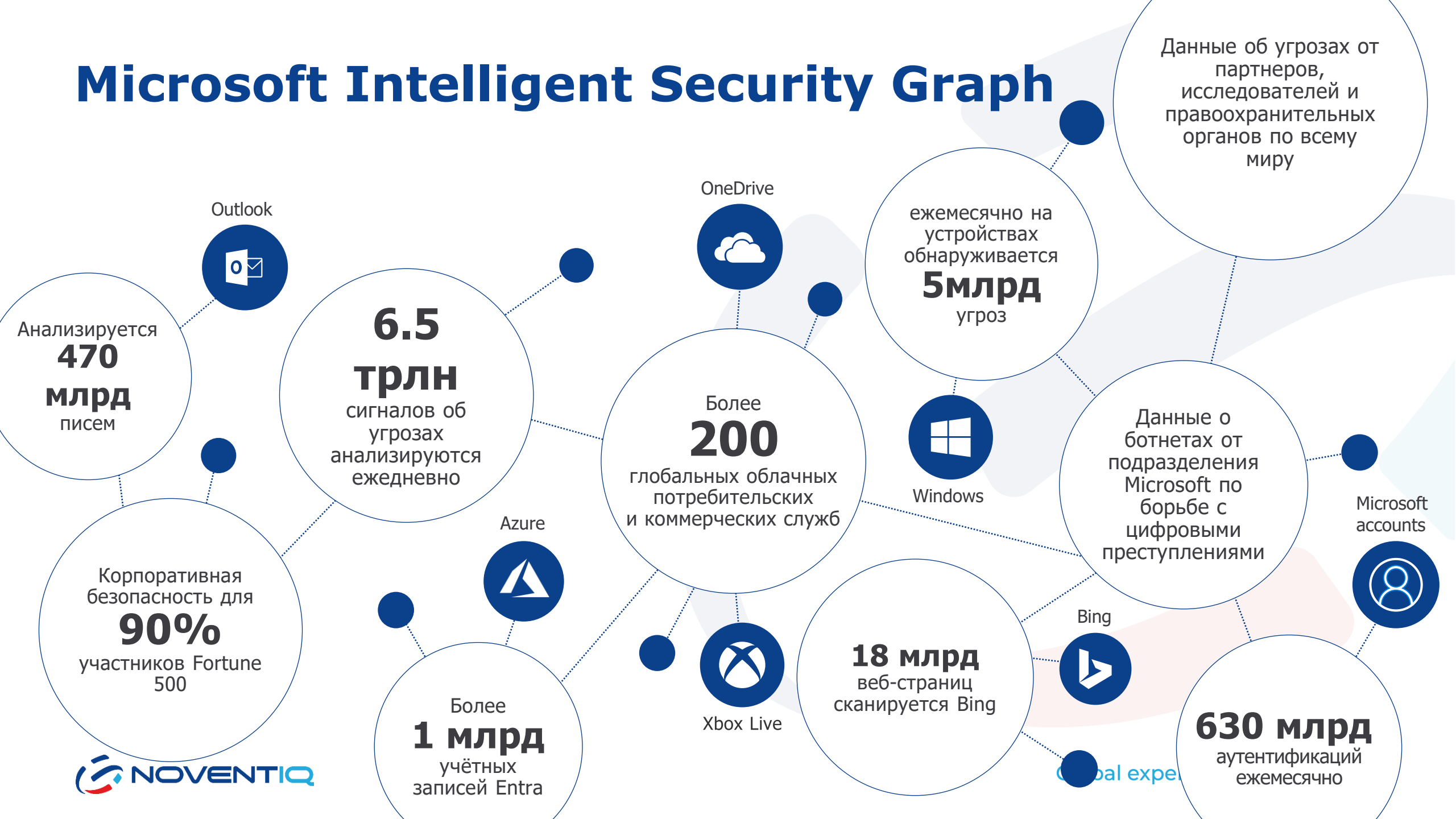
КОНТРОЛЬ

Определение политик безопасности и включение средств контроля

РУКОВОДСТВО

Повышение уровня безопасности благодаря встроенной аналитике и рекомендациям

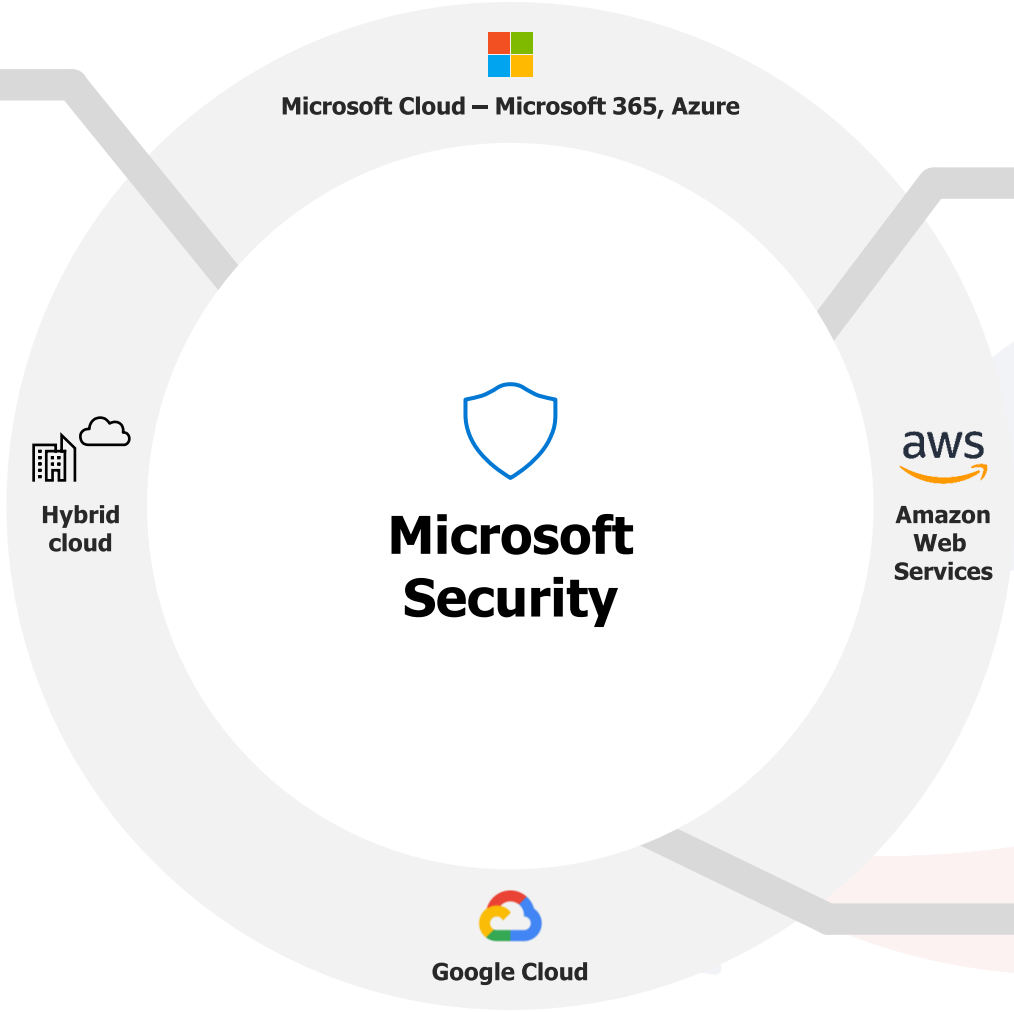
Microsoft Intelligent Security Graph



Комплексная безопасность Microsoft

Интеграция более 40 решений

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection



Data discovery
Data classification
Data loss prevention
Insider risk management
Data retention
Data deletion
Records management
eDiscovery
Audit
Risk assessment
Privileged access management
Compliance management
Information and messaging encryption

Identity and access management
Single sign-on
User provisioning
Multi-factor authentication
Passwordless authentication
Risk-based conditional access
Identity protection
Self-service password reset
Identity governance
Priviledged identity management
Endpoint management
Mobile application management
Mobile device management

NOVENTIQ

Global expertise, local outcomes

Gartner®

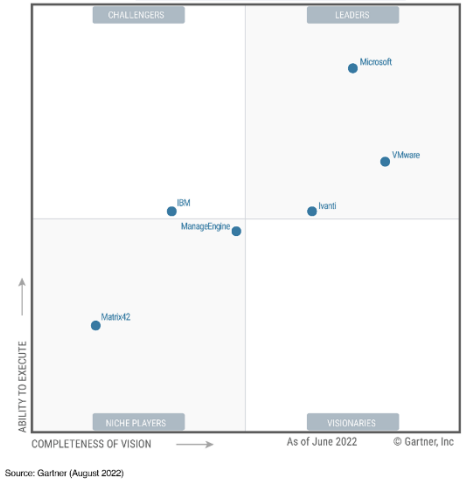
Microsoft Security—a Leader in 6 Gartner Magic Quadrant reports

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

Endpoint Protection Platforms



Unified Endpoint Management

Security Information and Event Management

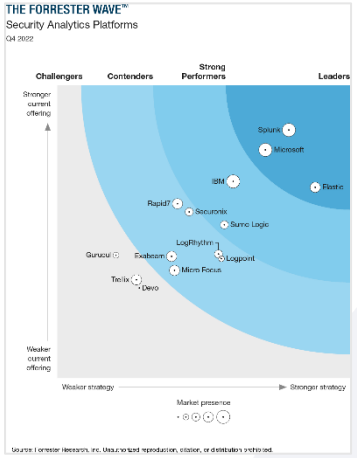
*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
*Gartner, Magic Quadrant for Enterprise Information Archiving, by Michael Hoeck, Jeff Vogel, Chandra Mukhyala. 24 January 2022.
*Gartner Magic Quadrant for Endpoint Protection Platforms, by Peter Firstbrook, Chris Silva. 31 December 2022
*Gartner, Magic Quadrant for Unified Endpoint Management Tools, Tom Cipolla, Dan Wilson, Chris Silva, Craig Fisler, August 1, 2022.
*Gartner, Magic Quadrant for Security Information and Event Management, Pete Shoard, Andrew Davies, Mitchell Schneider, 10 October 2022

NOVENTIQ

Global expertise, local outcomes

FORRESTER®

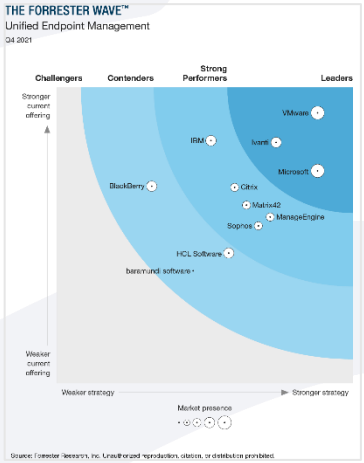
Microsoft Security—a Leader in 8 Forrester Wave and New Wave reports



