GIDS

De complete gids voor Privileged Access Management

Beheer van beheerdersaccounts, kosten, NIS2-verplichtingen, ROI, implementatie en trends. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Privileged accounts zijn de sleutel tot je hele IT-omgeving. Deze cijfers laten zien waarom bescherming onmisbaar is.

22%

van alle datalekken begint met gestolen of gecompromitteerde inloggegevens -- de hoogste aanvalsvector

Verizon DBIR 2025 [1]

USD 4,8M

Gemiddelde kosten per datalek via gestolen credentials

IBM Security 2024 [2]

+800%

Stijging credential theft in 2025 ten opzichte van voorgaande jaren

Security rapporten [3]

292 dagen

Gemiddelde tijd om een credential breach te identificeren en in te dammen

IBM Security 2024 [2]

71%

van corporate network access op het dark web bevat verhoogde (admin) rechten

Dark web analyses [4]

48%

Minder security-incidenten bij organisaties met een volwassen PAM-oplossing

Diverse security studies [5]

USD 3,6 mrd

Wereldwijde PAM-markt in 2024, groeiend met 21--23% per jaar

Precedence Research [6]

<9 mnd

Terugverdientijd van een PAM-investering volgens Forrester TEI-analyse

Forrester TEI [7]

1. Wat is Privileged Access Management?

PAM beschermt de accounts met de meeste rechten in je organisatie: de beheerders, service accounts en systemen die alles kunnen aanpassen, verwijderen of exporteren.

Een privileged account is elk account met verhoogde rechten: domeinadministrators, database-beheerders, cloud-admins, service accounts en API-keys. Deze accounts zijn het primaire doelwit bij cyberaanvallen, omdat ze toegang geven tot de kern van je IT-infrastructuur [8].

Privileged Access Management (PAM) is de discipline en technologie om deze accounts te identificeren, te beveiligen, te monitoren en te auditen. Het principe is eenvoudig: niemand heeft permanent beheerdersrechten nodig. Geef toegang alleen wanneer het nodig is, alleen voor de duur dat het nodig is, en log alles.

TYPEN PRIVILEGED ACCOUNTS

- **Domein-administrators** -- Volledige controle over Active Directory en alle gekoppelde systemen
- **Lokale administrators** -- Beheer van individuele servers en werkstations
- **Service accounts** -- Accounts voor applicaties en services die vaak vergeten worden maar brede rechten hebben
- **Cloud-administrators** -- AWS root, Azure Global Admin, Google Workspace Super Admin
- **Database-administrators** -- Directe toegang tot alle bedrijfsdata
- **Netwerk-administrators** -- Beheer van firewalls, switches en routers
- **Externe leveranciers** -- Third-party toegang voor onderhoud en support

2. Waarom PAM noodzakelijk is

De cijfers liegen niet: gestolen credentials zijn al meer dan tien jaar de meest gebruikte aanvalsvector. Zonder PAM ben je een open deur.

Volgens het Verizon Data Breach Investigations Report 2025 begint 22% van alle datalekken met gestolen of gecompromitteerde credentials -- de hoogste van alle aanvalsvectoren [1]. Over het afgelopen decennium was 31% van alle datalekken credential-gerelateerd [1].

De cijfers worden alleen maar alarmerender: credential theft steeg met 800% in 2025, ransomware-aanvallen namen toe met 179%, en identity-driven intrusions vormen nu 30% van alle aanvallen [3].

WAT ER GEBEURT ZONDER PAM

RISICO	IMPACT
Lateral movement	Aanvaller gebruikt admin-account om van systeem naar systeem te bewegen
Ransomware-verspreiding	Eenmaal domain admin = volledige encryptie van het netwerk
Data-exfiltratie	Admin-accounts hebben toegang tot alle bedrijfsdata
Insider threat	Gedeelde admin-wachtwoorden maken attributie onmogelijk
Compliance-falen	Geen audit trail = niet aantoonbaar NIS2-compliant

> **Het dark web perspectief**
>
> 71% van de corporate network access die op het dark web wordt aangeboden, bevat verhoogde rechten. De gemiddelde prijs: ~USD 2.700. Ongeveer 40% van het aanbod kost minder dan USD 1.000 [4]. Voor een crimineel is een admin-account kopen goedkoper dan hacken.

3. Kernfuncties van een PAM-oplossing

Een PAM-oplossing is meer dan een wachtwoordkluis. Dit zijn de functies die je nodig hebt.

