Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

JOONA KUUSISTO

Monimenetelmäinen Todentaminen

Cisco Duo: Käyttöönotto ja hallinta

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2022

Monimenetelmäinen Todentaminen
Cisco Duo: Käyttöönotto ja hallinta

Kuusisto, Joona
Satakunnan Ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Kesäkuu 2022
Ohjaaja: Grönholm, Jukka
Sivumäärä: 34
Liitteitä:

Asiasanat: MFA, Todentaminen, 2FA, Duo

Opinnäytetyö MFA-teknologiasta valittiin aiheeksi, koska aihe oli ajankohtainen asiakasyritykselle sillä yritys oli puskemassa Ciscon Duo MFA teknologian käyttöönottoa vakuutusyhtiöiden vaatimusten, sekä tietoturvan parantamisen takia.

Opinnäytetyössä tavoitteena oli opiskella ja tutkia MFA-teknologiaa ja sen perusteita, etuja ja heikkouksia, keskittyen Ciscon Duo MFA-palveluun, ja opiskella sen ja muiden palveluntarjoajien tuotteiden ominaisuuksia, sekä niiden tuomia hyötyjä yrityksille.

Tavoitteet saavutettiin opiskelemalla eri palveluntarjoajien dokumentaatiota, ja tutkien asiaan liittyviä kirjoja, missä kirjoitettiin eri todentamismenetelmien vahvuuksista ja heikkouksista.
Työn tuloksena oli tietämys todentamisteknologian vahvuuksista, tiettyjen todentamistapojen heikkouksista ja tieto hyödystä mitä se tuo tietosuojan parantamisella yrityksille.

Multi-Factor Authentication
Cisco Duo: Deployment and management

Kuusisto, Joona
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
June 2022
Supervisor: Grönholm, Jukka
Number of Pages: 34
Appendices:

Keywords: MFA, Authentication, 2FA, Duo

The subject for the thesis was chosen due to the subject being relevant at the time for the customer company, as they were in the process of trialing Cisco's Duo MFA-application for use within the company, due to requirements from insurance companies as well as to improve security within the company.

The goal for the thesis was to study and learn about MFA-technology, its basics, the strengths and weaknesses, with a focus on Cisco's Duo, and to study Duo and its competitors features and the advantages they bring to the companies.

The goals were achieved by studying the documentation from the different service providers, as well as studying books related to the subject, which contained information regarding the many different types of authentication.
As a result of the work on the thesis, I've gained knowledge about authentication technology, the strengths and weaknesses of different forms of authentication and the advantages it can bring in improving information security to a company.

SISÄLLYS

SYMBOLI- JA LYHENNELUETTELO

2FA

2-Factor Authentication eli kaksivaiheinen todentaminen. Todennus suoritetaan kirjautumisen yhteydessä, pyytäen käyttäjältä lisävahvistus, kuten kertakäyttöinen salasana

MFA

Multi-Factor Authentication eli monivaiheinen todentaminen. Todennus suoritetaan kirjautumisen yhteydessä, pyytäen käyttäjältä kaksi tai useampaa eri todennetta, kuten esimerkiksi sormenjälki ja kertakäyttöinen salasana.

Todentaminen

Käyttäjän henkilöllisyyden vahvistaminen esimerkiksi salasanalla.

Tunnistautuminen

Käyttäjä tunnistetaan esimerkiksi ID’n tai käyttäjätunnuksen perusteella.

OTP

One-Time Password eli kertakäyttöinen salasana. Kirjautumisen yhteydessä pyydetty usein ylimääräinen salasana, joka on aktiivinen vain tietyn aikaa.

1 JOHDANTO

Nykyajan maailmassa tietoturvallisuus on erityisen tärkeää datan suojaamiseksi. Teknologian nopean kehityksen takia tietomurrot yleistyvät ja eri tavat millä aiheuttaa tietomurto lisääntyvät jatkuvasti, josta syystä yksityishenkilöt ja yritykset hakevat jatkuvasti vahvempia tapoja suojata tietojaan.

Yritykset erityisesti voivat joutua hankkimaan vahvempia todentamismenetelmiä suojatakseen dataansa noudattaaksen erilaisia tietoturvalakeja (GDPR) ja esimerkiksi vakuutusyhtiöiden vaatimuksien takia.
Yleisimpiä ja eniten käytettyjä todentamistapoja ovat salasanat. Myös biometrinen todentaminen, sekä erilaiset PIN-koodit, kulkukortit sekä tunnuslauseet ovat yleisiä eri ympäristöissä. (Dasgupta, 2017, luku 1, kohta Introduction)

Nykypäivänä henkilöille ja yrityksille on useita eri vaihtoehtoja turvallisuuden parantamiseksi. Erilaiset niin-kutsutut salasanalompakot kuten LastPass, F-Secure Key ja Keeper sallivat käyttäjän hallinnoida salasanojaan useilla eri sivuilla ja varmistaa niiden eroavuuden ja turvallisuuden. Näiden lisäksi on myös erilaisia todentamisapplikaatioita kuten Cisco Duo, Google Authenticator, Microsoft Authenticator sekä muita, jotka pyytävät käyttäjiään tunnistautumaan applikaation kautta eri sivuille tai tietokoneelle kirjautuessaan, lisäten turvallisuutta.

Cimcorp suorittaa Cisco Duo todentamisohjelman käyttöönoton parantaakseen tietoturvallisuutta yhtiön sisällä sekä tavoittaakseen vakuutusyhtiöiden vaatimuksia.
Ciscon tuote tarjoaa yritykselle laajemman tuen kuin kilpailevat tuotteet, ja se on integroitavissa muiden Cisco tuotteiden kansssa, joita Cimcorp jo käyttää.

2 TODENTAMISTEKNOLOGIA

Todentamisella tarkoitetaan käyttäjän henkilöllisyyden vahvistamista, ja sillä estetään asiaton pääsy eri palveluihin. Tämä eroaa tunnistautumisesta, millä tarkoitetaan käyttäjän tunnusten pyytämistä, jonka jälkeen tämä todennetaan eri menetelmillä, kuten salasanalla.

Useat yritykset ovat myös ottaneet käyttöön niin-sanotun ”Zero Trust”-mallin, eli ”luottamattomuuden periaate”-mallin, vuoden 2020 jälkeen, jolloin pandemian takia suuri osa työntekijöistä rupesivat työskentelemään etänä, joka johti useisiin tietomurtoihin kun yhtiöt eivät olleet valmiita muutoksiin.

Zero Trust mallilla viitataan oletukseen, että jokainen kirjautumispyyntö voi olla mahdollinen tietomurto, joten jokainen pyyntö todennetaan riippumatta siitä, mistä pyyntö on peräisin tai mihin pyyntö on tehty.
(Microsoft, 2022)
Zero Trust perustuu kolmeen pääkohtaan:
Käyttäjän henkilöllisyyden varmistaminen, minimi-käyttöoikeuksien periaate sekä pahimman olettaminen.

Henkilöllisyyden varmistaminen tapahtuu juuri eri todentamismenetelmillä, ja aiemmin mainittuja epäsäännöllisyyksiä, kuten esimerkiksi todentamispyynnön saapuminen ulkomailta, vaikka käyttäjä olisi samana päivänä jo kirjautunut kotimaasta ei hyväksytä.
Minimi-käyttöoikeuksien periaatteella viitataan siihen, että käyttäjille annetaan käyttöoikeudet ja pääsy vain silloin kun niitä pyydetään, ja vain sinne mihin käyttäjän työrooli sen sallii.

Pahimman olettamisella tarkoitetaan ylempänä mainittua oletusta, että jokainen pyyntö voi olla potentiaalinen tietomurto. Näiden estämiseksi kerätään jatkuvasti käyttäjätietoja analytiikan hyödyntämiseksi iskujen estämisessä, ja verkkoja suojataan ja segmentoidaan.

Microsoft jakaa Zero Trust mallin kuuteen osaan: Identiteetti, laitteet, sovellukset, infrastruktuuri, verkko ja data.
Identiteettiä hallitaan juuri todentamismenetelmillä, varmistaen että kirjautumispyynnön tehnyt on oikea henkilö. Jaettuja tai yhdessä käytettyjä tunnuksia ei tule olla.
Päätelaitteita hallitaan yhtiön politiikkojen mukaan, pitäen huolta siitä että laite ja sen sovellukset sekä palomuurit ovat ajan tasalla ja noudattavat asetettua politiikkaa.

Sovelluksiin liittyen pätee laajalti samat säännöt kuin päätelaitteissa, sovellukset tulee pitää ajantasalla, hallita että käyttäjillä ei ole politiikan vastaisia sovelluksia koneilla, vain ainoastaan IT-osaston sallimia. (ns. Varjo-IT) Tulee myös sallia pääsy sovelluksiin mihin käyttäjillä on tarve.
Infrastruktuuri tulee rakentaa yhtiön turvallisuustarpeiden mukaan, varmistaen että resurssit pystytään tunnistamaan ja linkittämään applikaatioihin, sekä poikkeustilanteisiin pitää olla prosessi valmiina ja testattuna.
Verkko tulee segmentoida ja tietoliikenne tulee salata sisäverkossa kuten myös sovellusten välillä.
Data tulee luokitella sekä suojata kryptauksella sekä hallita työpaikalla sillä dataa voi helposti vuotaa muistitikkujen tai sähköpostin kautta.
(Salo, Antti. Elisa, 17.3.2021)

2.1 Todentamistyypit

Todentamistapoja on monia erilaisia, ja neljä erilaista päätyyppiä millä lähestyä sitä, joita voidaan yhdistää keskenään jolloin tuloksena on parempi ja turvallisempi todentamisprosessi. Yritykset pyrkivät valitsemaan ja yhdistämään näitä tyyppejä riippuen käyttäjien määrästä, turvallisuustarpeista, hinnasta ja monista muista syistä.
Tässä luvussa käsitellään nämä neljä päätyyppiä, sekä niihin liittyviä todentamistapoja.

