Voorbereid op

KEEPER

Beyond the Vault:

Het verbeteren van geprivilegieerd toegangsbeheer in de moderne onderneming

Juli 2025 EMA White Paper
door **Ken Buckler, CASP;** onderzoeksdirecteur,
informatiebeveiliging, risico- en nalevingsbeheer

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Inhoudsopgave

1 **Introduction**

2 **Zero Trust by Design**

2 Zero-trust en zero-knowledge

4 **Eenvoud van implementatie, configuratie en integraties**

4 Er is geen “Eenvoudsknop”, maar Keeper komt in de buurt

5 Speelt goed met anderen

6 Meer Doen met Minder Personeel

7 **Meer dan wachtwoord- en geheimenbeheer**

7 Geavanceerde PAM-mogelijkheden

9 **Algemene Tevredenheid**

9 Is uw PAM-oplossing bestand tegen de storm?

10 Functies en integraties zijn kritieke pijnpunten

11 **Betere oplossing, betere prioriteiten**

11 Andere PAM-implementaties maken het niet waar

13 **Methodologie**

Introduction

In een tijdperk van voortdurende cyberdreigingen en snelle digitale transformatie is “Privileged Access Management” (geprivilegieerd toegangsbeheer) (PAM) uitgegroeid tot een fundamentele beveiligingsdiscipline. Hedendaagse ondernemingen hebben meer nodig dan alleen het opslaan van aanmeldingsgegevens; ze hebben behoefte aan een uitgebreid framework dat kritieke bedrijfsmiddelen beschermt, toegang met minimale rechten handhaaft en naadloos integreert in zowel lokale als cloudomgevingen.

Effectief PAM begint met robuuste identiteitsverificatie en multi-factor authenticatie, waarbij hardwaretokens, mobiele goedkeuringen en biometrische controles worden gecombineerd, ondersteund door end-to-end encryptie en zero-knowledge beveiliging. Fijnmazige, op rollen gebaseerde controles en just-in-time provisioning binnen een zero-trust-architectuur zorgen ervoor dat gebruikers de minimaal noodzakelijke privileges ontvangen, waardoor de impact van inbreuken aanzienlijk wordt verminderd. Tegelijkertijd registreren auditlogboeken elke geprivilegieerde sessie, van uitgevoerde opdrachten tot visuele herhalingen en de duur van de sessie. De auditlogboeken worden vervolgens ingevoerd in geautomatiseerde compliance-engines die de werkwijzen afstemmen op de HIPAA-, SOX- en PCI DSS-normen, terwijl hercertificeringscampagnes verweesde of overtollige accounts elimineren.

Naadloze integratie met cloudservices en bestaande tools is essentieel. Injectie van aanmeldingsgegevens in scripts, pijplijnen en externe toegangspoorten houdt de productiviteit van gebruikers op peil zonder dat dit ten koste gaat van het toezicht. Geavanceerde gedragsanalyses en agentic AI maken vervolgens van PAM een actieve verdediging. Met realtime waarschuwingen en acties kunnen bedreigingen onmiddellijk worden geëlimineerd en privileges direct worden ingetrokken. Door deze controles uit te breiden naar derden via tijd- en apparaatgebonden delen, automatische wachtwoordrotatie en strikte goedkeuringsworkflows worden de risico’s van aannemers en de toeleveringsketen verder beperkt.

In dit whitepaper onderzoeken we de uitdagingen waarmee organisaties worden geconfronteerd bij het vervullen van deze PAM-prioriteiten en evalueren hoe het KeeperPAM-platform van Keeper Security zich verhoudt tot de bredere sector.

Zero Trust by Design

Zero-trust en zero-knowledge

Het is niet langer optioneel om vanaf het begin zero-trust-principes te integreren voor privileged access management – het is van essentieel belang. Een “zero trust by design”-framework behandelt elk verzoek om verhoogde privileges als inherent onbetrouwbaar, wat continue verificatie, strikte segmentatie en handhaven van minimale privileges vereist. Door over te stappen van statische, almachtige aanmeldingsgegevens naar tijdelijke, contextbewuste toegangstokens, kunnen organisaties het aanvalsoppervlak drastisch verkleinen en laterale bewegingen in het geval van een inbreuk beperken. Met “zero-trust by design” houdt elke toegangsbeslissing rekening met de gebruikersidentiteit, de apparaatstatus, de locatie, het tijdstip en de gedragscontext. Just-in-time-provisioning zorgt ervoor dat geprivilegieerde rechten alleen voor de exacte benodigde duur worden verleend en daarna automatisch worden ingetrokken. Fijnmazige, op rollen gebaseerde toegangscontroles minimaliseren overmatige machtigingen, terwijl multi-factor authenticatie en continue sessiebewaking beschermen tegen compromittering van aanmeldingsgegevens en interne bedreigingen.

