IAM (Identity Access Management) – Tutkimus yrityksen käyttöoikeushallinnan kehittämiseksi

Markus Julius Innanen

2025 Laurea

Laurea-ammattikorkeakoulu

IAM (Identity Access Management) – Tutkimus yrityksen käyttöoikeushallinnan kehittämiseksi

Julius Innanen

Tietojenkäsittely

Opinnäytetyö Toukokuu, 2025

Laurea-ammattikorkeakoulu Tiivistelmä
Tietojenkäsittely - Tradenomi
Tradenomi (AMK)

Markus Julius Innanen

IAM (Identity Access Management) – Tutkimus yrityksen käyttöoikeushallinnan kehittämiseksi

Vuosi 2025 Sivumäärä 33

Opinnäytetyö toteutettiin helsinkiläisessä pk-yrityksessä, jonka tavoitteena oli kehittää käyttäjähallinnan ja tietoturvan prosesseja. Yrityksen IT-hallinto tunnisti manuaalisten käyttöoikeusprosessien aiheuttavan viiveitä, virheriskejä ja haasteita GDPR-vaatimusten täyttämisessä. Tavoitteena oli siirtyä malliin, jossa käyttäjän elinkaaren hallinta – mukaan lukien liittyminen, siirtymät ja poistuminen – automatisoidaan HR- ja IAM-järjestelmän integraatiolla.

Tutkimuksessa kartoitettiin ja vertailtiin viittä eri IAM-järjestelmää, jotka soveltuvat Microsoft-ekosysteemissä toimivan pk-yrityksen tarpeisiin. Tietoperustana hyödynnettiin ajankohtaista kirjallisuutta ja asiantuntijalähteitä. Menetelminä käytettiin kirjallisuuskatsausta, vertailuanalyysiä ja empiiristä aineistoa, jota kerättiin toimeksiantajan IT-henkilöstön haastatteluista ja sisäisistä dokumenteista.

Tutkimuksen tulokset osoittivat, että markkinoilla on useita IAM-ratkaisuja, jotka tukevat käyttäjän elinkaaren automatisointia ja täyttävät pk-yrityksen tarpeet. Vertailuanalyysin perusteella Microsoft Entra ID Suite todettiin organisaatiolle parhaaksi näistä viidestä järjestelmästä. Sen keskeisiä hyötyjä olivat käyttöoikeuksien keskitetty hallinta, parantunut tietoturvan taso sekä merkittävästi vähentynyt manuaalinen työ IT-hallinnossa. Johtopäätöksenä suositeltiin IAM-ratkaisun käyttöönoton vaiheittaista suunnittelua, aloittaen nykytilan tarkasta kartoituksesta sekä tarvittavien integraatioiden määrittelystä.

Asiasanat: IAM, tietoturva, vertailututkimus

Laurea University of Applied Sciences
Business Information Technology
Bachelor of Business Administration (BBA)

Markus Julius Innanen

IAM (Identity Access Management) – Research for the Development of Company Access Rights Management

Year 2025 Pages 33

Abstract

This Bachelor's thesis was carried out in a Helsinki-based SME aiming to improve user management and information security processes. The company's IT administration identified significant delays, risk of errors, and compliance challenges related to GDPR due to manual user access management processes. The primary goal was to transition to a model in which user lifecycle management—including joining, moving internally, and leaving—is automated through integration between the HR and IAM systems.

The research identified and compared five different IAM systems suitable for an SME operating within the Microsoft ecosystem. The theoretical framework was based on current literature and expert sources. The research methods included a literature review, comparative analysis, and empirical data collection through interviews with the commissioning organization's IT personnel and analysis of internal documentation.

The results indicated several IAM solutions available in the market support the automation of user lifecycle processes and meet the needs of SMEs. Based on comparative analysis, Microsoft Entra ID Suite emerged as the most suitable system among the five evaluated for the organization. Key benefits included centralized management of access rights, enhanced information security, and significantly reduced manual work within IT administration. The thesis recommends a phased implementation approach, beginning with a detailed assessment of the current situation and required integrations.

Keywords IAM, cybersecurity, comparison

Sisällys

1 Johdanto

Opinnäytetyö tehdään helsinkiläiselle SMB-yritykselle. Yritys haluaa kartoittaa IAM-ratkaisujen mahdollista toteutusta, jotta tulevaisuudessa olisi helpompaa ottaa käyttöön IAM-järjestelmä. Tutkimus käsittelee IAM-järjestelmien ominaisuuksia sekä niitä IAM-palveluita, jotka täyttävät yrityksen vaatimukset.

Nykyisessä tilassa yrityksen tietoturvaa ja tietohallinnon tehokkuutta voidaan parantaa huomattavasti ottamalla käyttöön järjestelmä, jossa on toimeksiantajan vaatimuksien täyttävät ominaisuudet. IT-tuen ei tarvitse enää hoitaa manuaalisesti käyttäjien luontia tai poistamista. Käyttäjille jaetut roolit ja attribuutit ovat helpommin hallittavissa ja jaettavissa yhtenäisestä IAM-portaalinäkymästä. Tähän tarvitaan erillinen User Lifecycle Management -ominaisuus, jotta työntekijöiden Joiner-Mover-Leaver-prosessi voidaan toteuttaa tehokkaasti ja turvallisesti.

Uuden IAM-järjestelmän käyttöönotto tai nykyisen päivittäminen parantaisi merkittävästi yrityksen tietoturvaa ja helpottaisi yleisten tietoturvasäädösten noudattamista. Yrityksen liiketoimintaan liittyvät palvelut voidaan yhdistää yhden identiteetin taakse, mikä parantaa myös käyttäjäkokemusta yleisesti.

Opinnäytetyö sai alkunsa yrityksen ehdotuksesta sekä tutkimuksen tekijän kiinnostuksesta tietoturvaan.

2 Opinnäytetyön tausta ja tarkoitus

Toimeksiantajan organisaatio etsii IAM-järjestelmää (Identity and Access Management), jonka avulla voidaan tehostaa käyttäjähallinnan prosesseja ja parantaa tietoturvaa. Nykyisessä toimintamallissa käyttäjätunnusten luonti, käyttöoikeuksien määrittely ja tunnusten sulkeminen tapahtuvat pääosin manuaalisesti, mikä aiheuttaa hitautta, virhealttiutta ja hallinnollista kuormitusta. Erityisesti työntekijöiden organisaatiossa tapahtuvien muutosten, kuten työtehtävän vaihdon tai työsuhteen päättymisen yhteydessä, manuaalinen työ aiheuttaa epäjohdonmukaisuutta ja tietoturvariskejä.

IT-hallinto on tunnistanut käyttöoikeuksien hallinnan ja vanhojen tunnusten poistamisen erityisen haastavaksi. Ilman automatisoitua järjestelmää oikeuksien myöntäminen ja poistaminen jää helposti puutteelliseksi, jolloin järjestelmissä voi säilyä tarpeettomia tunnuksia tai liian laajoja käyttöoikeuksia. Tämä lisää tietoturvauhkia ja vaikeuttaa vaatimustenmukaisuuden toteuttamista.

Tavoitteena on siirtyä toimintamalliin, jossa käyttäjien elinkaarta — eli liittymistä organisaatioon, sisäisiä siirtymiä ja poistumisia — hallitaan automaattisesti HR-järjestelmän ja IAM-järjestelmän välisen integraation avulla. Ihannetilanteessa uudet työntekijätiedot siirtyisivät automaattisesti HR-järjestelmästä IAM-järjestelmään, joka loisi tarvittavat tunnukset ja käyttöoikeudet työntekijän tulevan työtehtävän perusteella. Työntekijän roolin muuttuessa käyttöoikeudet päivittyisivät automaattisesti valmiiksi määriteltyjen roolien mukaisesti. Työsuhteen päättyessä IAM-järjestelmä sulkisi käyttäjän tunnukset automaattisesti HR-järjestelmästä saadun tiedon perusteella.

Tämän opinnäytetyön tavoitteena on kartoittaa ja vertailla eri IAM-järjestelmiä, jotka tukevat edellä kuvatun Joiner-Mover-Leaver-prosessin automatisointia ja jotka soveltuvat erityisesti Microsoft-ekosysteemissä toimivan pk-yrityksen tarpeisiin. Tarkoituksena on löytää ratkaisu, joka parantaa IT-hallinnon tehokkuutta, vähentää manuaalista työtä, lisää tietoturvaa, parantaa käyttäjäkokemusta ja tarjoaa kustannustehokkaan mallin käyttäjähallinnan toteuttamiseen.

2.1 Aiheen valinta ja tutkimuksen relevanssi

Aiheen valinta tehtiin yhteisymmärryksessä toimeksiantajan kanssa. Tutkimuksen tekijällä oli mahdollisuus ehdottaa aihealuetta, johon opinnäytetyö kohdistettaisiin. Kiinnostuksen pohjalta päädyttiin tietoturvaan ja erityisesti IAM-ratkaisuihin.

2.2 Tutkimuskysymykset

Tutkimuskysymykset on laadittu tukemaan työn tavoitetta sekä ohjaamaan tutkimustyön suorittamista.

1. Mitkä ovat IAM-ratkaisujen ominaisuudet?
2. Millaisilla IAM-palveluilla saadaan toimeksiantajan vaatimukset täytettyä?
3. Millainen hinta IAM-järjestelmällä on?

Ensimmäinen tutkimuskysymys ohjaa tutkimusta keskittymään IAM-teknologian käytännön etuihin ja liiketoimintahyötyihin. Teoreettisessa viitekehyksessä tarkastellaan IAM-teknologian roolia organisaatioissa, mukaan lukien tietoturvan ja hallinnollisten prosessien kehittämisessä. Kysymys tukee johtopäätösten laatimista IAM-teknologian käyttöönoton näkökulmasta.

Toinen kysymys ohjaa tutkimuksen painopistettä teknologioiden vertailuun ja organisaation tarpeiden ymmärtämiseen. Tämä kysymys määrittää vertailun kriteerit sen perusteella, miten hyvin järjestelmät vastaavat yrityksen vaatimuksiin.

Kolmas kysymys painottaa taloudellista näkökulmaa. Kysymys tukee johtopäätösten ja suositusten laatimista erityisesti yrityksen päätöksentekijöille sekä selvittää, millaisia kustannuksia IAM-järjestelmältä voidaan odottaa.

Erilaisten järjestelmien välisiä eroja vertaillaan ja arvioidaan toimeksiantajan vaatimusten mukaisesti. Tutkimuksen tulokset auttavat henkilöstöä valitsemaan yritykselle sopivimman IAM-toteutuksen.

Tämä opinnäytetyö pyrkii vastaamaan kysymyksiin esittelemällä IAM-järjestelmiä, jotka kykenevät automaattisiin toimintoihin toimeksiantajan vaatimusten mukaisesti, sekä selvittämään, millä kustannustasolla tämä olisi mahdollista toteuttaa.

2.3 Tutkimuksen rajaus ja tavoitteet

Tutkimus rajataan käsittelemään yrityksen IAM-vaatimuksia. Nykytilanteessa toimintaa voidaan tehostaa HR-järjestelmän integraation automaation sekä käyttäjien elinkaaren hallinnan (ULM) avulla. IAM-järjestelmien valinta perustuu näihin kriteereihin.

