ЕЛЕКТРОННА КНИГА

Защо Zero Trust?

Възползвайте се от проактивна сигурност със Zero Trust

NOVENTIQ
Global expertise, local outcomes

Microsoft Solutions Partner

NOVENTIQ
Global expertise, local outcomes

За кого е това:

ИТ и бизнес ръководители, които искат да направят своите ИТ среди сигурни с помощта на структурата Zero Trust. Това ръководство представлява изчерпателно обяснение на структурата на Microsoft – Zero Trust, заедно с конкретни стъпки, които да бъдат предприети в две много важни опорни точки на една организационна стратегия за сигурност: Потребители и крайни устройства.

Защо Zero Trust?

Увеличаващото се разпространение на данни и устройства, увеличението на хибридния модел на работа и нарастващия брой усъвършенствани атаки намаляват ефективността на ИТ сигурността, базирана на определен периметър. ИТ професионалистите управляват огромно разнообразие от технологии. Бизнеси обикновено използват комбинация от инфраструктура в облака и локална, платформи и софтуер. Те могат да имат многобройни облачни доставчици и системи. Служители работят на лични устройства и лесно могат да осъществяват достъп до облачни приложения и услуги. Данните съществуват на повече места от всякога, което ги прави по-ценни, но и по-уязвими.

В отговор на това много организации възприемат структурата за сигурност Zero Trust.

Zero Trust представлява проактивен, интегриран подход за сигурност във всички пластове на дигиталното пространство, който изрично и постоянно потвърждава всяка транзакция, поддържа минимални привилегии и разчита на разузнаване, усъвършенствано разкриване и отговор на заплахи в реално време:

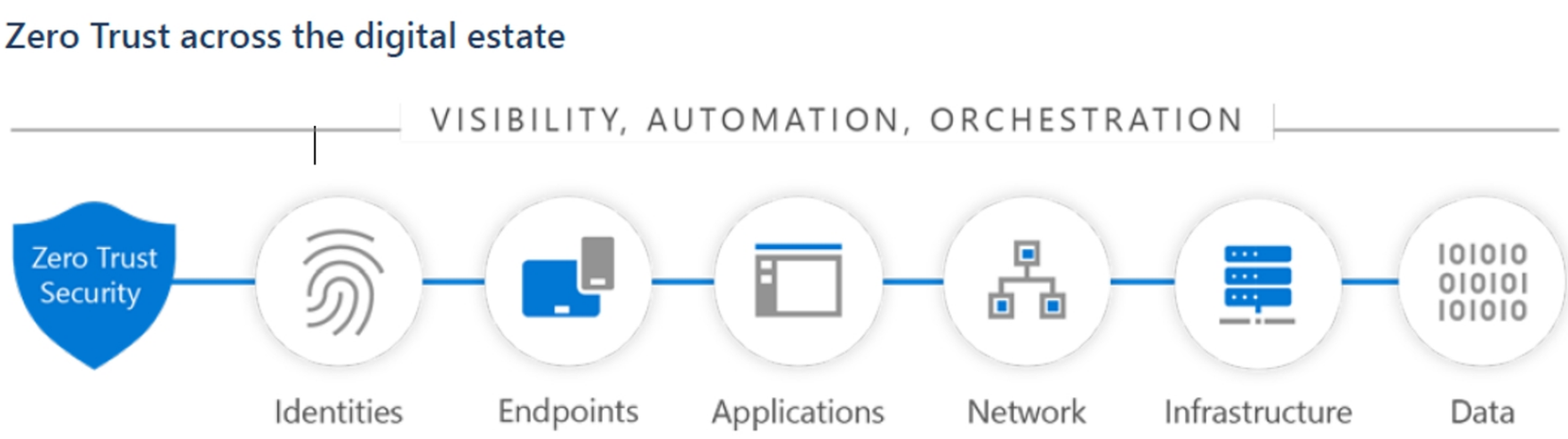
- **Проверявайте изрично:** Винаги удостоверявайте истинността и давайте разрешение на базата на всички налични данни, включително самоличност на потребител, местоположение, състояние на устройство, услуга или натоварване, класификация на данни и отклонения.
- **Предполагайте нарушение:** Намалете радиуса на разпространение (blast radius) и достъпа до отделни сегменти. Потвърдете цялостното криптиране и използвайте анализ, за да получите видимост, да управлявате разкриването на заплахи и да подобрите защитите.
- **Използвайте достъп с минимални привилегии**: Ограничете достъпа на даден потребител с моделите just-in-time (точно навреме) и just-enough-access (точно достатъчно достъп) (JIT/JEA) – базирани на риска приспособими политики и защита на данни, за да подпомогнете сигурността както на данните, така и на продуктивността.