“\[Wat betreft het beheer van geprivilegieerde toegang, zijn onze prioriteiten\] integratie met zero-trust-architectuur en een continu validatiekader”.
- IT-directeur, 500-749 werknemers die KeeperPAM gebruiken

De zero-knowledge-benadering van Keeper bij het ontwerpen van producten versterkt deze aanpak verder, waardoor alle versleuteling en ontsleuteling lokaal op uw apparaat plaatsvindt – alleen de versleutelde tekst wordt naar de cloud van Keeper verzonden. Een hoofdwachtwoord en al het daarvan afgeleid sleutelmateriaal verlaten nooit het gekozen apparaat, wat betekent dat de servers van Keeper geen toegang hebben tot onversleutelde gegevens of de sleutels die deze beschermen en deze ook niet kunnen opslaan. Zelfs indien hun infrastructuur zou worden geschonden, zouden aanvallers slechts een onleesbare reeks tekens verkrijgen, waardoor echte end-to-end vertrouwelijkheid wordt gegarandeerd.

Enquêtegegevens onderstrepen het effect van deze aanpak: 60% van de Keeper Security-gebruikers beschouwt hun PAM-implementatie als “zero knowledge” en “zero trust by design”, vergeleken met slechts 34,9% van de gebruikers van alle andere leveranciers. Deze kloof weerspiegelt een proactieve beveiligingsaanpak – Keeper-klanten benadrukken continue validatie, eliminatie van gedeelde accounts en geautomatiseerd beheer van de levenscyclus van privileges – in tegenstelling tot een reactievere, compliance-gedreven mindset elders.

Zero-trust PAM versnelt ook de naleving en de gereedheid voor audits. Elke bevoorrechte sessie wordt van begin tot eind geregistreerd – compleet met uitgevoerde opdrachten, visuele weergave en duurstatistieken – en voedt geautomatiseerde compliance-engines die zijn afgestemd op de HIPAA-, SOX- en PCI DSS-vereisten. In de praktijk versterken organisaties die zero-trust in hun PAM-architecturen integreren niet alleen hun verdediging, maar stroomlijnen zij ook hun activiteiten, verlagen zij de kosten die gepaard gaan met verweesde accounts en tonen zij meetbare verbeteringen in het beperken van inbreuken.

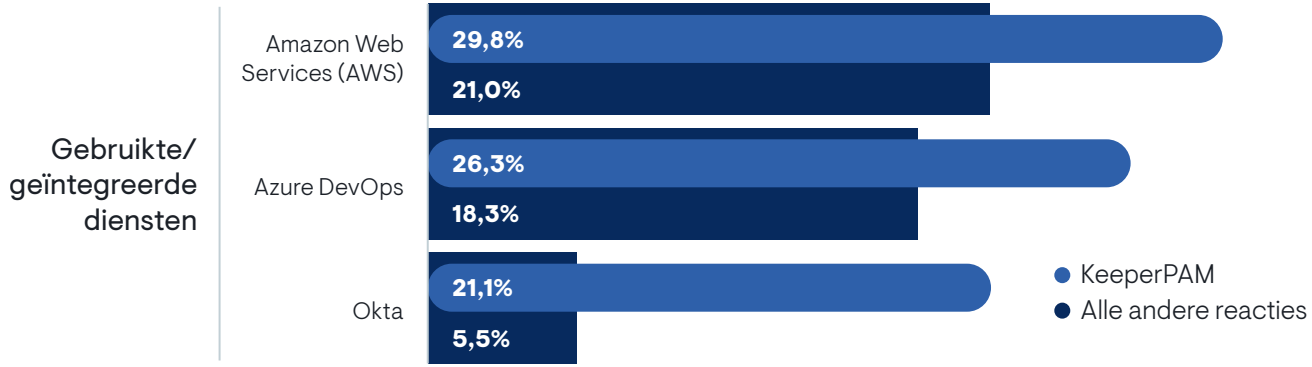
Uiteindelijk transformeert de zero-knowledge-benadering en het zero-trust-ontwerp van Keeper geprivilegieerde toegang van een potentiële aansprakelijkheid in een gecontroleerd, verifieerbaar proces – een proces dat zich in realtime aanpast aan veranderende risico’s en ervoor zorgt dat kritieke systemen veilig, compliant en veerkrachtig blijven.

Eenvoud van implementatie, configuratie en integraties

Er is geen “Eenvoudsknop”, maar Keeper komt in de buurt

De eenvoud van implementatie, configuratie en integratie kan bepalend zijn voor het rendement van een PAM-project. Volgens het onderzoek van EMA beoordeelde 60% van de klanten van Keeper Security de eerste implementatie als “zeer eenvoudig”, vergeleken met slechts 22,1% van de gebruikers van andere PAM-platforms. Omgekeerd noemde 10% van de klanten van alle andere oplossingen de implementatie “enigszins moeilijk” of “zeer moeilijk”, een pijnpunt dat volledig ontbreekt bij KeeperPAM-gebruikers. Het migreren van verouderde lokale PAM-tools naar de cloud vormt voor 39% van de organisaties nog steeds een uitdaging – complexiteit die de cloud-native architectuur van Keeper omzeilt. Integratieproblemen vormen een uitdaging voor 11% van de niet-Keeper-implementaties, waarbij vaak eigen connectoren en handmatige scripts nodig zijn om te koppelen aan SIEM, ticketing of DevOps-pijplijnen. De modulaire API’s, plug-and-play-connectoren en naadloze cloudorkestratie van KeeperPAM bieden snellere waardecreatie en minimaliseren operationele frictie.

