EBOOK

De ce Zero Trust?

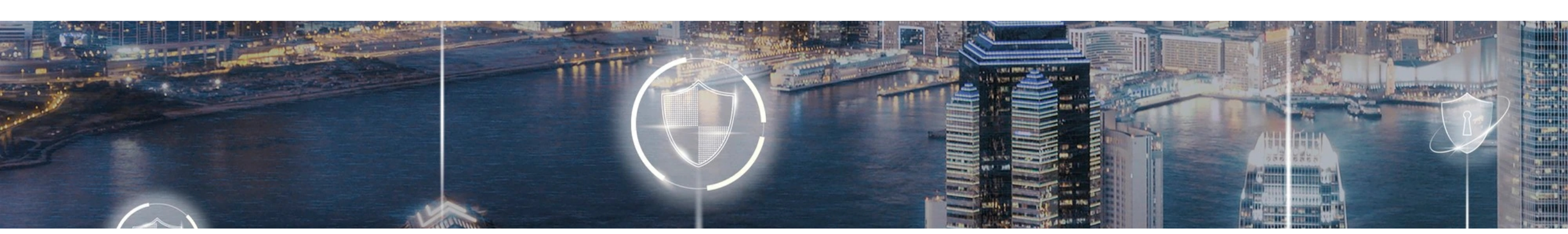
Adoptați securitatea proactivă cu Zero Trust

NOVENTIQ
Global expertise, local outcomes

Microsoft Solutions Partner

Cui i se adresează?

Liderilor IT și de afaceri care doresc să-și asigure mediile IT folosind un cadru de încredere zero (Zero Trust). Acest ghid prezintă o explicație cuprinzătoare a conceptului Microsoft Zero Trust, împreună cu măsuri specifice pentru a implementa oricare sau toate cele șase domenii cheie ale strategiei de securitate organizațională.



De ce Zero Trust?

Proliferarea datelor și dispozitivelor, creșterea muncii hibride și atacurile din ce în ce mai sofisticate reduc eficacitatea securității IT bazate pe perimetru. Profesioniștii IT gestionează o varietate enormă de tehnologii. Întreprinderile folosesc în mod obișnuit un mix de infrastructură cloud și local, platforme și software. Este posibil să aibă mai mulți furnizori și sisteme de cloud. Angajații lucrează pe dispozitive personale și pot accesa cu ușurință aplicațiile și serviciile cloud. Datele există în mai multe locuri ca niciodată, ceea ce o face mai valoroasă, dar și mai vulnerabilă.

Ca răspuns, multe organizații, inclusiv Microsoft, adoptă un cadru de securitate de încredere zero.

„Zero Trust” este o abordare proactivă și integrată a securității pe toate straturile proprietatii digitale care verifică în mod explicit și continuu fiecare tranzacție și se bazează pe inteligență, detectare avansată și răspuns în timp real la amenințări:

- **Verificați explicit:** autentificați întotdeauna și autorizați pe baza tuturor punctelor de date disponibile, inclusiv identitatea utilizatorului, locația, sănătatea dispozitivului, serviciul sau volumul de muncă, clasificarea datelor și anomaliile.

- **Fiți pregătiți pentru breșa de securitate:** minimizați raza de răspândire și segmentati accesul. Verificați criptarea end-to-end și utilizați rapoartele de analiză pentru a obține vizibilitate, a detecta amenințările și pentru a îmbunătăți apărarea.

