SECURITY DAYS

METŲ PROVERŽIS: IŠMANUS IT VALDYMAS SU MANAGEENGINE

GEDIMINAS MIKELIONIS
„Baltimax“ IT inžinierius

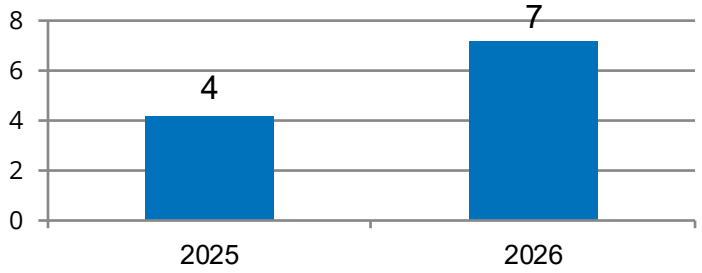
STATISTIKA

Pardavimų augimas: ne procentais, o kartais

ManageEngine

Lyginant vienodus laikotarpius, augimas matuojamas kartais.

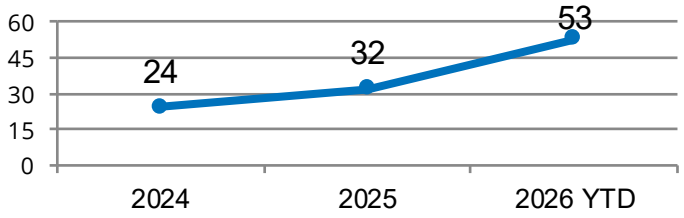
7,2× 2026 YTD YoY



Cloud jau tapo daugumos pasirinkimu

Per dvejus metus Cloud / On-premises dalis perėjo nuo maždaug ketvirtadalio iki daugiau nei pusės.

53% 2026 YTD aktyvių klientų

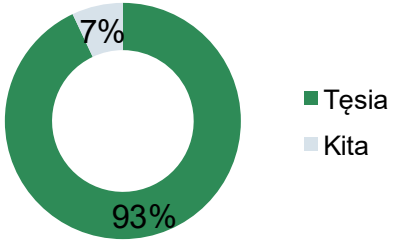


93% klientų nusprendžia toliau naudotis ManageEngine

Klientai ne tik lieka – dalis jų plečia naudojimą per upgrade ir cross-sell.

93%

Pasitikėjimo rodiklis, kuris stiprina žinutę apie sprendimų brandą.



	ManageEngine sprendimas	NIS2 poreikis
01	**Endpoint Central**	Galinių įrenginių sauga, pataisų diegimas, pažeidžiamumų ir turto valdymas, įrenginių kontrolė
02	**Firewall Analyzer**	Ugniasienių stebėsena, konfigūracijų auditas ir tinklo sauga
03	**ADManager Plus**	Tapatybių administravimas, prieigos valdysena ir Active Directory sauga
04	**ADSelfService Plus**	MFA, slaptažodžių sauga ir tapatybės apsauga
05	**PAM360**	Privilegijuotos prieigos valdymas ir privilegijuotų paskyrų sauga
06	**Log360**	SIEM, centralizuotas žurnalų registravimas, grėsmių aptikimas ir incidentų tyrimas
07	**OpManager**	Tinklo ir infrastruktūros stebėsena bei pasiekiamumas
08	**ServiceDesk Plus**	Incidentų ir pokyčių valdymas, ITSM procesai bei audito įrodymai
09	**RecoveryManager Plus**	Atsarginės kopijos ir atkūrimas Microsoft aplinkoms

Sektoriai, kuriems ManageEngine netinka

ManageEngine sektoriai Lietuvoje

- Viešasis administravimas
- Finansai
- Gamyba
- Telekomunikacijos
- Švietimas
- Sveikata
- Prekyba
- Transportas ir logistika
- IT ir technologijos
- Saugumo ir gelbėjimo tarnybos

ManageEngine ? ? ?