Speelt goed met anderen



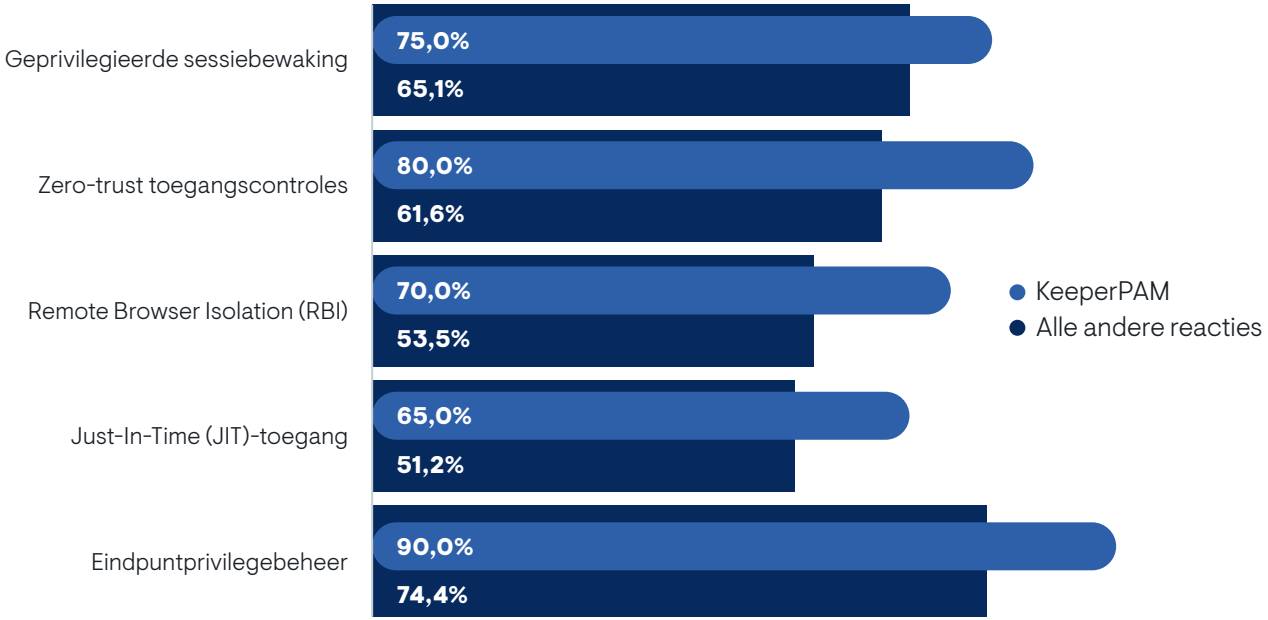
Naadloze integraties zijn een hoeksteen van elke moderne PAM-strategie, en ook hier loopt Keeper voorop. Kant-en-klare connectoren en API's maken snelle, bidirectionele integratie met kernplatforms mogelijk – of u nu EC2-instances opstart in Amazon Web Services, pijplijnen automatiseert in Azure DevOps of authenticatie centraliseert via Okta. Gebruikers van KeeperPAM melden een aanzienlijk hogere acceptatie van deze integraties in vergelijking met andere PAM-oplossingen, waardoor tijdrovende aangepaste scripts of handmatig onderhoud van connectoren overbodig wordt. Door geprivilegieerde aanmeldingsgegevens rechtstreeks in uw CI/CD-workflows, cloudconsoles en identiteitsproviders te integreren, minimaliseert KeeperPAM de frictie, verhoogt het de productiviteit van ontwikkelaars en zorgt het ervoor dat geheimen op elk niveau beschermd blijven.

Meer Doen met Minder Personeel

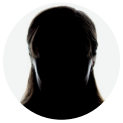
De personeelsbehoeften voor PAM-implementaties variëren sterk per platform. Slechts 15% van de klanten van Keeper Security geeft aan dat zij gespecialiseerd personeel nodig hebben voor het beheer van de implementatie, configuratie en integratie, dankzij de intuïtieve gebruikersinterface, begeleide installatiewizards en uitgebreide documentatie van Keeper. Daarentegen heeft 39,5% van de organisaties die andere PAM-oplossingen gebruiken één of meer fulltime beheerders nodig om hun omgevingen draaiende te houden. Die teams jongleren vaak met complex onderhoud van lokale apparatuur, op maat gemaakte scripts en handmatige connectorupdates, wat leidt tot een toename van het personeelsbestand en een overbelasting van de bestaande IT-middelen. Het cloudeigen ontwerp en de selfservice-tooling van Keeper minimaliseren de afhankelijkheid van gespecialiseerde vaardigheden. Beheerders kunnen nieuwe systemen onboarden, bevoegdheidsbeleidsregels aanpassen en integreren met SIEM- of DevOps-pijplijnen zonder uitgebreide aanpassingen. Uiteindelijk leidt een lagere personeelsbezetting tot snellere implementaties en duurzamere, betaalbare langetermijnactiviteiten.