Съвременната защита от заплахи е критичен компонент на всички три области, позволявайки на организациите да разкриват атаки и отклонения, автоматично да блокират и сигнализират рисково поведение, да предприемат защитни действия и да управляват нарастващия приток от данни, които представляват заплаха.

Колко лесно една организация може да приеме тези принципи е различно и зависи от редизвикателствата на нейната индивидуална сигурност, нуждите и способностите й. С други думи, пътят към Zero Trust е уникално за вашия бизнес.

За да ви помогне да стигнете дотам по-бързо, Microsoft разработи гъвкавата структура Zero Trust за направляване на внедряването. Тя предоставя задълбочено ръководство, обхващащо **шест основни рискови** области, с които се справя Zero Trust:

- **Потребители:** Потребители – Автоматизирайте разкриването на риска и отстраняването на риска и осигурете достъп до ресурси със силна идентификация в цялото дигитално пространство.
- **Крайни устройства:** Защитавайте по-голямото пространство за атаки, създадено от нарастващия брой и разнообразието от крайни устройства, използвайки гъвкав, интегриран подход към управлението.
- **Приложения:** Поддържайте силно обезпечен достъп на служители до облачни и мобилни приложения, а също така и отдалечен достъп до приложения в офисите на компанията.
- **Данни**: Класифицирайте, маркирайте и защитете данни в облачни среди и в офиса, за да подпомогнете предотвратяването на неуместно споделяне и да намалите вътрешните рискове.
- **Мрежа**: Намалете уязвимостите на сигурността, свързани с периметъра, включително нуждата от VPN и подобрете мащабируемостта на решенията за сигурност за среди, в които облакът все повече е център на IT услуги.
- **Инфраструктура**: Защитете хибридната инфраструктура, включително IT среди в офиси и облачни среди, с по-ефективно и автоматизирано управление.



Чрез възприемането на структурата Zero Trust в една или всички тези области, вие можете ефективно да модернизирате вашата технология за сигурност и процеси и да започнете да увеличавате в най-висока степен защитата срещу съвременните заплахи. Все пак всяка организация ще има различни приоритети в зависимост от своите настоящи възможности и нивото на риска, който дадена област на сигурност представлява. Това ръководство прави получаването на обширна представа за Zero Trust лесно за вас, както и получаването на подробна информация и приложими стъпки за 2 много важни опорни точки: Потребители и крайни устройства.

Архитектура на Microsoft Zero Trust

В тази електронна книга ще се съсредоточим върху първите 2 компонента на структурата Zero Trust, която сме идентифицирали като най-важна за малки и средни компании.

Основни принципи на Zero Trust

Потребители

Облачните приложения и увеличеното разпространение на хибридния модел на работа предефинираха периметъра на сигурност. Корпоративните приложения и данни също се местят от офиса в хибридни и облачни среди. Много организации разчитат на по-старо управление на самоличността и достъпа, изградено за свят с ясно разграничение на това кое е вътре и кое е извън мрежата.

Тези системи правят труден достъпа на хората до приложения и данни, които са им нужни, и създават пробойни в сигурността, предоставяйки изключителни привилегии на доверени потребители. Структура Zero Trust, включваща базирани на облака решения за самоличност на потребителите, като например многофакторно удостоверяване и еднократна идентификация (single sign-on (SSO)) в цялата средата, се вписва по-добре в съвременното работно пространство.

Контролиране на потребителите за структура Zero Trust

1 • Прилагайте многофакторно удостоверяване

Многофакторното удостоверяване помага за защита на вашите приложения, като изисква от потребителите да потвърдят своята самоличност, използвайки втори източник на валидиране, като например телефон или код, преди да се предостави достъп

- Инструменти като Microsoft Azure Active Directory (Azure AD) позволяват безплатно многофакторно удостоверяване.
- Многофакторното удостоверяване (MFA) на Azure Active Directory (Azure AD) подпомага сигурния достъп до данни и приложения, осигурявайки друго ниво на сигурност чрез използване на втора форма на удостоверяване. Организациите могат да активират многофакторно удостоверяване с условен достъп, за да може решението да подхожда на техните специфични потребности.