Todentamistyypit ovat seuraavat:

Tyyppi 1: Mitä sinä tiedät – Tajunnallinen tieto
Tyyppi 2: Mitä sinulla on – Omistuksessasi olevat tavarat
Tyyppi 3: Mitä sinä olet – Fysiologiset ja käyttäytymispiirteet
Tyyppi 4: Missä sinä olet – Sijaintiin liittyvät tiedot
(Dasgupta, 2017, luku 1, kohta Types of Authentication Approaches)

Osa palveluntarjoajista on myös ottanut käyttöön salasanattoman todentamisen, tai toisin tunnettuna ”modernin” todentamisen. Tällä viitataan todentamistapaan joka ei vaadi käyttäjältä salasanaa, kuten biometriikka, suojasavaimet ja puhelinapplikaatiot.

Duo kuvailee salasanatonta todentamista helpompana kirjautumisprosessina käyttäjille, sekä tapana parantaa turvallisuutta ja vähentää kuluja yhtiölle.
Security Boulevard sivusto raportoi, että 20-50% kaikista IT-tiketeistä liittyvät, tai ovat pyyntöjä salasanan resetointiin. (Security Boulevard, 2020), ja näiden tikettien käsittely maksaa aikaa ja rahaa yhtiöiden IT-osastoille. Duo perustelee salasanattoman todentamisen käyttöä tuotannolisuuden parantamisella, administraation työtaakan vähentämisellä, sekä salasanoihin liittyvien uhkien eliminaatiolla.
(Duo, 2022)

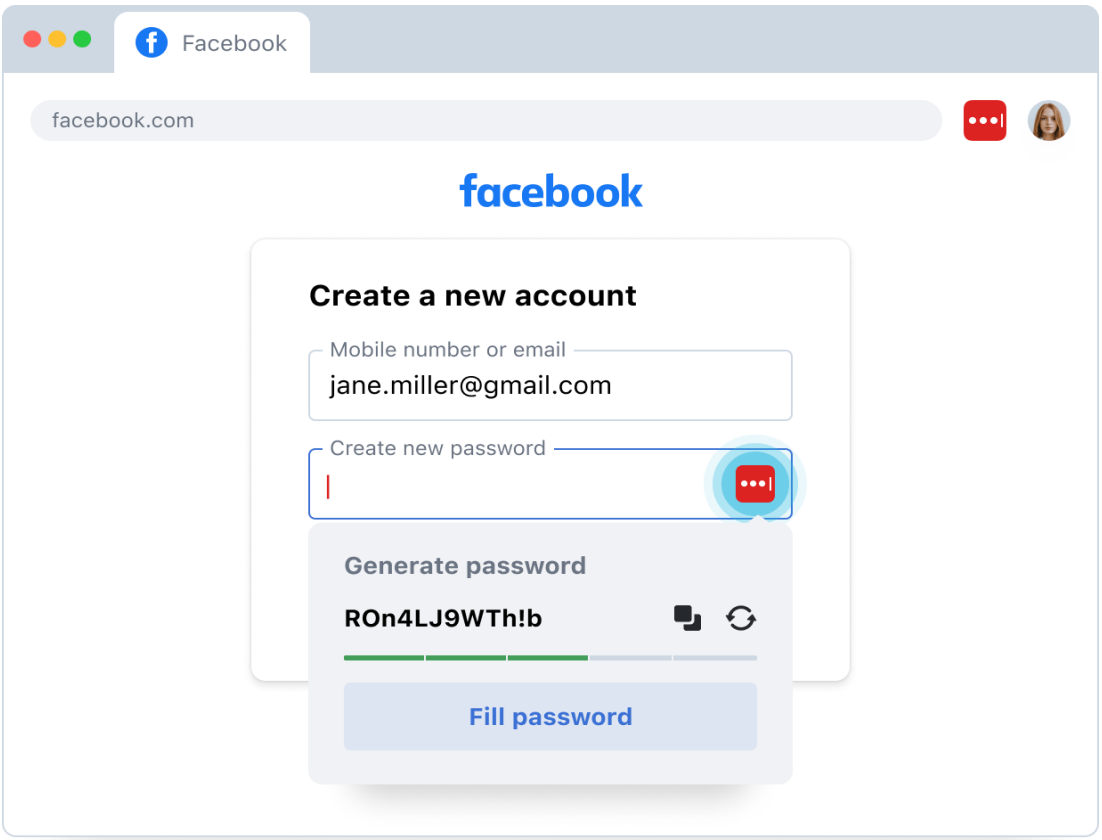
2.1.1 Tyyppi 1: Mitä sinä tiedät

Tyypin 1 todentaminen on kaikken yleisin, liittyen tietoon mitä vain käyttäjä, ja pohjalla oleva tunnistautumisjärjestelmä tietävät, kuten salasanat, koodit, PIN, avainfraasit ja turvakysymykset.

Yksi isoimpia ongelmia ykköstyypin todentamisen kanssa on se, että tietoa tulee helposti jaettua muiden kanssa, jonka avulla on mahdollista esiintyä todellisena käyttäjänä. Toinen iso ongelma on, että todentamistietoja on helppo löytää erilaisten työkalujen ja tekniikoiden avulla. Tyypin 1 todentaminen vaatii myös käyttäjältä paljon muistettavaa, joka johtaa helposti salasanojen toistamiseen joka on myös turvallisuusriski.

Yleisin tyypin 1 todentamistapa on salasana. Yleisesti salasanat vaihtelevat 6 ja 20 merkin pituuden välillä, mistä suurin osa on 6 ja 8 merkin pituuden välillä. Sivut saattavat vaatia pidempiä ja monimutkaisempia salasanoja jotka sisältävät merkkejä, pieniä ja suuria kirjaimia sekä numeroita. Ihmiset kuitenkin pystyvät muistamaan vain niin monta salasanaa ennen kuin vanhat unohtuvat, varsinkin jos salasanan päivitys väliajoin on pakollista. Keskiverto käyttäjällä on noin kuudesta seitsemään eri salasanaa, ja kun päivitys on pakollista käyttäjä helposti muokkaa vanhaa salasanaa lisäämällä erikoismerkkejä tai vaihtamalla kirjaimia. Todellisen pitkän ja satunnaisen salasanan ongelmana on se, että käyttäjän on erittäin vaikea muistaa salasanaa vihjeidenkin avulla, joten useasti nämä tulee kirjoitettua johonkin ylös.
Näistä syistä salasanat ovat helposti hakkerien arvattavissa ja opittavissa, jopa niin helposti että ympäri maailmaa pyritään nyt siirtymään todentamistapoihin joka ei riippuisi ainoastaan käyttäjän antamasta salasanasta.
(Grimes, R. A. (2020). *Hacking Multifactor Authentication*. Sivu 60, Knowledge-Based Authentication)

Näiden ongelmien välttämiseksi, yritykset vaativat usein käyttäjiltään väliajoin salasanan päivitystä, ja jotkut ovat myös sijoittaneet salasanan hallintaohjelmiin, tai niinsanottuihin salasanalompakoihin. Eri hallintaohjelmat voivat myös toimia omana todentamisohjelmana lisäten turvallisuutta, vaatien käyttäjän kirjautuessa esimerkiksi sormenjälkeä, tai vahvistusta tekstiviestillä.
Hallintaohjelmat sallivat käyttäjän tallentavan salasanoja yhteen keskeiseen paikkaan kirjautumisen yhteydessä, ja ilmoittavat käyttäjälle jos samaa salasanaa on käytetty usealla eri sivulla, ja jos salasana on ohjelman mielestä liian heikko, se tarjoaa käyttäjälle satunnaisesti luotua salasanaa toivotun merkkimäärän kokoon.
(LastPass, 2022)



(Kuva 1. Käyttäjän luonnin yhteydessä generoitu satunnainen salasana. LastPass 2022)

2.1.2 Tyyppi 2: Mitä sinulla on

Tyypin 2 todentaminen sisältää eri tapoja vahvistaa käyttäjän henkilöllisyys asioilla mitä käyttäjällä on, kuten henkilöllisyystodistukset, kulku- ja älykortit, suojausavaimet ja puhelimet.

Omistamiseen liittyvä todentaminen lisää turvallisuutta, mutta tässä tavassa on myös heikkouksia riippuen esineestä millä todennus tapahtuu. Esimerkiksi henkilökorttien ovat alttiita väärennöksille, ja myös inhimillisille virheille jos todentamisen suorittaa

henkilö. Yksi tyypin 2 heikkouksista on erilaisten henkilöllisyystodistusten ja laitteiden kuten puhelimien ja suojausavaimien korvaaminen on hidasta ja kallista tapauksissa joissa käyttäjä menettää esineen. Tälläiset todentamisvaihtoehdot vaativat myös käyttäjältä varovaisuutta niiden turvassapitämiseksi.

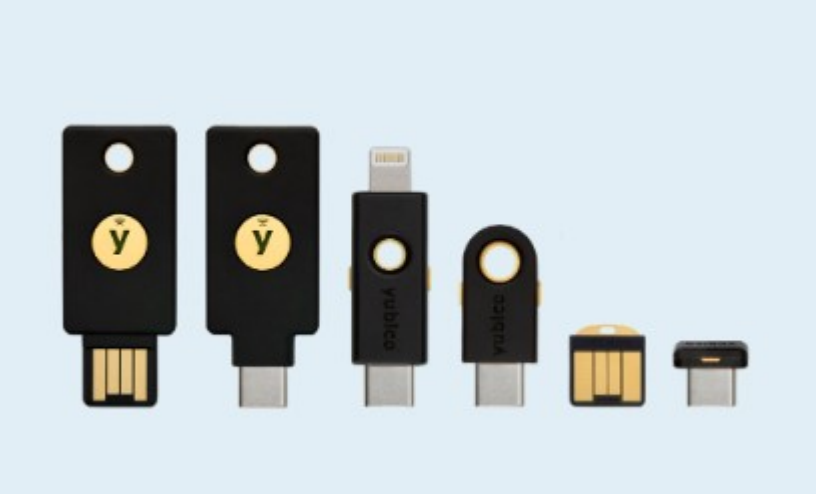
Suojausavaimien hyvänä puolena on, että ne on yleensä tehty tietylle järjestelmälle, joten niiden kopioiminen voi olla erittäin vaikeaa, vaikka niitä on helppo käyttää. Suojausavaimia on myös monia erilaisia, osa niistä voi vaatia biometrista tunnistautumista, yhdistäen tyypin 2 tyyppiin 3, osa voi vaatia fyysistä yhteyttä laitteeseen, tai langatonta verkkoyhteyttä, ja riippuen laitteesta ne voivat myös vaatia tietyn läheisyyden laitteeseen.
(Grimes, R. A. (2020). *Hacking Multifactor Authentication*. Sivu 81, Hardware Tokens)