Meer dan wachtwoord- en geheimenbeheer

Geavanceerde PAM-mogelijkheden



Moderne PAM vereist veel meer dan alleen het opslaan van aanmeldingsgegevens – het vereist een uitgebreide reeks functies die actief verdedigen, bewaken en zich aanpassen aan veranderende bedreigingen. KeeperPAM onderscheidt zich door geavanceerde mogelijkheden te bieden die veel oudere leveranciers simpelweg niet aanbieden of op grote schaal implementeren. Het monitoren van geprivilegieerde sessies is bijvoorbeeld van cruciaal belang voor het vastleggen van elke toetsaanslag, elk commando en elke visuele weergave van risicovolle activiteiten. Klanten van Keeper maken vaker gebruik van deze functie dan hun collega's, waardoor realtime detectie van bedreigingen en forensische analyse mogelijk wordt.



Het gebruik van PAM versterkt onze gegevensintegriteit en onze reputatie".
- VP Development/Engineering, 1.000-2.499 medewerkers, die KeeperPAM gebruiken

Zero-trust netwerktoegang breidt de principes van het minste privilege uit van wachtwoorden naar elke toegangsaanvraag. Keeper integreert contextuele beleidscontroles – apparaatstatus, locatie, tijd en gedragsnormen – om ervoor te zorgen dat zelfs geauthenticeerde sessies continu onder toezicht blijven. Deze gedetailleerde afbakening van bevoorrechte bewerkingen vermindert het potentiële blootstellingsvenster aanzienlijk in vergelijking met statische, alles-of-niets-modellen.

Remote browserisolatie (RBI) is nog een gebied waar Keeper de concurrentie overtreft. Door beheerconsoles te proxyen via geïsoleerde, beveiligde browsers, elimineren organisaties directe toegang tot eindpunten voor derden en aannemers, waardoor potentiële malware of diefstal van aanmeldingsgegevens effectief in quarantaine wordt geplaatst. Er zijn maar weinig andere PAM-oplossingen die RBI zo naadloos integreren; in plaats daarvan vereisen ze handmatige workarounds die zowel de veiligheid als de gebruikerservaring ondermijnen.

Just-in-time (JIT) provisioning en geautomatiseerd beheer van de levenscyclus van privileges maken de geavanceerde toolkit van Keeper compleet. Tijdelijke, tijdgebonden verhoging voorkomt dat permanente accounts met hoge privileges zich ophopen, terwijl automatische deprovisioning en hercertificeringscampagnes ervoor zorgen dat nalevingsvoorschriften worden nageleefd zonder handmatige inspanning. Ten slotte beschermt eindpuntprivilegebeheer – het verwijderen van lokale beheerdersrechten en het op verzoek toekennen van beperkte rechten – tegen zowel externe aanvallen als misbruik van binnenuit.

Door verder te kijken dan wachtwoorden en geheimen, transformeert Keeper PAM tot een actief verdedigingsplatform: een platform dat aanvallen anticipeert, zero-trust op elke laag handhaaft en de geavanceerde controles biedt die complexe omgevingen van vandaag de dag vereisen.