2 • Активирайте удостоверяване без парола

Методите за удостоверяване без парола осигуряват по-просто и по-сигурно удостоверяване в мрежата и на мобилните устройства. Тези методи позволяват на потребителите да извършват удостоверяване лесно и сигурно без нужда от парола.

- Ако имате AAD, може да активирате инструменти, като например приложението Microsoft Authenticator, така че потребителите да могат да влязат във всеки акаунт на Azure AD, без да използват парола. Microsoft Authenticator използва удостоверяване, базирано на ключ, за да активира удостоверяване на самоличност на потребител, която е свързана с устройство, когато устройството използва PIN или биометрични данни. Windows Hello за бизнеса използва същата технология.
- Въведете еднократна идентификация (SSO). Това премахва нуждата от управление на многобройни документи за удостоверяване на самоличност за един човек и предоставя по-добро преживяване на потребителя с по-малко опити за влизане.
- Започнете с група с нисък риск и обяснете ползите от премахването на пароли. Въведете MFA с опция за удостоверяване без парола, докато хората се почувстват комфортно с това, и след това започнете да премахвате пароли и зависимости от пароли във вашата среда.
- Microsoft Azure Active Directory (Azure AD) осигурява SSO изживяване на популярни приложения за софтуер като услуга (SaaS), локални приложения и създадени по поръчка приложения, които се намират на всеки облак, за всеки вид потребител и всяка самоличност.

3 • Прилагайте контроли за достъп с адаптивни, базирани на риска политики

Преминете отвъд простите решения за достъп/ блокиране и приспособете решения, базирани на нивото на риска – като например позволяване на достъп, блокиране, ограничаване на достъп или изискване на допълнителни доказателства като многофакторно удостоверяване.

- Условният достъп в Azure AD ви дава възможност да прилагате фини контроли на адаптивния достъп, като изискване за многофакторно удостоверяване, базирано на информация, свързана с потребителя, устройството, местоположението и информация за риска на сесията.

- Ще имате нужда от потребител с работещ Azure AD с Azure AD Premium или активиран пробен лиценз. Ако е необходимо, можете да създадете потребител с администраторски привилегии за условен достъп безплатно.

4 • Блокирайте наследеното удостоверяване

Една от най-честите насоки за атаки на злонамерени участници е да използват откраднати или възпроизведени идентификационни данни срещу наследени протоколи, като например SMTP, които не могат да използват предизвикателствата на съвременната сигурност.

- Наследените протоколи за удостоверяване като POP, SMTP, IMAP и MAPI не могат да прилагат MFA, което ги прави предпочитани входни точки за неприятели, атакуващи вашата организация.

- Най-лесният начин за блокиране на наследени протоколи в цялата организация е да създадете политика за условен достъп, приложима специално за клиенти на наследени протоколи за приложения към сървъри, която блокира достъпа.

- Разгръщайки блокиращата защита по отношение на наследените протоколи, ние препоръчахме постепенен подход, вместо блокирането за всички потребители наведнъж. Преди да можете да блокирате наследените протоколи във вашата директория, имате нужда първо да разберете дали вашите потребители имат приложения, които ползват наследени протоколи и как това засяга вашата цялостна директория.

5 • Автоматизирайте разкриването на риска и отстраняването му

Оценките на риска в реално време могат да помогнат за защита срещу компрометиране на самоличността по време на влизане и по време на сесии.

- Azure Identity Protection предоставя непрекъснато разкриване в реално време, автоматизирано отстраняване и свързано разследване за разузнаване относно рискови потребители и влизания, за да се справи с потенциални уязвимости

- Активирайте защита на самоличността, за да започнете. Вкарайте данни за сесии на потребители от Microsoft Defender за облачни приложения, за да обогатите Azure AD с възможно поведение на рискови потребители, след като те са удостоверени.

- Данни от защитата на самоличността могат да бъдат експортирани в други инструменти, за да бъдат архивирани и за по-нататъшно разследване, и за установяване на връзка. API, базирани на Microsoft Graph, позволяват на организациите да събират тези данни за по-нататъшно обработване, като например с тяхно SIEM решение.