Markkinoilla on laaja valikoima IAM-järjestelmiä, mutta tutkimuksessa tarkastellaan viittä järjestelmää. Tämä rajaus on tehty tutkimuksen laajuuden ja aikarajoitteiden vuoksi. Valitut järjestelmät edustavat keskeisiä, toimialalla tunnettuja ratkaisuja, jotka soveltuvat erityisesti pk-yrityksen tarpeisiin ja Microsoft-ekosysteemiin.

Vertailuanalyysi kohdistuu sekä yleisesti tunnettuihin IAM-toimijoihin että pienempien yritysten tarjontaan. Työhön ei sisälly ratkaisujen implementointia tai testausta, vaan se keskittyy järjestelmien vertailuun ja arviointiin niiden soveltuvuuden mukaan.

Tutkimuksen tavoitteena on esittää vaihtoehtoisia ratkaisuja, jotka täyttävät toimeksiantajan vaatimukset ja helpottavat tulevaa päätöksentekoa. Työ tarjoaa hyödyllistä tietoa myös yrityksen IT-johdolle, päättäjille ja teknisille asiantuntijoille, erityisesti niille, joilla ei ole ennestään kokemusta tai taustatietoa IAM-ratkaisuista.

2.4 IAM:n keskeiset käsitteet ja periaatteet

IAM-järjestelmät hyödyntävät eri menetelmiä ja tekniikoita käyttäjän henkilöllisyyden todentamiseksi.

IAM (Identity and Access Management)	IAM-järjestelmä hallitsee käyttäjien digitaalista identiteettiä ja pääsyä resursseihin.

2FA (Two-Factor Authentication)	Monitekijäinen todentamismenetelmä, joka vaati kaksi erillistä tunnistusvaihetta, kuten salasanan ja kertakäyttöisen koodin.
MFA (Multi-Factor Authentication)	Monivaiheinen tunnistautuminen, joka yhdistää vähintään kaksi eri todennustapaa, kuten salasanan, biometrisen tunnistuksen tai fyysisen avaimen. MFA sisältää 2FA:n erityisenä tapauksena.
SSO (Single Sign-On)	Ratkaisu, jonka avulla käyttäjä voi kirjautua kerran ja saada pääsyn useisiin järjestelmiin tai sovelluksiin ilman erillisiä kirjautumisia.
Käyttäjän elinkaaren hallinta (ULM)	Prosessi, joka kattaa käyttäjätilien luomisen, ylläpidon ja poistamisen työsuhteen aikana.
Privileged Access Management (PAM)	Työkalut ja prosessit, joilla hallitaan korkean riskin käyttäjäoikeuksia, kuten järjestelmänvalvojien pääsyä.
Zero Trust	Tietoturvamalli, jossa kaikki pääsy yrityksen resursseihin edellyttää todentamista ja luottamuksen jatkuvaa vahvistamista.
IAM-portaali (IAM Portal)	Keskitetty alusta, josta voidaan hallita käyttäjätilien oikeuksia ja pääsyä organisaation resursseihin. (Microsoft
Access Policy (Käyttöpolitiikka)	Säännöt, jotka määrittelevät, kenellä on pääsy resursseihin ja millä ehdoilla.
Role-Based Access Control (RBAC)	Pääsynhallintamalli, jossa käyttöoikeudet määräytyvät käyttäjän roolin perusteella, kuten työntekijä, esimies tai järjestelmänvalvoja.
Attribute-Based Access Control (ABAC)	Pääsynhallintamalli, jossa käyttöoikeudet perustuvat käyttäjän ominaisuuksiin, kuten sijaintiin, laitteeseen tai työtehtävään.
API-rajapinta	Sovellusohjelmointirajapinta, joka mahdollistaa IAM-järjestelmien integroinnin muihin sovelluksiin.

Identity Repository	Tietokanta, jossa IAM-järjestelmä säilyttää käyttäjien ja heidän tunnistetietojensa tiedot. Esim. Active Directory, Entra ID (Azure AD) ja LDAP.
Authentication (Todennus)	Prosessi, jossa vahvistetaan käyttäjän henkilöllisyys ennen pääsyn myöntämistä resursseihin esimerkiksi salasanan, kertakoodin tai biometrisen tunnistuksen avulla.
Authorization (Valtuutus)	Prosessi, jossa määritetään, mitä toimintoja todennettu käyttäjä saa suorittaa järjestelmässä tai sovelluksessa määriteltyjen käyttöoikeuksien perusteella.

(Haber & Rolls, 2020.)

3 IAM-ratkaisujen lähtökohdat

Yritykset, jotka hallitsevat käyttöoikeuksia manuaalisesti, voivat tehostaa toimintaansa ja parantaa tietoturvaa ottamalla käyttöön IAM-järjestelmän. IAM-järjestelmän avulla voidaan kehittää olemassa olevia käytäntöjä ja lisätä tietoturvaa. Uusien käyttäjien oikeuksien avaaminen, käyttöoikeuksien keskittäminen sekä käyttäjien poistuminen ja siihen liittyvien oikeuksien sulkeminen voidaan toteuttaa tehokkaasti ja turvallisesti IAM-järjestelmän avulla. (Niemi 2024.)

Identity and Access Management (IAM) on kehys, joka sisältää prosesseja, käytäntöjä ja teknologioita, joiden avulla organisaatio pystyy hallinnoimaan digitaalisia identiteettejä ja niihin liittyvää pääsyä eri resursseihin.

Yksi suurimmista haasteista tietoturvakehyksissä on niiden monimutkaisuus. Identiteetinhallinta on osa useimpia, ellei kaikkia virallisia tietoturvakehyksiä. Identiteetti on usein osa kokonaisuutta, joskus oma lukunsa, mutta harvoin keskiössä.

Identiteetinhallinta voidaan jakaa viiteen osa-alueeseen:

1. Todennus (Authentication)
   Todennus on prosessi, jolla varmistetaan käyttäjän henkilöllisyys ennen pääsyn myöntämistä tietojärjestelmiin, tietoihin, verkkoihin, fyysisiin alueisiin ja muihin resursseihin.

2. Valtuutus (Authorization)
   Valtuutus on oikeus suorittaa toiminto, joka perustuu sinun todennukseesi. Henkilöllisyytesi ja siihen liittyvä tili saavat oikeudet suorittaa tiettyjä toimintoja, ja niiden suorittaminen voidaan myös evätä perustuen todennukseen.
3. Hallinnointi (Administration)
   Hallinnointi tarkoittaa konfiguraatioiden ja muutosten hallitsemista.
4. Tarkastus (Audit)
   Käytetään todistamaan hallintoprosesseja sekä käytössä olevia käytäntöjen noudattamista.
5. Analyysi (Analysis)
   Analyysi on toiminnallisten turvallisuustietojen saamista jatkuvaan identiteettiin määrittelyyn sekä käsittelyyn liittyen.
   (Haber & Rolls, 2020.)

3.1 IAM:n rooli ja merkitys organisaatioissa

Käyttäjän identiteetin hallinta on olennainen osa tietoturvaa. Identity and Access Management (IAM) varmistaa, että oikeat identiteetit saavat pääsyn heille määriteltyihin resursseihin. Viitekehys sisältää erilaisia prosesseja, käytäntöjä ja teknologioita, joiden avulla voidaan hallita digitaalista identiteettiä ja seurata käyttäjien pääsyä. Identiteetinhallintaa tarvitaan tietoturvan parantamiseen, käyttäjätietojen käytön valvontaan sekä käyttöoikeuksien myöntämiseen työtehtävien mukaisesti. (Singh, Warraich & Thakkar, 2023.)

IAM on tärkeä työkalu yrityksille tietoturvan vahvistamisessa. Identiteetin merkitys korostuu, koska sitä hyödynnetään usein hyökkäyksen aloituspisteenä kohdeorganisaation verkkoon. Huonosti toteutettu monivaiheinen todennus (MFA), kehittyneet tietojenkalastelumenetelmät (phishing), automatisoidut kirjautumistekniikat ja vanhentuneet järjestelmät altistavat organisaatiot hyökkäyksille.

Identiteetistä on tullut digitaalisen infrastruktuurin ja sovellusten keskiö. Tämä tarkoittaa, että IAM:n roolia on vahvistettava — se ei ole enää vain yksi ominaisuus, vaan keskeinen toiminnallinen osa-alue. (Strom, 2024.)

IAM:lla on merkittävä rooli tietojen käsittelyssä. Kyberturvallisuudessa kirjautumistietojen hallinta vaatii IAM-ratkaisuja, joiden avulla voidaan hallita käyttöoikeuksia ja käyttäjätunnuksia tehokkaasti. IAM-järjestelmä tarjoaa keinon seurata käyttäjätoimintoja ja valvoa todennuksia.

Yksi IAM-järjestelmän keskeisimmistä ominaisuuksista on sen kyky integroitua organisaation IT-infrastruktuuriin ja noudattaa erilaisia tietoturvakäytäntöjä identiteettien hallinnassa.

Vaatimustenmukaisuutta hallinnoivat ohjelmistot auttavat automatisoimaan ja seuraamaan IAM-toiminnan eri osa-alueita.

Nykyiset järjestelmät ja palvelimet täydentyvät pilvipalveluilla, jotka tarjoavat joustavia tietoturvaratkaisuja erilaisilla työkaluilla. Tämä tekee identiteetinhallinnasta entistä monimutkaisempaa. Datakeskeinen todennus toimii perustavanlaatuisena tietoturvatoimintona, joka voidaan toteuttaa useilla eri ratkaisuilla.

IAM-järjestelmän keskeinen tehtävä on käyttöoikeuksien ja käyttäjätunnusten automatisointi, tallentaminen ja valvonta tietoturvan parantamiseksi. Sen avulla voidaan välttää pitkäaikaisten käyttöoikeustietojen jakaminen ja estää luvaton pääsy. Käyttäjien todennuksen hallinta on keskeinen osa pääsynhallinnan parhaita käytäntöjä. Se auttaa estämään luvattomat kirjautumisyritykset ja suojaa tietoja tietomurroilta. (Singh, Warraich & Thakkar, 2023.)

3.2 Käyttäjien hallinta

"*Nykyistä tehokkaampi käyttäjätunnistus ja sovelluksiin kirjautuminen on todellisen tietoyhteiskunnan edellytys.*" (Vesajoki, 2010.)

IT-tukihenkilöiden työajasta suuri osa kuluu rutiinitehtäviin, kuten uusien käyttöoikeuksien myöntämiseen, unohtuneiden salasanojen palauttamiseen ja vanhentuneiden käyttäjäoikeuksien hallintaan. Perinteiset kirjautumismenettelyt tekevät IT-osaston työstä jatkuvaa kiiretyötä, jättäen vähän aikaa tehtävien kehittämiselle ja tuottavalle innovoinnille.

Ammattimaiset verkkorikolliset keräävät kaiken rahanarvoisen tiedon. Yrityksen asiakasrekisterin, tuotekehityssuunnitelmien tai henkilö- ja luottokorttitietojen vuotaminen voi johtaa mainehaittoihin ja sanktioihin, joiden vaikutukset liiketoimintaan voivat olla kohtalokkaita. (Vesajoki, 2010.)