Yksi yleisimpiä suojausavaimia on kertakäyttöinen salasana (One-Time Password, OTP) laitteet tai applikaatiot. Applikaatioista esimerkkeinä on esimerkiksi Google Authenticator, mihin käyttäjä voi liittää eri käyttäjätunnuksiaan, jolloin kirjautumisen yhteydessä sivusto vaatii käyttäjää kirjoittamaan applikaatiossa näkyvän lyhytaikaisen koodin. Jos käyttäjä ei syötä koodia siihen mennessä kun koodi päivittyy, sivusto hylkää kirjautumisyrityksen ja käyttäjä joutuu käyttämään uutta koodia. Kertakäyttöisissä salasanoissa on myös heikkouksia, sillä koodit eivät ole oikeasti satunnaisia, ja valmistajalla on usein tiedossa laitteiden siemenluku, joten tietomurron tapahtuessa suojausavain voi olla altistunut.
(Yubico, 2022)

(Kuva 2. Esimerkki fyysisestä kertakäyttöisestä salasana laitteesta. Microcosm, 2022)

Cimcorp käyttää Cisco Duon omaa mobiiliapplikaatiota todentamiseen yhtiön puhelimissa. Henkilöillä joilla ei ole työsuhdepuhelinta käyttävät Yubico yhtiön YubiKey 5 NFC suojausavainta. YubiKey avaimet pystytään integroimaan Duoon.

YubiKey 5 NFC avaimessa on mahdollisuus käyttää yksi- kaksi tai monivaiheista todentamista. Yksivaiheinen todentaminen onnistuu yksinkertaisella salasanattomalla ”tap-n-go” menetelmällä, koskettamalla avainta NFC-lukijaan. Tämän voi myös yhdistää salasanaan, luoden avaimesta kaksivaiheisen todentamisen, ja tarvittaessa myös käyttää PIN-koodia, jolloin avain suorittaa monivaiheista todentamista. Avain voidaan myös yhdistää fyysisesti koneen USB-porttiin NFC-lukijan sijaan. (Yubico, 2022)



(Kuva 3. YubiKey 5 sarjan suojausavaimia. Yubico, 2022)

2.1.3 Tyyppi 3: Mitä sinä olet

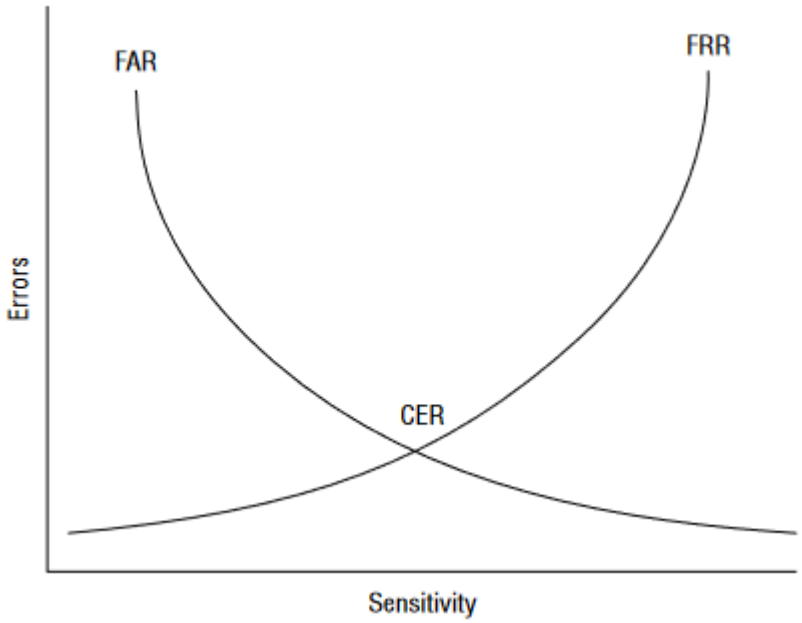
Tyypin 3 todentaminen sisältää asioita mitä käyttäjä on. Uniikkeja asioita henkilölle, kuten biometristä todentamista esimerkiksi sormenjälkien, kämmenjäljen, äänitunnisteen, kasvotunnisteen tai silmäskannauksen avulla.

Koska tämä todentamistyyppi liittyy käyttäjän henkilöllisyyteen, siihen liittyviä todentamistapoja on hyvin vaikea kopioida, ja lähes mahdoton varastaa tai kadottaa.
Biometriseen tunnistautumiseen liittyy myös ongelmia. Isoissa käyttäjäryhmissä tulee aina löytymään henkilöitä kenen biometriikka ei välttämättä vastaa tallennettua päivä päivältä, mistä tahansa syystä.
Käyttäjää luodessa applikaatio pyytää käyttäjältä toivottua biometrista tietoa, ja pyytää jatkossa tätä kun käyttäjä kirjautuu sisään. Esimerkiksi sormenjälki tai kasvotunniste ovat nykyään yleisiä älypuhelimissa.

Biometriikkaa voidaan myös huijata. Roger A. Grimesin kirjassa ”Hacking Multifactor Authenticator”, kirjoittaja kertoo esimerkiksi geelisormien, sormenjälkijauheen toimivan sensorin huijaamisessa ja jopa parin hengähdyksen puhaltaminen sensorille herättää aiemmat sormenjäljet tarpeeksi huijaamaan joitain sensoreita, eli esimerkiksi juuri sormenjälkitunnistimet eivät kuitenkaan ole täydellisiä, vaikka tälläiset huijastavat eivät olisikaan yleisimpiä, sillä ne vaatisivat hyökkääjän fyysisen läsnäolon.
(Grimes, R. A. (2020). *Hacking Multifactor Authentication*. Sivu 325, Attacks Against Biometrics)

Biometrinen todentaminen voi myös olla epätarkka, antaen käyttäjille vääriä positiivisia tai negatiivisia tuloksia.
Väärällä positiivisella tarkoitetaan todentamistulosta joka on määritelty oikeaksi, vaikka tuloksen olisi pitänyt olla virheellinen (False-Acceptance Rates, FAR), ja väärällä negatiivisella tarkoitetaan todentamistulosta joka on määritelty virheelliseksi, vaikka tuloksen pitäisi olla oikea (False Rejection Rates, FRR). On myös olemassa ristikkäisvirhetaso (Crossover Error Rate, CER), missä FAR ja CER virheet ovat yhtäläiset.
Peruskäyttäjä on voinut kokea ainakin vääriä negatiivisia tuloksia yrittäessään avata älypuhelintaan sormenjälkitunnistimella, ja syystä tai toisesta tämä ei ole lukenut käyttäjän sormenjälkeä oikein, vaikka se on aiemmin toiminut, ja käyttäjä on joutunut yrittämään useamman kerran ennen kuin sormenjälkitunnistin lukee sormenjäljen oikein ja avaa puhelimen käyttäjälle.
Biometrisellä tunnistautumisella on paljon suurempi määrä näitä vääriä negatiivisia ja positiivisia tuloksia verrattuna muihin todentamismuotoihin.

Isona ongelmana on myös, että jos biometrista dataa onnistutaan varastamaan, vahinko on pysyvää, sillä biometrisen datan muuttaminen on mahdotonta, verrattuna esimerkiksi varastettuun tai kadotettuun suojausavaimeen, missä tapauksessa avain korvataan uudella, ja vanha mitätöidään.



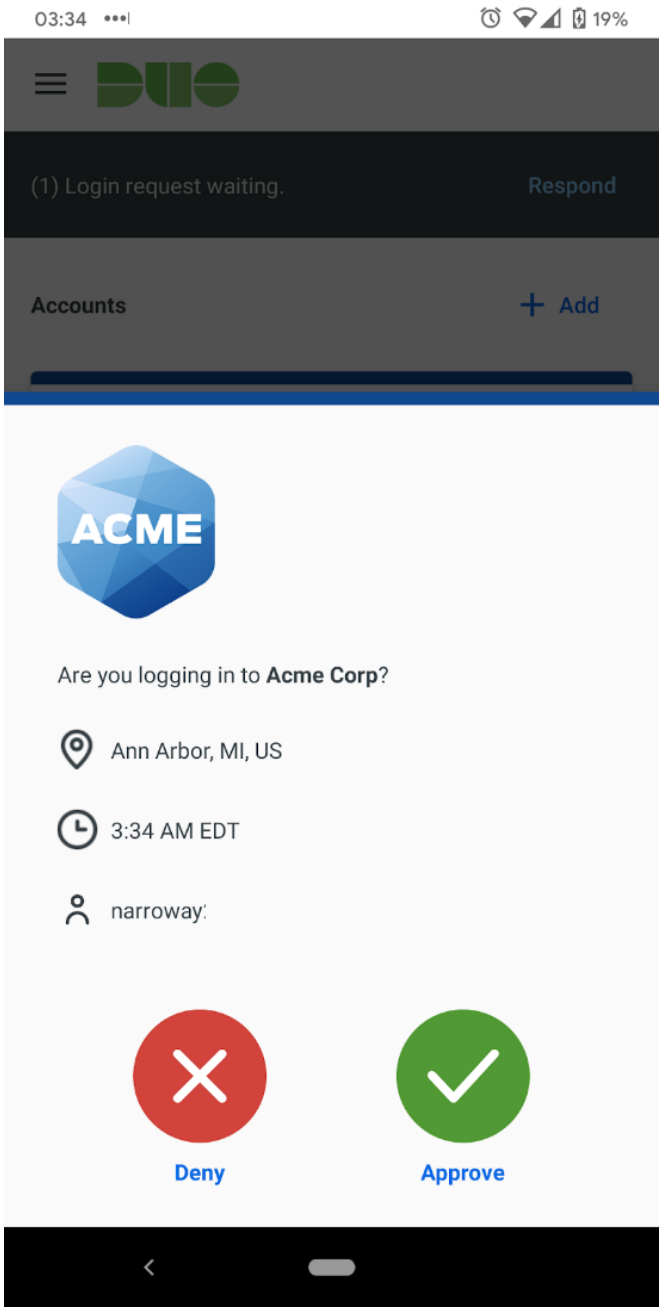
(Kuvio 1. Biometrisen tunnistautumisen virhe-vertailu. Grimes, R. A. (2020). *Hacking Multifactor Authentication*. Sivu 341, Attacks Against Biometrics)

2.1.4 Tyyppi 4: Missä sinä olet

Neljäs ja viimeinen päätyyppi liittyy käyttäjän sijaintiin todentaakseen käyttäjän henkilöllisyyden. Yleisemmin tämä todennetaan GPS signaalin tai IP-osoitteen kautta, ja sijaintiin perustuvaa todentamista käytetään usein yhdessä muiden todentamistyyppien kanssa. Tällä pystytään todentamaan mistä ja milloin käyttäjä on yrittänyt kirjautua sisään.