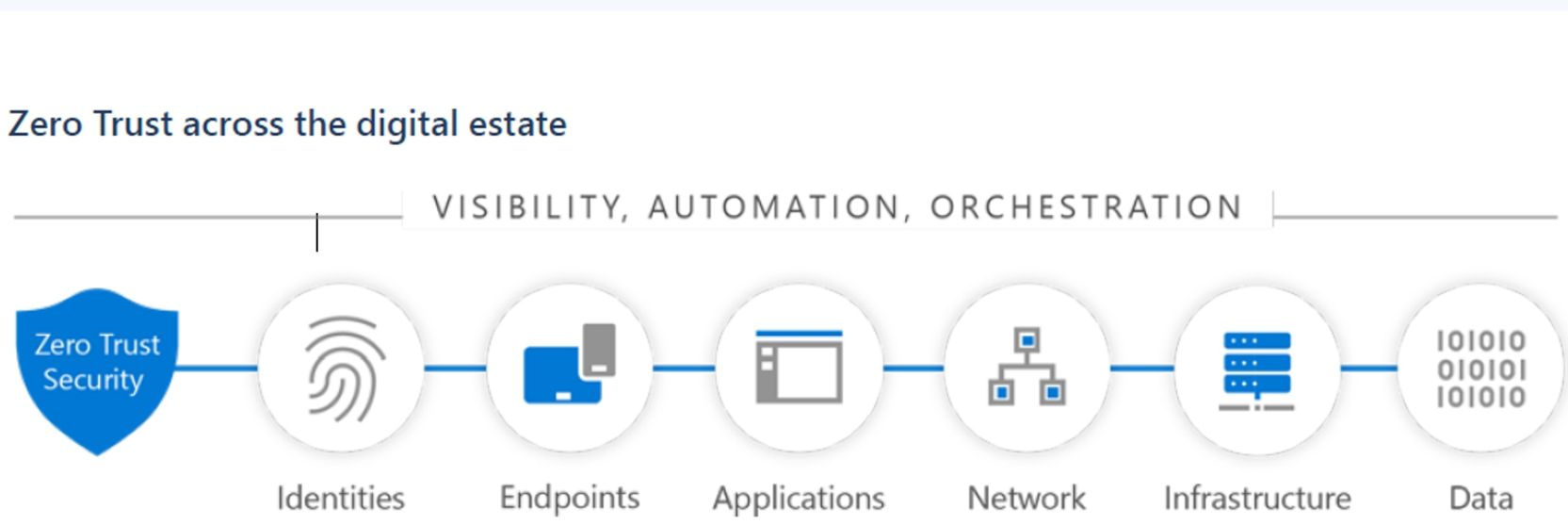
- **Utilizați accesul cel mai puțin privilegiat**: limitați accesul utilizatorilor oferind acces la o anumită oră agreată sau pentru un timp limitat (ex: la ora 20:00 pentru 30 de minute sau 2 ore începând cu ora 20:00), politici adaptive bazate pe riscuri și protecție a datelor pentru a ajuta la securizarea atât a datelor, cât și a productivității.

Protecția modernă a amenințărilor este o componentă critică a tuturor celor trei domenii, permițând organizațiilor să detecteze atacuri și anomalii, să blocheze automat și să semnalizeze comportamentul riscant, să ia măsuri de protecție și să gestioneze influxul din ce în ce mai mare amenințări.

Cât de ușor poate adopta o organizație aceste principii variază în funcție de provocările sale individuale de securitate, nevoile și capacitățile sale. Cu alte cuvinte, călătoria către Zero Trust este unică pentru afacerea dvs.

Pentru a vă ajuta să ajungeți mai repede acolo, Microsoft a dezvoltat un cadru flexibil Zero Trust pentru a ghida adoptarea. Acesta oferă îndrumări cuprinzătoare care acoperă cele șase **domenii cheie de risc** abordate de Zero Trust:

- **Identitate:** Automatizarea detectării și remedierii riscurilor și accesul sigur la resurse cu autentificare puternică pe întreaga proprietate digitală.
- **Aplicații:** Mențineți accesul extrem de sigur al angajaților la aplicațiile cloud și mobile, precum și acces securizat la distanță la aplicațiile de business de tip Enterprise găzduite în infrastructura on-premises.
- **Rețea:** Reduceți vulnerabilitățile de securitate bazate pe perimetru, inclusiv nevoia de VPN -uri și îmbunătățiți scalabilitatea soluțiilor de securitate pentru medii în care cloud-ul este din ce în ce mai mult centrul serviciilor IT.
- **Endpoints**: Apărați suprafața de atac mai mare creată de numărul tot mai mare și diversitatea dispozitivelor finale folosind o abordare flexibilă și integrată a administrării acestora.
- **Date**: Clasificați, etichetați și protejați datele din mediile cloud și local pentru a preveni partajarea necorespunzătoare și reducerea riscurilor utilizatorilor.
- **Infrastructură**: Protejați infrastructura hibridă, inclusiv mediile IT și cloud locale, cu un management mai eficient și automat.