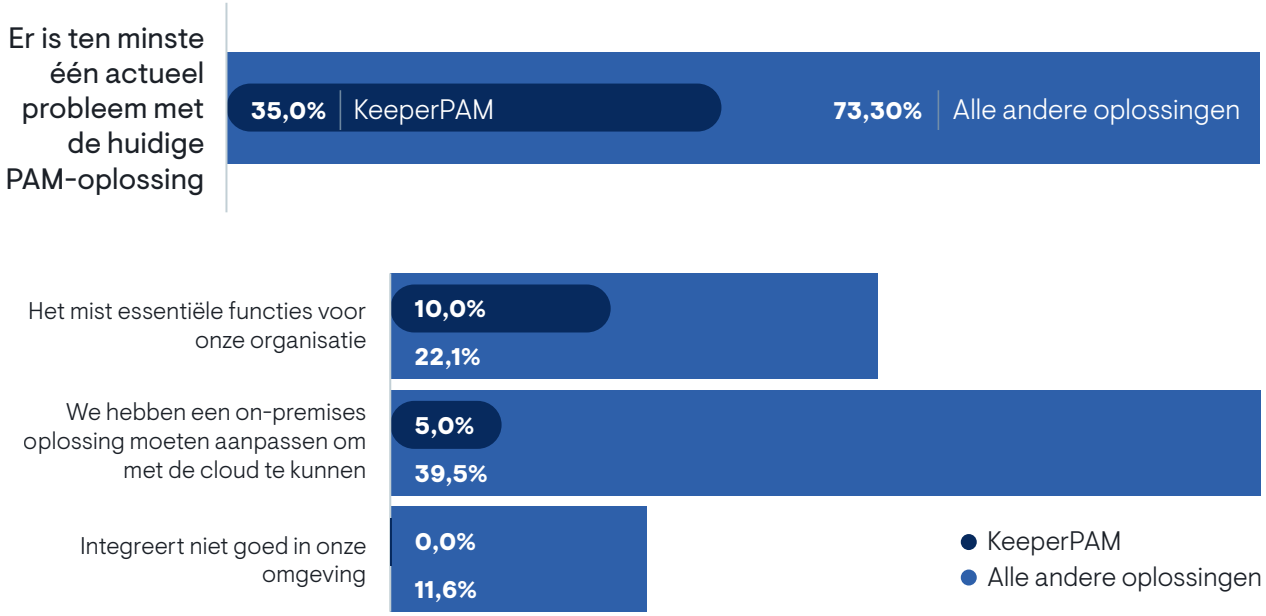
Algemene Tevredenheid

Is uw PAM-oplossing bestand tegen de storm?

Klanttevredenheid is de ultieme graadmeter voor de waarde en levensduur van een PAM-oplossing. Wanneer 5% van de organisaties die andere platforms gebruiken actief op zoek is naar een vervanging, duidt dit op kritieke tekortkomingen in betrouwbaarheid, bruikbaarheid en/of ondersteuning. Daarentegen heeft geen enkele gebruiker van Keeper Security aangegeven van plan te zijn hun PAM-tool te vervangen, wat onderstreept dat Keeper in staat is om aan veranderende beveiligings- en operationele behoeften te voldoen.

Bovendien geeft 75% van de klanten van Keeper aan “zeer tevreden” te zijn, wat aanzienlijk hoger is dan de 53,5% “zeer tevreden”-beoordeling van gebruikers van concurrerende leveranciers. Hoge tevredenheid correleert met snellere acceptatie, effectievere risicobeperking en lagere totale eigendomskosten, omdat tevreden teams investeren in diepere integraties en geavanceerdere functies. In een omgeving waar bevoorrechte toegang voortdurend wordt aangevallen, is het kiezen van een platform dat zijn gebruikers tevreden stelt niet alleen een pré, maar van cruciaal belang.

Functies en integraties zijn kritieke pijnpunten



Ondanks hun cruciale rol, ondervinden veel PAM-implementaties aanhoudende obstakels. Drieënzeventig procent van de organisaties die geen Keeper-oplossingen gebruiken, meldt ten minste één belangrijke uitdaging, vergeleken met slechts 35% van de Keeper-klanten. Veelvoorkomende pijnpunten zijn onder meer het ontbreken van essentiële functionaliteiten, waardoor teams genoodzaakt zijn om tools van derden te gebruiken, slechte integratie in de bestaande infrastructuur en de hoofdpijn van het aanpassen van lokale platforms om cloudomgevingen te ondersteunen. Gebruikers van KeeperPAM ondervinden deze problemen veel minder vaak dankzij de uitgebreide functieset, de native cloud-first architectuur en de uitgebreide bibliotheek met connectoren. Door hiaten in functionaliteit te minimaliseren en hybrid implementaties te vereenvoudigen, biedt Keeper niet alleen snelle waardecreatie, maar vermindert het ook de last van probleemoplossing en workarounds, waardoor beveiligingsteams zich kunnen richten op proactieve risicobeperking in plaats van op het blussen van brandjes veroorzaakt door beperkingen van verouderde systemen.

Betere oplossing, betere prioriteiten

Andere PAM-implementaties maken het niet waar

Prioriteitsgebied	Keeper Klanten	Andere PAM-oplossingen
Authenticatie	Continue, zero-trust	Op rollen gebaseerde, MFA
Beheer van aanmeldingsgegevens	Elimineer statische/gedeelde aanmeldingsgegevens	Basisbediening en toegang monitoren
Training	Expliciete prioriteit	Niet benadrukt
Automatisering	Focus op risicobeperking (omdat	Process efficiency focus
het proces is al efficiënt)	Focus op procesefficiëntie	Minimum regulatory compliance
Naleving	Misbruik van aanmeldingsgegevens en focus op audits	Minimale naleving van regelgeving