Sijaintiin perustuva todentaminen on siitä erittäin tehokas, että yhtiö voi esimerkiksi

määrätä kirjautumiset sallituiksi vain tietyistä sijainneista, ja altistunut käyttäjä huomataan helposti esimerkiksi siitä, että käyttäjä itse on kirjautunut yhtiön tiloissa, tai kotoaan etätyöskennellessä, ja tuntia myöhemmin toinen kirjautumispyyntö tulee eri maasta, jolloin toinen näistä kirjautumisista on väärä, ja käyttäjä tulee lukita.



(Kuva 4. Esimerkki Duo Push-ilmoituksesta, joka sisältää käyttäjän sijainnin ja kirjautumisen kellonajan. Duo, 2022)

3 MFA PALVELUNTARJOAJAT JA NIIDEN VERTAILU

Cisco Duo, Microsoft Azure AD Multifactor Authentication, LastPass MFA, Okta MFA

Kuten aiemmissa luvuissa on kuvailtu, MFA-palvelut auttavat asiakkaitaan parantamaan tietoturvallisuuttaan huomattavasti. Tästä johtuen, eri palveluntarjoajia on useita, ja kilpailu näiden palveluntarjoajien välillä on kovaa.
Tässä luvussa vertaamme osaa suosituista MFA-palveluista keskenään, ja listaamme niiden hyviä ja huonoja puolia, sekä eri palveluiden tarjoamia todentamistapoja.

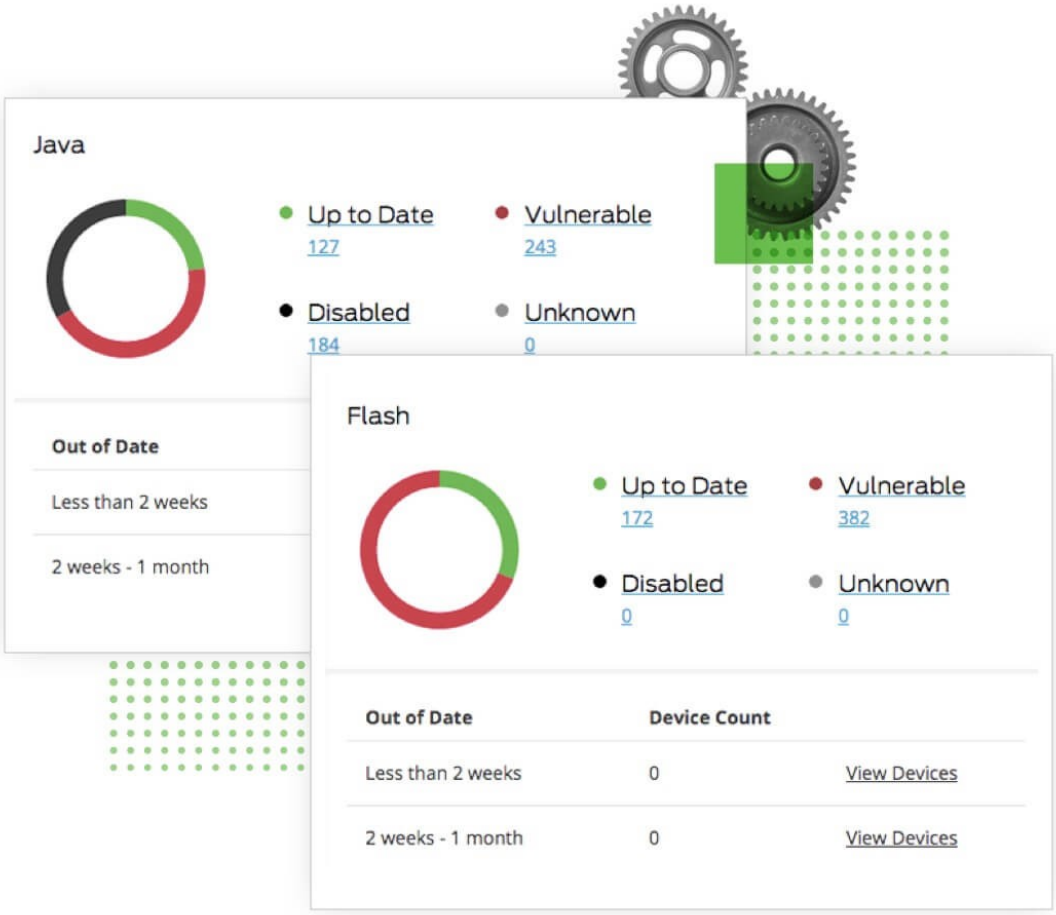
3.1 Cisco Duo

Duo Security on Ciscon Lokakuussa 2018 ostama MFA-palveluita tarjoava yhtiö, jonka seurauksena Duo Security sai nimen Cisco Duo.
Osana Ciscon tuotesarjaa, Duo on myös mahdollista integroida muihin Ciscon omiin tuotteisiin, joka oli yksi syistä miksi Cimcorp valitsi Duon yhtiön MFA-ratkaisuksi.

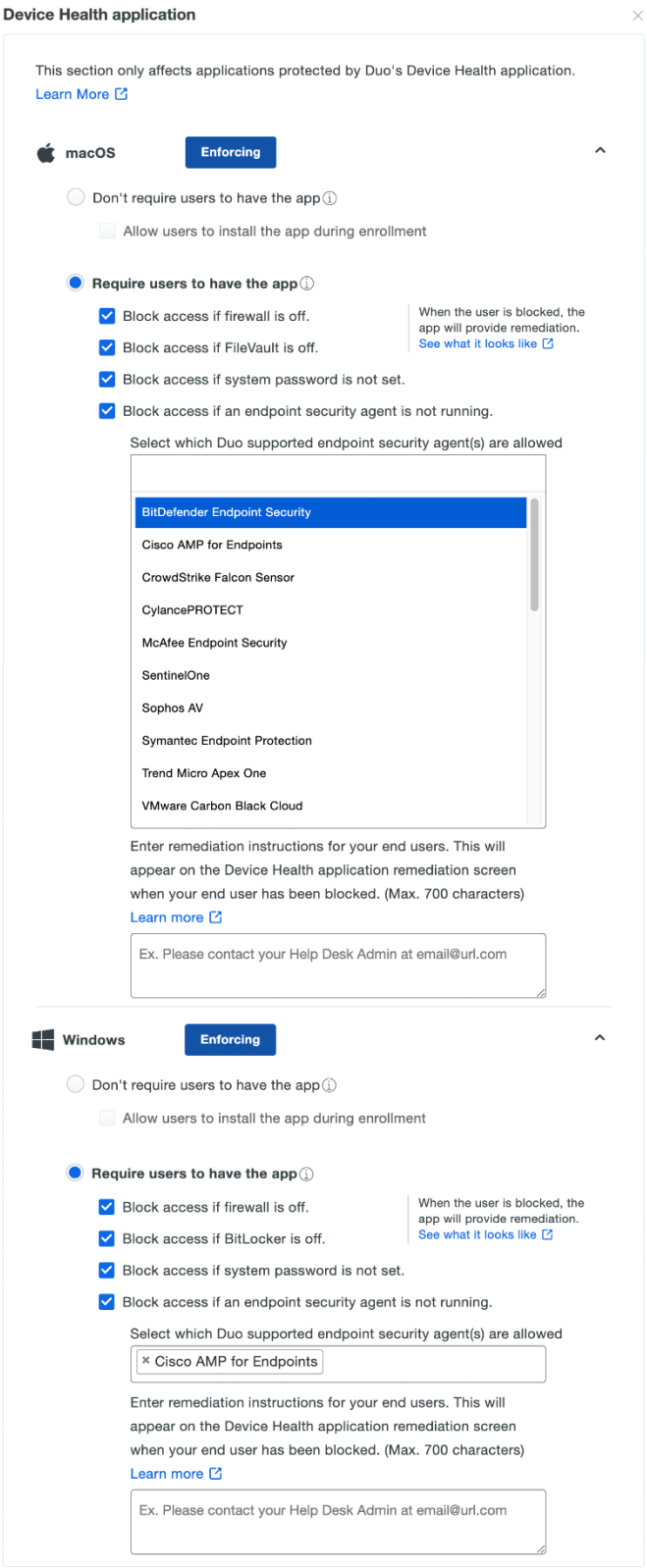
Duolla pystyy todentamaan henkilön usealla eri tavalla. Kirjautumisen yhteydessä lähetettävä push-ilmoitus (kuva 4) on yksi näistä, jonka voi yhdistää myös esimerkiksi biometriikkaan, jolloin sijainnin ja ajan lisäksi, ilmoitus vahvistaa henkilön identiteetin esimerkiksi sormenjäljellä.

Duon lisäksi on mahdollisuus asentaa käyttäjien koneisiin Duo Device Health Application, ja tämä voidaan myös asettaa vaatimukseksi käyttäjien kirjautumiselle, eli käyttäjältä jolla applikaatiota ei ole, evättäisiin kirjautuminen.