3.3 Käyttöoikeuksien hallinta

Organisaation käyttöoikeuksien hallinnassa käytetään korkean käyttöoikeuden rooleja, kuten admin, system administrator, domain administrator ja privileged user. Näiden roolien haltijoilla on laajemmat käyttöoikeudet organisaation sisällä, ja niiden turvallinen hallinta on erityisen tärkeää. Tätä varten käytetään Privileged Access Managementia (PAM).

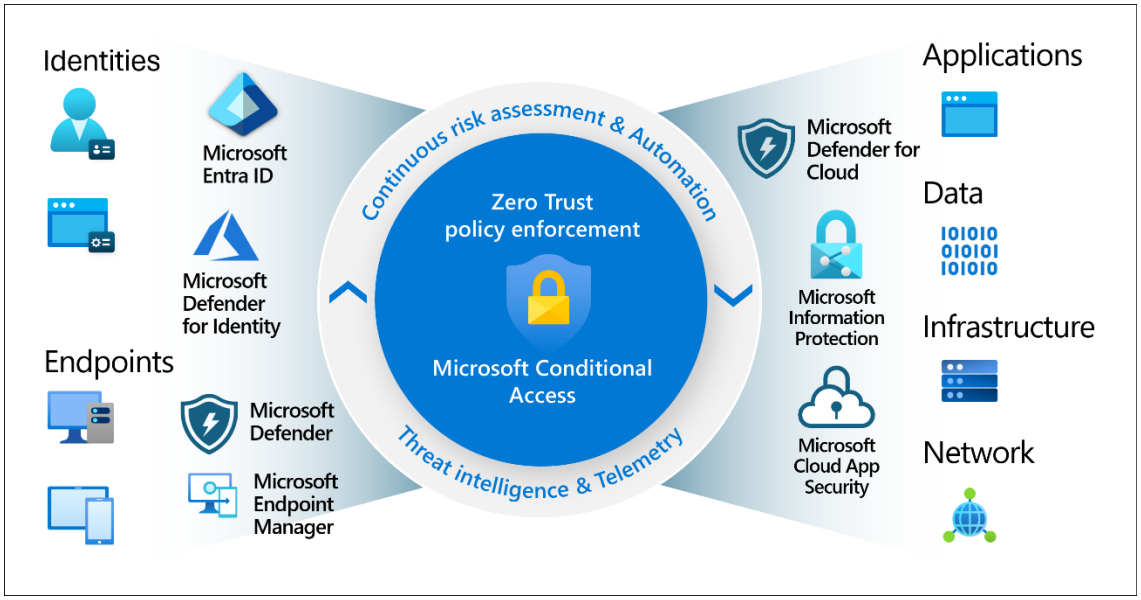
PAM on menetelmä, jonka tarkoituksena on suojata, hallita ja valvoa etuoikeutettujen roolien käyttöä eri resursseihin. Käytäntö sisältää useita hallittavia komponentteja, kuten etuoikeutetut identiteetit, sertifikaatit, avaimet, tilit, valtuustiedot ja salasanat. PAM:n tavoitteena on vähentää riskejä sallimalla pääsy vain niille etuoikeutetuille identiteeteille ja resursseille, jotka vaativat järjestelmänvalvojan tai pääkäyttäjän oikeudet tehtävien suorittamiseen. PAM

pyrkii erottamaan etuoikeutettujen roolien käytön päivittäisistä toiminnoista, mikä luo pohjan Least Privilege -periaatteelle.

Least Privilege Principle tarkoittaa, että käyttäjille myönnetään vain ne oikeudet, jotka ovat välttämättömiä heidän työtehtäviensä suorittamiseksi. Tämä periaate ohjaa koko identiteetin, tilin ja käyttöoikeuksien elinkaaren hallintaprosessia. Least Privilege -malli parantaa järjestelmän vakautta, yleistä tietoturvaa ja pienentää käyttäjätilien väärinkäytön riskiä.

Least Privilege on yksi identiteetinhallinnan parhaista käytännöistä käyttöoikeuksien hallinnassa. Sen toteutuksessa voidaan hyödyntää RBAC-mallia (Role-Based Access Control), joka rajoittaa käyttöoikeudet käyttäjän roolin mukaan. Näin käyttäjille myönnetään vain ne oikeudet, jotka ovat tarpeen työtehtävien suorittamiseen. Tämä tukee Least Privilege -periaatetta, joka minimoi tarpeettomat käyttöoikeudet ja vähentää tietoturvariskejä. (Haber & Rolls, 2020.)

3.4 Tietoturvan parantaminen

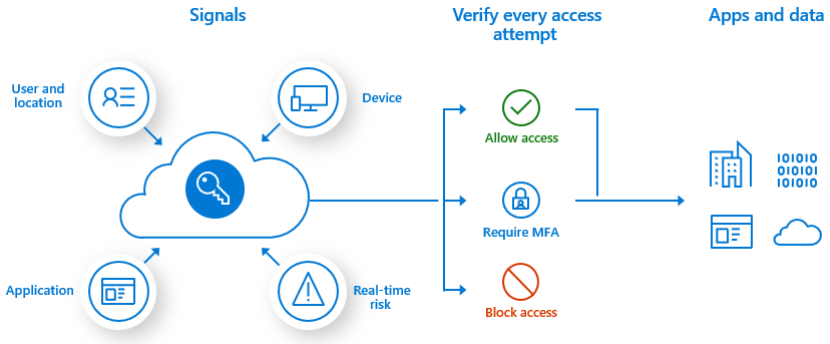


Kuva 1: Zero Trust -käytännön toteutus. (Microsoft Learn, 2025.)

Kyberuhkien kehittyessä organisaatiot ottavat yhä laajemmin käyttöön kehittyneitä tietoturvakehyksiä suojellakseen digitaalista infrastruktuuriaan. Yksi merkittävä malli tietoturvan parantamisessa on Zero Trust Architecture (ZTA), joka perustuu periaatteeseen "*älä koskaan luota, varmista aina*".

ZTA olettaa, että sekä sisäiset että ulkoiset verkot voivat vaarantua, mikä edellyttää jokaisen pääsypyynnön huolellista todennusta, valtuutusta ja jatkuvaa valvontaa. IAM-järjestelmän integrointi Zero Trust -periaatteisiin luo vahvan tietoturvakehyksen, joka kykenee tehokkaasti torjumaan nykyaikaisia haavoittuvuuksia. (Kuva 1.)

Zero Trust -mallissa IAM:lla on keskeinen rooli varmistaessaan, että vain valtuutetut käyttäjät saavat pääsyn organisaation resursseihin. Yksi tärkeimmistä osa-alueista on jatkuva todennus: käyttäjien henkilöllisyydet ja käyttöoikeudet on tarkistettava toistuvasti. (Filho, 2025.)



Kuva 2: Conditional Access edellyttää monivaiheista tunnistautumista. (Microsoft Learn, 2025)

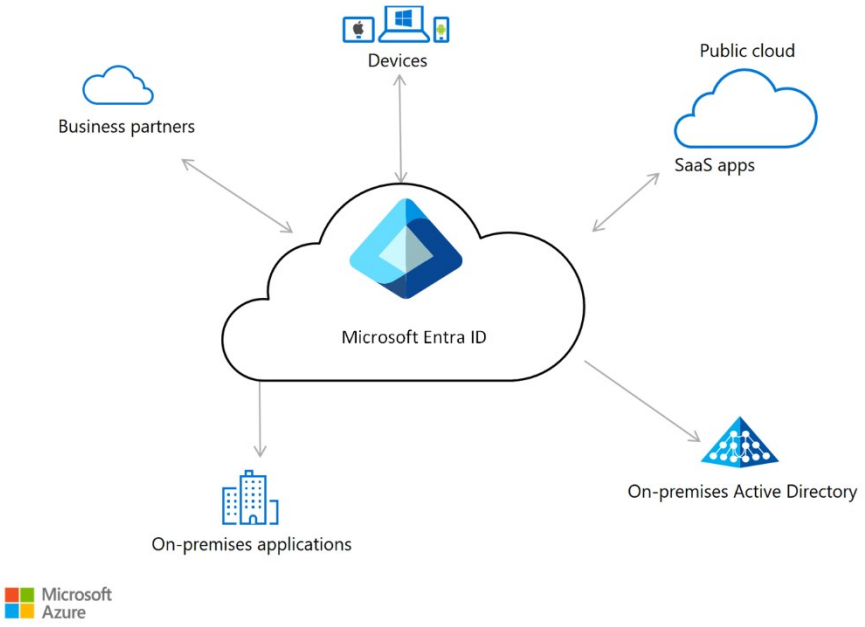
IAM-ratkaisut hyödyntävät erilaisia mekanismeja, kuten kertakirjautumista (SSO), monitekijätodennusta (MFA) ja roolipohjaista pääsynhallintaa (RBAC), turvallisten pääsykäytäntöjen varmistamiseksi. Esimerkiksi MFA edellyttää käyttäjältä usean todennustavan käyttöä – kuten salasanan ja biometrisen tunnisteen – lisäten ylimääräisen suojakerroksen yksinkertaisen salasanasuojauksen lisäksi. (Kuva 2.)

Salauksen ohella organisaatioiden tulee ottaa käyttöön myös muita turvatoimia, kuten kulunvalvonta ja todennus, joilla varmistetaan, että vain valtuutetut henkilöt tai järjestelmät voivat käyttää arkaluontoisia tietoja. Monitekijätodennuksen (MFA) ja vahvojen identiteetinhallintakäytäntöjen avulla voidaan merkittävästi vähentää luvatonta pääsyä suojattuihin tietoihin. (Ali & Weng, 2025.)

3.5 IT-hallinnon tehostaminen

IAM tarjoaa organisaatioille merkittäviä hyötyjä erityisesti tietoturvan, kustannustehokkuuden ja hallinnollisen sujuvuuden näkökulmasta. Automatisoimalla rutiinitehtäviä käyttövaltuushallinnassa voidaan vähentää manuaalisen työn määrää sekä systematisoida käyttäjien valtuutusten ja järjestelmäkäyttöoikeuksien hallintaa. (Helsingin Kuntasektori, 2013.)

Automatisoitu käyttäjien luonti ja poistaminen vähentää manuaalista työtä ja minimoi inhimilliset virheet, mikä parantaa järjestelmien tietoturvaa ja tehokkuutta. Käyttäjien elinkaaren hallinta varmistaa, että uudet työntekijät saavat tarvittavat käyttöoikeudet heti työsuhteen alussa ja että poistuvien työntekijöiden pääsyoikeudet poistetaan viiveettä. Tämä nopeuttaa työn aloitusta ja lopetusta, vähentää käyttöoikeuksiin liittyviä riskejä ja keventää IT-osaston hallinnollista kuormitusta. (Helsingin Kuntasektori, 2013.)



Kuva 3: Microsoftin identiteetinhallinnan perusarkkitehtuuri. (Microsoft, 2025.)

IAM-järjestelmän käyttö mahdollistaa keskitetyn pääsynhallinnan, jolloin organisaatiolla on ajantasainen tieto siitä, kenellä on ollut käyttöoikeudet tiettyihin resursseihin tai järjestelmiin. Tämä vapauttaa tietohallinnon resursseja muihin kriittisiin tehtäviin, tehostaa käyttöoikeuksien hallintaa ja valvontaa sekä vähentää manuaalisen työn tarvetta. Tuloksena IT-hallinnon kokonaistehokkuus paranee.