ManageEngine privati įmonė, pelningai veikianti nuo pat įkūrimo

20+
Metai šioje srityje

6,000+
ManageEngine darbuotojai

60+
Produktų IT suvaldymui

190
Šalyse operuoja

30+
Biurų visame pasaulyje

ManageEngine pasitiki

ManageEngine laikosi tarptautinių saugumo ir privatumo standartų

ISO/IEC 20000
Valid up to: 29-July-2027

SOC 2 + HIPAA

GDPR

SOC 2

Reguliacijos

HIPAA
(Health Insurance Portability and Accountability Act)

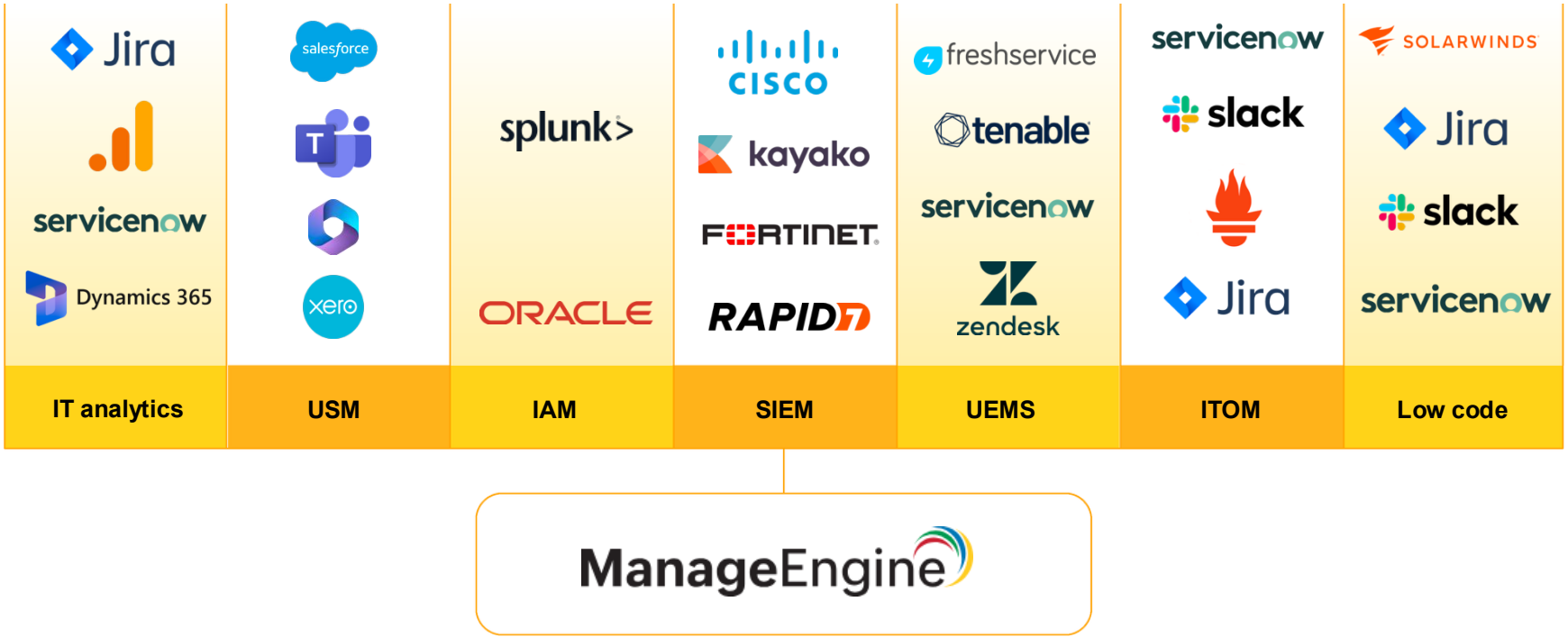
DPDPA
(Digital Personal Data Protection Act)