Prin adoptarea unui cadru Zero Trust în unul sau în toate domeniile, vă puteți moderniza eficient tehnologia și procesele de Securitate și să maximizați protecția împotriva amenințărilor moderne. Cu toate acestea, fiecare organizație va avea priorități diferite în funcție de capacitățile sale curente și de nivelul de risc reprezentat de o anumită zonă de securitate. Acest ghid vă ajută să obțineți o imagine de ansamblu amplă a Zero Trust, precum și informații detaliate și pași de acțiune pentru domeniile dvs. de interes.

Arhitectura Microsoft Zero Trust

În aceast eBook ne vom concentra pe primele 2 componente ale cadrului Zero Trust, pe care le-am identificat ca fiind cele mai importante pentru companiile mici și mijlocii.

Fundamentele Zero Trust

Identități

Aplicațiile cloud și creșterea muncii hibride au redefinit perimetrul de securitate. Aplicațiile și datele corporative trec, de asemenea, de la medii on-premise la medii hibride și cloud. Multe organizații se bazează pe gestionarea mai veche a identității și a accesului, construită pentru o lume cu o linie clară între ceea ce este în interior și ceea ce este în afara rețelei.

Aceste sisteme îngreunează accesul oamenilor la aplicațiile și datele de care au nevoie și creează lacune de securitate prin acordarea de privilegii excesive utilizatorilor de încredere. Un cadru Zero Trust, care încorporează soluții de identitate bazate pe cloud, cum ar fi autentificarea cu mai mulți factori și autentificarea unică (SSO) în toate mediile, este mai potrivit pentru locul de muncă modern.

Controale de identitate pentru un cadru Zero Trust

1 • Implementați autentificarea cu mai mulți factori

Autentificarea cu mai mulți factori vă protejează aplicațiile solicitând utilizatorilor să-și confirme identitatea folosind a doua sursă de validare, cum ar fi un telefon sau un token, înainte să fie acordat accesul.

- Instrumente precum Microsoft Azure Active Directory (Azure AD) permit autentificarea în mod gratuit cu mai mulți factori.
- Autentificarea multifactor (MFA) Azure Active Directory (Azure AD) ajută la protejarea accesului la date și aplicații, oferind încă un nivel de securitate prin utilizarea unei a doua forme de autentificare. Organizațiile pot activa autentificarea cu mai mulți factori cu Acces condiționat pentru ca soluția să se potrivească nevoilor lor specifice.

2 • Activați autentificarea fără parolă

Metodele de autentificare fără parolă oferă o experiență de autentificare mai simplă și mai sigură pentru web și dispozitive mobile. Aceste metode permit utilizatorilor să se autentifice ușor și în siguranță, fără să fie nevoie de parolă.

- Dacă aveți AAD, puteți activa instrumente precum aplicația Microsoft Authenticator, astfel încât utilizatorii să se poată conecta la orice cont Azure AD fără utilizarea unei parole. Microsoft Authenticator utilizează autentificarea bazată pe chei pentru a activa un credențial de utilizator care este legat de un dispozitiv care utilizează un PIN sau date biometrice. Windows Hello for Business folosește o tehnologie similară.
- Implementați conectarea unică (SSO). Acest lucru elimină nevoia acordării mai multor acreditări pentru aceeași persoană și oferă o experiență mai bună utilizatorului cu mai puține solicitări de conectare.
- Începeți cu un grup cu risc scăzut și explicați beneficiile eliminării parolelor. Implementați MFA cu o opțiune de autentificare fără parolă până când oamenii se simt confortabil cu aceasta și apoi începeți să înlocuiți parolele și dependența de parole.
- Microsoft Azure Active Directory (Azure AD) oferă o experiență SSO pentru software popular ca aplicații de service (SaaS), aplicații la sediu și aplicații personalizate care se află pe orice cloud pentru orice tip de utilizator și identitate.

3 • Implementați controale de acces prin politici adaptative, bazate pe risc

Treceți dincolo de simple decizii de acces/blocare și adaptați deciziile în funcție de apetitul pentru risc, cum ar fi permiterea accesului, blocarea, limitarea accesului sau solicitarea de dovezi suplimentare, cum ar fi autentificarea cu mai mulți factori.