Keeper Security stelt organisaties in staat om over te stappen van een onderhoudsgerichte, compliance-gedreven instelling naar een proactieve beveiligingsgerichte instelling. KeeperPAM-klanten elimineren statische en onveilig gedeelde aanmeldingsgegevens door middel van een zero-knowledge kluis-engine die tijdelijke geheimen met minimale rechten uitgeeft, waardoor zowel externe aanvalsvectoren als misbruik van binnenuit aanzienlijk worden verminderd in vergelijking met traditionele benaderingen die alleen een kluis bieden. Continue authenticatie en zero-trust toegangscontroles – inclusief apparaatstatuscontroles, geolocatie en gedragsanalyses – zorgen ervoor dat elke sessie lang na een eenmalige MFA-prompt onder controle blijft, waardoor het voor aanvallers vrijwel onmogelijk wordt om gestolen aanmeldingsgegevens onopgemerkt te misbruiken. De risicogerichte automatisering van Keeper behandelt de volledige levenscyclus van privileges – van ontdekking en onboarding tot automatische rotatie en deprovisioning – voorkomt wildgroei van aanmeldingsgegevens en verweesde accounts, terwijl veel andere oplossingen alleen goedkeuringsworkflows of compliance-rapportage automatiseren. Belangrijk is dat klanten van Keeper expliciet het opleiden en bewustmaken van hun personeel

integreren als een essentiële beveiligingsmaatregel, waarbij zij erkennen dat menselijke factoren net zo cruciaal zijn als technologie voor het stimuleren van acceptatie en het voorkomen van risicovolle workarounds.

"Ik kan dankzij constante monitoring van geprivilegieerde accounts 's nachts beter slapen".
– VP Development/Engineering, 2.500-4.999 medewerkers, met KeeperPAM

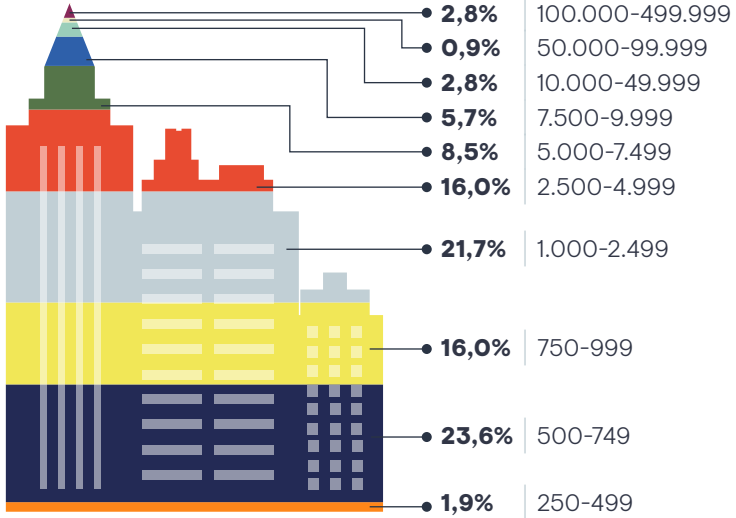
Daarentegen leggen gebruikers van andere PAM-tools vaak de nadruk op traditionele controles, zoals op rollen gebaseerde toegang, auditing na toegang en operationele efficiëntie, wat een reactieve mentaliteit weerspiegelt die worstelt met ontbrekende functies, kwetsbare integraties en de complexiteit van het aanpassen van lokale oplossingen voor de cloud. De cloud-native architectuur en uitgebreide bibliotheek met plug-and-play-connectoren van Keeper elimineren deze problemen en maken een snelle integratie mogelijk met SIEM-platforms, identiteitsproviders zoals Okta en CI/CD-pijplijnen in AWS of Azure DevOps. Geavanceerde mogelijkheden zoals monitoring van geprivilegieerde sessies, isolatie van browsers op afstand, just-in-time provisioning en beheer van eindpuntbevoegdheden zijn allemaal native aan Keeper, waardoor de implementatie soepeler verloopt en de continue personeelsbehoefte afneemt.

Door deze next-generation functies te combineren met een naadloze gebruikerservaring, stelt Keeper beveiligingsteams in staat om bedreigingen te anticiperen, continue bescherming te handhaven en hun geprivilegieerde toegangsomgeving daadwerkelijk te versterken.