Security Analytics Platform

Enterprise Email Security

Endpoint Security Software as a Service

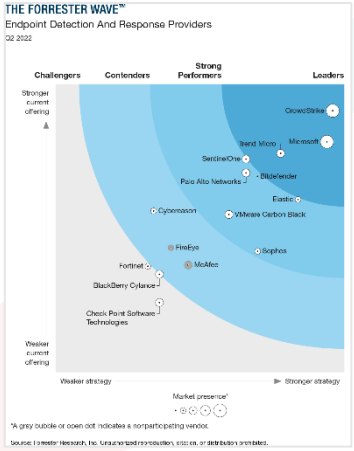


Unified Endpoint Management

Data Security Platforms

Cloud Security Gateways

Identity As a Service



Endpoint Detection And Response (EDR)

1. The Forrester Wave™: Security Analytics Platforms, Q4 2022, Allie Mellen with Joseph Blankenship, Caroline Provost, Kara Hartig, December 2022
2. The Forrester Wave™: Enterprise Email Security, Q2 2023, Jess Burn with Joseph Blankenship, Angela Lozada, Michael Belden. June 12, 2023.
3. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
4. The Forrester Wave™: Unified Endpoint Management (UEM), Q4 2021, Andrew Hewitt, Will McKeon-White November 2021
5. The Forrester Wave™: Data Security Platforms, Q1 2023, Heidi Shey, March 2023
6. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021
7. The Forrester Wave™: Identity As A Service (IDaaS) For Enterprise, Q3 2021" by Sean Ryan, August 2021
8. The Forrester Wave™: Endpoint Detection And Response Providers, Q2 2022, Allie Mellen, April 2022

NOVENTIQ

Global expertise, local outcomes

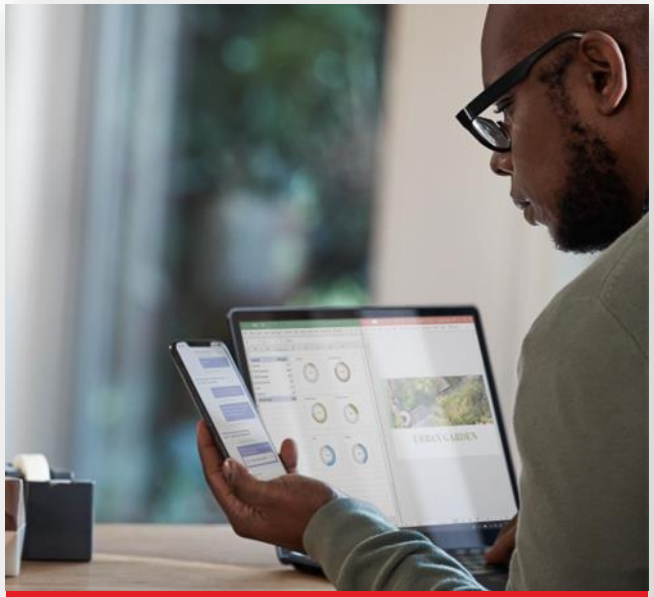
Прогнозы 2024

- Атаки на системы мгновенных платежей и банковские приложения
- Атаки на цепочки поставок как услуга
- Вырастет число атак с использованием ИИ
- Больше бэкдоров в пакетах программ с открытым исходным кодом
- Преступники будут чаще полагаться на ошибки в конфигурации устройств и сервисов
- Атак нулевого дня станет меньше, а количество уязвимостей первого дня возрастёт
- Сложность защиты учётных записей и рост атак на пользовательские сеансы
- Автоматическое создание фишинга в Telegram-ботах
- Вымогатели будут искать новые способы принуждения к выплате
- Консолидация ИБ инструментов и технологий

NOVENTIQ

Global expertise, local outcomes

Multi-Factor Authentication



Поддерживается большое количество способов аутентификации

Включая беспарольный доступ

- Microsoft Authenticator
- Windows Hello
- Ключи безопасности FIDO2
- Биометрия

- Push Уведомления
- Программные одноразовые пароли
- Аппаратные одноразовые пароли
- SMS, Звонки

Включение MFA предотвращает 99.9% атак на учётные данные

Conditional Access

Microsoft Defender for Identity

Защита локальной Active Directory

Анализ сетевого трафика

Инспекция трафика: NTLM, Kerberos, LDAP, RPC, DNS, SMB

События и данные Active Directory

Проверка и отслеживание событий безопасности и профилирование объектов AD

Анализ поведения пользователей

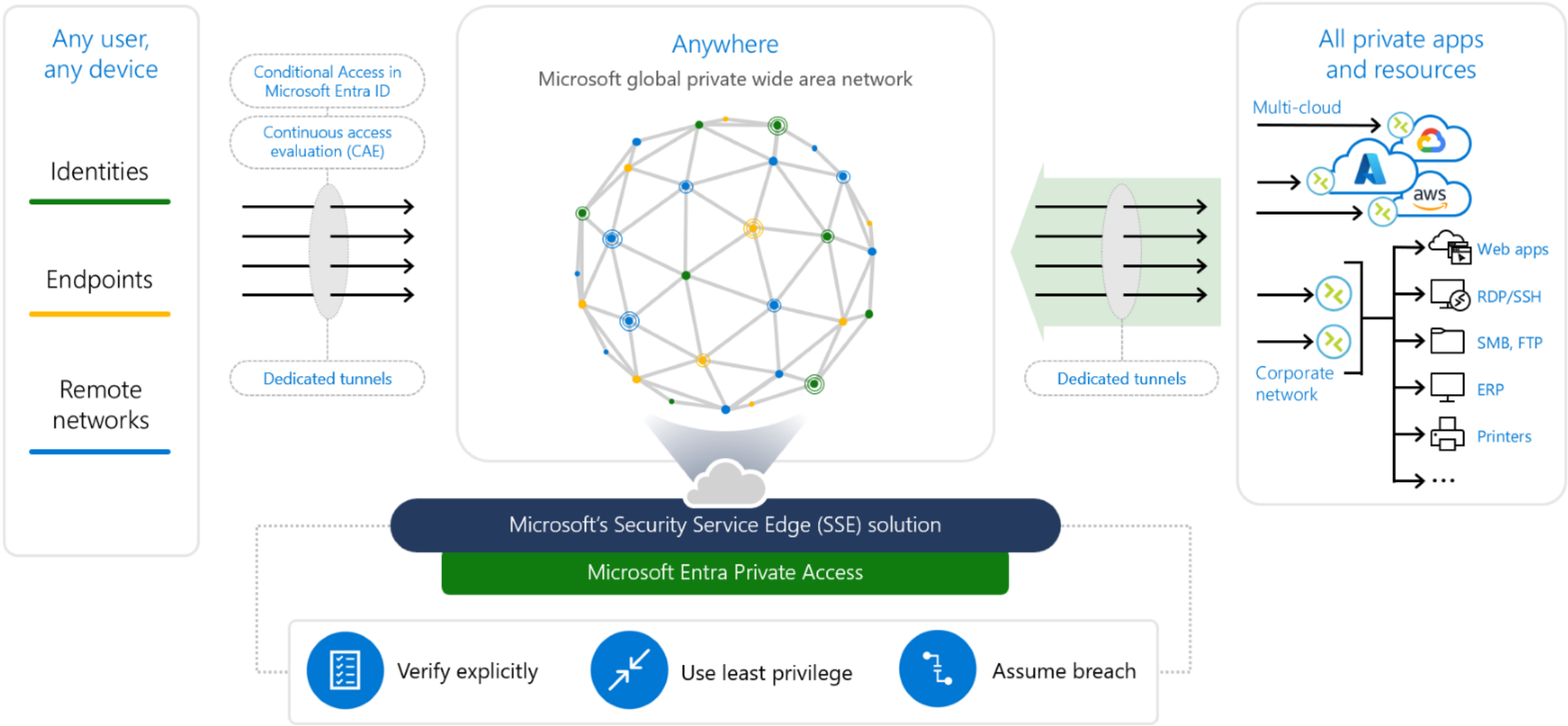
Профилирование поведения пользователей и сущностей, выявление аномалий поведения

Облачное обнаружение в реальном времени

Обогащение и корреляция данных в облаке в реальном времени

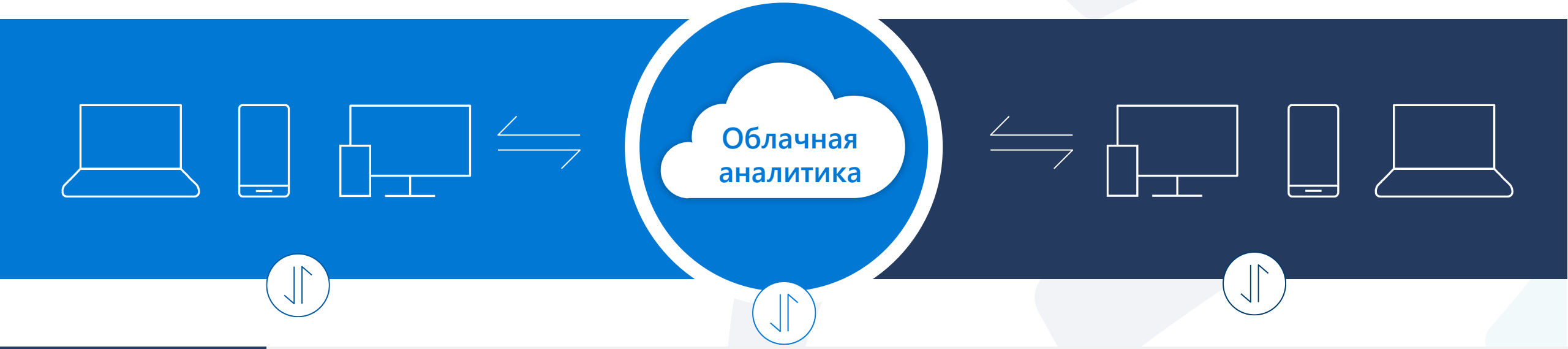
Microsoft Security Service Edge

(предварительная версия)



Microsoft Endpoint Manager

Intune + Microsoft Endpoint Configuration Manager



Microsoft endpoint manager

Единая консоль управления

Configuration Manager		Microsoft Intune	
Desktop Analytics	Autopilot Endpoint Security	Политики App Protection	Endpoint Analytics