- Accesul condiționat în Azure AD vă permite să aplicați controale de acces adaptative ajustate, cum ar fi solicitarea de autentificare cu mai mulți factori în funcție de contextul utilizatorului, dispozitiv, locație și informații privind riscul sesiunii.

- Veți avea nevoie de un tenant Azure AD funcțional cu Azure AD Premium sau licență de probă activată. Dacă este necesar, puteți crea gratuit unul cu drepturi de administrator.

4 • Blocați autentificarea veche

Unul dintre cei mai obișnuiți vectori de atac pentru autorii rău intenționați este reprezentat de utilizarea acreditărilor furate sau reluate din protocoale vechi, cum ar fi SMTP, care nu pot face față provocărilor de securitate moderne.

- Protocoalele de autentificare vechi precum POP, SMTP, IMAP și MAPI nu pot activa MFA, devenind puncte de intrare preferate pentru inamicii care vă atacă organizația.

- Cel mai simplu mod de blocare a autentificării vechi din întreaga organizație este prin configurarea unei politici de acces condiționat care se va aplica mai ales clienților cu autentificarea veche și va bloca accesul.

- În timp ce inițiați blocarea autentificării vechi, vă recomandăm o abordare treptată, nu o dezactivați pentru toți utilizatorii simultan. Înainte să puteți bloca autentificarea veche în directorul vostru, trebuie să aflați mai întâi dacă utilizatorii voștri au aplicații care folosesc autentificarea veche și cum afectează acest lucru directorul la modul general.

5 • Automatizați detectarea și remedierea riscurilor

Evaluările riscurilor în timp real pot ajuta în protecția împotriva compromiterii identității în momentul autentificării și în timpul sesiunilor.

- Azure Identity Protection oferă detecție continuă în timp real, remediere automată și inteligență conectată pentru a investiga utilizatorii și conectările cu risc pentru a rezolva potențialele vulnerabilități.

- Activați Identity Protection pentru a începe. Introduceți date despre sesiunile utilizatorilor din Microsoft Defender pentru aplicații cloud pentru a îmbogăți Azure AD cu un posibil comportament riscant al utilizatorului după autentificare.

- Datele din Identity Protection pot fi exportate în alte instrumente pentru arhivare și investigare și corelare ulterioară. API-urile bazate pe Microsoft Graph permit organizațiilor să colecteze aceste date pentru prelucrare ulterioară, cum ar fi cu soluția SIEM.

6 • Îmbogățiți-vă soluția Identity and Access Management (IAM) cu mai multe date

Cu cât furnizați mai multe date soluției voastre IAM, cu atât mai mult vă puteți îmbunătăți securitatea cu acces granular și o mai bună vizibilitate asupra utilizatorilor care accesează resursele organizației.

- Azure Active Directory (Azure AD), Microsoft Defender pentru aplicații în cloud și Microsoft Defender pentru Endpoint operează împreună pentru o procesare mai bună a semnalului în luarea deciziilor.
- Configurați accesul condiționat în Microsoft Defender pentru Endpoint, Microsoft Defender pentru Identity și Microsoft Defender pentru aplicații cloud.

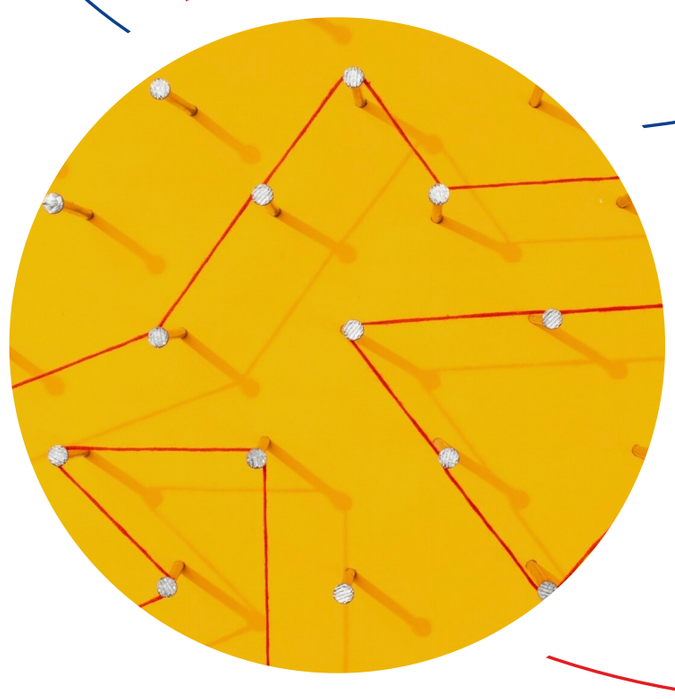
7 • Îmbunătățiți-vă nivelul de securitate a identității