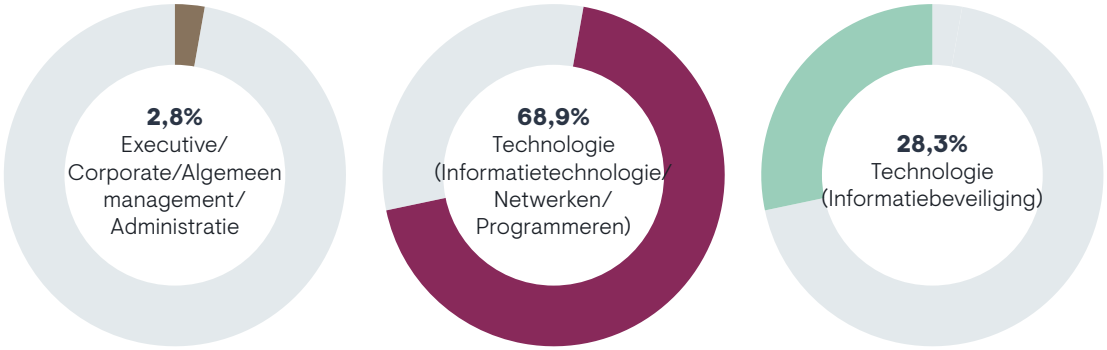
Methodologie

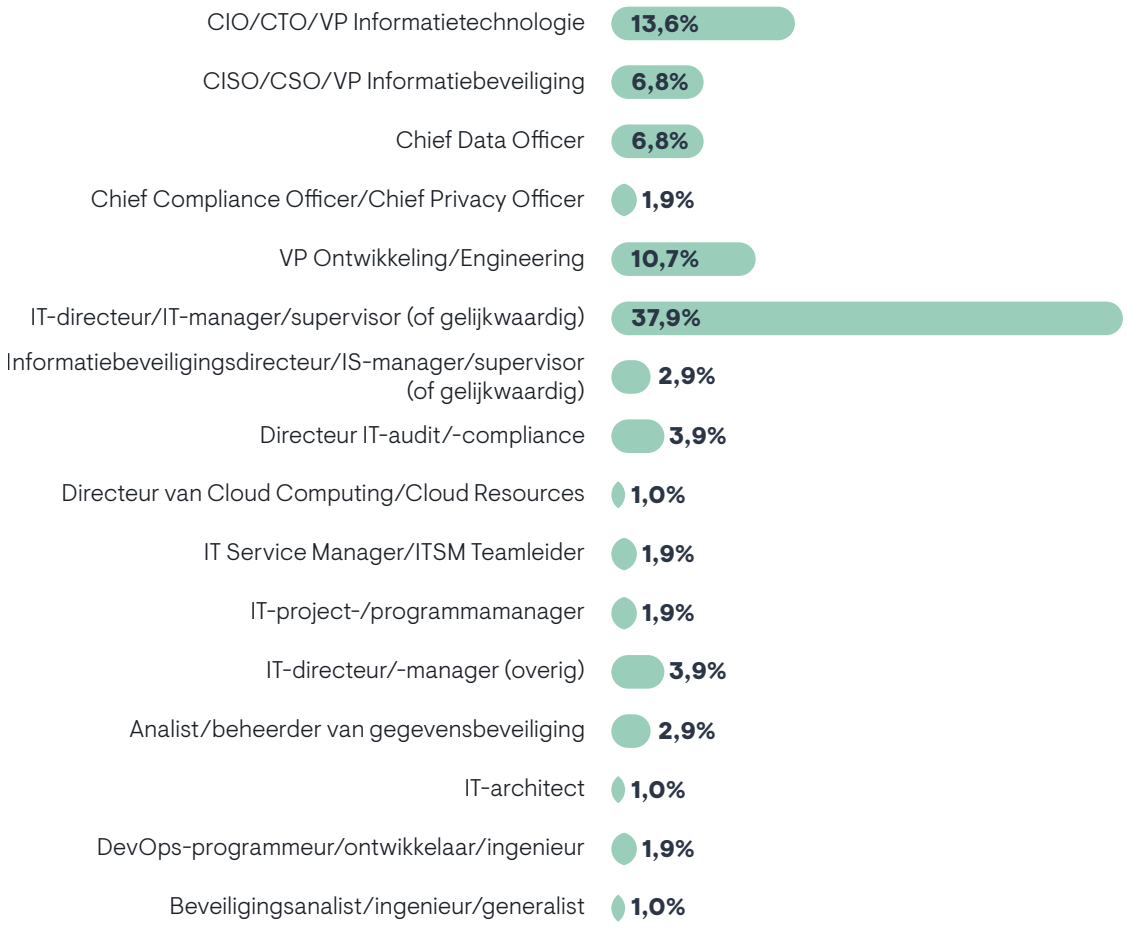
In totaal 106 professionals die gebruikmaken van BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity of StrongDM per juni 2025. Alle gegevens in dit whitepaper zijn gebaseerd op de enquêtereacties en open antwoorden met betrekking tot prioriteiten en uitdagingen op het gebied van geprivilegieerd toegangsbeheer in de onderneming.