FUNCTIE	WAT HET DOET	WAAROM HET ERTOE DOET
Password vaulting	Centrale, versleutelde opslag van alle privileged wachtwoorden	Geen gedeelde wachtwoorden meer op post-its of in spreadsheets
Automatische rotatie	Wachtwoorden worden automatisch gewijzigd na gebruik of op schema	Gestolen wachtwoord is snel waardeloos
Just-in-Time (JIT) access	Tijdelijke, beperkte toegang alleen wanneer nodig	Geen permanent beheerdersrecht, kleiner aanvalsoppervlak
Sessie-monitoring	Opname en logging van alle privileged sessies	Forensisch bewijs, compliance, detectie van misbruik
Multi-factor authenticatie	Extra verificatielaag voor toegang tot privileged accounts	NIS2-verplichting, voorkomt credential theft
Account discovery	Automatische detectie van alle privileged accounts in je omgeving	Je kunt niet beschermen wat je niet kent
Audit en rapportage	Gedetailleerde logs en rapporten van wie, wat, wanneer heeft gedaan	NIS2/DORA compliance bewijs
Least privilege enforcement	Gebruikers krijgen precies de rechten die ze nodig hebben, niet meer	Kernprincipe van zero trust

4. Wat kost PAM?

PAM-oplossingen varieren van EUR 2 tot EUR 100+ per gebruiker per maand. De keuze hangt af van je omvang en behoeften.

SEGMENT	KOSTEN PER MAAND	JAARLIJKS (INDICATIE)	KENMERKEN
Klein MKB (10–25 pers.)	EUR 2--10/ gebruiker	EUR 500--3.000	Cloud-based, basisfunctionaliteit
Middelgroot MKB (25–100 pers.)	EUR 10--50/ gebruiker	EUR 3.000--60.000	Password vault, sessie-opname, MFA
Groot MKB (100–250 pers.)	EUR 50--100/ gebruiker	EUR 60.000--300.000	Volledig platform, JIT, audit
Enterprise (250+ pers.)	Maatwerk	EUR 100.000--500.000+	On-premise/hybrid, integraties

Let op: de kosten hierboven zijn gebaseerd op alle gebruikers. In de praktijk betaal je vaak alleen voor privileged users. Een organisatie met 100 medewerkers maar slechts 10 beheerders betaalt dan aanzienlijk minder [9].

VERBORGEN KOSTEN

- **Implementatie:** EUR 5.000--50.000 afhankelijk van complexiteit en integraties
- **Training:** EUR 2.000--10.000 voor admin- en gebruikerstraining
- **Consultancy:** EUR 150--250/uur voor architectuur en configuratie
- **Onderhoud:** 15--20% van licentiekosten per jaar

TIP

Reken niet per gebruiker maar per privileged account. Een MKB-bedrijf met 50 medewerkers heeft typisch 5--15 privileged accounts. Bij EUR 50/account/maand is dat EUR 3.000--9.000 per jaar -- een fractie van de kosten van een datalek.

5. PAM en NIS2/DORA compliance

NIS2 maakt PAM een verplicht onderdeel van je cybersecurity-strategie. Geen luxe, maar een wettelijke eis.

Artikel 21 van de NIS2-richtlijn schrijft specifieke maatregelen voor die direct verband houden met privileged access management [10]:

NIS2-MAATREGEL	PAM-RELEVANTIE
Toegangsbeleid (art. 21.2.i)	Directe verplichting: identity & access management, inclusief privileged access
MFA (art. 21.2.j)	Multi-factor authenticatie voor alle gebruikers, prioriteit voor beheerders
Risicoanalyse	Privileged accounts als hoog-risico identificeren en behandelen
Incidentenbehandeling	Audit trails van privileged sessies als forensisch bewijs
Ketenbescherming	Toegang van externe leveranciers beheren en monitoren via PAM

Onder NIS2 mogen gebruikers niet langer standaard beheerdersrechten hebben. Toegangscontrole moet gestructureerd worden ingericht, met het least privilege-principe als uitgangspunt [10].

> **DORA AANVULLING VOOR FINANCIELE SECTOR**
>
> DORA schrijft aanvullend voor: strikte scheiding van taken (Segregation of Duties), logging en monitoring van alle privileged activiteiten, regelmatige toegangsreviews, en ICT-risicobeheer inclusief third-party access. PAM is voor financiele instellingen geen optie maar een vereiste [11].

6. Het implementatietraject

Een succesvolle PAM-implementatie begint niet met tooling maar met inzicht in je huidige situatie.

1 Account discovery

WEEK 1--3

Identificeer alle privileged accounts: user accounts, service accounts, application accounts, shared accounts. Je kunt niet beschermen wat je niet kent.

2 Risicoclassificatie

WEEK 2--4

Categoriseer accounts op risico: welke geven toegang tot kritieke systemen? Welke worden gedeeld? Welke zijn van externe partijen?

3 Beleid opstellen

WEEK 3--6

Definieer je PAM-beleid: wie mag wat, wanneer, hoe lang? Leg vast hoe je omgaat met noodtoegang (break-glass) en uitzonderingen.