Другие возможности управления конечными точками в Microsoft 365

Microsoft Intune

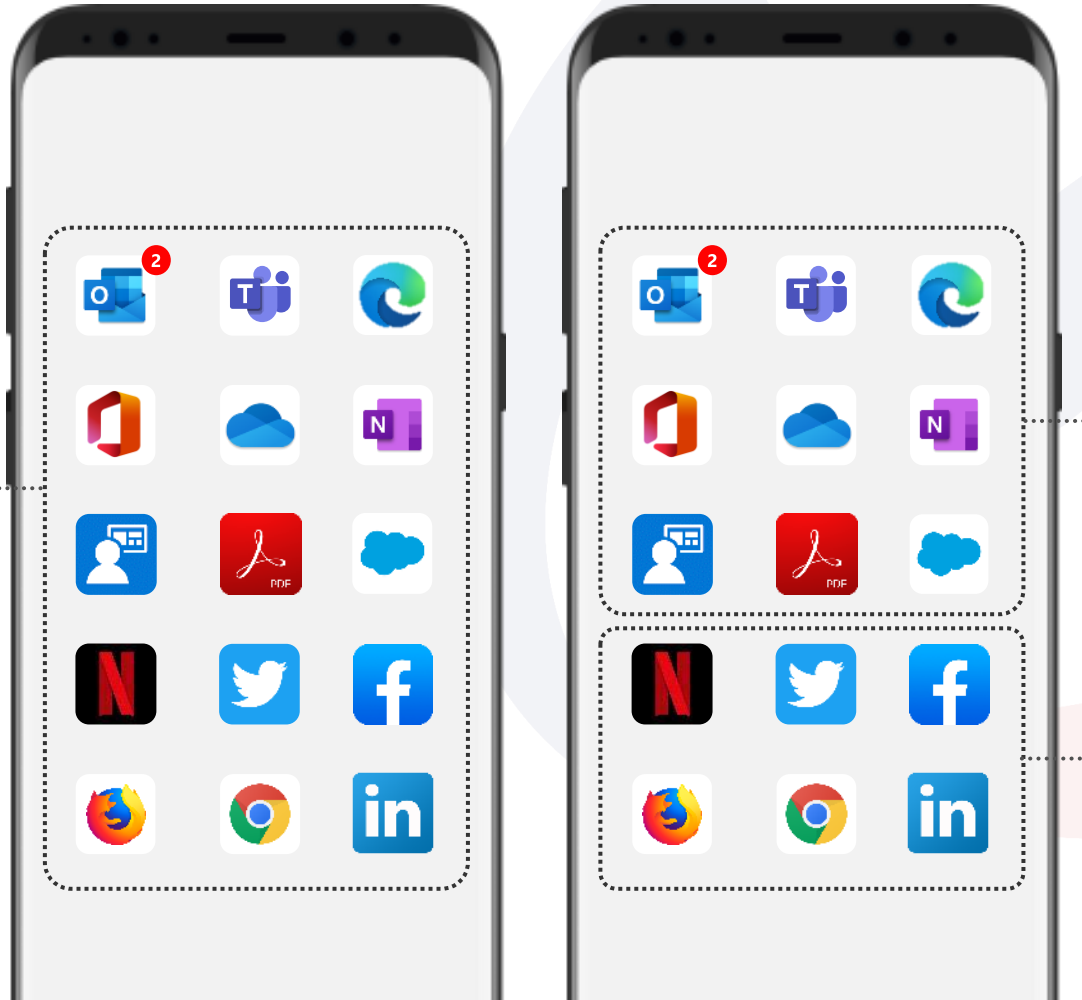
Mobile **device** management (MDM)

Условный доступ:

Ограничение доступа к управляемым и соответствующим требованиям устройствам и приложениям

Регистрация устройств

Распространение настроек, сертификатов и профилей устройств



Mobile **application** management (MAM)

Условный доступ :
Ограничение доступа приложений к электронной почте и файлам

Multi-identity policy

Управляемые приложения
(корп. данные)

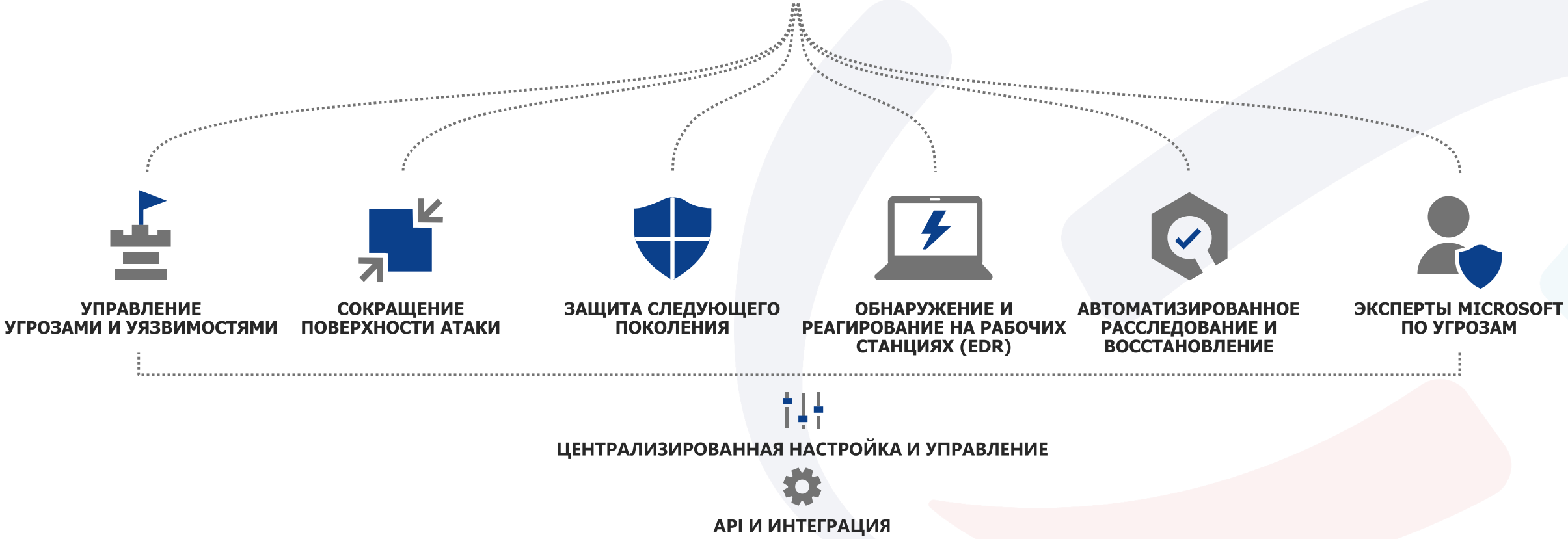
Персональные приложения
(частные данные)

NOVENTIQ

Global expertise, local outcomes

Microsoft Defender for Endpoint

У злоумышленников нет шансов



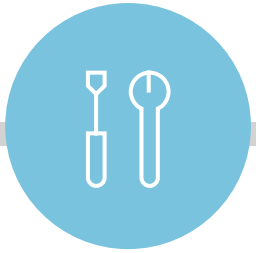
Microsoft Vulnerability Management Add-On

Microsoft Defender Vulnerability Management

Снижение рисков за счёт непрерывного обнаружения уязвимостей, определения приоритетов на основе рисков и их устранения.

Непрерывное обнаружение и мониторинг

Интеллектуальная приоритезация на основе рисков



Устранение и контроль

Углублённая оценка уязвимостей

Расширенная инвентаризация и оценка в масштабе всей организации

- Оценка базового уровня безопасности
- Оценка аппаратного обеспечения и «прошивок»
- Аудит цифровых сертификатов
- Анализ сетевых ресурсов
- Оценка расширений браузера
- Сканирование с аутентификацией для детальной оценки уязвимостей

Использование данных об уязвимостях из различных источников данных в едином представлении с помощью Security Recommendations.

Использование аналитики угроза Microsoft для определения приоритетности уязвимостей

Определение появления риска благодаря отображению новых уязвимостей на временной шкале

Microsoft Defender for Office 365

Edge protection

- Network throttling
- IP reputation/throttling
- Domain reputation
- Directory-based edge filtering
- Backscatter detection
- Enhanced filtering for on-prem routing

Sender intelligence

- Account compromise detection
- DMARC DKIM, SPF, ARC
- Intra-org spoof intelligence
- Cross-domain spoof intelligence
- Bulk filtering
- Mailbox intelligence
- Mailbox intelligence impersonation
- User impersonation
- micr0soft.com
- Domain impersonation

Content filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Heuristic clustering
- ML models
- Tenant allow/block lists
- URL reputation blocking
- Content heuristics
- Safe attachments
- Linked content detonation
- URL detonation

Post-delivery protection

- Safe links
- Phish zero-hour auto-purge
- Malware zero-hour auto-purge
- Spam zero-hour auto-purge
- Campaigns
- End-user reporting
- Office clients
- OneDrive/SharePoint
- URL detonation

Cloud App Discovery

Обнаружение и оценка «теневого ИТ»

Обнаружение «теневого ИТ»

Определите, какие приложения используются в вашей организации, из каталога приложений, включающего более 26 000 облачных и пользовательских приложений

Определение уровня риска приложений

Понимание рисков, связанных с обнаруженными приложениями, на основе более чем 90 факторов риска, включая факторы безопасности, отраслевые и законодательные нормы, с возможностью настройки оценки рисков

Оценка соответствия

Оцените, соответствуют ли обнаруженные приложения стандартам соответствия вашей организации по таким факторам, как GDPR или отраслевым стандарты, например HIPAA.

Анализ использования

Наглядная структура использования на основе данных о трафике, пользователях и IP-адресах, категориях приложений и устройствах. Отчёты для высокоуровневого обзора и детальные рекомендации.

Управление облачными приложениями

Начните управлять облачными приложениями, используя один из инструментов, таких как разрешение или блокировка, подключение приложения к Entra ID для использования SSO, пометка приложения для проверки или его блокировка на сетевом уровне.

Непрерывный мониторинг

Получайте уведомления о появлении новых уязвимых приложений или приложений с высокой интенсивностью использования для постоянного контроля над облачными приложениями.

Узбекистан в статистике кибератак

Топ 3 по проценту пользователей, атакованных банковским вредоносным ПО:

1. Таджикистан
2. Узбекистан
3. Иран

Топ 3 по числу компьютеров, подвергшихся по крайней мере одной локальной атаке вредоносного ПО:

1. Таджикистан
2. Бангладеш
3. Узбекистан

Топ 3 по числу атак криптомайнеров:

1. Таджикистан
2. Кыргызстан
3. Узбекистан

Глобальный индекс кибербезопасности:

1. США

...