Kertakirjautumisratkaisun (SSO) käyttöönotto tehostaa käyttäjätunnusten hallintaa keskittämällä kirjautumisprosessin yhteen järjestelmään. Tämä vähentää erillisten tunnusten tarvetta ja minimoi salasanoihin liittyvät ongelmat, kuten unohtamiset ja toistuvat nollaukset. Lisäksi SSO parantaa käyttäjäkokemusta nopeuttamalla pääsyä eri sovelluksiin ja palveluihin ilman toistuvaa tunnistautumista. Tietoturva vahvistuu, kun käyttäjät voivat hallita pääsyään yhden turvallisen kirjautumisprosessin kautta ilman heikkoja tai uudelleenkäytettyjä salasanoja. Tämä vähentää IT-hallinnon työkuormaa ja tukipyyntöjä, vapauttaen resursseja muihin kriittisiin tehtäviin ja parantaen kokonaisvaltaista hallintaa. (Kuva 3.)

3.6 Organisaation IAM vaatimukset

Nykyistä käyttäjähallintaa voidaan kehittää ja tehostaa IAM-ratkaisun avulla. Tällä hetkellä prosessit suoritetaan pääosin manuaalisesti, mikä altistaa virheille ja hidastaa käyttöoikeuksien hallintaa. IAM-järjestelmä nopeuttaa näitä prosesseja ja vähentää käyttäjävirheiden riskiä. Käyttöoikeuksia hallitaan hybridiympäristössä: paikallisesti Active Directory Users and Computers (ADUC) -työkalulla ja pilviympäristössä Microsoft Entra ID:n kautta.

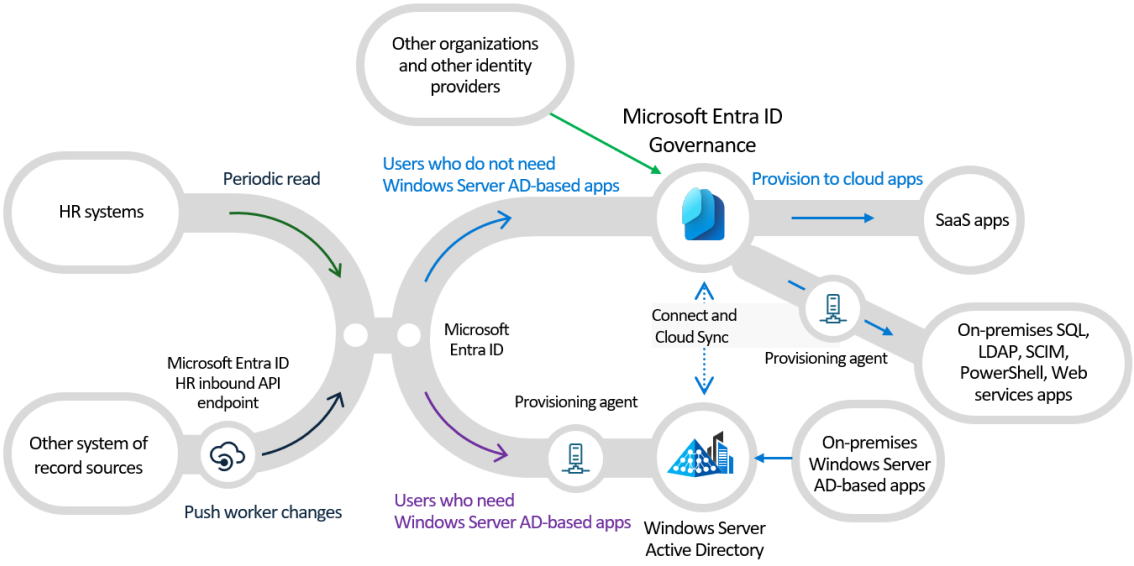
Nykyisen käytännön keskeisiä ongelmia ovat muun muassa:

- käyttäjien oikeuksien sulkemisen viiveet
- ylimääräiset tai tarpeettomat käyttöoikeudet
- vanhojen työntekijöiden tunnusten säilyminen järjestelmissä
- resurssien hallinnan hajanaisuus eri käyttöliittymissä

Empiirisen tutkimuksen havaintojen perusteella erityisesti poistuneiden tai roolia vaihtaneiden työntekijöiden käyttöoikeuksien sulkeminen viivästyy säännöllisesti, mikä aiheuttaa sekä tietoturvariskin että hallinnollista kuormitusta. Toimeksiantajan IT-hallinto kokee tämän ongelman kriittisenä, ja tunnistaa tarpeen automatisoidulle käyttäjähallinnalle.

Kattavamman IAM-järjestelmän käyttöönotto mahdollistaa:

- keskitetyn hallinnan ja selkeämmän näkyvyyden käyttöoikeuksiin
- tietoturvan parantamisen
- prosessien automatisoinnin
- kustannussäästöt
- kevennetyn IT-osaston työkuorman



Kuva 4: Käyttäjän elinkaaren hallinta. (Microsoft Learn, 2025.)

Organisaation työnkuvassa Joiner–Mover–Leaver-prosessin toteutusta voidaan tehostaa User Lifecycle Management (ULM) -ominaisuudella. Tämä parantaa uusien, nykyisten ja poistuneiden työntekijöiden tunnusten hallintaa ja antaa IT-hallinnolle paremman näkyvyyden koko domainin käyttäjätietoihin. (Kuva 4.)

Yhteenvetona voidaan todeta, että nykyinen manuaalinen käyttäjähallinta aiheuttaa merkittäviä haasteita erityisesti tehokkuudessa, tietoturvassa ja käyttöoikeuksien ajantasaisuudessa. Hybridimallin käyttöoikeuksien hallinta on hajanaista, altistaa virheille ja hidastaa oikeuksien sulkemista. Vaatimukset täyttävä uusi IAM-ratkaisu mahdollistaa prosessien automatisoinnin, keskitetyn hallinnan ja ajantasaisen näkymän käyttäjätietoihin.

4 Tutkimusmenetelmät ja aineistonkeruu

Tutkimus keskittyy organisaation sisäiseen identiteetin- ja käyttöoikeuksien hallintaan (IAM) sekä sen kehittämiseen soveltuvan IAM-teknologian avulla. Työssä tarkastellaan IAM-ratkaisujen keskeisiä ominaisuuksia, hyötyjä ja kustannuksia. Tutkimus painottuu erityisesti kohdeorganisaation käyttäjähallinnan tehostamiseen ja tietoturvan parantamiseen esittelemällä sopivia IAM-järjestelmävaihtoehtoja.

Tutkimuksesta on rajattu pois käyttöönotto- ja testausprosessit, jotta työn laajuus pysyy hallittavana. Käyttöönottoa tulisi tarkastella erillisenä kokonaisuutena. IAM-ratkaisun käyttöönottaminen riippuu organisaation koosta ja tarpeista, ja onnistunut toteutus edellyttää huolellista suunnittelua sekä laaja-alaista asiantuntemusta, jotta järjestelmä voidaan sovittaa osaksi organisaation rakenteita ja prosesseja.

Vaikka IAM on keskeinen osa säädösten noudattamista ja tietosuojan varmistamista, pienet ja keskisuuret yritykset kohtaavat usein haasteita kattavien IAM-ratkaisujen käyttöönotossa. Yleisiä haasteita ovat muun muassa rajalliset budjetit, puutteellinen tekninen asiantuntemus sekä vaikeudet mukauttaa järjestelmiä yrityskohtaisiin vaatimuksiin.

4.1 Kirjallisuuskatsaus

Kirjallisuuskatsauksen tavoitteena on luoda teoreettinen perusta opinnäytetyölle. Katsauksessa tarkastellaan IAM:n keskeisiä käsitteitä ja periaatteita, sen roolia ja merkitystä organisaatioissa sekä IAM-ratkaisujen ominaisuuksia.

Kirjallisuuskatsauksessa hyödynnetään monipuolisesti akateemisia julkaisuja, alan raportteja ja asiantuntija-artikkeleita, jotta saadaan kokonaisvaltainen kuva IAM-järjestelmien toiminnallisuudesta. (Mannila, 2021.)

4.2 Vertailuanalyysi

Vertailuanalyysin avulla arvioidaan eri IAM-ratkaisujen soveltuvuutta toimeksiantajan vaatimusten mukaisesti. Vertailuun valitaan IAM-järjestelmiä, jotka täyttävät toimeksiantajan asettamat vaatimukset, ja tarkastellaan niiden hinnoittelua.

Vertailuanalyysin tulokset esitetään taulukon ja kuvausten avulla, joissa tuodaan esiin eri järjestelmien hinnoittelutiedot ja ominaisuudet. Analyysin tiedot kerätään avoimista lähteistä sekä toimittajien omasta dokumentaatiosta. (Lipska, 2025.)

Vertailuanalyysissä on rajattu tarkastelu viiteen IAM-järjestelmään, jotka valittiin niiden kyvykkyyksien ja yhteensopivuuden perusteella toimeksiantajan vaatimusten kanssa. Valinta perustuu siihen, että nämä järjestelmät edustavat markkinoiden keskeisimpiä ja relevantteja ratkaisuja pk-yritykselle, joka toimii Microsoft-ekosysteemissä.

4.3 Empiirinen tutkimus

Empiirisen tutkimuksen tavoitteena on selvittää toimeksiantajayrityksen nykytilanne käyttäjähallinnan osalta sekä kartoittaa sen tarpeet ja odotukset IAM-ratkaisulle. Tutkimus toteutettiin kvalitatiivisella lähestymistavalla, jossa aineistoa kerättiin havainnoimalla yrityksen sisäisiä dokumentteja sekä keskusteluilla IT-henkilöstön kanssa. Tämä lähestymistapa mahdollistaa syvällisen ymmärryksen käytännön prosesseista ja kehityskohteista ilman laajamittaista kenttätyötä. (Heikkilä, 2014.)

Havaintoja kerättiin erityisesti tilanteista, joissa käyttäjätunnusten hallinta on osoittautunut tehottomaksi tai tietoturvariskien lähteeksi. Dokumentoinnin avulla selvitettiin muun muassa prosessien manuaalisuuden aiheuttamia haasteita.

Poistettujen tai siirtyneiden työntekijöiden tilien deaktivointi viivästyy, mikä aiheuttaa tarpeettomien tunnusten jäämisen käyttöön. Tätä pidetään merkittävänä tietoturvariskinä ja hallinnollisena kuormituksena.

Empiirisessä aineistossa nousi esiin selkeä tarve automaattiselle provisioinnille, joka vähentäisi manuaalisten virheiden määrää, nopeuttaisi uusien työntekijöiden pääsyä järjestelmiin ja varmistaisi viiveettömän pääsynhallinnan työsuhteen päättyessä. Toiveena on, että käyttäjätilin luonti, roolimäärittelyt ja poistot voidaan tulevaisuudessa automatisoida suoraan HR-järjestelmästä IAM-ratkaisuun.