GDPR

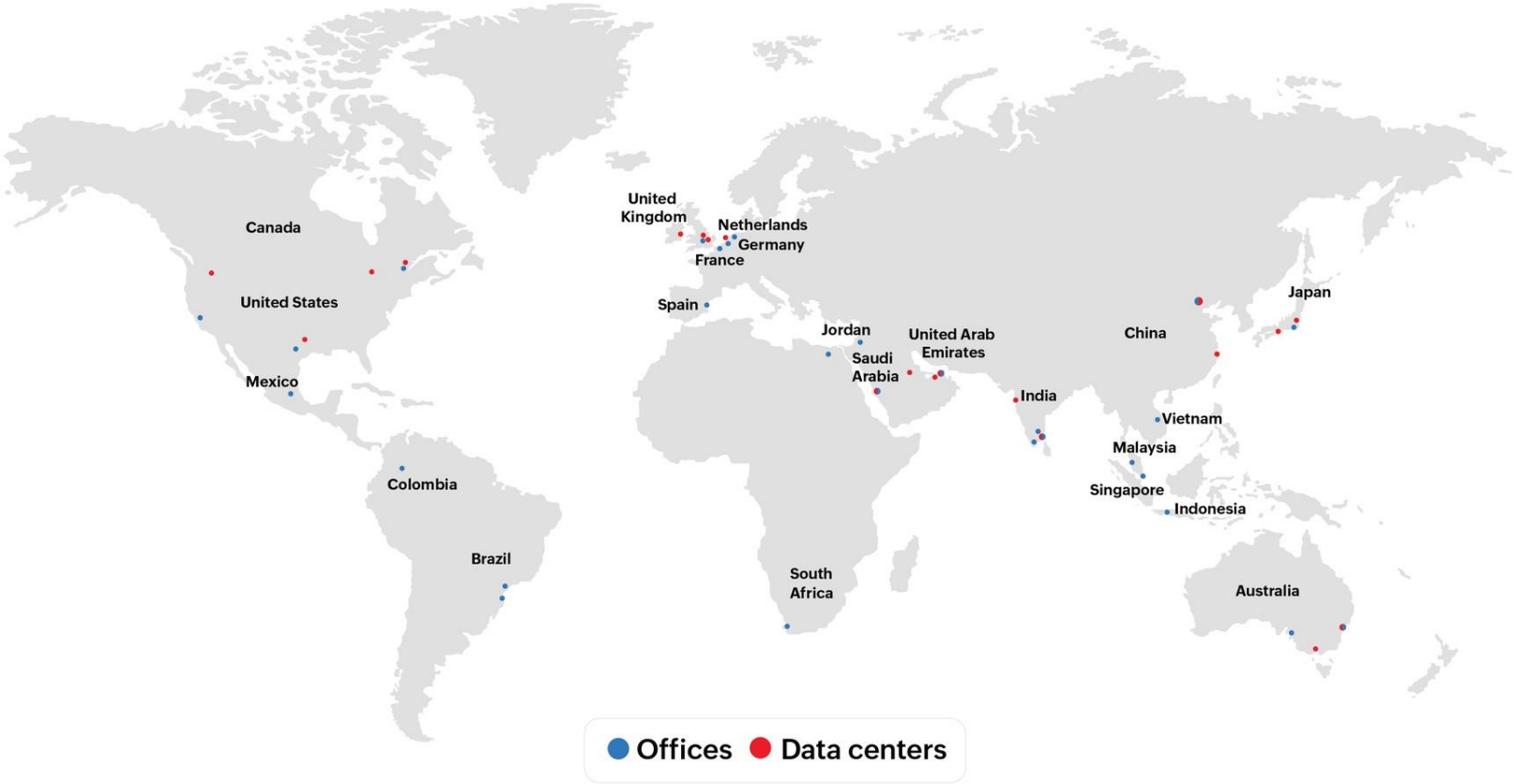
DORA

PCI DCC

Integracijos

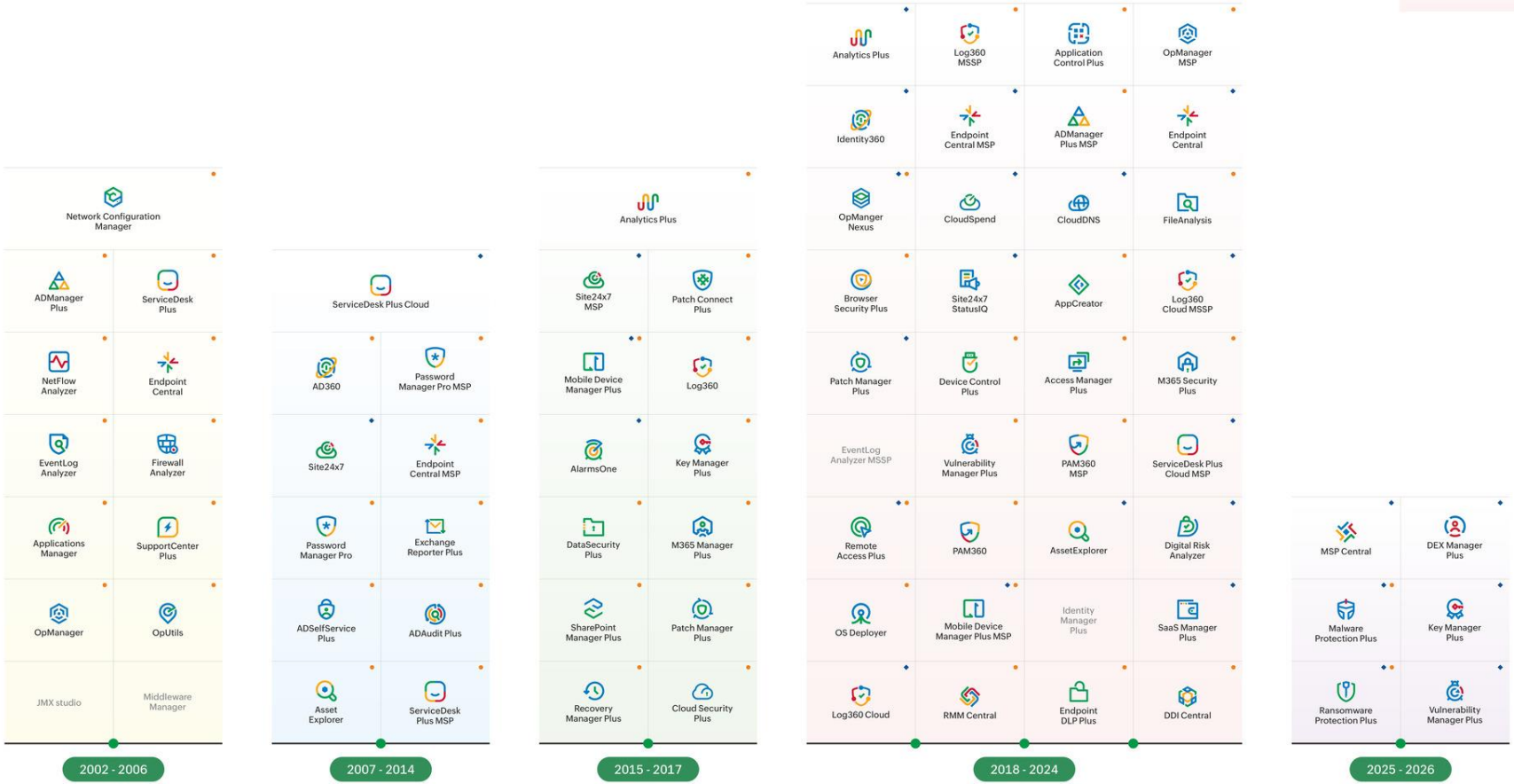


Biurai ir duomenų centrai



ManageEngine

- On-prem
- Cloud



Bestseleriai Lietuvoje

ManageEngine AD360

ManageEngine Log360 (SIEM)

ManageEngine Endpoint Central (UEM)

ManageEngine AD360

AD360 – svarbiausios funkcijos

Tapatybės ir prieigos valdymo platforma skirta AD, Microsoft 365 ir debesijos aplinkoms.

Tapatybės gyvavimo ciklo valdymas

(automatizavimas, orkestravimas)

Automatizuotas naudotojų kūrimas, keitimas ir šalinimas kataloguose bei debesijos programose.

MFA

(įrenginiai, VPN, RDP, aplikacijos)

Saugesni prisijungimai pagal laiką, vietą, IP adresą ar naudojamą įrenginį.

SSO – vienkartinis prisijungimas

(SAML, OAuth, OIDC, MFA apsauga)

Vieno paspaudimo prieiga prie verslo ir debesijos aplikacijų iš vieno SSO portalo.

Savitarnos slaptažodžių valdymas

(Paskyrų atrakinimas, sinchronizacija)

Mažiau IT užklausų: naudotojai patys atstato slaptažodžius ir atsirakina paskyras.

AI grįsta tapatybių analitika