Duo sallii ylläpitäjien seurata Device Health Applicationin avulla käyttäjien laitteiden tilaa, kuten asennettua päivitystasoa, biometriikkaa ja palomuuria. Tätä voidaan käyttää estämään käyttäjien kirjautumisen eri paikkoihin, jos laite ei ole ajan tasalla. (Duo, 2022)



(Kuva 5. Esimerkkinä käyttäjien Java ja Flash tilan seuranta. Duo pystyy ilmoittamaan monellako käyttäjällä nämä ohjelmat eivät ole ajan tasalla. Duo, 2022)

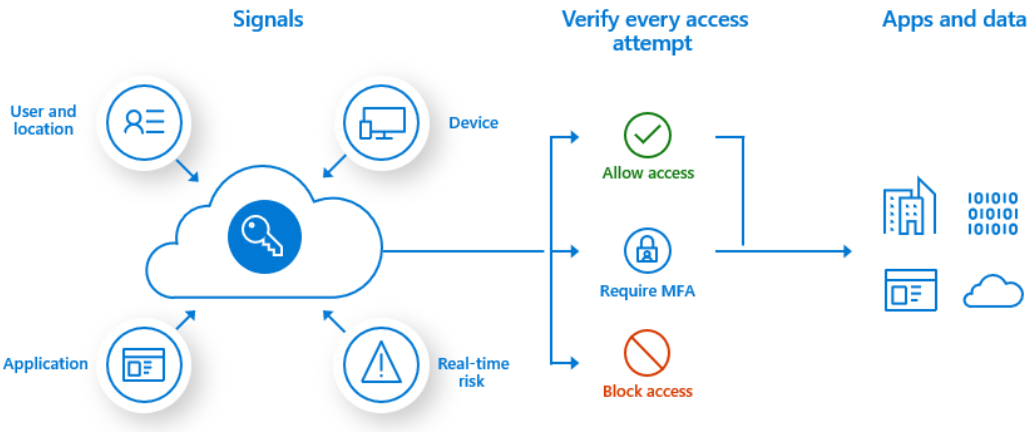


(Kuva 6. Esimerkki Device Health Applicationin eri asetuksista. Duo, 2022)

3.2 Microsoft Azure AD Multifactor Authentication

Microsoftin Azure AD vaatii käyttäjältä kaksi tai useampaa todentamismenetelmää, ja sillä pystytään myös lisäämään turvallisuutta käyttäjän salasanan uudistamispyynnölle. Eri todentamiskeinoja Azure AD'lla ovat muun muassa Microsoftin oma todentamisapplikaatio, Windows Hello, FIDO2 suojausavaimet, OATH hardware- ja software todisteet, OTP't, sekä tekstiviestit ja puhelut.

Azure AD mahdollistaa myös identiteetti suojan aktivoinnin, jolloin todentaminen reagoi tiettyihin tapahtumiin, kuten tuntemattomasta IP-osoitteesta kirjautuminen, mahdottomat matkustusetäisyydet, haavoittuvista laitteista kirjautuminen sekä tuntemattomista sijainneista kirjautuminen, ja näitä voidaan hallita käyttäjien tai ryhmien mukaisesti.
Yksi toinen mahdollisuuksista on jos käyttäjän salasana ilmestyy Microsoftin tai Microsoftin kumppanien tietoon altistuneena salasanana, voidaan asettaa näille käyttäjille pyyntö luoda uusi salasana todentamisen yhteydessä ennen kuin käyttäjä voi jatkaa kirjautumista.
(Microsoft, 2022)

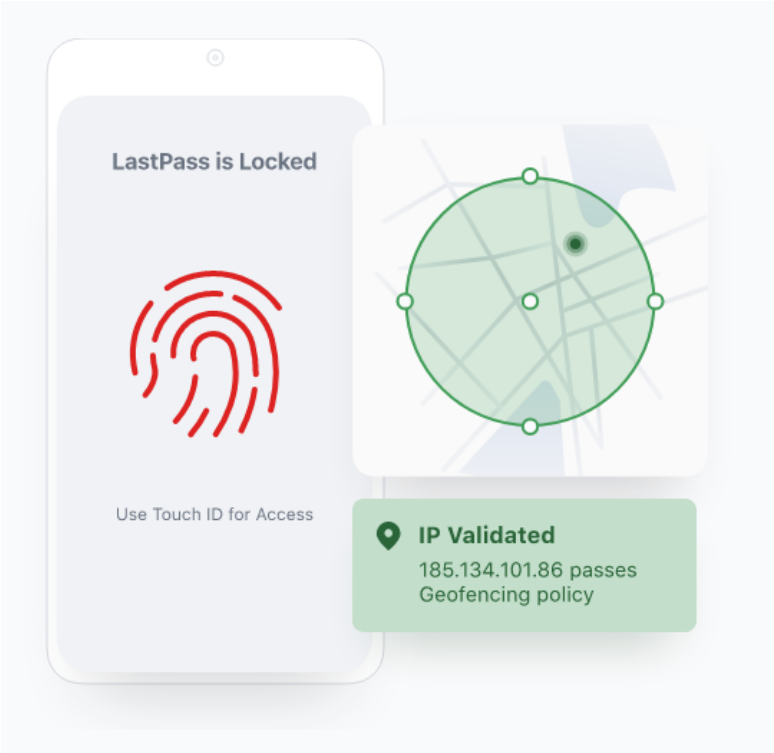


(Kuva 7. Kaavio MFA'n toiminnasta, Microsoft Azure AD. Microsoft, 2022)

3.3 LastPass MFA

LastPass toimii salasananhallinta ja todentamisohjelmien tuottajana.
LastPass MFA sisällyttää adaptiivisen todentamisen, käyttäen henkilön sijaintia ja/tai IP-osoitetta, sekä kirjautumisaikaa, yhdessä biometristen vaihtoehtojen kanssa käyttäjän todentamiseen. Ohjelma tukee myös salasanatonta todentamista, joka vähentää IT-tuen työmäärää.
Todentamistapoina ovat push-notifikaatiot, biometriikka, kuten sormenjäljet ja kasvotunniste, äänitunniste, SMS koodit ja OTP't.

LastPass MFA tukee myös integraatiota eri käyttäjätietokantoihin, kuten AD, Azure AD, Okta ja OneLogin.
Ylläpitäjät pystyvät myös näkemään esimerkiksi MFA-palveluun liittyneiden määrän, ja palvelun käyttöprosentin. Muita mahdollisuuksia on erilaisten sääntöjen määrittäminen, joka sallii ylläpitäjien rajata pääsyä tiettyihin IP-osoitteisiin, tai vain tiettyinä aikoina.
(LastPass, 2020)



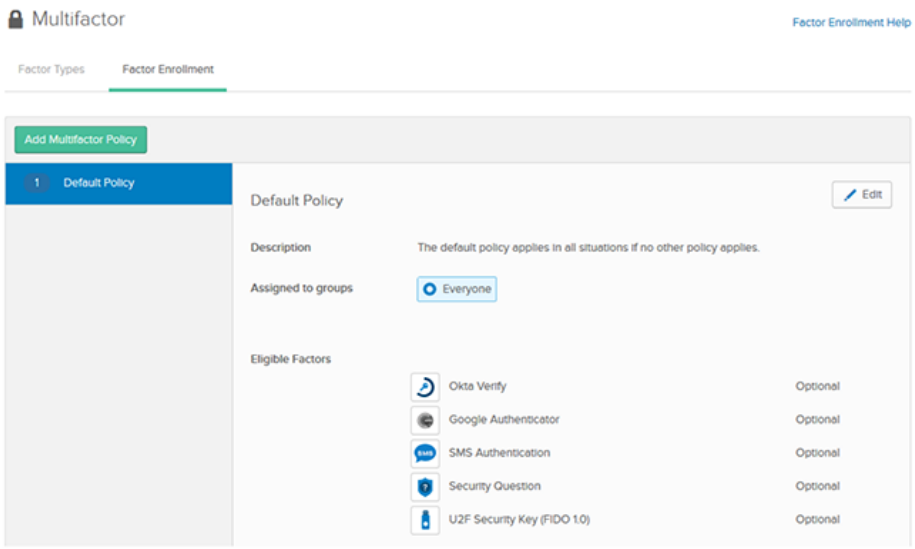
(Kuva 8. Esimerkki LastPass MFA-palvelun tarjoamasta IP-osoite rajauksesta. LastPass 2022)

3.4 Okta

Okta on vuonna 2009 perustettu tietoturvayritys, joka tarjoaa MFA palveluiden lisäksi myös käyttäjätietokanta-palveluita, käyttäjien hallintaa, työnkulun hallintaa sekä yritysmarkkinointi integraatiota.

Okta tukee salasanatonta kirjautumista ja MFA vaihtoehtoina on biometriikka, joka tukee myös kolmannen osapuolen biometriikkalaitteita toivottaessa, Push-notifikaatiot applikaation kautta, salasanat, suojausavaimet, SMS, puhelut ja sähköposti.
Okta sallii MFA vaihtoehtojen hallinnan, antaen käyttäjille mahdollisuuden poistaa tietyt todentamistyypit käytöstä.