Tätä empiiristä aineistoa hyödynnetään tutkimuksen vertailuanalyysissä, jossa arvioidaan eri IAM-järjestelmien kykyä vastata esiin nousseisiin käytännön tarpeisiin.

4.4 Aineiston kerääminen ja analyysi

Tämän opinnäytetyön aineisto koostuu monipuolisista lähteistä, kuten alan asiantuntijaraporteista, julkaistuista tutkimuksista, tuotekohtaisista dokumentaatioista sekä palveluntarjoajien verkkosivuista. Aineistoa kerättiin erityisesti niistä lähteistä, jotka käsittelevät identiteetin- ja käyttöoikeuksien hallintaa (IAM), sen teknologisia ratkaisuja ja käyttöönoton parhaiden käytäntöjen vaikutuksia organisaatioiden toimintaan.

Tarkastelun kohteena olivat erityisesti näkökulmat, jotka korostavat IAM-ratkaisujen merkitystä tietoturvalle, hallinnolliselle tehokkuudelle ja riskienhallinnalle. Lisäksi perehdyttiin eri IAM-teknologioiden toiminnallisiin ominaisuuksiin sekä kustannusrakenteisiin. Tarkoituksena oli muodostaa kattava kokonaiskuva niistä vaihtoehdoista, jotka soveltuvat erityisesti pk-yrityksen tarpeisiin Microsoft-ekosysteemissä toimivassa ympäristössä.

Aineiston analyysissä hyödynnettiin vertailuanalyysiä, jossa IAM-järjestelmien ominaisuuksia ja hinnoittelumalleja tarkasteltiin suhteessa toimeksiantajayrityksen tarpeisiin. Analyysin keskiössä oli arvioida, miten hyvin eri IAM-ratkaisut vastaavat organisaation Joiner–Mover–Leaver-prosessien automatisointitarpeeseen ja kustannustehokkuuteen. Vertailun avulla pyrittiin tunnistamaan sekä keskeiset hyödyt että mahdolliset haasteet kunkin järjestelmän käyttöönotossa.

4.5 Luotettavuus ja validiteetti

Tutkimuksen luotettavuutta arvioidaan tarkastelemalla reliabiliteettia ja validiteettia. Reliabiliteetti pyritään varmistamaan käyttämällä luotettavia ja asiantuntevia lähteitä, kuten ajantasaisia akateemisia julkaisuja, asiantuntijaraportteja ja tuotedokumentaatioita. Kirjallisuuskatsauksen avulla pyritään varmistamaan, että tutkimuksen analyysi perustuu ajankohtaiseen ja relevanttiin tietoon.

Validiteettia vahvistetaan vertailemalla useista lähteistä kerättyä tietoa ja arvioimalla sen yhteensopivuutta. Vertailuanalyysi tukee tutkimuksen luotettavuutta, koska se kohdistuu suoraan toimeksiantajan vaatimuksiin ja tuo esiin järjestelmien ominaisuuksia ja hinnoittelumalleja.

Lisäksi tutkimuksen validiteettia parantaa empiirinen näkökulma, joka perustuu toimeksiantajan IT-hallinnon kanssa käytyihin keskusteluihin sekä sisäisten dokumenttien tarkasteluun. Tämä tuo tutkimukseen käytännönläheistä ymmärrystä nykyisten prosessien haasteista, kuten käyttäjätunnusten sulkemisen viiveistä ja manuaalisten virheiden riskeistä. Empiirinen aineisto tukee myös vaatimusten määrittelyä, mikä parantaa tutkimustulosten sovellettavuutta käytännössä.

Vaikka tutkimus on laaja ja vertailu pohjautuu viiteen eri IAM-järjestelmään, on tärkeää huomioida, että vertailun rajoittaminen näihin viiteen järjestelmään on ollut käytännöllinen valinta. Mikäli vertailua olisi laajennettu useampiin järjestelmiin, tutkimuksen laajuus olisi kasvanut merkittävästi, mikä olisi voinut vaikuttaa tutkimuksen syvyyteen ja ajallisiin resursseihin. Tämä rajaus on kuitenkin perusteltu, sillä vertailu tarjoaa riittävän kattavan kuvan markkinoiden tärkeimmistä ja relevantimmista ratkaisuista pk-yrityksen tarpeisiin. Tämä valinta mahdollistaa syvällisemmän tarkastelun ja käytännönläheisempien suositusten tekemisen toimeksiantajalle.

5 IAM-järjestelmien esittely

IAM-ratkaisut ovat keskeinen osa organisaatioiden kyberturvallisuusstrategioita. Ne varmistavat, että oikeat henkilöt saavat oikeanlaisen pääsyn oikeisiin järjestelmiin, oikeaan aikaan ja oikeasta syystä. IAM ei ole enää pelkästään tekninen ratkaisu, vaan olennainen osa organisaation riskienhallintaa, tiedon suojausta ja sääntelyvaatimusten noudattamista.

Modernit IAM-järjestelmät mahdollistavat tehokkaan käyttäjäidentiteettien elinkaaren hallinnan alkaen käyttäjän luomisesta, roolien ja käyttöoikeuksien määrittelystä aina tunnusten poistamiseen työsuhteen päättyessä. Ne tukevat kertakirjautumista (SSO), monivaiheista tunnistautumista (MFA), ehdollista pääsyä sekä oikeuksien hallintaa itsepalveluportaalien kautta. Käytännössä IAM-järjestelmä toimii siltana käyttäjän, sovellusten ja pääsynhallintapolitiikkojen välillä.

Järjestelmien käyttöönotto voi vaihdella merkittävästi eri tuotteiden ja toimintaympäristöjen mukaan. Joissakin tapauksissa voidaan hyödyntää nopeasti käyttöön otettavia valmiita pilvipalveluratkaisuja, kun taas toisissa tilanteissa vaaditaan laajaa integraatiotyötä ja räätälöintiä. (Microsoft Learn, 2025.)

Seuraavaksi esitellään viisi eri IAM-tuotetta. Jokaista tarkastellaan keskeisten ominaisuuksien, soveltuvuuden ja mahdollisten rajoitusten näkökulmasta. Tuotteet on valittu seuraavin perustein: yhteensopivuus toimeksiantajan nykyisen järjestelmän kanssa, markkinoiden suosituimmat ratkaisut, kustannustehokkuus, toimeksiantajan ehdottama vaihtoehto sekä suomalainen tuote.

5.1.1 Microsoft Entra ID

Microsoft Entra ID, aiemmin Azure AD, on Microsoftin pilvipohjainen identiteetin- ja pääsynhallintapalvelu. Se on työssä esiteltävistä tuotteista suosituin ja toimii toimeksiantajan nykyisenä IAM-järjestelmänä. Entra ID on syvästi integroitu Microsoftin ekosysteemiin, mukaan lukien Microsoft 365, Azure ja muut pilvipalvelut.

Palvelu tarjoaa laajan valikoiman ominaisuuksia, kuten kertakirjautumisen (SSO), monivaiheisen tunnistautumisen (MFA), ehdollisen pääsyn (Conditional Access), identiteetin suojauksen ja etuoikeutettujen identiteettien hallinnan (PIM). Se tukee myös hybriditunnistautumista yhdistämällä paikallisen Active Directory -infrastruktuurin pilviympäristöön, mikä mahdollistaa yhtenäisen identiteetinhallinnan molemmissa ympäristöissä. (Cayosoft, 2025.)

Microsoft-keskeiselle organisaatiolle Entra ID tarjoaa houkuttelevan ratkaisun, koska se integroituu saumattomasti olemassa oleviin järjestelmiin. Lisäksi Microsoft 365- tai Azure-tilaukset voivat tuoda kustannusetuja. Microsoft-ympäristön tuttuus helpottaa myös järjestelmän käyttöönottoa ja hallintaa. (Peerspot, 2025.)

Entra ID tarjoaa useita eri lisenssimalleja, jotka soveltuvat organisaation erilaisiin tarpeisiin – aina maksuttomasta versiosta edistyneempiin P1- ja P2-tasoihin sekä laajennettuun Entra Suite -pakettiin.

Lisenssivaihtoehdot:

Taulukko 1: Microsoft Entra ID -lisenssien ominaisuudet sekä hinnoittelu.

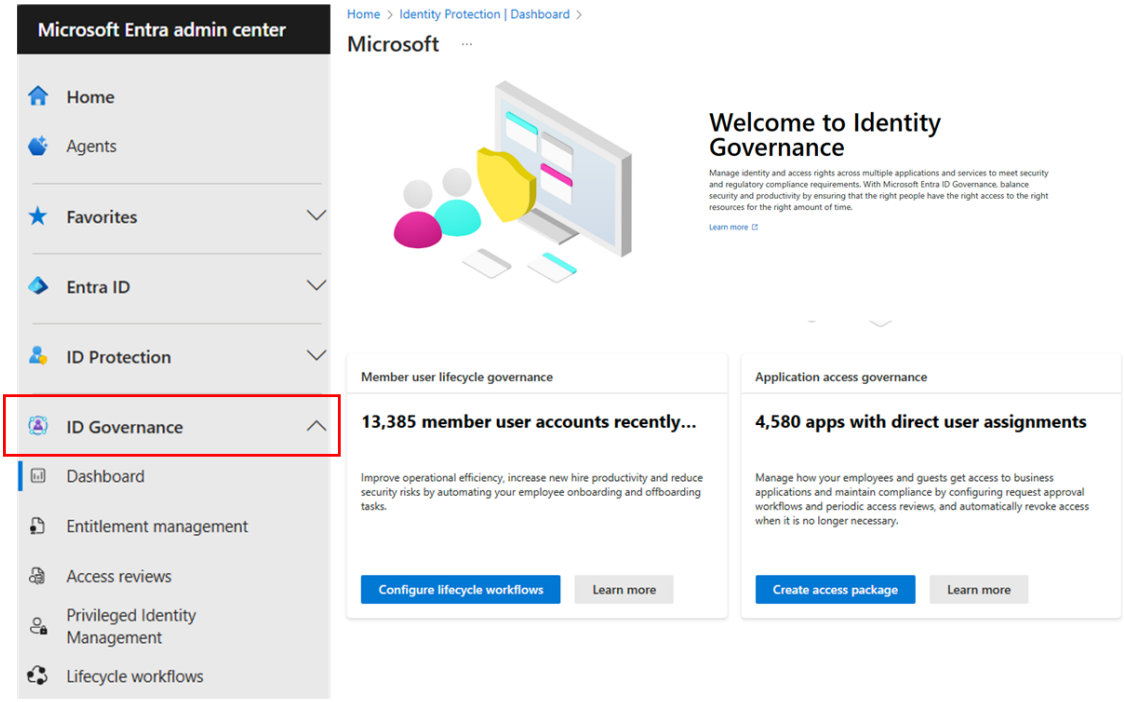
Lisenssin nimi	Ominaisuudet	Hinnoittelu
Entra ID Free	Perustason identiteetinhallinta ja turvakäytännöt. Ei tue ehdollista pääsyä tai elinkaaren hallintaa.	0 € (sisältyy Microsoft 365/Azure-vuokraan)
Entra ID P1	P1-lisenssi lisää Free-version toiminnallisuuksiin mm. Hybrid-identiteetin tuen, käyttäjän self-service-ominaisuudet, ehdollisen pääsyn (Conditional Access) ja perusmonivaiheisen tunnistautumisen.	Maksaa 5.60 €/käyttäjä/kk (vuosisitoumuksella).
Entra ID P2	P2 sisältää P1:n ominaisuudet sekä edistyneet identiteetin suojaus- ja valvontaominaisuudet kuten Identity Protection ja Privileged Identity Management (PIM).	Maksaa 8.40 €/käyttäjä/kk (vuosisitoumuksella).
Entra Suite	Yhdistää verkon pääsynhallinnan, identiteetin suojauksen, Governance-ominaisuudet ja identiteettitodentamisen (Verified ID) yhteen pakettiin.	Maksaa 11.20 €/käyttäjä/kk (vuosisitoumuksella).