(UEBA, audito ataskaitos, realaus laiko įspėjimai)

Įtartinų prisijungimų, failų prieigos ir kitų rizikingų veiksmų aptikimas.

RBAC ir prieigos delegavimas

(help desk rolės, detali kontrolė)

Technikai atlieka IT užduotis be perteklinių administratoriaus teisių.

ManageEngine AD360 panaudojimo atvejis

1. Personalo skyriaus inicijuojamas veiksmas

Priimant naują darbuotoją, keičiantis jo pareigoms ar jam išeinant, procesą inicijuoja personalo skyrius.

2. Taisyklės ir patvirtinimas

AD360 parenka šabloną pagal rolę, padalinį ir lokaciją; jautrios teisės keliauja į *approval workflow*.

3. Automatinis patvirtinimas

Sukuriamos arba keičiamos AD, M365 ir Google Workspace paskyros, grupės, paštas ir licencijos.

4. Saugumo įjungimas

Įjungiami MFA, SSO, slaptažodžių savitarna ir prieigos politikos prieš vartotojui pradedant darbą.

5. Auditas ir darbuotojo išėjimo procesas

Planinės ataskaitos ir įspėjimai rodo rizikas; išeinant darbuotojui teisės ir paskyros uždaromos.

ManageEngine Log360

Log360 – svarbiausios funkcijos

SIEM platforma logų analizei, grėsmių aptikimui ir incidentų atsakui.