4 Tooling selecteren en implementeren

WEEK 4--10

Kies een PAM-oplossing die past bij je omgeving. Begin met password vaulting voor de hoogst-risico accounts en bouw van daaruit uit.

5 Gefaseerde uitrol

WEEK 8--16

Rol PAM gefaseerd uit: eerst IT-beheerders, dan service accounts, dan externe leveranciers. Niet alles tegelijk -- dat creeert weerstand.

6 Training en communicatie

DOORLOPEND

Train beheerders op de nieuwe werkwijze. Leg uit waarom PAM nodig is. Gebruikersweerstand is de grootste uitdaging -- niet de techniek.

7 Monitoring en optimalisatie

DOORLOPEND

Monitor gebruik, detecteer afwijkingen, optimaliseer processen. PAM is geen eenmalig project maar een doorlopend proces.

7. Veelgemaakte fouten

De meeste PAM-projecten falen niet op techniek, maar op aanpak. Deze fouten kun je vermijden.

#	FOUT	WAAROM HET FOUT GAAT
1	**Te restrictief beginnen**	Gebruikers creeren workarounds en shadow IT. Rol gefaseerd uit met feedback van gebruikers
2	**Geen accountinventarisatie**	Onbekende privileged accounts blijven onbeschermd -- juist die worden uitgebuit
3	**Service accounts vergeten**	Vaak meer service accounts dan user accounts, met hogere rechten en geen wachtwoordrotatie
4	**Geen HR-koppeling**	Ex-medewerkers behouden admin-toegang. Integreer PAM met onboarding/offboarding processen
5	**Legacy systemen negeren**	Oudere systemen zijn niet altijd compatibel. Plan migratie of workarounds vooraf
6	**Alleen password vaulting**	PAM is meer dan een wachtwoordkluis. Sessie-monitoring, JIT access en audit trails zijn even belangrijk
7	**Gedeelde admin-accounts behouden**	"Iedereen kent het wachtwoord" is het grootste risico. Ieder zijn eigen account met eigen audit trail
8	**Geen break-glass procedure**	Als PAM uitvalt, heb je een noodprocedure nodig. Plan dit vooraf, niet tijdens een crisis

TIP

"PAM is alleen voor grote bedrijven" is de gevaarlijkste misvatting. Een MKB-bedrijf met 5 admin-accounts en geen PAM is kwetsbaarder dan een enterprise met 500 beheerde accounts.

8. ROI en business case

PAM betaalt zichzelf terug in minder dan 9 maanden. De cijfers zijn overtuigend.

KOSTENVERMIJDING

BESPARING	BEDRAG PER JAAR
Onboarding/offboarding efficientie	USD 332.000 (gemiddelde organisatie)
Vereenvoudigde onboarding	USD 182.000
Audit evidence collection	USD 60.000
Security incident response + audit	USD 623.000

Organisaties met volwassen PAM-oplossingen rapporteren 48% minder security-incidenten en besparen gemiddeld USD 3,3 miljoen per jaar aan breach-gerelateerde kosten [5].

Een Forrester Total Economic Impact-analyse voor cloud-based PAM toont een totale drie-jaars benefit van USD 914.562, met een volledige ROI in minder dan 9 maanden [7].

> **MKB-berekening (50 medewerkers, 10 privileged accounts)**
>
> Investering jaar 1: EUR 25.000 (licenties + implementatie + training). Structureel: EUR 12.000/jaar. Vermeden kosten (conservatief): EUR 35.000/jaar (breach-risicoreductie, audit-besparing, operationele efficientie, lagere verzekeringspremie). Terugverdientijd: ~12 maanden.

9. Een PAM-oplossing kiezen

De markt telt tientallen PAM-oplossingen. Focus op wat past bij jouw omvang, complexiteit en budget.

SELECTIECRITERIA

CRITERIUM	WAAROM HET ERTOE DOET
Deployment model	SaaS (lagere drempel, minder beheer) vs on-premise (meer controle, hogere kosten)
Account discovery	Automatische detectie van alle privileged accounts in je omgeving
JIT access	Tijdelijke toegang in plaats van permanente rechten -- kernprincipe van moderne PAM
Sessie-monitoring	Opname en logging van sessies voor compliance en forensisch onderzoek
Integraties	Koppeling met je IAM, SIEM, ITSM en HR-systemen
Multi-cloud support	Als je Azure, AWS of Google Cloud gebruikt, moet PAM alle omgevingen dekken
Gebruiksvriendelijkheid	Te complex = workarounds. Kies een oplossing die beheerders daadwerkelijk willen gebruiken
Compliance rapportage	Ingebouwde rapporten voor NIS2, DORA, ISO 27001 audits

> **Onafhankelijk vergelijken?**
>
> Op ibgids.nl/word-gematcht vind je een gratis matchingtool die je koppelt aan PAM-leveranciers die passen bij jouw situatie, omgeving en budget. Onafhankelijk, zonder verplichtingen.