Scorul de securitate a identității din Azure AD vă ajută să evaluați nivelul de securitate a identității, analizând cât de bine mediul dumneavoastră respectă recomandările privind cele mai bune practici pentru securitate furnizate de Microsoft.

- Scorul de securitate al identității este disponibil pentru toate edițiile Azure AD.
- Pentru a vedea istoricul scorului, vizitați portalul Microsoft 365 Defender și revizuiți scorul general Microsoft Secure. Puteți revizui și modificările aduse scorului general de securitate făcând click pe View History. Alegeți o anumită dată pentru a vedea ce controale au fost activate pentru ziua respectivă și ce puncte ați câștigat pentru fiecare dată.

Întrebați un expert Noventiq despre scorul vostru de identitate.

Endpoints



Compania modernă are o diversitate foarte mare de dispozitive finale (endpoints) care accesează date, dar nu toate acestea sunt gestionate sau chiar deținute de organizație, având diferite configurații ale dispozitivelor și nivele a patch-urilor software. Acest lucru creează o suprafață masivă de atac. Cadrul Zero Trust de la un capăt la altul vă poate ajuta să îmbunătățiți securitatea dispozitivelor finale, astfel încât să puteți activa o muncă hibridă mai sigură și să profitați de strategiile care depind de dispozitive, cum ar fi IoT sau arhitectura edge computing.

Protecția dispozitivelor finale cuprinde monitorizarea și protejarea lor împotriva amenințărilor cibernetice. Endpoint-urile protejate includ desktop-uri, laptop-uri, smartphone-uri, tablete și alte dispozitive. Organizațiile au nevoie de o soluție cuprinzătoare care să permită identificarea tuturor dispozitivelor mobile și chiar a dispozitivelor de rețea, cum ar fi routerele. Și în plus, managementul vulnerabilităților, protecția dispozitivelor finale și detectarea și răspunsul acestora (EDR).

Elementele esențiale ale Zero Trust pentru dispozitivele finale

Zero Trust este o călătorie, nu o destinație. Deoarece afectează fiecare aspect al securității IT, poate părea copleșitor la început. O abordare în etape vizând mai întâi zonele cu impact mare și efort redus poate duce la îmbunătățiri rapide și la clarificarea pașilor de urmat. Puteți construi o strategie mai amplă pe măsură ce înaintați. Important este să demarați procesul.

Implementarea cu succes a Zero Trust poate ajuta la îmbunătățirea securității într-o lume în care munca se bazează pe dispozitive, aplicații și date în afara controalelor bazate pe perimetru. Acesta ajută la reducerea riscului de încălcare a accesului la date și vă menține afacerea în funcțiune 24/7.

- **Înregistrați dispozitive cu Azure AD :** Pentru a monitoriza securitatea și riscul în mai multe dispozitive finale utilizate de orice persoană, aveți nevoie de vizibilitate pentru toate dispozitivele și punctele de acces care vă pot accesa resursele.

- **Asigurați conformitatea cu Microsoft Purview:** Odată ce aveți identitatea pentru toate dispozitivele finale care accesează resursele organizației, și înainte de a acorda accesul, asigurați-vă că acestea îndeplinesc cerințele minime de securitate stabilite de organizație.

- **Înregistrați dispozitive pentru utilizatori externi cu Endpoint Manager** : Înregistrarea dispozitivelor folosite de utilizatori externi (contractori, furnizori, parteneri etc.) în soluția voastră MDM este o modalitate excelentă de a vă proteja datele și de a vă asigura că utilizatorii beneficiază de accesul de care au nevoie pentru a-și desfășura activitatea.

- **Activați evaluarea în timp real a riscurilor dispozitivelor**: Odată înregistrate dispozitivele la furnizorul vostru de identitate, puteți aduce semnalul respectiv în deciziile pe care le luați pentru a permite doar accesul dispozitivelor sigure și conforme.