Grėsmių aptikimas

(informacija apie grėsmes, grėsmių medžioklė, tamsusis internetas)

Išorinės ir vidinės grėsmės aptinkamos naudojant atnaujinamus indikatorius ir pažangią analizę.

Realaus laiko saugumo analitika

(logai, AD auditas, vieninga konsolė)

Įvykiai ir kritiniai resursai stebimi realiuoju laiku, kad tyrimai būtų greitesni ir tikslesni.

UEBA – elgsenos analitika

(ML, anomalijos, rizikos įvertinimas)

Aptinkamas neįprastas naudotojų ir sistemų elgesys, įskaitant vidines grėsmes bei duomenų nutekėjimo riziką.

SOAR ir incidentų atsakas

(playbook’ai, pranešimai, automatizavimas)

Automatizuoti veiksmų scenarijai ir incidentų valdymas.

AI SOC su Zia

(įžvalgos, tyrimai, rekomenduojami veiksmai)

DI apibendrina logus, įspėjimus ir incidentus, susieja su MITRE ATT&CK.

DLP, CASB ir atitiktis

(duomenų apsauga, shadow IT, audito šablonai)

Stebima jautrių failų prieiga, debesijos veikla ir atitikties ataskaitos su saugiu logų archyvavimu.

ManageEngine Log360 panaudojimo atvejis

1. Logų surinkimas

VPN, AD, ugniasienės, endpoint ir debesijos įvykiai siunčiami į vieną Log360 konsolę.

2. Koreliacija ir UEBA

Taisyklės ir elgsenos analitika atpažįsta brute force, „impossible travel“ ir rizikingą prisijungimą.

3. Incidento sukūrimas

Įvykiai sujungiami į vieną incidentą; pridedama laiko juosta, rizika ir įrodymai.

4. SOAR playbook

Playbook izoliuoja įrenginį, blokuoja IP, sustabdo sesiją, sukuria incidentą ir praneša SOC.

5. Uždarymas ir auditas

SOC inicijuoja atitinkamus veiksmus.

ManageEngine EndpointCentral

ManageEngine Endpoint central – svarbiausios funkcijos

Viskas, ko reikia – įrenginiams, vartotojams ir IT komandai.

Centralizuotas Darbo vietų valdymas

(kompiuteriai, serveriai, mobilieji įrenginiai)

Vieninga galinių įrenginių, inventoriaus ir konfigūracijų kontrolė.

Pataisų ir pažeidžiamumų valdymas

(OS, trečiųjų šalių programos, zero-day)

Automatizuotas skenavimas, testavimas ir spragų šalinimas.

Endpoint apsauga ir EDR

(grėsmių aptikimas, tyrimas, reagavimas)

Aptinka grėsmes realiuoju laiku ir izoliuoja įrenginius.

Programų diegimas ir kontrolė

(programų katalogas, šablonai, privilegijos)

Centralizuotas diegimas, leidimų politika ir allowlist / blocklist kontrolė.

Nuotolinė pagalba

(nuotolinis valdymas, įrašai, sistemos įrankiai)

Greitesnis trikčių šalinimas be fizinio priėjimo prie įrenginio.

Duomenų sauga ir atitiktis

(DLP, šifravimas, auditai ir ataskaitos)

Jautrių duomenų aptikimas, nutekėjimo prevencija ir aiškios atitikties ataskaitos.

ManageEngine Endpoint Central: automatizuotas pataisų valdymo procesas

1. Inventorizacija

Endpoint Central automatiškai surenka darbo stočių, serverių, OS ir trečiųjų šalių programų inventorių.

2. Pažeidžiamumų analizė

Sistema sinchronizuoja pažeidžiamumų bazę, nuskenuoja įrenginius ir nustato trūkstamas pataisas.

3. Testavimas ir politika

Pataisos pirmiausia diegiamos testų grupei, tada taikoma diegimo politika: pranešimai, perkrovimai ir išimtys.

4. Automatinis diegimas

Patvirtintos pataisos pagal grafiką diegiamos tinkle, nuotoliniams įrenginiams su valdomais perkrovimais.

5. Ataskaita ir kontrolė

Komanda mato atitikties būseną, nesėkmingus diegimus, rizikos mažėjimą ir gauna pilną ataskaitą.

Cloud

On-premises

MSP

Pabaigai

- Iki 25 d.v. sprendimą naudokite nemokamai
- Išbandykite nemokamai 30 d.
- POC savarankiškai arba su Baltimax komanda
- Užsukite į mūsų ManageEngine stendą

ManageEngine

Susisiekite:

Gediminas Mikelionis
Gediminas@baltimax.com

ManageEngine
www.baltimax.com/manageengine/