10. Trends 2025--2026

PAM evolueert van wachtwoordkluis naar kerncomponent van Zero Trust architectuur.

TECHNOLOGISCHE VERSCHUIVINGEN

TREND	IMPACT
Just-in-Time (JIT) access	Geen standing privileges meer -- toegang alleen wanneer nodig, voor de duur dat het nodig is
Zero Standing Privilege (ZSP)	Alle privileged toegang is tijdelijk en context-afhankelijk. Het eindpunt van de JIT-evolutie
Cloud-native PAM (SaaS)	Lagere drempel voor MKB, geen on-premise beheer nodig, snellere implementatie
PAM + ITDR integratie	Identity Threat Detection and Response: real-time detectie en revocatie bij verdacht gedrag
Machine identity management	AI-agents en workloads als privileged identities -- een nieuw domein dat snel groeit
Behavioral analytics	Afwijkend gebruikersgedrag automatisch detecteren en blokkeren

MARKTONTWIKKELINGEN

- **Democratisering:** Betaalbare SaaS-oplossingen maken PAM toegankelijk voor MKB
- **Reguleringsdruk:** NIS2 en DORA maken PAM verplicht voor steeds meer sectoren
- **Verzekeraarseisen:** 47% van organisaties past security-postuur aan op eisen van cyberverzekeraars [6]
- **Consolidatie:** PAM-leveranciers worden overgenomen door grotere identity platforms
- **Zero Trust:** PAM als kerncomponent van Zero Trust architectuur

WAT BETEKENT DIT VOOR JOU?

- Begin met password vaulting en JIT access voor je hoogst-risico accounts
- Kies een SaaS-oplossing als je snel wilt starten zonder grote voorinvestering
- Integreer PAM met je NIS2-compliance traject -- het is een verplichte maatregel
- Vergeet service accounts niet -- die vormen vaak het grootste onbeschermde risico

Bronnenlijst

[1] **Verizon** -- 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[2] **IBM Security** -- Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

[3] **The Hacker News** -- The Evolving Role of PAM in Cybersecurity. https://thehackernews.com/2025/02/the-evolving-role-of-pam-in.html

[4] **DeepStrike** -- Compromised Credential Statistics 2025. https://deepstrike.io/blog/compromised-credential-statistics-2025

[5] **Delinea** -- Building IT Business Cases: Cost-justifying a PAM Project. https://delinea.com/blog/building-it-business-case-cost-justifying-privileged-access-management

[6] **Precedence Research** -- Privileged Access Management Market Size. https://www.precedenceresearch.com/privileged-access-management-market

[7] **CyberArk / Forrester TEI** -- Business Benefits of PAM as a Service. https://www.cyberark.com/resources/blog/breaking-down-the-business-benefits-and-cost-savings-of-cyberark-privileged-access-management-as-a-service

[8] **Microsoft** -- Wat is Privileged Access Management (PAM). https://www.microsoft.com/nl-nl/security/business/security-101/what-is-privileged-access-management-pam

[9] **StrongDM** -- PAM Pricing Simplified. https://www.strongdm.com/blog/privileged-access-management-pricing

[10] **Kappa Data** -- Privileged Access Management en NIS2. https://nis2.kappadata.nl/security-frameworks/protect/privileged-access-management-pam/

[11] **Avatier** -- PAM: A Must-Have for NIS2 and DORA Compliance. https://www.avatier.com/blog/mastering-access-management-the-key-to-nis2-and-dora-compliance/

[12] **Delinea** -- Building IT Business Cases: Cost-justifying a PAM Project. https://delinea.com/blog/building-it-business-case-cost-justifying-privileged-access-management

[13] **Mitigata** -- Top PAM Trends to Watch in 2026. https://mitigata.com/blog/top-pam-trends/

[14] **Netwrix** -- PAM solutions market: 2026 guide. https://netwrix.com/en/resources/blog/privileged-access-management-solutions-market/

[15] **Digital Trust Center** -- NIS2 Toegangsbeleid. https://www.digitaltrustcenter.nl/nis2/toegangsbeleid

[16] **CBS** -- Cybersecuritymonitor 2024. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[17] **Heimdal Security** -- PAM best practices, implementation and tools. https://heimdalsecurity.com/blog/privileged-access-management-best-practices-implementation-and-tools/

[18] **NCSC** -- Cybersecuritybeeld 2025. https://www.ncsc.nl/nieuws/cybersecuritybeeld-2025-dreigingen-divers-en-onvoorspelbaar-digitale-basishygiene-op-orde-blijft-cruciaal