69. Монако
70. Узбекистан
71. Иордания

Which countries have the worst (and best) cybersecurity? (comparitech.com)
Global Cybersecurity Index 2020 (ITU Publications)

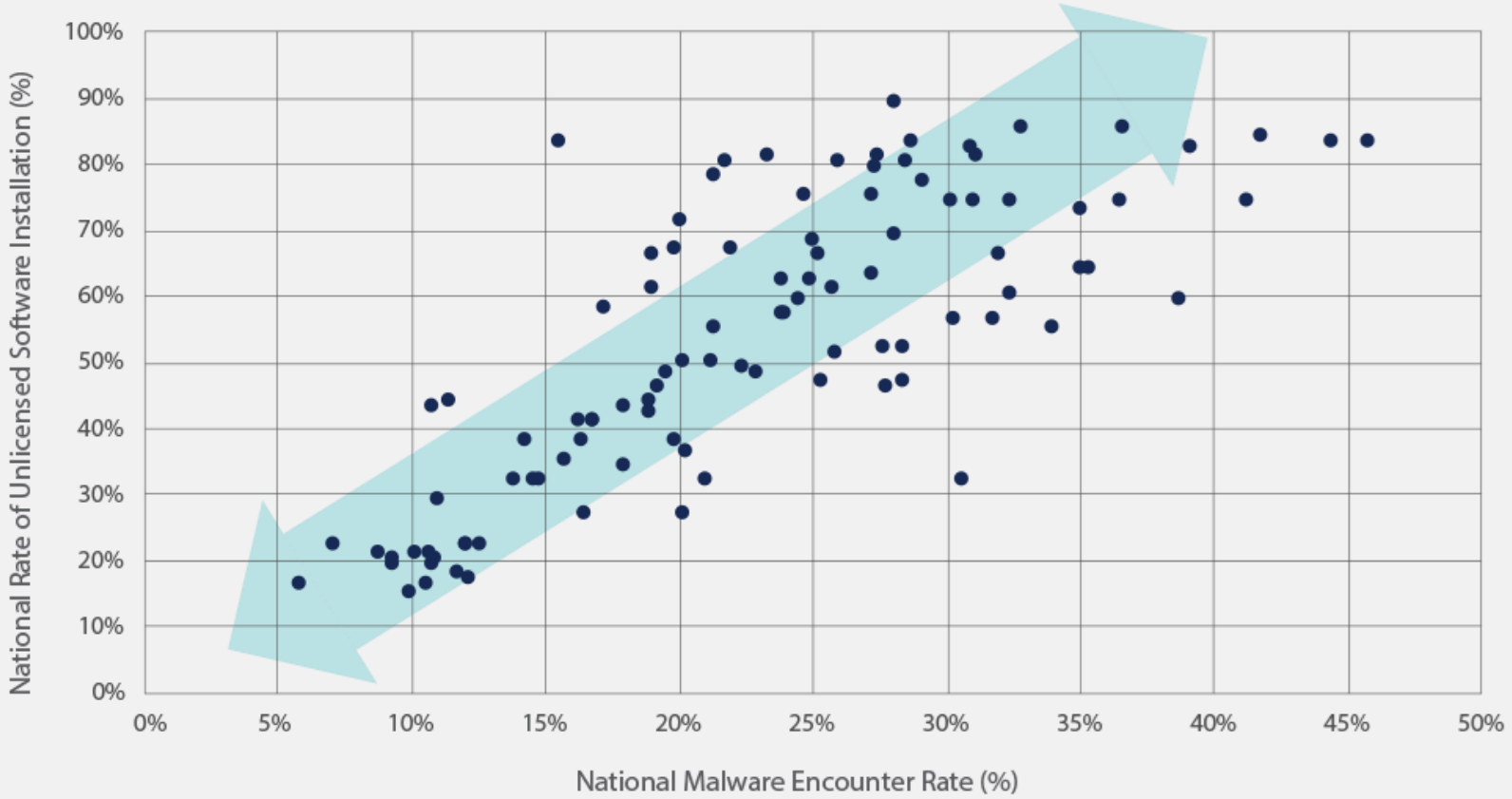
Узбекистан в статистике ИБ

91.	Kyrgyzstan	37.66	42.96	-5.30
92.	Mexico	37.66	51.46	-13.80
93.	Vietnam	36.36	47.69	-11.33
94.	Uzbekistan	36.36	49.00	-12.64
95.	South Africa	36.36	49.24	-12.88
96.	Armenia	35.06	55.06	-20.00
97.	Montenegro	35.06	57.79	-22.73
98.	Kuwait	35.06		

National Cyber Security Index (NCSI), September, 2023
NCSI :: Ranking

Пиратство и вероятность заражения

Доля используемого нелицензионного ПО и частота заражения ПК тесно связаны

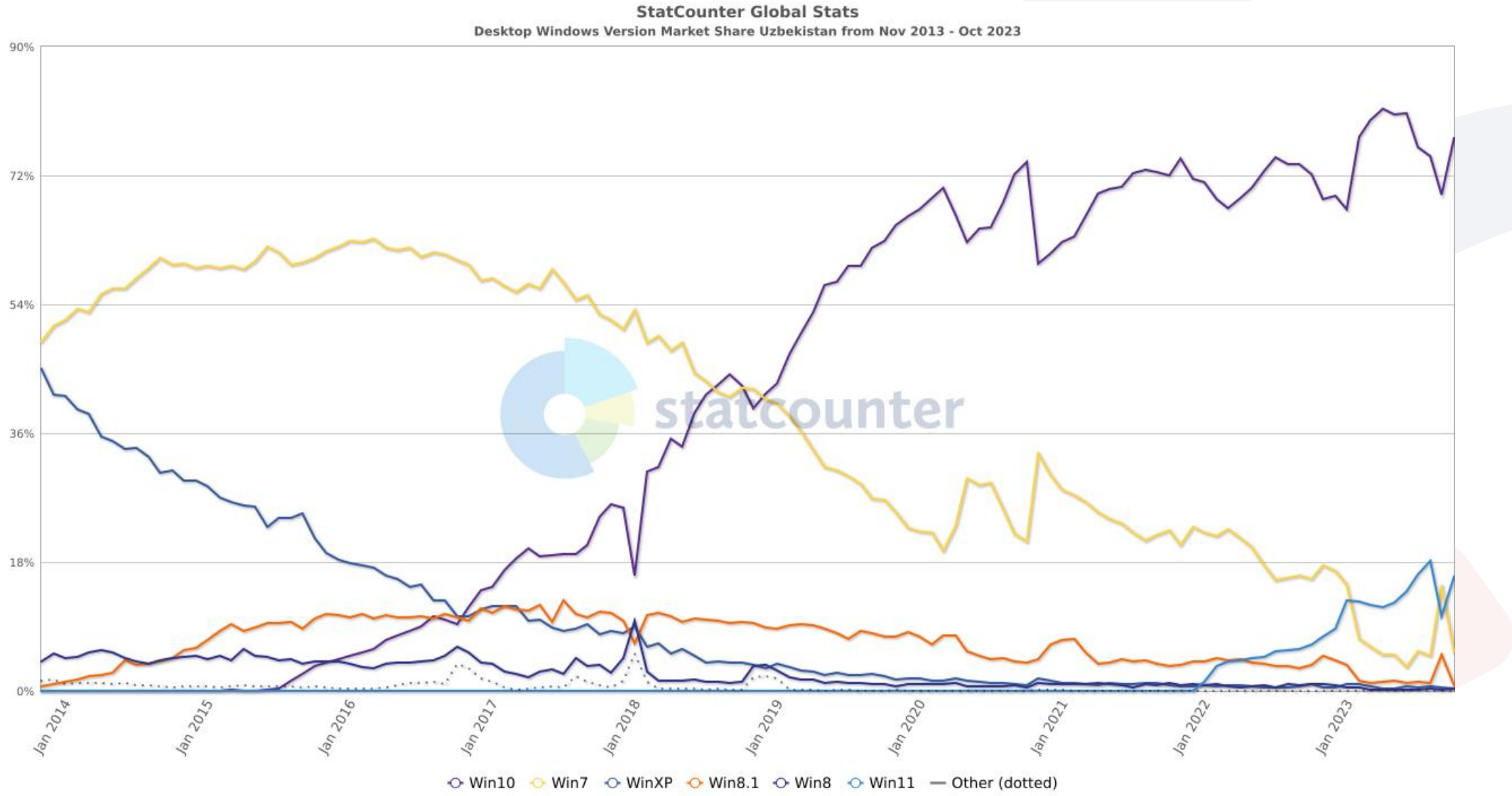


Источник: IDC InfoBrief

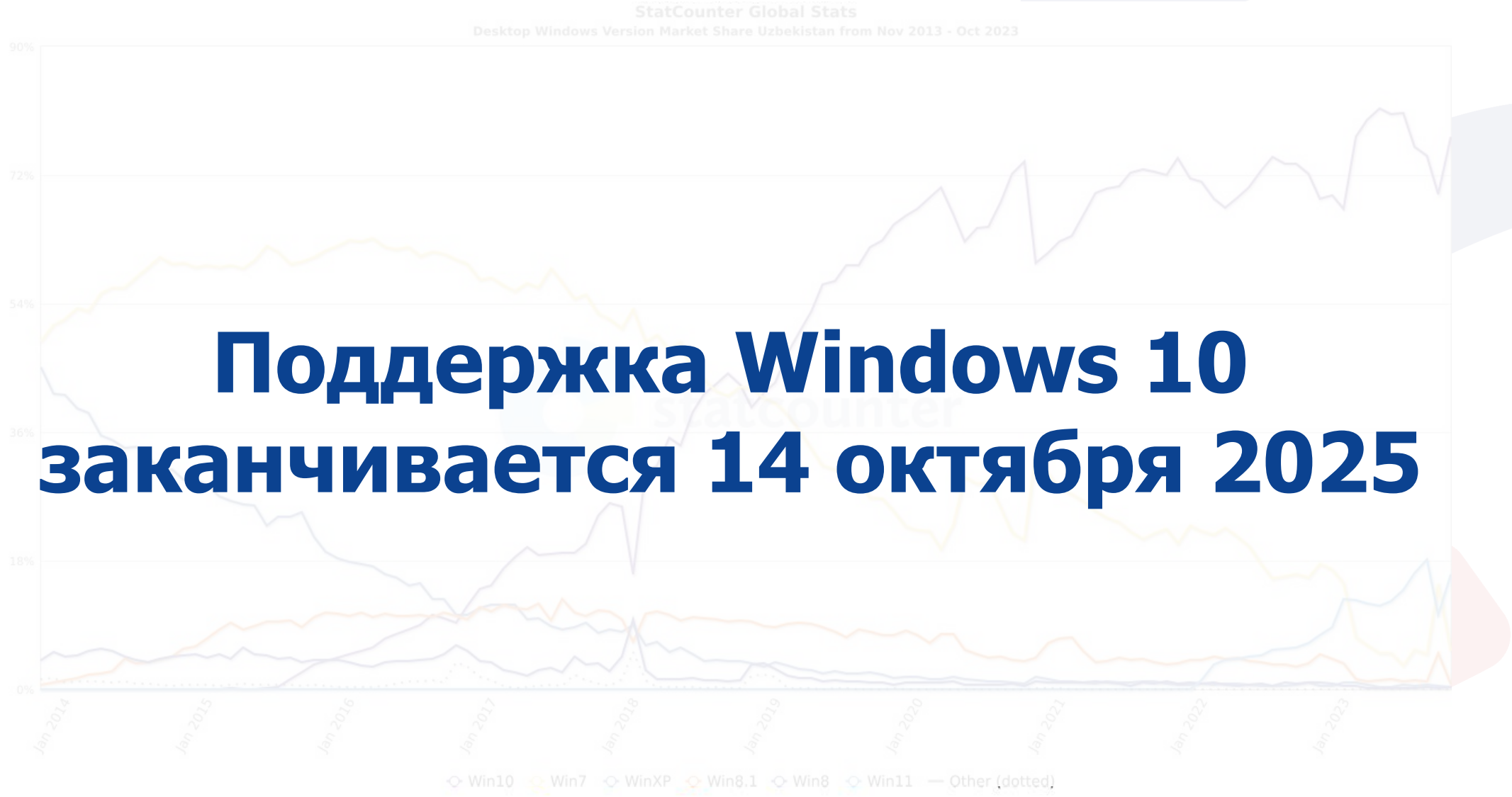
Пиратство и кибербезопасность не совместимы!