Laajennukset ja lisäosat:

- Entra ID Governance: Mahdollistaa identiteetin elinkaariprosessien ja käyttöoikeusarviointien automaation. Hinta: 6,60 €/käyttäjä/kk. Vaatii vähintään P1- tai P2-lisenssin.

Kustannusvaikutus toimeksiantajalle:

Toimeksiantajalla on tällä hetkellä käytössä Entra ID P2 -lisenssi (8,40 €/kk per käyttäjä). Päivitys Entra Suite -pakettiin nostaisi hinnan 11,20 €/kk, eli lisäkustannus olisi 2,80 €/käyttäjä/kk.



Kuva 5: Entra ID Identity Governance. (Microsoft Learn, 2025)

Governance-lisäosan hankkiminen P2-lisenssin päälle maksaisi yhteensä 15 €/kk per käyttäjä (8,40 € + 6,60 €), mikä tekee Suite-paketista selvästi kustannustehokkaamman. Lisäksi Suite-paketti sisältää ominaisuuksia kuten Verified ID ja Private Access ilman erillisiä lisenssejä. (Kuva 5.)

Toimeksiantajan vaatimukset täyttävä lisenssipaketti olisi siis Entra Suite, hinnalla 11,20 €/käyttäjä/kk. (Microsoft, 2025.)

5.1.2 Okta Workforce Identity

Okta Workforce Identity on pilvipohjainen identiteetin- ja pääsynhallintaratkaisu (IAM). Se tarjoaa työkalut käyttäjien tunnistamiseen, valtuuttamiseen ja hallintaan eri sovelluksissa ja palveluissa. Sen vahvuuksia ovat käyttäjäystävälliset työnkulut sekä hyvä integraatio useiden eri järjestelmien kanssa. Ratkaisu yksinkertaistaa sovellusten käyttöä poistamalla tarpeen muistaa useita salasanoja ja parantaa näin käyttäjäkokemusta.

Okta tarjoaa laajan sovellusintegraatioiden ekosysteemin ja on erityisen vahva kertakirjautumisessa (SSO) ja monivaiheisessa tunnistautumisessa (MFA). Sen pilvipohjainen arkkitehtuuri mahdollistaa skaalautuvuuden erilaisiin ympäristöihin.

Okta voi kuitenkin olla pk-yrityksille kallis ratkaisumalli modulaarisen hinnoittelunsa vuoksi, ja sen konfigurointi saattaa vaatia erikoisosaamista. Vaikka Okta on teknisesti tehokas, suomalaiselle Microsoft-keskeiselle pk-yritykselle sen lisenssikustannukset voivat olla liian korkeat suhteessa hyötyihin. (Peerspot, 2025.)

Hinnoittelu ja ominaisuudet:

- Starter (6 USD/kk per käyttäjä): Sisältää keskeiset IAM-toiminnot, kuten Universal Directoryn, viisi työnkulkua (Workflows), kertakirjautumisen (SSO) ja monivaiheisen tunnistautumisen (MFA).
- Essentials (17 USD/kk per käyttäjä + 1 500 USD vuosimaksu): Sisältää kaikki Starterin ominaisuudet sekä:
    - Adaptive MFA -automaatio
    - User Lifecycle Management -työkalut
    - Access Governance -politiikat
    - Privileged Access -moduulin

Essentials-taso mahdollistaa käyttäjien provisioinnin ja deprovisioinnin automatisoinnin koko elinkaaren ajalta, vastaten näin toimeksiantajan määrittämiä vaatimuksia elinkaaren hallinnan ja tietoturvan osalta.

Toimeksiantajan vaatimukset täyttävä kokonaispaketti olisi Essentials-lisenssi, jonka hinnoittelu on 17 USD/kk per käyttäjä + 1 500 USD vuosimaksu. (Okta, 2025.)

5.1.3 miniOrange

miniOrange on identiteetin- ja pääsynhallintaratkaisu (IAM), joka tarjoaa laajan valikoiman ominaisuuksia organisaatioiden identiteetinhallinnan tarpeisiin. Vaikka se ei ole yhtä tunnettu kuin Okta tai Microsoft Entra ID, miniOrange pyrkii tarjoamaan joustavan ja monipuolisen vaihtoehdon erityisesti organisaatioille, jotka etsivät kustannustehokasta ratkaisua laajoilla integraatiomahdollisuuksilla.

miniOrange tukee keskeisiä IAM-toimintoja, kuten kertakirjautumista (SSO), monivaiheista tunnistautumista (MFA), käyttäjähallintaa, pääsynhallintaa ja identiteetin suojausta. Se tukee yleisimpiä tunnistusprotokollia, kuten SAML, OAuth ja OpenID Connect, mikä mahdollistaa integraation lukuisiin pilvi- ja verkkosovelluksiin.

Microsoft-keskeiselle organisaatiolle erityisen kiinnostavaa on miniOrangen tuki Active Directory -integraatioille sekä sen yhteensopivuus Microsoft 365:n ja muiden Microsoft-palveluiden kanssa. Tämä mahdollistaa yhtenäisen identiteetinhallintakokemuksen ilman tarvetta siirtyä kokonaan pois Microsoftin ekosysteemistä.

Mahdollisia heikkouksia ovat miniOrangen pienempi markkinaosuus ja tunnettuus verrattuna alan johtaviin toimijoihin, kuten Microsoftiin ja Oktaan. Tämä voi tarkoittaa rajallisempaa käyttäjäyhteisöä ja vähemmän valmiita integraatioita joihinkin harvinaisempiin sovelluksiin. Lisäksi on tärkeää arvioida tarkasti, kattavatko sen ominaisuudet organisaation tarpeet, erityisesti jos vaaditaan erittäin kehittyneitä toiminnallisuuksia.

miniOrangen User Lifecycle Management (ULM) -moduuli on sisäänrakennettu, eikä se vaadi erillistä lisäosaa. Käyttäjän lisääminen HR-järjestelmään käynnistää automaattisesti provisioinnin.

Ratkaisun hinnoittelu on joustava ja erityisesti pk-yrityksille kilpailukykyinen. Toimeksiantajan tarpeisiin soveltuvat parhaiten Premium- tai Enterprise IAM Suite -lisenssit:

- Premium: 2,50 $ / käyttäjä / kk
- Enterprise: 3,00 $ / käyttäjä / kk

Lisäksi miniOrange tarjoaa ilmaisen kokeilujakson, jonka aikana voidaan testata alustan ydintoimintoja ennen sitoutumista. Tämä madaltaa käyttöönoton kynnystä erityisesti pienemmille organisaatioille.

Yhteenvetona miniOrange on markkinoiden kustannustehokkaimpia IAM-ratkaisuja. Se tarjoaa toimivan kokonaisuuden työntekijän elinkaaren hallintaan, automaatioon ja provisiointiprosessien hallintaan ilman lisäkustannuksia perustoiminnoissa. (miniOrange, 2025.)

5.1.4 Matrix42 (Efecte)

Matrix42 Identity Governance and Administration (IGA) on eurooppalainen IAM-ratkaisu, joka keskittyy identiteettien ja käyttöoikeuksien hallintaan erityisesti automaation ja helppokäyttöisyyden avulla. Se tarjoaa valmiita toimintamalleja, tuotantoonvientiprosesseja sekä laajan integraatiotuen, joiden avulla käyttäjien provisiointi, deprovisiointi ja pääsynhallinta voidaan automatisoida tehokkaasti.

Ratkaisu on suunniteltu nopeaan ja kustannustehokkaaseen käyttöönottoon, ja se skaalautuu joustavasti organisaation koon kasvaessa ilman suuria lisäinvestointeja infrastruktuuriin. Saatavilla on eri tasoisia lisenssipaketteja (Starter, Growth, Enterprise), jotka soveltuvat niin pienille kuin suurille organisaatioille. Natiivi Azure AD -integraatio tekee siitä erityisen sopivan Microsoft-ympäristöissä toimiville yrityksille.

Matrix42 ei julkaise tarkkoja hinnoittelutietoja IGA-moduulilleen. Hinnoittelu määräytyy organisaation käyttäjien lukumäärän perusteella sekä tarvittavien ominaisuuksien ja integraatioiden perusteella. Lopullinen kustannus koostuu valituista moduuleista, käyttöönottotarpeista,

tuesta ja mahdollisista koulutuksista, ja se toimitetaan räätälöitynä tarjouksena Matrix42:n myyntitiimin kautta.

Yhteenvetona Matrix42 IGA tarjoaa Microsoft-keskeisille organisaatioille vahvan vaihtoehdon, joka painottaa nopeaa käyttöönottoa, valmiita automaatioita ja joustavaa skaalausta. Tuotteesta on saatavilla 30 päivän kokeiluversio, jonka avulla voidaan arvioida sen soveltuvuutta ennen käyttöönottoa. (Matrix42, 2025.)

5.1.5 Appmore IAM

Appmore on suomalainen IT-yritys, joka on perustettu vuonna 2012 ja keskittyy liiketoimintasovellusten toteutuksiin ServiceNow-alustalla. Yrityksen tarjoama IAM as a Service on hallinnoitu, pilvipohjainen Identity and Access Management -ratkaisu, joka mahdollistaa skaalautuvan käyttäjäidentiteettien ja käyttöoikeuksien hallinnan ilman omaa paikallista infrastruktuuria.

Palvelu toimii jaetussa ympäristössä, eikä asiakkaan tarvitse tehdä omia laite- tai ohjelmistoinvestointeja. Ratkaisu on käyttövalmis ilman monimutkaisia asennuksia tai räätälöityjä agentteja. Tämä tekee siitä kustannustehokkaan vaihtoehdon erityisesti organisaatioille, jotka haluavat vähentää alkuinvestointeja ja operatiivisia kustannuksia. (Appmore, 2025)

Appmore IAM on suunniteltu erityisesti ServiceNow-asiakkaille, jotka arvostavat keskitettyä ITSM- ja IAM-hallintaa samassa ympäristössä. Ratkaisu hyödyttää erityisesti organisaatioita, jotka haluavat automatisoida käyttäjien elinkaaren hallintaa, vaativat tarkkaa auditointia ja hyödyntävät ServiceNow-alustan prosesseja.

Palvelu toimii täysin hallinnoidusti ilman asiakkaan omaa instanssia ja sisältyy ServiceNow:n SaaS-malliin. Tämän vuoksi erillisiä IAM-lisenssejä tai asennusmaksuja ei tarvitse hankkia muilta toimittajilta. Hinnoittelu perustuu käyttäjämäärään ja valittuihin toiminnallisuuksiin ja määritellään tarjouskohtaisesti. Tarkka kustannus selviää ainoastaan ottamalla yhteyttä Appmoren myyntiin.