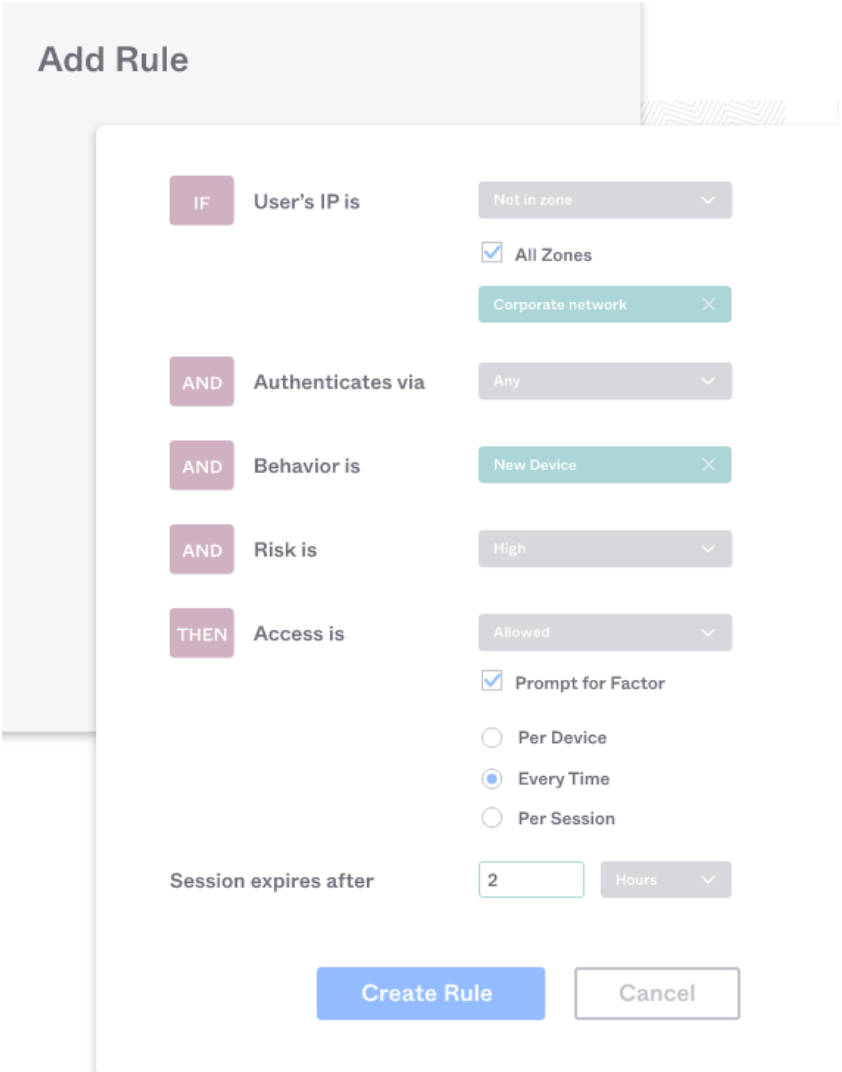
Oktan MFA-palvelu tarjoaa myös adaptoivaa todentamista, ja pystyy myös automaattisesti torjumaan pyynnöt epäilyttävistä IP-osoitteista, käyttäen Oktan omaa tietokantaa missä on listattuna osoitteet joista hyökkäyksiä on yritetty aiemmin.
Palvelu tarjoaa myös ylläpitäjille tavan hallita eri asetuksia, kuten heikompien MFA vaihtoehtojen poistamista käytöstä kuten SMS, Email, äänitunniste ja turvallisuuskysymykset, joka parantaa turvallisuutta eri hyökkäyksiä vastaan.



(Kuva 9. Esimerkki Oktan MFA vaihtoehtojen hallinnasta. Okta, 2022)

Muita vaihtoehtoja on sallita käyttäjien raportoida suoraan epäilyttäviä kirjautumisyrityksiä laitteeltaan, jotka näkyvät suoraan ylläpitäjien työpöydällä, ja istuntoajan hallinta.

Ylläpitäjät voivat myös määritellä riskitasoja kirjautumisiin, ja jos kirjautuminen vastaa asetettuja riskitasoja, se automaattisesti evätään.



(Kuva 10. Esimerkki Oktan riskienhallinnan paneelista. Okta, 2022)

Okta tukee myös tiettyjä kolmannen osapuolen MFA tarjoajia, kuten Duo, Google ja YubiKey

Palvelu tarjoaa myös käyttäjille itsepalvelun rekistöröitymiselle MFA käyttäjäksi ja salasanan palauttamiseksi, joka säästää aikaa käyttäjiltä sekä IT-osastolta.

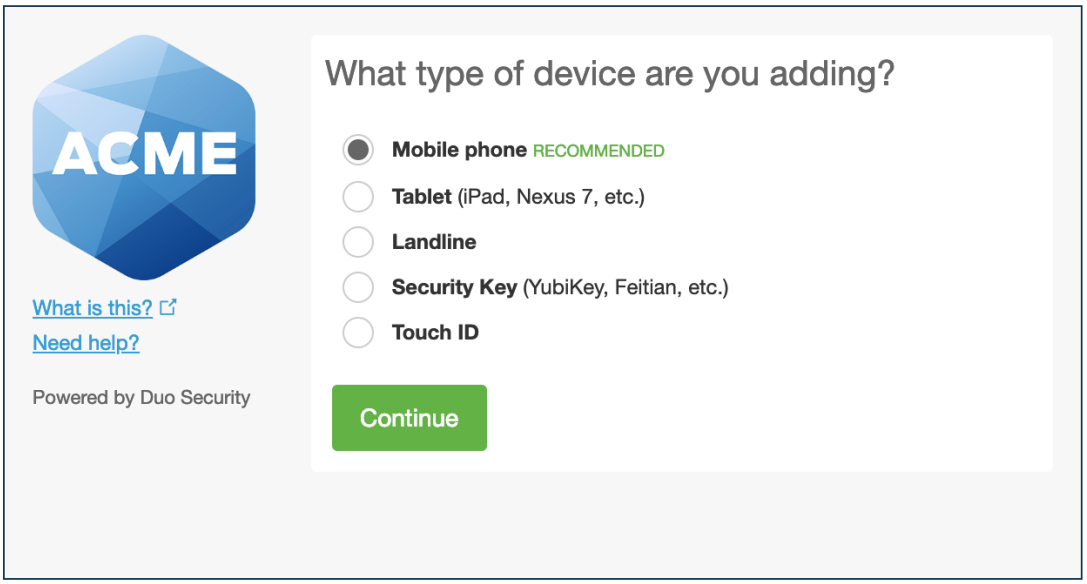
(Okta, 2022)

4 CISCO DUO

Cisco Duo on Cimcorpin valitsema MFA-palveluntarjoaja, joten sen ominaisuuksia tullaan käymään tarkemmin läpi tässä luvussa.

4.1 Ominaisuuksia käyttäjille

Duo tukee käyttäjien itse-ilmoittautumista Duo Self-Enrollment ominaisuuden avulla. Ylläpitäjät lähettävät käyttäjille linkin, jota kautta henkilö voi asentaa Duon päätelaitteelleen, eri asetusten mukaisesti, vahvistaen lopuksi henkilön laitteen joko soitolla tai tekstiviestillä. Riippuen asetuksista, lisäyksen jälkeen käyttäjä voi myös mahdollisesti muokata nykyistä laitettaan tai lisätä uuden laitteen todentamista varten.

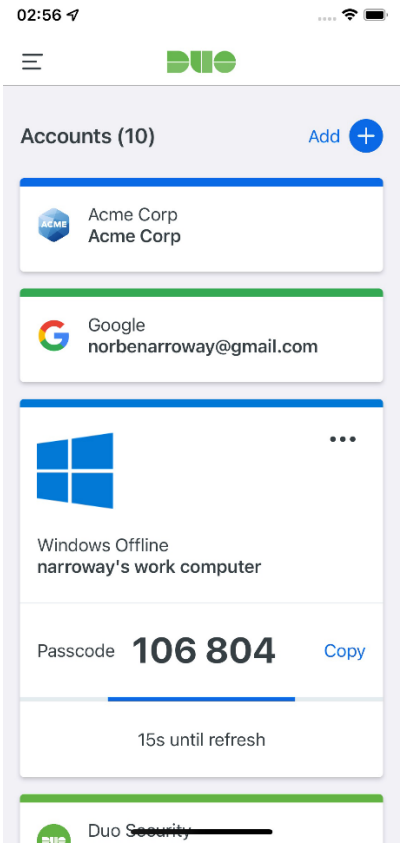


(Kuva 11. Duo kysyy käyttäjältä asentamisvaiheessa laitetyyppiä. Duo 2022)

Muita mahdollisuuksia käyttäjälle on varmuuskopion tekeminen duolla suojatuista tileistä, joka voidaan palauttaa samalle laittelle tai siirtää tarpeen mukaan uudelle laitteelle. Nämä tilit deaktivoidaan automaattisesti vanhalla laitteella jos varmuuskopio tuodaan uuteen laitteeseen.

Myös Offline-pääsy on mahdollista jos ylläpitäjät sallivat sen, mahdollistaen kirjautumisen suojattuun laitteeseen tai tiliin ilman verkkoyhteyttä. Tässä tapauksessa

normaalin Push-notifikaation tai muun todentamistavan sijaan, Duo tarjoaa käyttäjälle 6-numeroisen tunnuksen kirjautumiseen, joka vaihtuu uuteen 30-sekunnin välein. Toisena vaihtoehtona on käyttää vaatimuksia täyttävää suojausavainta.



(Kuva 12. Esimerkki Offline-kirjautumisesta. Duo, 2022)