Если вы заинтересованы в повышении уровня киберзащиты, вам стоит использовать только лицензионные продукты.

Распространение ОС Windows в Узбекистане



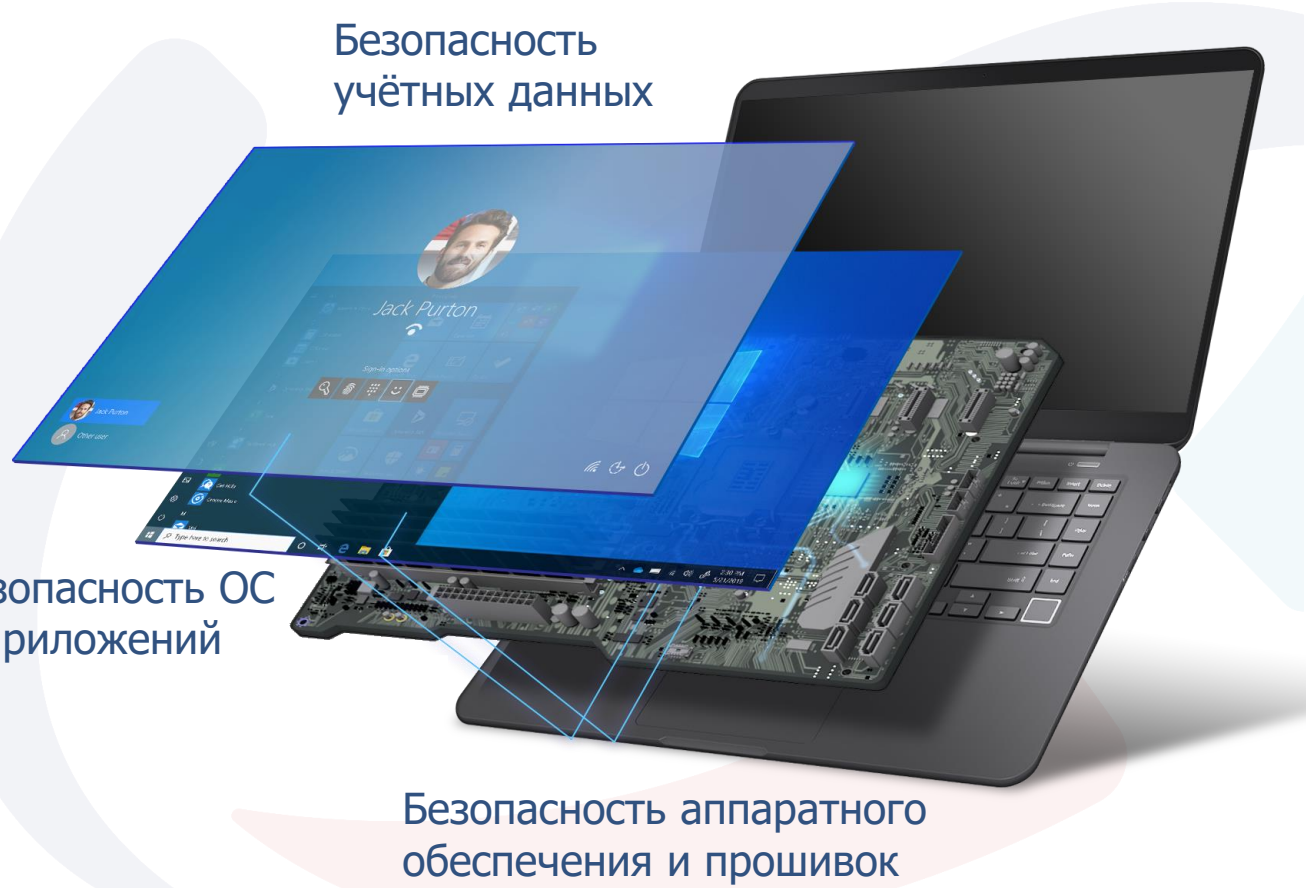
Распространение ОС Windows в Узбекистане



Поддержка Windows 10 заканчивается 14 октября 2025

Windows 11 Security

- Защита аппаратного обеспечения и прошивок: Многоуровневая защита устройства, включающая аппаратный корень доверия, безопасную загрузку, а также защиту на основе виртуализации и защиту целостности кода на основе гипервизора.
- Безопасность операционной системы: Защита и шифрование данных с помощью встроенных инструментов безопасности ОС
- Безопасность приложений: Уверенность в используемых приложениях
- Безопасность и конфиденциальность пользователей: Защита учётных данных и условный доступ



Защита платформы Windows

До взлома → После взлома

Вне АРМ

Office 365 (Email)

- Сокращение векторов атак через email
- Детонация в облачной «песочнице»

Edge (Браузер)

- Усиленная защита
- Сокращение векторов атак через скрипты
- Контейнеризация приложения
- Блокировка загрузок на основе репутации
- SmartScreen

На АРМ

Ограничение устройств

- Windows 10S
- Application Control
- Credential Guard
- Virtual Secure Mode

Сокращение поверхности атак

- Настраиваемый набор правил

App Guard (Виртуализованная безопасность)

- Изоляция приложений

Контроль доступа к папкам

- Только разрешенные приложения могут изменять данные

Защита от эксплойтов

- Блокировка характерных техник эксплойтов

Защита сети

- Фильтрация сетевого трафика на уровне устройства

Microsoft Defender for Endpoint / До взлома (AV)

- Улучшенная защита с помощью ML и эвристики
- Мгновенная защита с помощью облака
- Улучшенное обнаружение эксплойтов

Microsoft Defender for Endpoint / До взлома (Анализ поведения)

- Улучшенное обнаружение с помощью анализа поведения и машинного обучения
- Возможности сканирования памяти

Microsoft Defender for Endpoint / После взлома (Анализ поведения)

- Визуализации дерева процессов
- Возможность поиска артефактов
- Изоляция машины
- Автоматизация реагирования на инциденты

Вне АРМ

OneDrive (Хранилище)

- Надёжное облачное хранилище с поддержкой версионности файлов
- Возможность восстановления на момент времени

Microsoft Security Compliance Toolkit

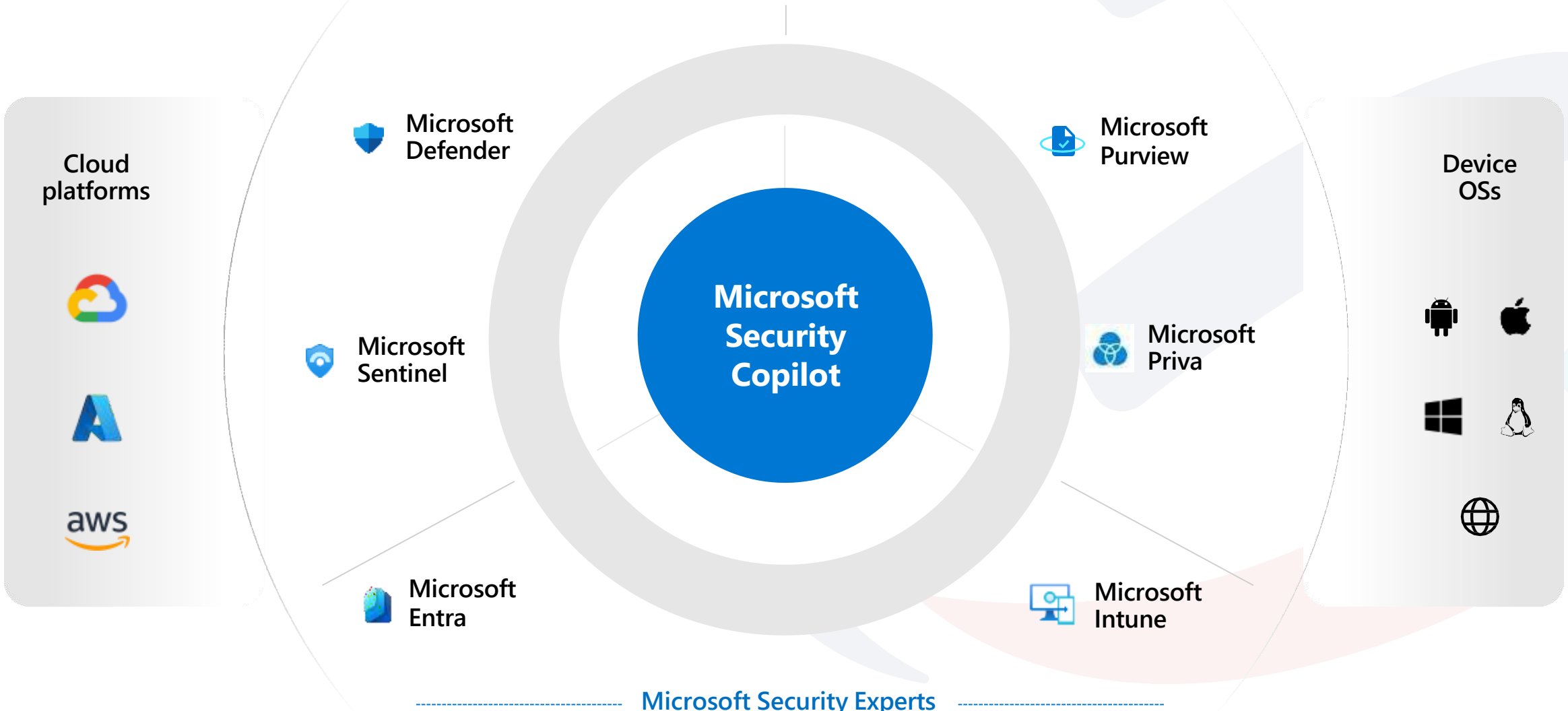
Базовые политики безопасности для:

- Windows 10 *(1507-22H2)*
- Windows 11 (21H2-22H2)
- Windows Server *(2012 R2 - 2022)*
- Microsoft Office *(2016 и Microsoft 365 Apps)*
- Microsoft Edge *(Последняя версия)*

Дополнительные инструменты:

- Документация
- Объекты групповой политики
- Инструмент анализа и сравнения групповых политик (GPO)
- Инструмент автоматизации управления объектами локальной групповой политики (LGPO)
- Инструмент настройки дескрипторов безопасности
- Инструмент конвертации GPO в правила политик

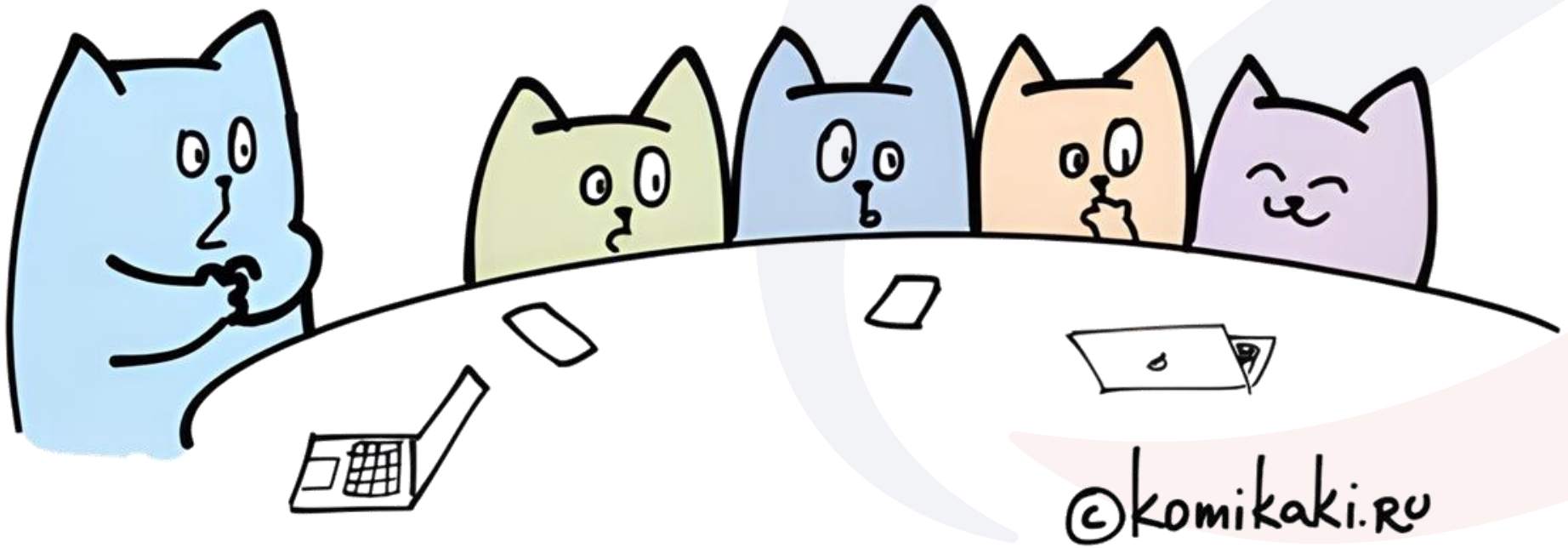
Microsoft Security Portfolio



Зачем нужен консалтинг?

Зачем нужен консалтинг?

Зачем нужен консалтинг?



Услуги Noventiq

Первое знакомство

Подробно с решением можно ознакомиться на встрече с Архитектором Microsoft:

- На демо-стенде продемонстрируем функционал
- Рассмотрим сценарии использования
- Ответим на вопросы

PoC (Proof of Concept) решения в вашей инфраструктуре:

- Предоставление лицензий, если их нет
- Подготовка инфраструктуры
- Настройка решения для пилотной группы
- Сопровождение при пилотировании

Важно. Все настройки проведённые в рамках пилота остаются в вашем тенанте. По итогам вы получаете подготовленную инфраструктуру и готовое к использованию решение

Внедрение Microsoft 365

Дополняем сервисы Microsoft экспертизой Noventiq

Специалисты компании Noventiq помогут внедрить решения, входящие в состав продуктов Microsoft 365 (Office 365, Enterprise Mobility + Security, Windows 10/11).

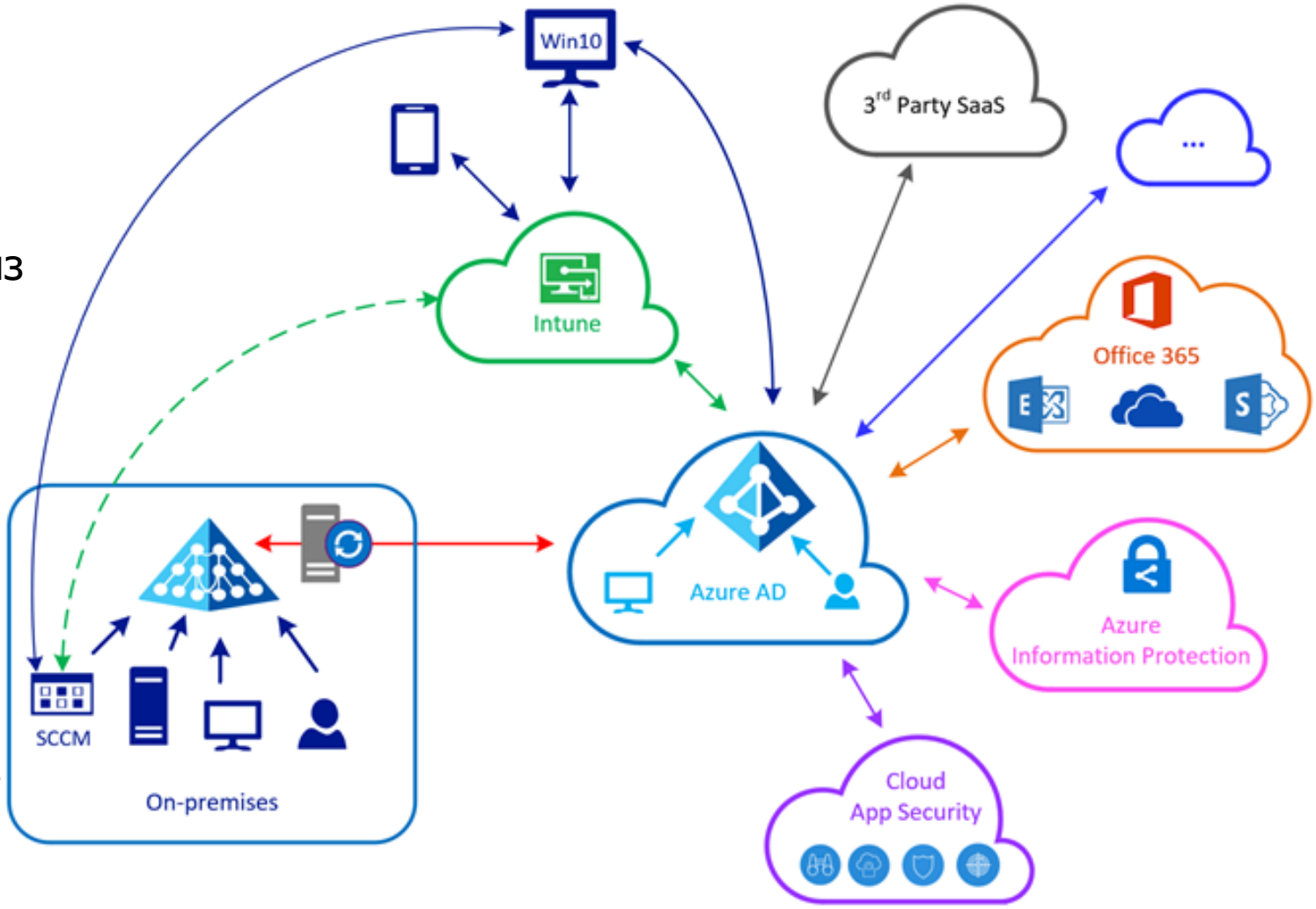
Включает в себя:

- Аудит инфраструктуры
- Разработка целевой архитектуры
- Создание гибридной инфраструктуры
- Развёртывание решений
- Передачу знаний и компетенций
- Рекомендации по использованию

Соответствие локальному законодательству

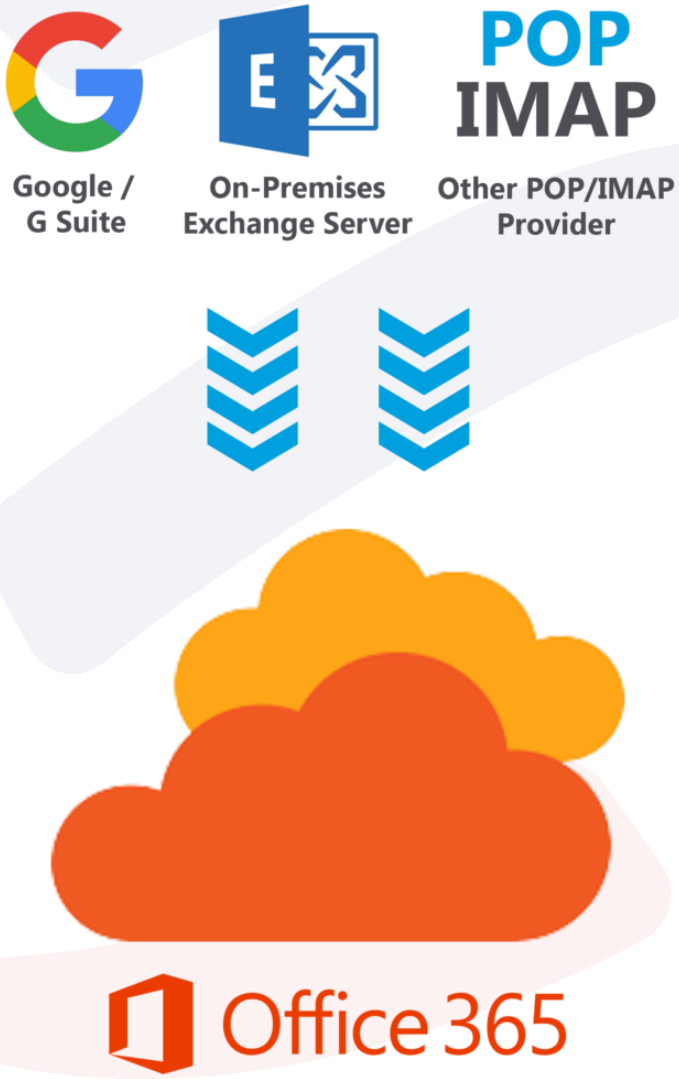
Настройка синхронизации учетных записей между локальной Microsoft AD и Entra ID – локализация первичных персональных данных и управление ресурсами в Azure, используя существующие аккаунты пользователей из единого каталога.