- **Înregistrați dispozitive la Microsoft Endpoint Manager**: Odată ce accesul la date este acordat, posibilitatea de a controla ceea ce face utilizatorul cu datele organizației dunmeavoastra devine esențială pentru diminuarea riscului.

- **Activați accesul pentru dispozitive care nu sunt administrate de Microsoft Endpoint Manager** : Accesul angajaților la resurse necesare de pe dispozitive neadministrate poate fi esențial pentru menținerea productivității. Cu toate acestea, protecția datelor rămâne imperativă.

- **Aplicați politicile de prevenire a pierderii de date pe dispozitivele voastre:** Odată ce accesul la date este acordat, controlul a ceea ce utilizatorul poate face cu datele voastre este esențial. De exemplu, dacă un utilizator accesează un document cu identitate corporativă, ar trebui să existe mecanisme care să împiedice salvarea documentului într-o locație neprotejată sau partajarea acestuia într-o aplicație de comunicare sau de chat pentru publicul larg.

Concluzii

Prin adoptarea unui cadru Zero Trust în una sau în toate aceste domenii, vă puteți moderniza eficient tehnologia și procesele de securitate și puteți începe să maximizați protecția în fața amenințărilor moderne. Cu toate acestea, fiecare organizație va avea priorități diferite în funcție de capacitățile sale actuale și de nivelul de risc reprezentat de o anumită zonă de securitate. Acest ghid vă ajută să obțineți o imagine de ansamblu amplă a Zero Trust, precum și informații detaliate și pași de acțiune pentru domeniile dvs. de interes.

Microsoft pledează pentru Zero Trust, întrucât a crescut securitatea și eficiența în mediul propriu al companiei. Ținând cont de acest lucru, Microsoft construiește capabilități Zero Trust care se integrează și se extind pe soluțiile sale tehnologice, cum ar fi controale granulare de acces, izolarea rețelei prin proiectare și detectarea încercărilor de acces suspecte bazată pe IA a încercărilor de acces suspecte. Mai mult, funcțiile și serviciile de securitate Microsoft sunt concepute pentru a funcționa împreună, ajutând echipele IT să-și simplifice adoptarea și managementul continuu a suitei de tehnologii de securitate. Noventiq este furnizor global de soluții Microsoft. Dispunem de resursele și competențele necesare pentru implementarea soluțiilor Microsoft, chiar și în cele mai sofisticate arhitecturi.

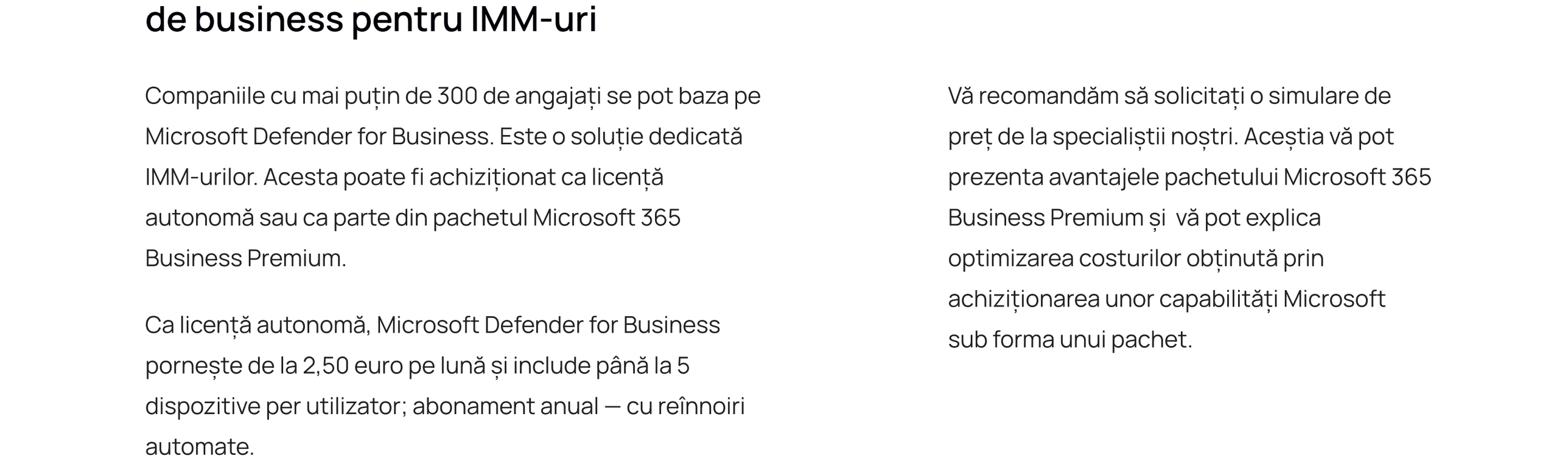
Există mai multe soluții oferite de Microsoft pentru a sprijini companiile să își securizeze identitățile și dispozitivele. Microsoft Defender for Business și Defender for Endpoints au seturi extinse de caracteristici care pot sprijini atingerea obiectivelor de Zero Trust pentru organizația voastră. Experții Noventiq vă pot îndruma în implementarea celor două opțiuni și pot discuta cu voi despre pachete mai complexe pentru a găsi pachetul care răspunde cel mai bine cerințelor companiei voastre.