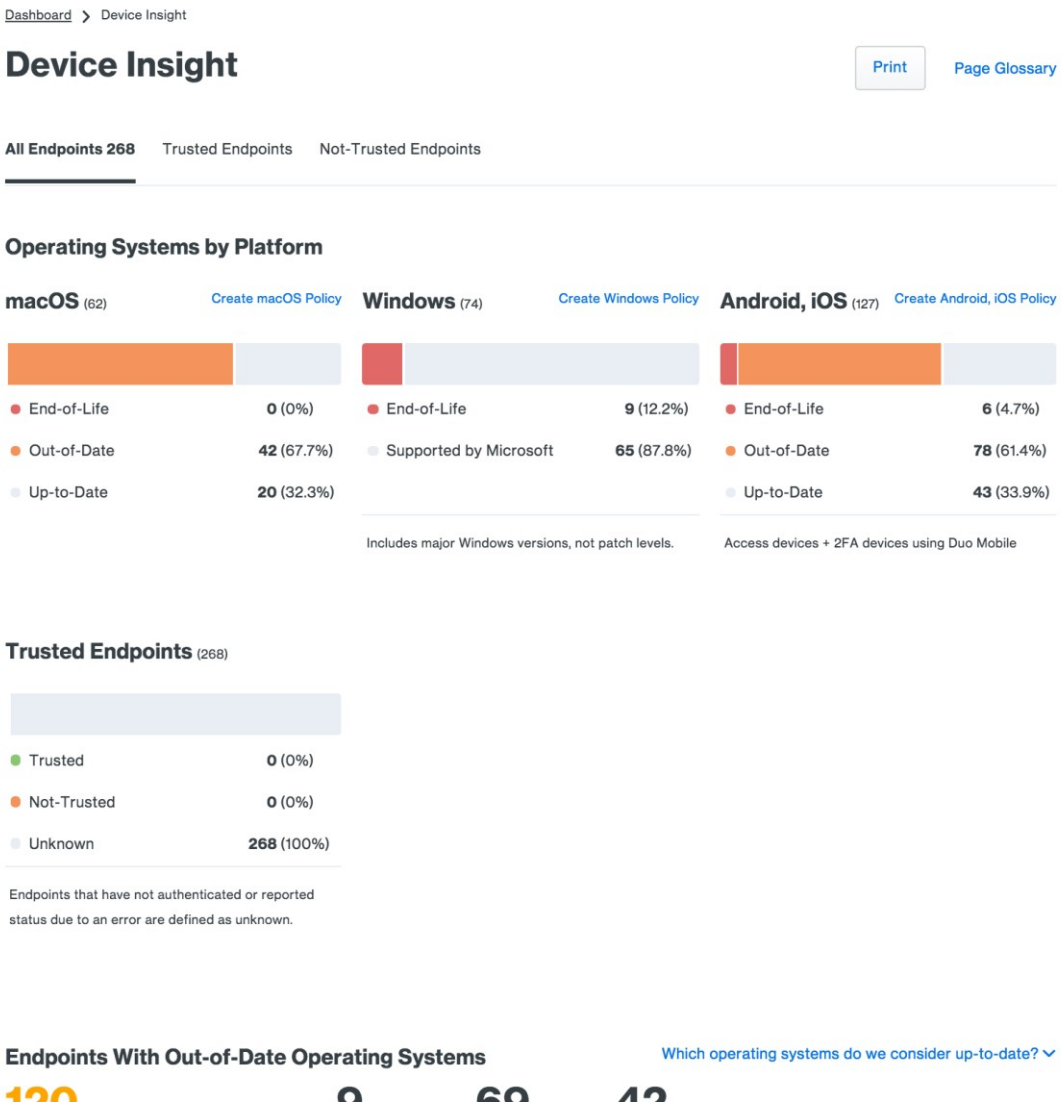
Ylläpitäjän määrittelemänä, aiemmin mainittu Device Health Application ilmoittaa myös käyttäjille eri sovellusten tilanteesta, varoittaen käyttäjää jos ne eivät ole ajan tasalla.

4.2 Ominaisuudet ylläpitäjille

Ylläpitäjien ominaisuuksista puhuessa käytämme Duo Beyond-tason palveluvaihtoehtoja

Ylläpitäjille tarjotaan useita vaihtoehtoja käyttäjien- ja laitteidenhallintaan Duon ylläpitäjäpaneelin kautta. Ylläpitäjät pystyvät määrittelemään duon politiikkaa käyttäjä- tai ryhmätasolla, sallia käyttäjien ohittavan todentamisen, tarkistella

päätelaitteiden käyttöjärjestelmien ja ohjelmien päivitystasoa ja käyttömääriä, ja asettaa riskiprofiileja.



(Kuva 13. Device Insight näkymä, jossa ylläpitäjät näkevät käyttäjien laitteiden käyttöjärjestelmät ja niiden päivitystasot. Duo, 2022)

Ylläpitäjillä on käytössään voimakkaita työkaluja taatakseen tietoturvan voimassaolon. Yllä olevassa kuvassa näkyy käyttöjärjestelmätiedot, ja niiden päivitysaste. Device Insight sivu antaa myös tietoa puhelimen suojaominaisuuksista, kuten onko ruudun lukitus päällä, tai onko biometriikka käytössä.

Tämän tiedon perusteella ylläpitäjä pystyy esimerkiksi päivittämään politiikkaa vaatimaan vaikka viikon sisällä koneen olevan päivitetty, tai pääsy evätään Duo-

todentamisen yhteydessä. Myös tiettyjen käyttöjärjestelmien, laitetyyppien ja selainten täysi blokkaus on mahdollista.

Sivulla näkyy myös jos laitteelle on tehty jotain valmistajan vastaisia asetuksia, kuten puhelimen suojauksen murtaminen, niinkutsuttu ”jailbreak”. Tällä tarkoitetaan laitteen suojausten kiertämistä, jolloin käyttäjä voi asentaa laitteelleen ohjelmia joita valmistaja ei ole hyväksynyt, ja sallia käyttäjälle täydet oikeudet laitteeseen, mikä ei normaalisti olisi mahdollista. Tämä aiheuttaa myös suuren tietosuojariskin, sillä kolmannen osapuolen sovellukset eivät ole valmistajan testaamia ja takaamia.

(Kaspersky, 2022)

5 DUO KÄYTTÖÖNOTTO CIMCORPILLA

Duon käyttöönotto Cimcorpilla on aloitettu vuonna 2021, tavoitteena saavuttaa vakuutusyhtiöiden asettamat vaatimukset, kutsumalla testiryhmä käyttämään Duoa laitteillaan. Testaus aloitettiin Windows-kirjautumisen yhteydessä vaaditulla todentamisella käyttäjiltä. Osalle käyttäjistä jaettiin myös YubiKey suojausavaimia.

Käyttöönottoa nopeutettiin vuonna 2022, Venäjän aloittaman sodan seurauksena, yhtiön tietoturvan parantamiseksi, jolloin Duo-ohjelmaa ruvettiin asentamaan ja vaatimaan kaikilta työntekijöiltä. Asennus suoritettiin ryhmissä, ja käyttämällä Ciscon Meraki-ohjelmaa jonka kautta Duon Device Health Application asennettiin käyttäjien koneille.

Vaatimuksina onnistuneelle kirjautumiselle Cimcorpilla on Device Health Applicationin vaatimusten täyttö (Päivitykset, virus-suoja & käyttöjärjestelmä ajan tasalla), laite tunnistetaan hyväksytyksi Cimcorpin laitteeksi ja että henkilöllisyys on todennettu käyttäjänimen, salasanan ja MFA'n kautta. Yleisimmin tällä hetkellä on käytössä henkilöstön työpuhelimiin asennettu Duo applikaatio, mutta suojausavaimia on myös käytössä.

Isoimpina haasteina tällä hetkellä on ollut Pohjois-Amerikan osalta työntekijöiden paluu takaisin toimistolle etätöistä, jotta tarvittaessa asennukset sekä suojausavaimet saataisiin toimitettua henkilöille, joilla ei ole työpuhelinta.
Cimcorpilla on suunnitteila työsuhdepuhelin jokaiselle työntekijälle tulevaisuudessa, joka tulee myös toimimaan yhtenä todentamislaitteena.
Duoa laajennetaan Cimcorpin eri palveluihin jatkuvasti, ja tavoitteena on vaatia todentaminen työntekijöiltä jokaiseen palveluun tulevaisuudessa.

5.1 Cisco Meraki

Cisco Meraki tarjoaa asiakkailleen Meraki Systems Manager ohjelmistoa, joka sallii päätelaitteiden hallintaa etänä, sallien IT-osaston puskea päivityksiä tai asennuksia käyttäjien koneille tarvittaessa.
Meraki Systems Manager on myös käytettävissä mobiililaitteiden päivittämiseen.
Cimcorp käynnisti laajalti Systems Managerin käyttöönoton vastauksena Heinäkuussa alkaneelle sodalle, parantaakseen tietosuojaansa mahdollisilta hyökkäyksiltä, ottaen huomioon sinä aikana olleen etätyösuosituksen, jonka takia suuri osa työntekijöistä töimi etänä.
(Cisco Meraki, 2022)

Duo Device Health Application asennettiin Meraki System Managerin avulla työntekijöiden laitteisiin.

5.2 Duo Device Health Application

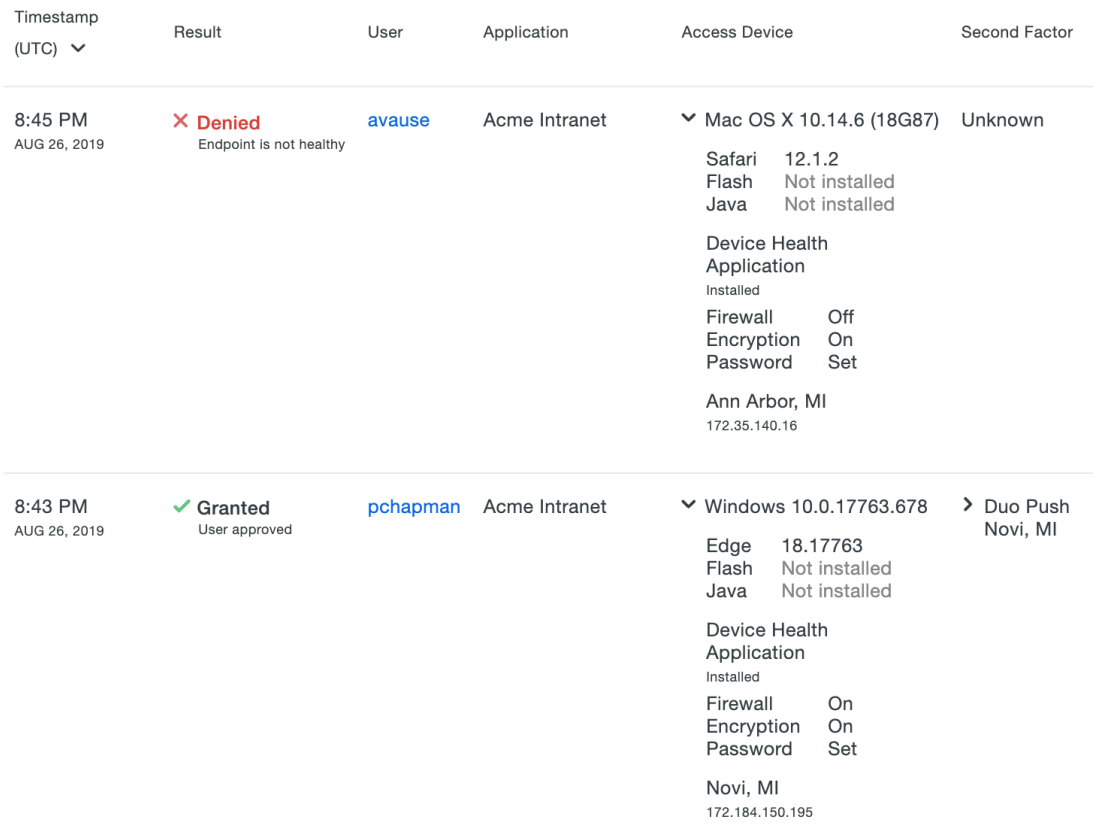
Device Health Application antaa ylläpitäjille enemmän tapoja hallinnoida politiikkaa, rajaamalla käyttäjien pääsyä kun heidän laitteensa eivät vastaa vaadittuja turvallisuusmääritteitä.