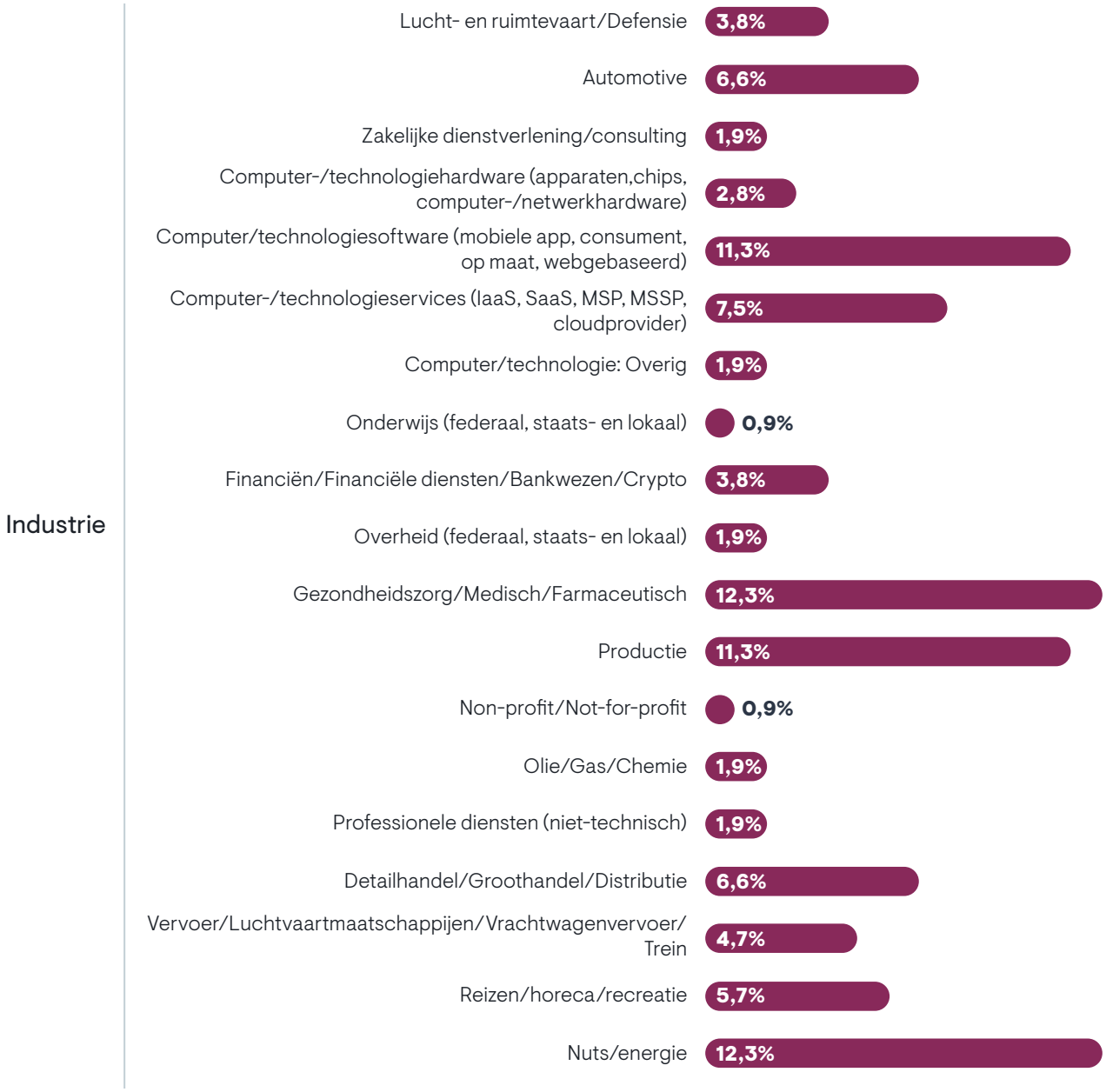
Organisatiegrootte



Rol van de respondent




CIO/CTO/VP Informatietechnologie
13,6%
CISO/CSO/VP Informatiebeveiliging
6,8%
Chief Data Officer
6,8%
Chief Compliance Officer/Chief Privacy Officer
1,9%
VP Ontwikkeling/Engineering
10,7%
IT-directeur/IT-manager/supervisor (of gelijkwaardig)
37,9%
Informatiebeveiligingsdirecteur/IS-manager/supervisor (of gelijkwaardig)
2,9%
Directeur IT-audit/-compliance
3,9%
Directeur van Cloud Computing/Cloud Resources
1,0%
IT Service Manager/ITSM Teamleider
1,9%
IT-project-/programmamanager
1,9%
IT-directeur/-manager (overig)
3,9%
Analist/beheerder van gegevensbeveiliging
2,9%
IT-architect
1,0%
DevOps-programmeur/ontwikkelaar/ingenieur
1,9%
Beveiligingsanalist/ingenieur/generalist
1,0%


Industrie
Lucht- en ruimtevaart/Defensie
3,8%
Automotive
6,6%
Zakelijke dienstverlening/consulting
1,9%
Computer-/technologiehardware (apparaten,chips, computer-/netwerkhardware)
2,8%
Computer/technologiesoftware (mobiele app, consument, op maat, webgebaseerd)
11,3%
Computer-/technologieservices (IaaS, SaaS, MSP, MSSP, cloudprovider)
7,5%
Computer/technologie: Overig
1,9%
Onderwijs (federaal, staats- en lokaal)
0,9%
Financiën/Financiële diensten/Bankwezen/Crypto
3,8%
Overheid (federaal, staats- en lokaal)
1,9%
Gezondheidszorg/Medisch/Farmaceutisch
12,3%
Productie
11,3%
Non-profit/Not-for-profit
0,9%
Olie/Gas/Chemie
1,9%
Professionele diensten (niet-technisch)
1,9%
Detailhandel/Groothandel/Distributie
6,6%
Vervoer/Luchtvaartmaatschappijen/Vrachtwagenvervoer/Trein
4,7%
Reizen/horeca/recreatie
5,7%
Nuts/energie
12,3%

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4577.081325-NL