6 • Обогатете вашето решение за управление на самоличността и достъпа (IAM) с повече данни

Колкото повече данни предоставите на вашето решение за управление на самоличността и достъпа (IAM), толкова повече ще можете да подобрите нивото на вашата сигурност с решения за постепенен достъп и по-добра видимост по отношение на потребители, извършващи достъп до корпоративни ресурси.

- Azure Active Directory (Azure AD), Microsoft Defender за облачни приложения и Microsoft Defender за крайни устройства работят заедно, за да осигурят обогатено обработване на сигнали за взимане на по-добри решения.
- Конфигурирайте условен достъп в Microsoft Defender за крайни устройства, Microsoft Defender за потребители и Microsoft Defender за облачни приложения.

---

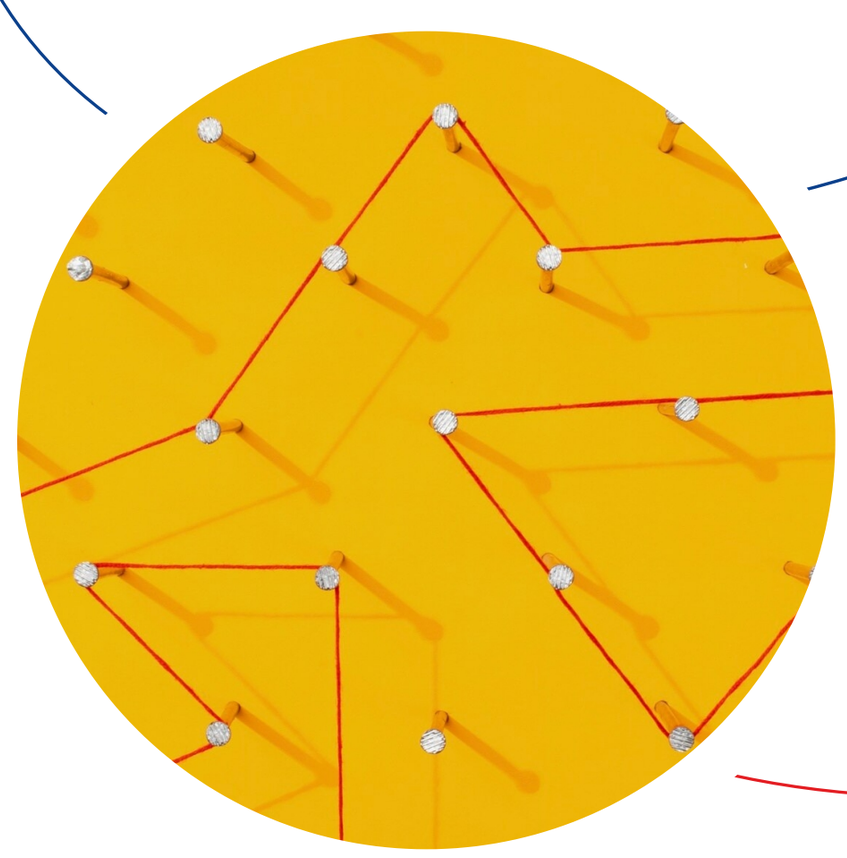
7 • Подобрете състоянието на вашата сигурност по отношение на данните за самоличност.

Резултатът за сигурност на самоличността в Azure AD ви помага да оцените състоянието на вашата сигурност по отношение на самоличността чрез анализиране на това доколко вашата среда е в съответствие с препоръките за най-добри практики за сигурност на Microsoft.

- Резултатът за ниво на сигурност на самоличността е наличен във всички версии на Azure AD
- За да разгледате хронологията на резултатите ви, посетете портала на Microsoft 365 Defender и прегледайте цялостния резултат на Microsoft за сигурността. Можете да преглеждате промени в цялостния ви резултат за сигурността, като щракнете върху „Преглед на хронологията“. Изберете определена дата, за да видите кои контроли са били активирани на този ден и какви точки са спечелени за всяка една.

→ Призив за действие: попитайте специалист от Noventiq относно вашия резултат за самоличността.