Microsoft Defender for Business pune la dispoziție multe capabilități de business pentru IMM-uri

Companiile cu mai puțin de 300 de angajați se pot baza pe Microsoft Defender for Business. Este o soluție dedicată IMM-urilor. Acesta poate fi achiziționat ca licență autonomă sau ca parte din pachetul Microsoft 365 Business Premium.

Ca licență autonomă, Microsoft Defender for Business pornește de la 2,50 euro pe lună și include până la 5 dispozitive per utilizator; abonament anual — cu reînnoiri automate.

Vă recomandăm să solicitați o simulare de preț de la specialiștii noștri. Aceștia vă pot prezenta avantajele pachetului Microsoft 365 Business Premium și vă pot explica optimizarea costurilor obținută prin achiziționarea unor capabilități Microsoft sub forma unui pachet.



Planul 1 și Planul 2 pentru Defender for Endpoints securizează dispozitive din puncte finale în întreaga multiplatformă

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				

Companiile cu abonament Enterprise Agreement și Enterprise Agreement pot beneficia de oferta de 50% reducere pentru Microsoft Defender pentru Endpoints disponibilă până la 30 iunie 2023

(Se aplică clauzele și condițiile necesare. Contactați-ne pentru toate detaliile și criteriile de eligibilitate.)

Discutați cu un consultant Noventiq pentru a vă ajuta să alegeți cea mai potrivită opțiune pentru nevoile companiei voastre.

Despre Noventiq

Noventiq este un important furnizor global de soluții și servicii pentru transformare digitală și securitate cibernetică, cu sediul principal și listat la Londra. Compania implementează, facilitează și accelerează transformarea digitală pentru afacerile clienților săi, conectând peste 75.000 de organizații din toate sectoarele cu sute din cei mai buni furnizori IT de clasă înaltă, alături de propriile servicii și soluții.

Cu o cifră de afaceri de 1,1 miliarde USD în anul fiscal 2021, Noventiq este în prezent una dintre companiile cu cea mai rapidă creștere din sector. Creșterea Noventiq este susținută de strategia sa tridimensională de a-și extinde aria geografică, portofoliul și canalele de vânzare. Strategia este susținută de abordarea sa activă în domeniul fuziunilor și achizițiilor, permițând companiei să profite de trendurile industriei. De la începutul anului calendaristic 2022, Noventiq a anunțat achiziția a 5 companii din India, Turcia și Emiratele Arabe Unite, acoperind diverse aspecte ale transformării digitale.

Cei 3900 de angajați ai Noventiq lucrează în aproape 60 de țări din Asia, America Latină, Europa de Est și Africa – piețe cu potențial de creștere semnificativ.

Domenii

Transformare digitală, securitate cibernetică, managementul informațiilor, infrastructură hibridă modernă, soluții multi-cloud, soluții pentru locurile de muncă ale viitorului, inginerie software, dezvoltare software, furnizor IT pentru piețe emergente și consultanță IT.

NOVENTIQ
Global expertise, local outcomes

Noventiq – expertiză globală, rezultate locale

easterneurope@noventiq.com