- Настройка тенанта, подтверждение владения доменом, настройка соответствующих записей в DNS.
- Установка сервера Entra ID Connect, активация синхронизации (понадобиться виртуальная или физическая машина)
- Настройка DNS и активация сервисов
- Активация SSO



Миграция Exchange Server/ Exchange Online

Дополняем сервисы Microsoft экспертизой Noventiq



- Миграция с любой системы электронной Почты
- Гибридная конфигурация AD и Exchange
- Тренинг и инструкции для администраторов
- Готовый сервис за 1 неделю

Microsoft Entra ID

Дополняем сервисы Microsoft экспертизой Noventiq

Entra ID Free	• MFA для администраторов • MFA для Office 365	Бесплатно/ В составе Office 365 / M365 Business
Entra ID P1	• MFA • Conditional Access • Password Protection for AD • Application Proxy	• EMS E3 • M365 E3 • M365 Business Premium
Entra ID P2	• PIM • Identity Protection	• EMS E5 • M365 E5 • M365 E3 + Security E5

NOVENTIQ

Global expertise, local outcomes

Enterprise Mobility & Security

Дополняем сервисы Microsoft экспертизой Noventiq

Рабочие станции

- Обновления
- Распространение ПО
- Управление антивирусом
- Шифрование дисков (Bitlocker)
- Контроль выполнения приложений
- Стандартизация конфигураций

EMS E3
M365 E3
M365 Business Premium

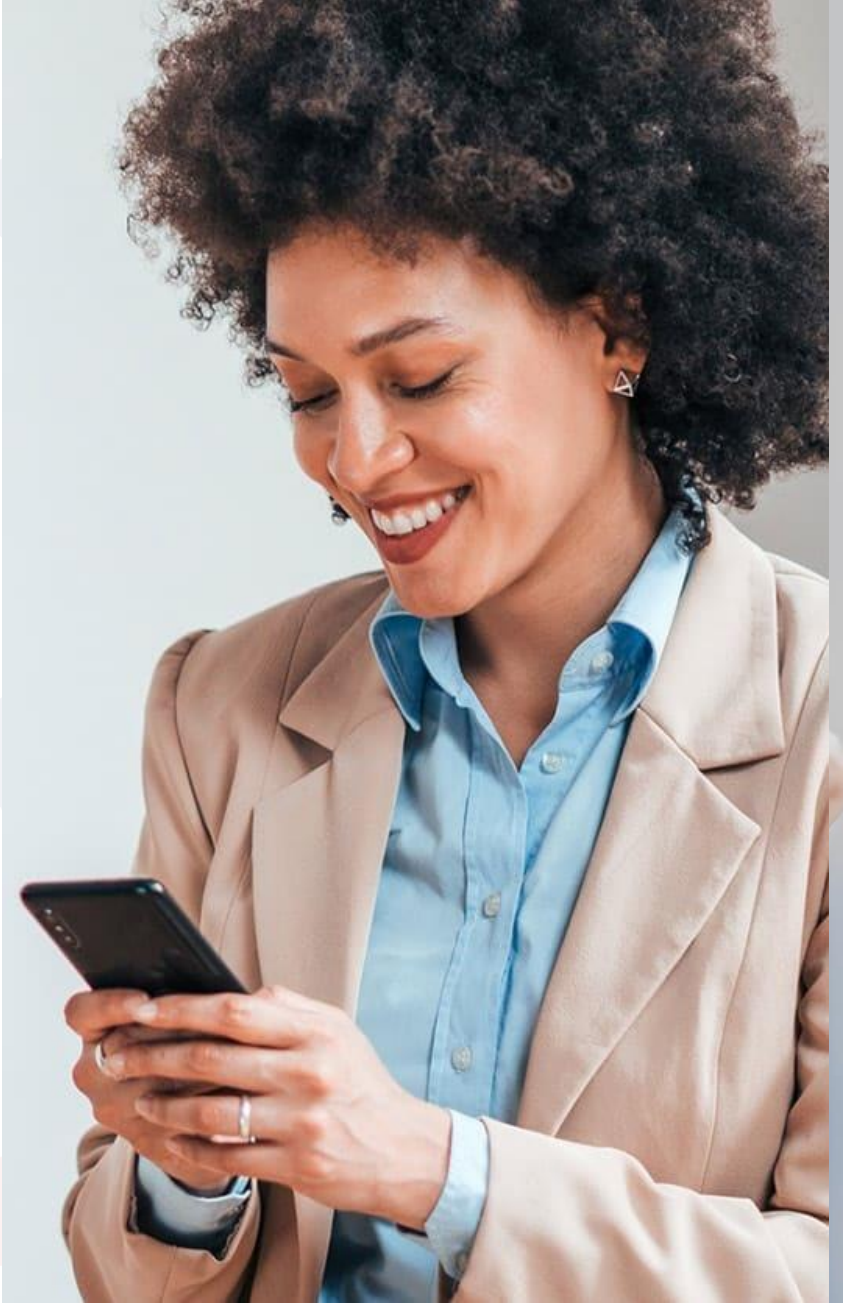
Мобильные устройства

- Управление Android
- Управление iOS
- Защита и шифрование корпоративных данных
- Конфигурация/управление устройствами в режиме киоска

EMS E3
M365 E3
M365 Business Premium
Device CAL

Intune Suite

- Удалённая помощь
- Управление приложениями через VPN туннель
- Управление привилегированными учётными записями
- Расширенная аналитика
- Управление специализированными устройствами



NOVENTIQ

Global expertise, local outcomes

Microsoft Purview Information Protection

Дополняем сервисы Microsoft экспертизой Noventiq

Пилотирование

- Предоставление тестовых лицензий
- Настройка базовых политик

Внедрение

- Разработка правил контроля
- Создание реестра данных
- Настройка политик контроля

Консалтинг

- Разработка регламента реагирования
- Легализация контроля

Сопровождение

- Поддержание работоспособности
- Оптимизация работы
- Расследование инцидентов

Microsoft 365 Defender - XDR платформа

Дополняем сервисы Microsoft экспертизой Noventiq

Microsoft 365 Defender объединяет сигналы об угрозах безопасности из всех решений Microsoft 365 и сторонних решений. Позволяя видеть общую картину по текущим состоянию безопасности в организации.
Машинное обучение и технологии ИИ позволяют снизить количество ложных срабатываний, сосредоточившись только на важных и критических событиях.
Выявив угрозу и определив источник – вы сможете мгновенно реагировать на угрозы, в дальнейшем автоматизировав реакцию на инциденты.

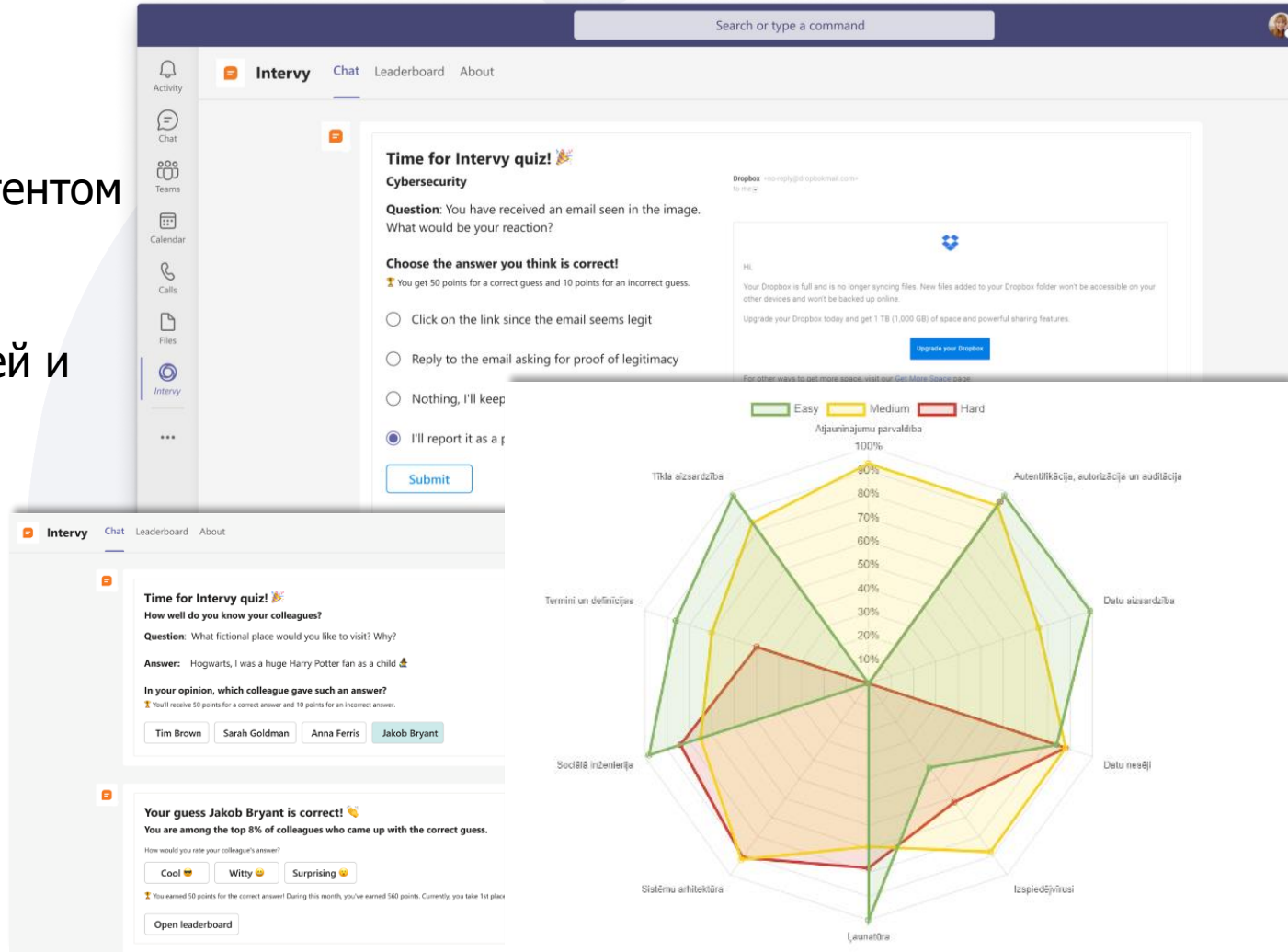
- Защита от постоянных атак по всем доменам
- Устранение ложных сигналов
- Автоматическое устранение последствий на затронутых атаками активах
- Выявление угроз