Lisäksi Appmore korostaa säästöjä, jotka syntyvät, kun erillisiä HR-, ITSM- ja IAM-ohjelmistolisenssejä ei tarvita. Palvelu kattaa automaattisen provisioinnin ja deprovisioinnin koko käyttäjän elinkaaren ajalta ilman erillisiä moduulikustannuksia.

Yhteenvetona Appmoren IAM-ratkaisu on suunniteltu erityisesti ServiceNow-alustalle. Koska toimeksiantajan nykyinen ympäristö ei perustu ServiceNow-alustalle, käyttöönottaminen edellyttäisi erillistä suunnittelua ja toteutusta. Soveltuvuuden arvioimiseksi tarkemmin voidaan Appmoren verkkosivuilta tilata demoesitys ja pyytää alustava hinnoittelu. (Appmore, 2025.)

5.2 IAM-ratkaisujen kustannusrakenne ja investointitarpeet

Kaikki tarkastellut IAM-tuotteet toimivat pääosin SaaS-mallilla, jossa kuukausimaksu per käyttäjä kattaa ohjelmistolisenssit, palvelininfrastruktuurin ja ylläpidon. Microsoft Entra ID:n lisenssit (P1/P2) voivat sisältyä jo olemassa oleviin Microsoft 365 -tilauksiin, mikä vähentää lisäkustannuksia.

Okta ja miniOrange käyttävät modulaarista hinnoittelumallia, jossa lisätoiminnallisuudet vaikuttavat hintaan. Edullisimmillaan miniOrange tarjoaa käyttöoikeuden perustoimintoihin alle 3 $ / käyttäjä / kk. Okta on kalliimpi, mutta sisältää kattavan ominaisuuskokonaisuuden erityisesti Essentials-tasolla.

Matrix42 IGA ja Appmore IAM hinnoitellaan tarjouksen perusteella. Näissä ratkaisuissa kustannukset määräytyvät käyttäjämäärän, valittujen ominaisuuksien, integraatioiden sekä tarvittavan käyttöönoton ja konsultoinnin mukaan. Molemmat palveluntarjoajat tarjoavat koekäyttömahdollisuuden, jonka avulla ratkaisun soveltuvuutta voidaan arvioida ennen käyttöönottoa. (Taulukko 2.)

Taulukko 2: IAM Hinnoittelut.

IAM-Järjestelmä	Hinnoittelut
Microsoft Entra ID	Päivitys nykyisestä 8.40 € -> 11.20 € = 2.80 € käyttäjä/kuukaudessa, maksetaan vuosittain. Entra Suite tilauksella myös ylimääräisiä ominaisuuksia vaatimusten lisäksi käytettäväksi.
Okta	17 $ käyttäjä/kuukaudessa, maksetaan vuosittain. Myös erillinen 1,500 $ sopimusmaksu vuodessa.
miniOrange	2.5 $ - 3 $ käyttäjä/kuukaudessa, maksetaan vuosittain. Myös kokeiluversio saatavilla.
Matrix42 IGA	Hinnoittelu sovitaan erikseen myynnin kanssa. Käytettävät ominaisuudet sekä käyttäjämäärät vaikuttaa hintaan. Starter lisenssi sisältää vaadittavat ominaisuudet. Kokeiluversio saatavilla.
Appmore	Hinnoittelu sovitaan erikseen myynnin kanssa.

5.3 Teknologian valinnan vaikutukset organisaation tietoturvaan ja toimintaan

Valittu IAM-ratkaisu vaikuttaa merkittävästi organisaation identiteetinhallinnan turvallisuustasoon sekä prosessien automatisointiin. Pilvipohjaiset ratkaisut, joissa on valmiina kertakirjautuminen (SSO) ja monivaiheinen tunnistautuminen (MFA), vahvistavat salasanapolitiikkaa ja vähentävät inhimillisten virheiden sekä tilien väärinkäytön riskiä.

Joustava integraatio Active Directory -infrastruktuuriin mahdollistaa yhtenäisen hallintakonsolin käytön sekä pilvi- että paikallisympäristöissä. Valittu teknologia vaikuttaa myös organisaation kykyyn reagoida muutoksiin: automaattinen provisiointi ja deprovisiointi varmistavat, ettei käyttäjätilejä jää aktiiviseksi työsuhteen päätyttyä. (Kaipiainen, 2024.)

5.4 IAM-ratkaisujen ominaisuuksien vertailu

Valitut IAM-työkalut on valittu vastaamaan toimeksiantajan vaatimuksia, ja ne tarjoavat kaikki tärkeimmät IAM-toiminnot, kuten Single Sign-On (SSO), Multi-Factor Authentication (MFA), Privileged Identity Management (PIM), Privileged Access Management (PAM), Role-Based Access Control (RBAC) ja Attribute-Based Access Control (ABAC). Nämä työkalut tukevat käyttäjien elinkaaren hallintaa, joka oli toimeksiantajan keskeinen vaatimus.

Näiden järjestelmien vertailussa on keskitytty erityisesti seuraaviin kriteereihin: hinnoittelu, käyttöönoton helppous sekä niiden yhteensopivuus toimeksiantajan nykyiseen IT-ekosysteemiin. Nämä kriteerit ovat keskeisiä, sillä ne vaikuttavat suoraan järjestelmän käyttöönottoprosessiin, kustannuksiin ja kykyyn integroitua olemassa olevaan infrastruktuuriin.

Entra ID Suite tarjoaa erittäin kilpailukykyisen hinnoittelun ja on hyvin yhteensopiva toimeksiantajan nykyisen Microsoft-ekosysteemin kanssa. Käyttöönotto on sujuvaa ja nopeaa, koska järjestelmä integroituu suoraan AD:n kanssa, joka on jo käytössä organisaatiossa. Tämä tekee Entra ID:stä erittäin houkuttelevan vaihtoehdon, erityisesti koska se minimoi järjestelmän käyttöönoton ja ylläpidon kustannukset. Lisäksi sen ominaisuudet, kuten SSO ja MFA, parantavat merkittävästi tietoturvaa ja käyttäjäkokemusta.

Okta tarjoaa erinomaiset integraatio-ominaisuudet, erityisesti monenlaisiin kolmannen osapuolen sovelluksiin, mikä tekee siitä erittäin toimivan työkalun monimutkaisessa IT-ympäristössä. Kuitenkin sen hinnoittelu on huomattavasti korkeampi verrattuna muihin vaihtoehtoihin, mikä voi olla merkittävä tekijä pk-yritykselle. Käyttöönotto vaatii teknistä osaamista ja syvällistä ymmärrystä organisaation rakenteesta, mikä voi lisätä alkuinvestointia ja viivästyttää käyttöönottoa. Okta on kuitenkin vahva vaihtoehto, jos yrityksellä on jo laajempia integraatiotarpeita ja se on valmis panostamaan käyttöönoton alkuvaiheeseen.

miniOrange tarjoaa erittäin kilpailukykyisen hinnoittelun ja toimii hyvin nykyisessä organisaation ekosysteemissä, erityisesti Microsoft 365:n kanssa. Kuitenkin järjestelmän käyttöönotto

vaatii erillisen projektin ja huolellisen suunnittelun, koska se tarvitsee integraatioita eri järjestelmiin ja tarvittavat lisäosat. Vaikka hinnaltaan miniOrange on houkutteleva, käyttöönoton kustannukset voivat nousta, mikäli integraatiot eivät ole valmiiksi määriteltyjä. Järjestelmä on kuitenkin kustannustehokas vaihtoehto, mikäli resursseja löytyy käyttää sitä tehokkaasti.

Matrix42:n hinnoittelusta ei ole saatavilla tarkkoja tietoja ilman suoraa yhteydenottoa myyntihenkilöstöön. Tämä tekee sen vertailun osalta hieman epäselväksi, sillä hinnoittelu saattaa vaihdella riippuen valitusta paketista ja järjestelmän laajuudesta. Käytännön toteutuksen kannalta tämä tuo epävarmuutta, ja järjestelmän soveltuvuuden arviointi jää pitkälti tarjoajan määriteltäväksi. Jos Matrix42:n tarjoamat paketit sopivat kuitenkin tarpeisiin, se voisi tarjota kattavan ja joustavan ratkaisun, mutta sen soveltuvuus on vielä epäselvää ilman tarkempaa hintatietoa ja demoja.

Appmore tarjoaa joustavan pilvipohjaisen IAM-ratkaisun, mutta sen hinnoittelusta ei ole vielä tietoa ilman suoraa yhteydenottoa. Järjestelmän soveltuvuus jää avoimeksi, sillä sen täysimittainen arviointi vaatii tarkempia teknisiä demoja ja keskusteluja yrityksen kanssa. Tämä saattaa tuoda lisää viivettä päätöksentekoon, sillä arviointi ja päätöksenteko edellyttävät täydellistä ymmärrystä sekä järjestelmän toiminnallisuuksista että sen kustannusrakenteesta. Appmore on kuitenkin kiinnostava vaihtoehto erityisesti pienemmille organisaatioille, jotka arvostavat joustavuutta ja pienempiä alkuinvestointeja.

Yhteenveto: Kaikki tarkastellut IAM-järjestelmät kykenevät suorittamaan toimeksiantajan vaatimat käyttäjien elinkaaren hallinnan toiminnot, mutta niiden käyttöönotto- ja integrointiprosessit eroavat merkittävästi toisistaan. Käyttöönoton helppous, hinnoittelu ja järjestelmän yhteensopivuus nykyiseen ekosysteemiin ovat keskeisiä valintakriteereitä.

Entra ID Suite erottuu edukseen sen helppokäyttöisyyden ja kustannustehokkuuden ansiosta, kun taas Okta tarjoaa vahvan integraatio- ja turvallisuusratkaisun mutta vaatii suurempia alkuinvestointeja. miniOrange on hyvä vaihtoehto kustannustehokkuuden kannalta, mutta sen käyttöönotto vaatii enemmän resursseja ja suunnittelua. Matrix42:n ja Appmore:n vertailu jää kuitenkin avoimeksi ilman tarkempaa hintatietoa ja demoja, mikä saattaa rajoittaa niiden soveltuvuutta. Näin ollen käyttöönotto- ja integraatioprosessit on huomioitava huolellisesti kunkin järjestelmän osalta, sillä ne vaikuttavat merkittävästi kokonaiskustannuksiin ja käyttöönoton aikarajaan.

5.5 Johtopäätökset

IAM-järjestelmien hinnoitteluvaihtelut (2 € – 16 € / käyttäjä / kk) osoittavat, että organisaation on tärkeää arvioida huolellisesti omat tarpeensa ja budjettinsa ennen järjestelmän valintaa. Microsoftin Entra Suite voi tarjota sujuvan siirtymän ja lisäarvoa IT-hallinnolle, erityisesti

nykyisen Entra ID -integraation pohjalta. Päivitys P2-lisenssistä Suite-versioon on kustannustehokas ratkaisu, sillä lisäkustannus on vain 2,80 € / käyttäjä / kk nykyiseen konfiguraatioon nähden.