Health Applicationilla on kolme pääkomponenttia:

1. Duo politiikat jotka vaikuttavat pääsyoikeuksiin riippuen laitteen tilasta.
2. Applikaatio windows ja macOs järjestelmille, joka vahvistaa laitteen turvatilan todentamisen yhteydessä.
3. Ylimääräiset päätelaitteen tiedot jotka ovat näkyvissä Duon ylläpitäjäpaneelissa

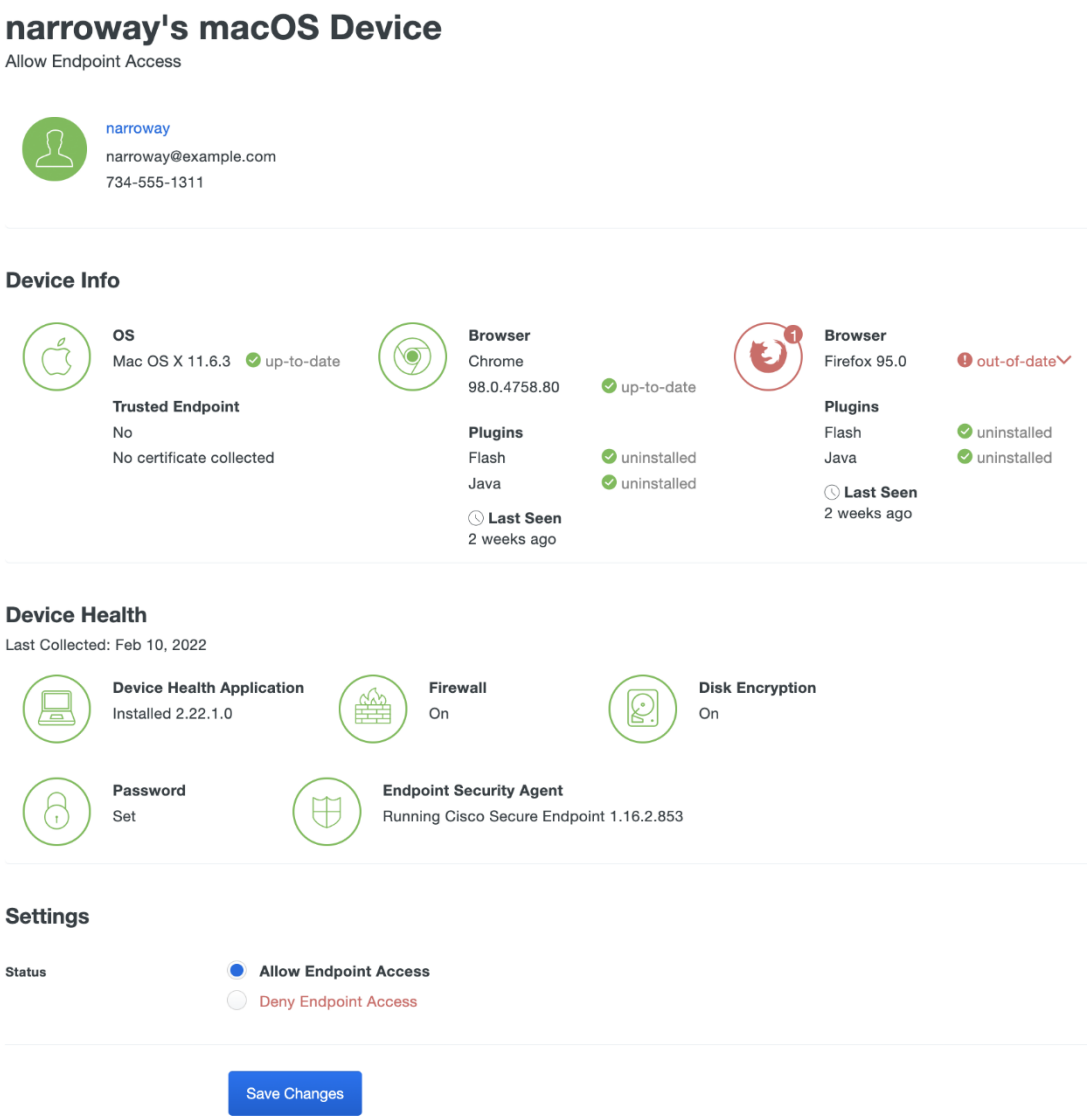
Tilanteessa, missä käyttäjä ei vastaa asetettuja turvallisuusmääritteitä, Duo tarjoaa käyttäjälle askeleita, millä korjata tilanne määritteiden mukaiseksi.
Health Applicationin voidaan asettaa vaikuttamaan macOS tai Windows-päätelaitteisiin, tai molempiin ja sillä on kolme toimintatapaa jotka vaikuttavat pääsyvatiimuksiin. (Kuva 6.)

Applikaatio pystyy myös vahvistamaan käyttäjältä hyväksytyn virussuojan olemassaolon päätelaitteelta ennen kuin Duo sallii käyttäjän sisäänpääsyn.



(Kuva 14. Esimerkki logitiedoista, ylemmän käyttäjän pääsy on evätty, koska palomuuri ei ole päällä. Duo, 2022)

Hallintapaneelissa ylläpitäjät pystyvät näkemään listan tiedoista joita health application kerää, tarjoten mahdollisuuden filteroida käyttöjärjestelmän ja/tai version mukaan, ja ilmoittaa myös turvallisuuspuutteista, ja kertoo myös syyn kuten pois päältä oleva palomuuri. Ylläpitäjät pystyvät myös tarkastelemaan yksittäisiä laitteita tarkemmin.



(Kuva 15. Esimerkki yksittäisen laitteen tiedoista hallintapaneelissa.)

6 YHTEENVETO

Opinnäytetyön aikana olen tutustunut eri todentamismenetelmiin ja suojauskeinoihin, joka on ollut mielenkiintoinen tehtävä jonka kautta olen oppinut paljon.
Työn aikana olen myös pyrkinyt miettimään todentamisen käyttöönottoa peruskäyttäjien näkökulmasta, ja miten siitä tehtäisiin mahdollisimman vaivatonta.
Potentiaalinen salasanaton todentaminen voisi tulevaisuudessa olla tähän hyvä vaihtoehto, joka nopeuttaisi kirjautumista ja vähentäisi salasanojen kanssa tappelemista, käyttäjiltä sekä IT-osastolta.

Olen käyttänyt aikaa Duon dokumentaatioon tutustumiseen ja seurannut käyttöönottoa ja todentamisen laajenemista eri Cimcorpin käyttämiin palveluihin. Tavoitteena on tulevaisuudessa olla tiukemmin mukana Duon käyttöönotossa ja pyrkiä laajentamaan osaamistani liittyen tietoturva-asioihin.

LÄHTEET

Dasgupta, D. a., Roy, A. a. & Nag, A. a. (2017). *Advances in User Authentication* (1st ed.2017.). Springer International Publishing.

2MasterIT. https://2masteritezproxy.skillport.com/skillportfe/assetSummaryPage.action?assetid=RW$1517:_ss_book:138110#summary/BOOKS/RW$1517:_ss_book:138110

Grimes, R. A. (2020). *Hacking Multifactor Authentication*.

Security Boulevard (11.2.2020) Eliminate Password Reset Tickets to Increase Profits

https://securityboulevard.com/2020/02/eliminate-password-reset-tickets-to-increase-profits/

Microsoft (2022) Evolving Zero Trust

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Salo, Antti. 17.3.2021 – Zero Trust – Nollaluottamus modernin turvallisen ICT-ympäristön perustana

https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/

Duo (2022) Passwordless Authentication

https://duo.com/solutions/passwordless

LastPass (23.5.2022) How LastPass works.

https://www.lastpass.com/how-lastpass-works

Yubico (23.5.2022) What is a One-Time Password (OTP)

https://www.yubico.com/resources/glossary/otp/

One-Time Password (OTP) Tokens

https://www.microcosm.com/it-security-hardware/oath-otp-authentication-tokens#tokens

Yubico (23.5.2022) YubiKey 5 Series

https://resources.yubico.com/53ZDUYE6/as/q3uxbe-6n9olc-9ywi4w/YubiKey_5_Series_Product_Brief.pdf

Cisco Duo (23.5.2022) Duo Mobile on Android

https://guide.duo.com/android

Cisco Duo (3.6.2022) Duo Device Health Application

https://duo.com/docs/device-health

Cisco Duo (3.6.2022) Device Visibility

https://duo.com/product/device-trust/device-visibility

Microsoft (3.6.2022) Azure AD Multi-factor Authentication

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

LastPass (6.6.2022) Multifactor Authentication

https://www.lastpass.com/products/multifactor-authentication

Okta (6.6.2022) Disable Weaker MFA factors in factor enrollment policies

https://help.okta.com/en/prod/Content/Topics/Security/healthinsight/strong-factors.htm

Okta (6.6.2022) About Multifactor Authentication

https://help.okta.com/en/prod/Content/Topics/Security/mfa/about-mfa.htm

Okta (6.6.2022) Okta End-User Experience

https://www.okta.com/okta-end-user-experience/

Duo (6.6.2022) Duo Authentication for Windows Logon

https://guide.duo.com/rdp#offline-access

Duo (6.6.2022) Enrollment Guide

https://guide.duo.com/enrollment

Duo (9.6.2022) Duo Administration – Device Insight

https://duo.com/docs/insight

Kaspersky (9.6.2022) What is Jailbreaking

https://www.kaspersky.fi/resource-center/definitions/what-is-jailbreaking

Meraki, Cisco (9.6.2022) Systems Manager

https://meraki.cisco.com/products/systems-manager/

Cisco Duo (9.6.2022) Duo Device Health Application

https://duo.com/docs/device-health