Крайни устройства



Модерната компания има невероятно разнообразие от крайни устройства, осъществяващи достъп до данни, но не всички тези крайни устройства се управляват или дори не всички се притежават от организацията, което води до различни конфигурации на устройства и софтуерни нива на корекции. Това създава огромно поле за атаки. Цялостната структура Zero Trust може да ви помогне да подобрите сигурността на крайните устройства, така че да можете да осигурите по-сигурна хибридна работа и да се възползвате от стратегии, зависещи от устройства като например IoT и edge computing.

Защитата на крайни устройства включва контрол и защита на крайни устройства срещу кибератаки. Защитените крайни устройства включват настолни компютри, лаптопи, смартфони, таблети и други устройства. Организациите имат нужда от задълбочено решение, което позволява откриване на всички крайни устройства и дори мрежови устройства, като рутери. И в допълнение – управление на уязвимости, защита на крайни устройства, разкриване на крайни устройства и отговор (EDR).

Най-важното в Zero Trust за крайни устройства.

Zero Trust е пътуване, а не крайна точка. Като се има предвид, че съдържа предпоставки за всеки аспект на ИТ сигурността, първоначално може да изглежда като нещо непреодолимо. Постепенен подход, насочен към области с високо въздействие с малко усилия, може да доведе до бързи подобрения и да разясни кои да бъдат следващите стъпки. Можете да разработите по-обширна стратегия в движение. Важното е да положите началото.

Успешното прилагане на Zero Trust може да помогне за подобряване на сигурността в свят, в който работата зависи от устройства, приложения и данни извън обхвата на контролите, базирани на определен периметър. Това позволява намаляване на риска от нарушения, свързани с данни, и поддържа функционирането на вашия бизнес непрекъснато.

- **Регистрирайте устройства в Azure AD:**
  За да контролирате сигурността и риска в многобройни крайни устройства, използвани от всеки, вие имате нужда от видимост на всички устройства и точки за достъп, които може да имат достъп до вашите ресурси.

- **Гарантирайте съответствие с Microsoft Purview:** След като разполагате със самоличността зад всички крайни устройства, имащи достъп до корпоративни ресурси, и преди предоставяне на достъп, трябва да се уверите, че те отговарят на минималните изисквания за сигурност, определени от вашата организация.

- **Регистрирайте устройства за външни потребители в Endpoint Manager** : Регистрирането на устройства от външни потребители (като изпълнители, вендори, партньори и т.н.) във вашето MDM решение е страхотен начин да осигурите защита на вашите данни и тези потребители да имат достъпа, от който се нуждаят, за да вършат своята работа.

- **Разрешете оценка на риска на устройства в реално време**: След като сте регистрирали вашите устройства при вашия доставчик на самоличност, можете да пренесете този сигнал във вашите решения за достъп, за да позволявате достъп само на безопасни и отговарящи на изискванията устройства.

- **Регистрирайте устройства в Microsoft Endpoint Manager**: Веднъж след като е предоставен достъп до данни, възможността да контролирате какво върши потребителят с вашите корпоративни данни се явява от критична важност за смекчаване на риска.

- **Позволете достъп за устройства, които не се контролират, с Microsoft Endpoint Manager**: Да позволите на вашите служители да имат достъп до подходящи ресурси от устройства, които не се контролират, може да е много важно за поддържане на производителността. Все пак защитата на вашите данни остава задължителна.

- **Прилагайте политики за предотвратяване на загубата на данни на вашите устройства:**
  След като е предоставен достъп, контролирането на това какво може да прави потребителят с вашите данни е от критично значение. Например, ако потребител получи достъп до документ от корпоративен характер, трябва да има механизъм за предотвратяване запазването на документа на незащитено място или споделянето му при комуникация на потребителя или в приложение за разговори.

Заключение

Чрез възприемането на структурата Zero Trust, вие можете ефективно да модернизирате вашата технология за сигурност и процеси и да започнете да увеличавате в най-висока степен защитата срещу съвременните заплахи. Все пак всяка организация ще има различни приоритети в зависимост от своите настоящи възможности и нивото на риска, който дадена област на сигурност представлява. Това ръководство прави получаването на обширна представа за Zero Trust лесно за вас, както и получаването на подробна информация и приложими стъпки за 2 много важни опорни точки: Потребители и крайни устройства.