Jatkotoimenpiteinä suositellaan Matrix42 IGA:n ja Appmore IAM:n hinnoittelun tarkempaa selvittämistä sekä demoversioiden hyödyntämistä. Näin voidaan muodostaa kattavampi käsitys näiden järjestelmien tarjoamista mahdollisuuksista ja kokonaiskustannuksista.

5.6 Keskeiset löydökset ja suositukset organisaatioille

Tutkimuksen keskeisenä löydöksenä voidaan todeta, että toimeksiantajayritys hyötyy merkittävästi nykyisen Entra ID -ratkaisun käytöstä. Organisaatiolla on jo olemassa oleva infrastruktuuri IAM-toimintojen osalta, mikä tekee Entra ID Suite -lisenssin käyttöönotosta loogisen ja kustannustehokkaan seuraavan vaiheen. Entra ID Suite tarjoaa laajan ominaisuuskattauksen, joka vastaa toimeksiantajan määrittämiä vaatimuksia. Ratkaisu tukee sekä tietoturvan vahvistamista että IT-hallinnon operatiivista sujuvuutta.

Vaikka myös muut tarkastellut IAM-ratkaisut – kuten Okta, miniOrange, Matrix42 IGA ja Appmore IAM – tarjoavat toiminnallisuuksia, jotka voivat täyttää toimeksiantajan tarpeet, niiden käyttöönotto edellyttäisi laajempaa suunnittelua, uusien integraatioiden rakentamista sekä mahdollisesti merkittäviä lisäkustannuksia. Lisäksi näiden järjestelmien käyttöönotto vaatii asiantuntijoiden panosta sekä aikaa vievän projektin läpivientiä. Monet toimittajat tarjoavat kuitenkin konsultointia ja esiselvityspalveluita, joiden avulla voidaan tarkemmin arvioida järjestelmien soveltuvuutta, kokonaiskustannuksia ja käyttöönottoon liittyviä riskejä.

Näin ollen suositeltavin ratkaisu toimeksiantajalle on päivittää nykyinen Entra ID P2 -lisenssi Entra ID Suite -lisenssitasolle. Tämä vaihtoehto hyödyntää jo käytössä olevia resursseja, minimoi käyttöönottoriskiä ja tuo IAM-toiminnot vastaamaan toimeksiantajan vaatimuksia.

5.7 Luotettavuuden ja validiteetin arviointi

Tutkimuksen teoriaviitekehys perustuu ajankohtaisiin ja asiantunteviin lähteisiin, mikä tukee työn luotettavuutta. Käytetyt artikkelit ja teokset ovat tunnettujen asiantuntijoiden kirjoittamia, mikä vahvistaa esitetyn tiedon validiteettia.

Vertailuanalyysissä hyödynnetyt materiaalit ovat pääasiassa yritysten omia dokumentaatioita ja verkkosivuja, joiden avulla järjestelmien ominaisuuksia on voitu vertailla tarkasti. On kuitenkin huomioitava, että erityisesti hinnoittelutiedot voivat muuttua ajan myötä, joten niiden ajantasaisuus on tarkistettava erikseen ennen lopullista päätöksentekoa.

6 Yhteenveto

Tämän opinnäytetyön tavoitteena oli selvittää identiteetin- ja pääsynhallinnan (IAM) järjestelmien roolia ja merkitystä, sekä esittää vaihtoehtoisia IAM-ratkaisuja, jotka täyttävät toimeksiantajan vaatimukset käyttäjien elinkaaren hallinnan tehostamiseksi, tietoturvan parantamiseksi ja IT-hallinnon työkuorman keventämiseksi.

Tutkimus käynnistyi teoriaosuuden laatimisella, jossa tarkasteltiin IAM-järjestelmien keskeisiä ominaisuuksia ja hyötyjä. Teoreettisen viitekehyksen perusteella IAM-ratkaisut parantavat organisaation tietoturvaa, tehostavat IT-hallinnon toimintaa ja lisäävät läpinäkyvyyttä käyttöoikeuksien hallintaan. Ne ovat erityisen tärkeitä nykyajan jatkuvasti muuttuvassa IT-ympäristössä, jossa manuaaliset prosessit ja käyttäjähallinnan virheet muodostavat merkittäviä riskejä.

Vertailuosiosta muodostui tutkimuksen ydin, jossa arvioitiin viittä IAM-ratkaisua: Microsoft Entra ID, Okta, miniOrange, Matrix42 IGA ja Appmore IAM. Kunkin järjestelmän ominaisuudet ja hinnoittelumallit selvitettiin toimeksiantajan tarpeiden pohjalta. Vaihtoehtoisten järjestelmien käyttöönotto edellyttää kuitenkin asiantuntijaresursseja ja huolellista suunnittelua. Monet toimittajat tarjoavat konsultointi- ja tukipalveluita kartoitus- ja käyttöönottoprosessien tueksi, mikä helpottaa kokonaisuuden hallintaa.

Tutkimuksen keskeinen havainto on, että olemassa olevan Microsoft-ympäristön hyödyntäminen ja käytössä oleva Entra ID -ratkaisu tekevät Entra ID Suite -lisenssipäivityksestä kustannustehokkaimman ja käytännössä helpoimman vaihtoehdon toimeksiantajalle. Päivitys mahdollistaa IAM-toimintojen laajentamisen ilman tarvetta uuden järjestelmän täydelle käyttöönotolle.

Opinnäytetyön tavoitteet saavutettiin: IAM-järjestelmien toimintaperiaatteet ja hyödyt kartoitettiin, järjestelmävaihtoehtoja vertailtiin ja toimeksiantajalle sopivin ratkaisu hinnoitteluineen tunnistettiin. Lisäksi työ esittelee vaihtoehtoisia IAM-toimittajia, joiden osalta voidaan tarvittaessa tehdä lisäselvityksiä, erityisesti Matrix42:n ja Appmoren kohdalla.

Lähteet

Niemi, K. (2024). *Identiteetin ja pääsynhallinta (IAM)*. Artikkeli. Viitattu 17.12.2024. https://www.ej-eng.org/index.php/ejeng/article/view/3074/1425

Singh, C., Warraich, J. & Thakkar, R. (2023). *IAM Identity Access Management – Importance in Maintaining Security Systems within Organizations*. Tutkimus. Viitattu 13.2.2024. https://www.ej-eng.org/index.php/ejeng/article/view/3074/1425

Strom, D. (2024). *What is IAM? Identity and access management explained*. Artikkeli. Viitattu 13.2.2025. https://www.csoonline.com/article/518296/what-is-iam-identity-and-access-management-explained.html

Haber, M. J. & Rolls, D. (2020). *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. E-kirja. Viitattu 13.2.2025. https://books.google.fi/books?hl=fi&lr=&id=zfrEDwAAQBAJ...

Vesajoki, K. (2010). *Avaimet tietoyhteiskuntaan*. Lehtiartikkeli. Viitattu 19.2.2025. https://www.yumpu.com/fi/document/read/38546089/guru-1-2010pdf-salcom-group-oy

Filho, W. L. (2025). *The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies*. Tutkimus. Viitattu 20.2.2025. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/76836

Ali, B. & Weng, J. (2025). *Cloud Security and Remediation Strategies: Addressing Security Vulnerabilities in the Digital Age*. Tutkimus. Viitattu 20.2.2025. https://www.researchgate.net/

Mannila, M. (2021). *Kirjallisuuskatsaus opinnäytetyön muotona*. Verkkojulkaisu. Viitattu 5.5.2025. https://energiaa.vamk.fi/artikkelit/osaaminen/kirjallisuuskatsaus-opinnaytetyon-muotona/

Lipska, Z. (2025). *Mitä on vertailuanalyysi ja miten sitä käytetään?* Verkkojulkaisu. Viitattu 5.5.2025. https://firmbee.fi/mika-on-vertailuanalyysi-ja-miten-sita-kaytetaan

Heikkilä, T. (2014). *Tilastollinen tutkimus*. E-kirja. Viitattu 5.5.2025. https://laurea.finna.fi/Record/3amk.268931

Microsoft Learn. (2025). *What is identity and access management (IAM)?* Artikkeli. Viitattu 3.3.2025. https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management

Cayosoft. (2025). *Strengthening Security with Microsoft Entra ID Governance*. Artikkeli. Viitattu 4.3.2025. https://www.cayosoft.com/microsoft-entra/microsoft-entra-id-governance/

Peerspot. (2025). *Microsoft Entra ID Reviews*. Artikkeli. Viitattu 4.3.2025. https://www.peerspot.com/products/microsoft-entra-id-reviews

Microsoft. (2025). *Microsoft Entra plans and pricing*. Artikkeli. Viitattu 4.3.2025. https://www.microsoft.com/en-ie/security/business/microsoft-entra-pricing

Peerspot. (2025). *Okta Workforce Identity Reviews*. Artikkeli. Viitattu 5.3.2025. https://www.peerspot.com/products/okta-workforce-identity-reviews

Okta. (2025). *Okta Pricing*. Artikkeli. Viitattu 10.3.2025. https://www.okta.com/pricing/

miniOrange. (2025a). *Why Migrate from Microsoft Entra ID to miniOrange?* Artikkeli. Viitattu 12.3.2025. https://www.miniorange.com/iam/why-miniorange/microsoft-entra-id-alternative

miniOrange. (2025b). *IAM & CIAM Pricing*. Artikkeli. Viitattu 12.3.2025. https://www.miniorange.com/iam/pricing

Matrix42. (2025). *Matrix42 IGA Solution Summary*. Verkkojulkaisu. Viitattu 17.3.2025. https://publications.matrix42.com/view/660420719/18/

Appmore. (2025). *IAM as a service*. Artikkeli. Viitattu 2.4.2025. https://appmore.com/iam-as-a-service/

Kaipiainen, E. (2024). *Käyttöoikeuksien hallinta Microsoft Entra ID Governance -työkalulla*. Verkkojulkaisu. Viitattu 5.5.2025. https://securecloud.fi/microsoft-entra-id-governance-webinaari/

StealthLabs. (2020). *Why companies need identity and access management?* Verkkojulkaisu. Viitattu 20.2.2025. https://www.stealthlabs.com/blog/why-companies-need-identity-and-access-management/

Microsoft. (2025). *Identity Architecture Design*. Verkkojulkaisu. Viitattu 18.5.2025. https://learn.microsoft.com/en-us/azure/architecture/identity/identity-start-here

Microsoft Learn. (2025). *Zero Trust security in Azure*. Viitattu 19.5.2025. https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust

Microsoft Learn. (2025). *Require MFA for all users with Conditional Access*. Viitattu 19.5.2025.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength

Microsoft Learn. (2025). *Govern the employee lifecycle with Microsoft Entra ID Governance*. Viitattu 19.5.2025 https://learn.microsoft.com/en-us/entra/id-governance/scenarios/govern-the-employee-lifecycle

Microsoft Learn. (2025). *Microsoft Entra ID Governance*. Viitattu 19.5.2025. https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

Opinnäytetyössä on käytetty ChatGPT:tä tekstin kieliasun muokkaamiseen ja tekstin sujuvoittamiseen.

Julkaisemattomat lähteet

Kuviot

Kuvat

Taulukot