Платформа включает следующие решения: Defender for Identity, Defender for Office 365, Microsoft Cloud App Security, Defender for Endpoint, Defender for Cloud, Defender for Servers, Microsoft Sentinel

Intervy

Вовлекающее обучение кибергигиене и осведомлённость пользователей

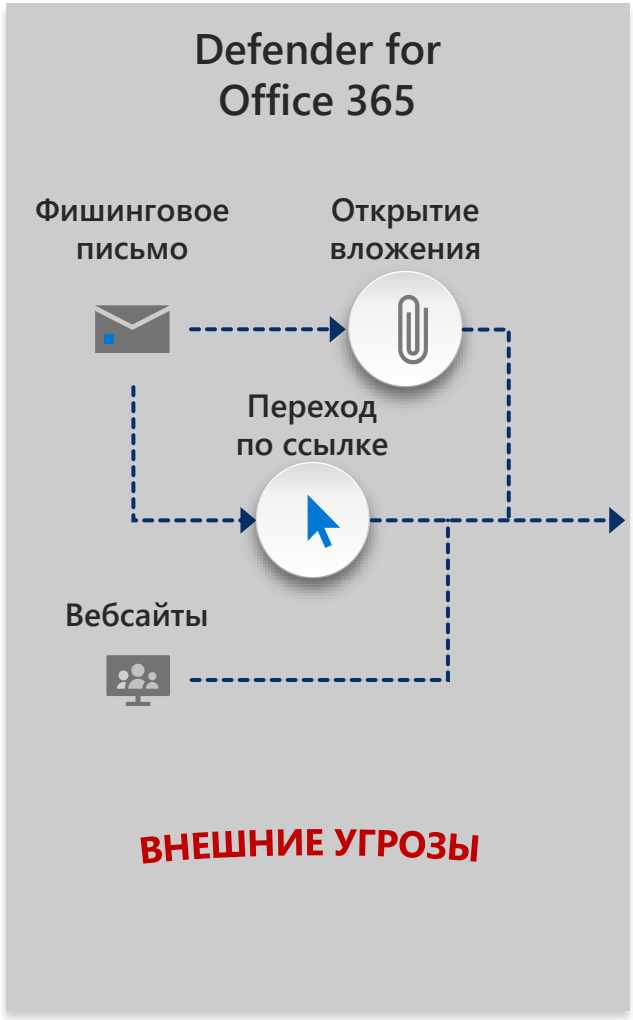
- Платформа микрообучения с готовым контентом
- Вовлекающее и интерактивное обучение
- Настраиваемые учебные курсы по кибербезопасности для различных отраслей и ролей
- Расширенная отчетность и аналитика для отслеживания прогресса сотрудников
- Искусственный интеллект адаптирует курс к навыкам и целям сотрудников
- Регулярные обновления контента
- Полная интеграция в Teams



Global expertise, local outcomes

Microsoft Attack Simulator

Дополняем сервисы Microsoft экспертизой Noventiq

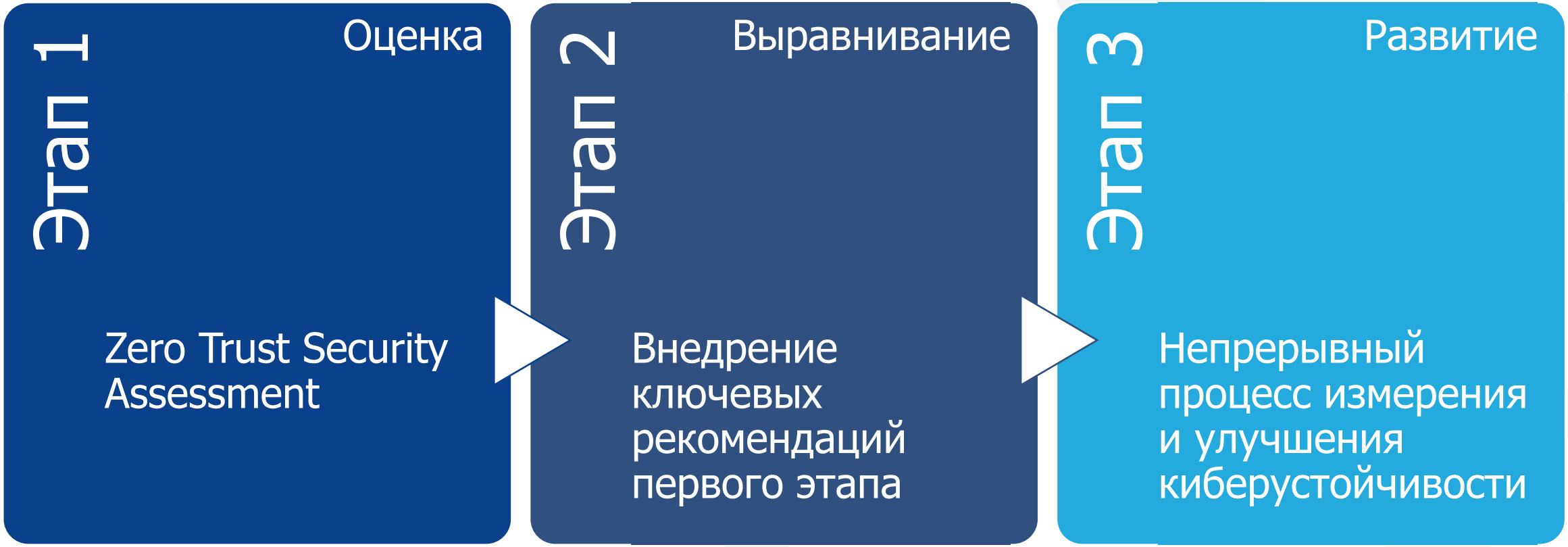


Инструмент **Attack Simulator** позволяет смоделировать учебную фишинговую атаку на сотрудников вашей организации.

Доступны следующий виды атак:

- **Сбор учётных данных:** Злоумышленник отправляет получателю сообщение с фишинговой ссылкой.
- **Вредоносные вложения:** Злоумышленник отправляет получателю сообщение, содержащее вредоносное вложение.
- **Ссылка во вложении:** Злоумышленник отправляет получателю сообщение, содержащее фишинговую ссылку внутри вложения.
- **Ссылка на вредоносное ПО:** злоумышленник отправляет получателю сообщение, содержащее ссылку на файл, размещённый на известном файлообменном сервисе.
- **Drive-by-url:** Злоумышленник отправляет получателю сообщение, содержащее URL-адрес. При переходе по ссылке веб-сайт пытается скрытно запустить вредоносный код.
- **OAuth Consent Grant:** URL-ссылка просит пользователя предоставить разрешения на данные для вредоносного приложения Azure.

Zero Trust Managed Services



- Программа оценки и повышения уровня кибербезопасности
- Zero Trust как основная концепция
- Индивидуальный план совершенствования для каждого заказчика
- Secure Score как критерий оценки успеха

Zero Trust Security Assessment

- На основе адаптированной модели зрелости нулевого доверия CISA
- Оценивает текущее состояние по всем компонентам нулевого доверия
- Определяет персонализированное, основанное на рисках целевое состояние зрелости для конкретного заказчика
- Предоставляет эффективные рекомендации, позволяющие достичь максимального результата.
- Основа для рекомендаций по выравниванию и развитию

А вы готовы к катастрофе?

Premier Services

- Обследование инфраструктуры.
- Разработка стратегии резервного копирования и восстановления
- Повышение безопасности
- Улучшение производительности
- Глубокое техническое обучение.
- Инцидентная поддержка 24/7

Что такое ваучер Noventiq?

Ваучеры Noventiq это уникальный ИТ-продукт для организаций любого размера, который учитывает все актуальные потребности и запросы клиентов. Ваучеры исчисляются в днях услуг, которые можно потратить на поддержку или внедрение любого продукта Microsoft силами сертифицированных инженеров Noventiq по низкой стоимости.

5

5 дней = 40 часов, подходит под проекты аудита и оптимизации инфраструктуры, проведение воркшопов по технологиям, подготовки плана развёртывания, документации

10

10 дней = 80 часов, подходит под проекты обновления устаревших версий продуктов, настройки и модернизации текущих ИТ-систем, построение гибридов, установка критически важных обновлений и патчей

15

15 дней = 120 часов, подходит под проекты внедрения продуктов с нуля на пилотной группе пользователей, или миграции на платформу Microsoft или интеграции с продуктами иных вендоров, консалтинг по иным вопросам, связанным с инфраструктурой заказчика

ваучер действует 1 год с момента его приобретения, а также при заключении, продлении расширении соглашения Microsoft

NOVENTIQ

Global expertise, local outcomes

Техническая поддержка

Поддержка по решениям безопасности из стека Microsoft 365.

Продукты: Entra ID, MFA, Conditional Access, Self-service password reset, Single Sign-on, Application Proxy, Azure Information Protection, Intune, Microsoft Endpoint Manager, BitLocker, Exchange Online Protection, , Defender for Office 365, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps…

Включает в себя:

- консультации технического пользователя
- приём и регистрация обращений в Service Desk (телефон, почта, портал)
- удалённые подключения для разрешения инцидентов
- эскалация обращений и взаимодействие с вендором
- предоставление статистики по обращениям по форме исполнителя
- администрирование учётных записей, групп, ролей, подписок, лицензий, почтовых ящиков и политик.

Дополнительно: срок действия 1 год; по окончании срока действия или включённых часов предлагается пролонгация соглашения.

NOVENTIQ
Global expertise, local outcomes

Спасибо!

Sergey.Zhuykov@Noventiq.com

+7 705 311 62 12