Microsoft се застъпва за Zero Trust отчасти защото структурата е увеличила сигурността и ефективността в собствената среда на компанията. На базата на този опит Microsoft развива възможностите на Zero Trust, които интегрират и разширяват неговите решения за технологии, като например контроли за постепенен достъп, умишлено изолиране на мрежа и базирано на изкуствен интелект разкриване на опити за подозрителен достъп. В допълнение, функциите и услугите за сигурност на Microsoft са проектирани, за да работят заедно, помагайки на ИТ екипи да опростят възприемането и текущото управление на техния набор технологична сигурност. Noventiq е глобален доставчик на решения за Microsoft. Ние имаме правилните ресурси и компетенции за прилагане на решенията на Microsoft, дори в най-сложните архитектури.

Има няколко решения, предлагани от Microsoft, за подкрепа на бизнеси, за обезпечаване на техните идентичности и устройства. И Microsoft Defender за бизнес, и Defender за крайни устройства имат разширени функции, които могат да подпомогнат целите на Zero Trust за вашата организация. Експертите на Noventiq с удоволствие ще ви преведат и през двете опции и ще обсъдят по-разширени пакети, за да намерят този, който най-добре отговаря на изискванията на вашата компания.

Microsoft Defender за бизнес предоставя много възможности за компаниите от малкия и среден бизнес.

Компании с по-малко от 300 служители могат да разчитат на Microsoft Defender за бизнес. Това е решение, посветено на малкия и среден бизнес. То може да бъде закупено като самостоятелен лиценз или като част от премиум пакета на Microsoft 365 за бизнес.

Като самостоятелен лиценз Microsoft Defender за бизнес започва от 2,50 € за потребител на месец и включва до 5 устройства на потребител, годишен абонамент – автоматични обновявания.

Препоръчваме ви да поискате примерна цена от нашите специалисти. Те ще ви покажат предимствата на премиум пакета на Microsoft 365 за бизнес и оптимизирането на разходите чрез придобиването на широки възможности на Microsoft под формата на пакет.

План 1 и План 2 на Defender за крайни устройства обезпечават крайни устройства в цялото ви предприятие с множество платформи.

Defender for Endpoint Plan 2

Defender for Endpoint Plan 1

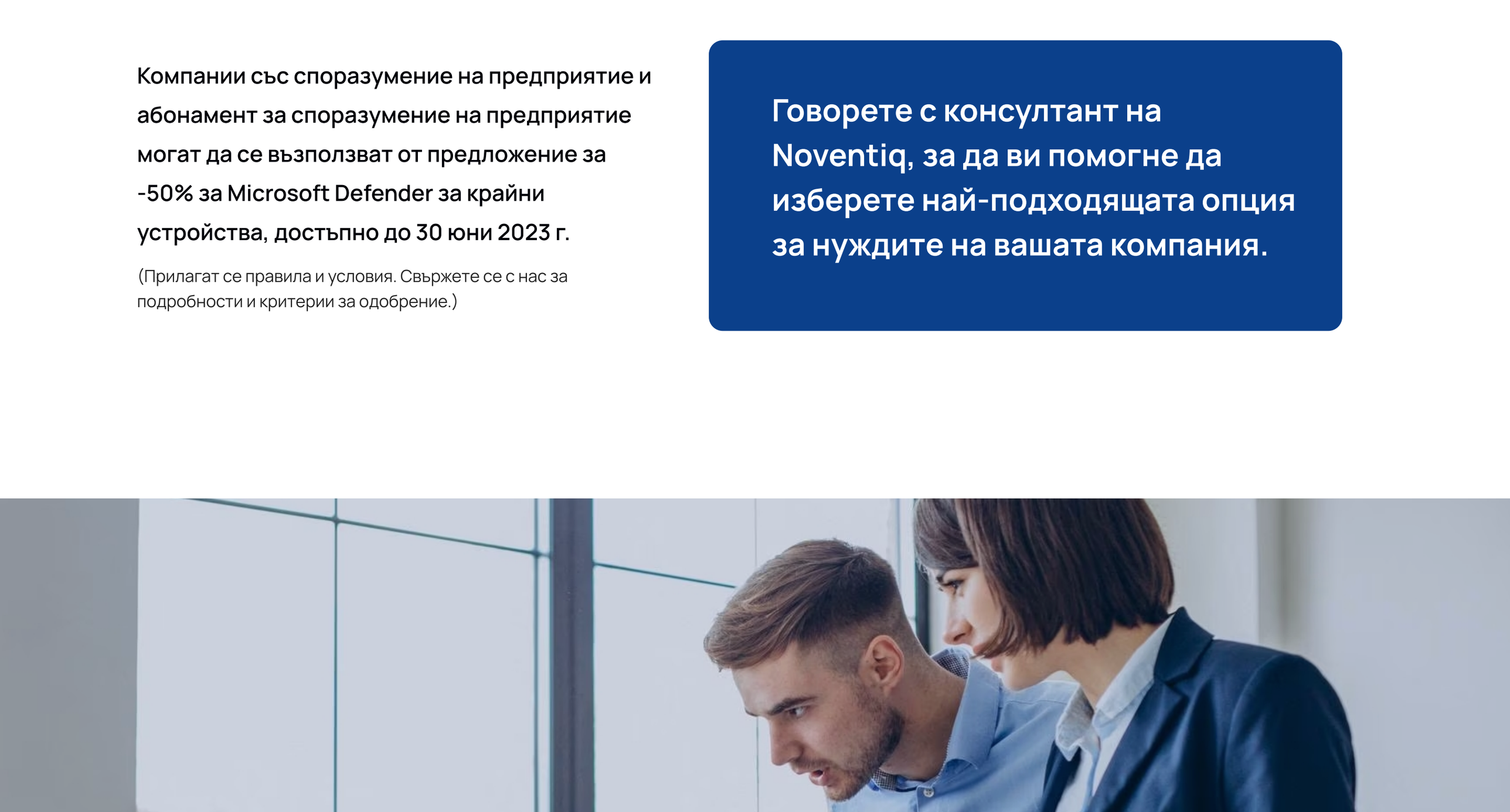
Block at First Sight	Centralized Management	Cross-Platform Support	Enhanced ASR	Manual Response Actions	Temper Protection	Web Content Filtering

Advanced Hunting	Automated Investigation & Response	Defender for Cloud Apps Integration	Endpoint Detection & Response	Evaluation Lab	Microsoft Threat Exprets	MIP Integration
Threat Analytics	Vulnerability Management (core)	6-Months Searchable Data				

Компании със споразумение на предприятие и абонамент за споразумение на предприятие могат да се възползват от предложение за -50% за Microsoft Defender за крайни устройства, достъпно до 30 юни 2023 г.

(Прилагат се правила и условия. Свържете се с нас за подробности и критерии за одобрение.)

Говорете с консултант на Noventiq, за да ви помогне да изберете най-подходящата опция за нуждите на вашата компания.



За Noventiq

Noventiq е водещ доставчик на глобални решения и услуги за дигитална трансформация и киберсигурност, която е със седалище и регистрация в Лондон. Компанията подпомага, улеснява и ускорява дигиталната трансформация на бизнесите на своите клиенти, свързвайки над 75 000 организации от всички сектори със стотици от най-добрите ИТ посредници, заедно със своите собствени услуги и решения.

С оборот от 1,1 милиарда щатски долара през финансовата 2021 г., понастоящем Noventiq е една от най-бързо разрастващите се компании в сектора. Израстването на Noventiq се подсилва от нейната триизмерна стратегия за разширяване на своите география, портфолио и канали за продажби. Стратегията е подкрепена от активния подход на Noventiq към сливания и придобивания, позволявайки на компанията да се възползва от настоящото консолидиране в сектора. От началото на календарната 2022 г., Noventiq обяви придобиването на 5 компании в Индия, Турция и ОАЕ, обхващащи различни аспекти на дигиталната трансформация. Служителите на Noventiq, които са 3900 души, работят в почти 60 държави в Азия, Латинска Америка, Източна Европа и Африка – пазари със значителен потенциал за растеж.

Отличителни области

Дигитална трансформация, киберсигурност, управление на информацията, съвременна хибридна инфраструктура, решения в множество облачни пространства, решения за бъдещи работни места, софтуерно инженерство, разработване на софтуер, ИТ доставчик за възникващи пазари и ИТ консултант.

NOVENTIQ
Global expertise, local outcomes

Noventiq – глобален опит, резултати на местно ниво.

easterneurope@noventiq.com