Webinaari: Liiketoimintatietojen turvaaminen Microsoftin pilvipalveluiden avulla

Matti Väliniemi, Jukka Niiranen

23.10.2019

Äänessä

Matti Väliniemi
Senior System Consultant
+358 50 568 6475
matti.valiniemi@elisa.fi

https://bloggerz.cloud/

Jukka Niiranen
Product Lead
+358 44 555 5029
jukka.t.niiranen@elisa.fi

https://survivingcrm.com/

Aamun aiheita

- Microsoft tietoturvayrityksenä
- Liiketoimintasovellusten tietoturvaominaisuudet: Dynamics 365
- Pääsynhallinta ja vahva tunnistautuminen
- Tiedon luokittelu ja suojaaminen
- Pilvisovellusten käytön seuranta ja hallinta
- Yhteistyökumppanien identiteetinhallinta

Microsoft = tietoturvayritys

Liiketoimintaympäristön muutokset

Uudet mahdollisuudet

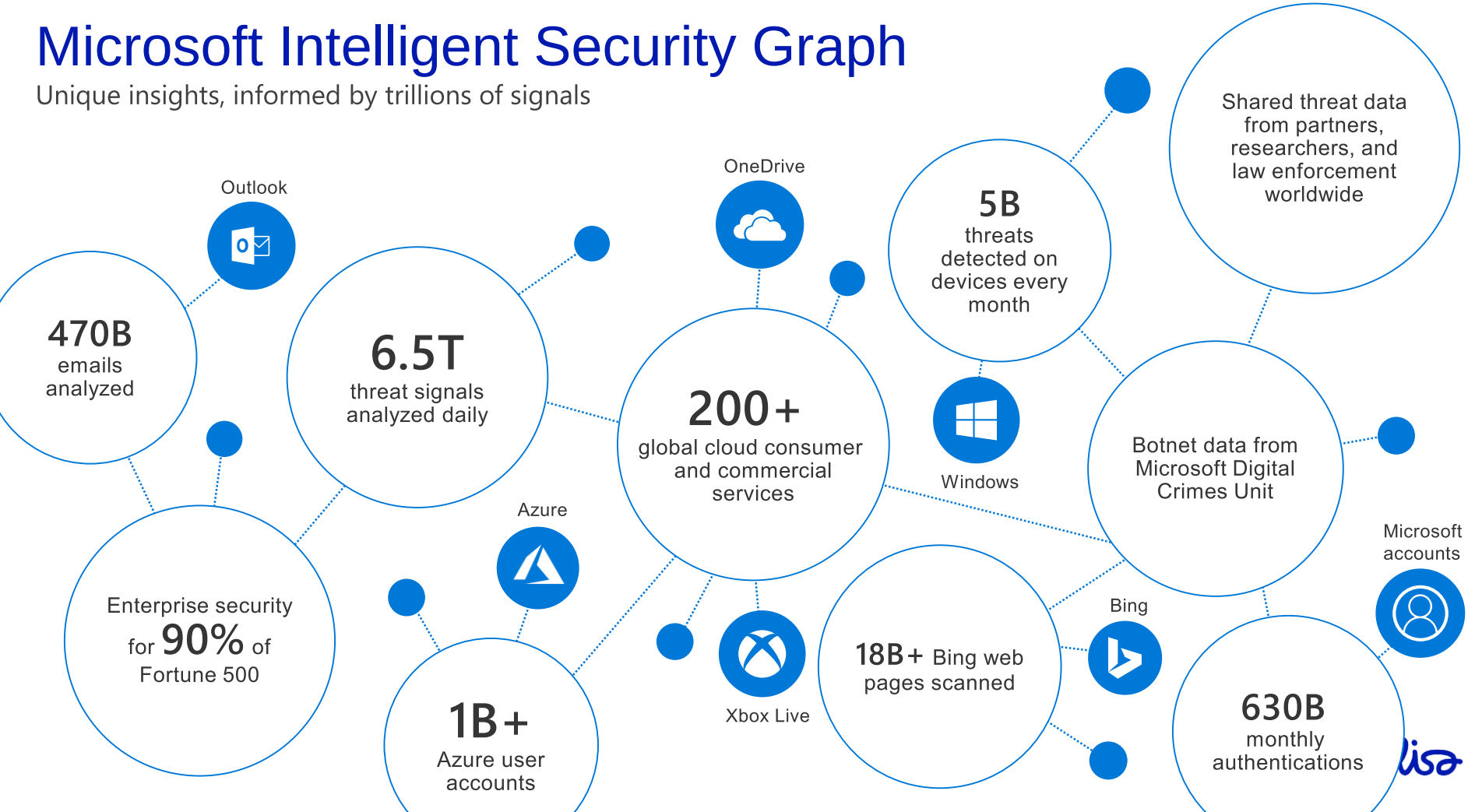
- Jokainen organisaatio on nyt teknologiaorganisaatio
- Työtä tehdään sijainnista riippumatta, yhä monipuolisemmalla sovellus- ja laitekirjolla
- Dataa on kaikkialla ja sitä syntyy kaikista älykkäistä laitteista

Uudet uhat

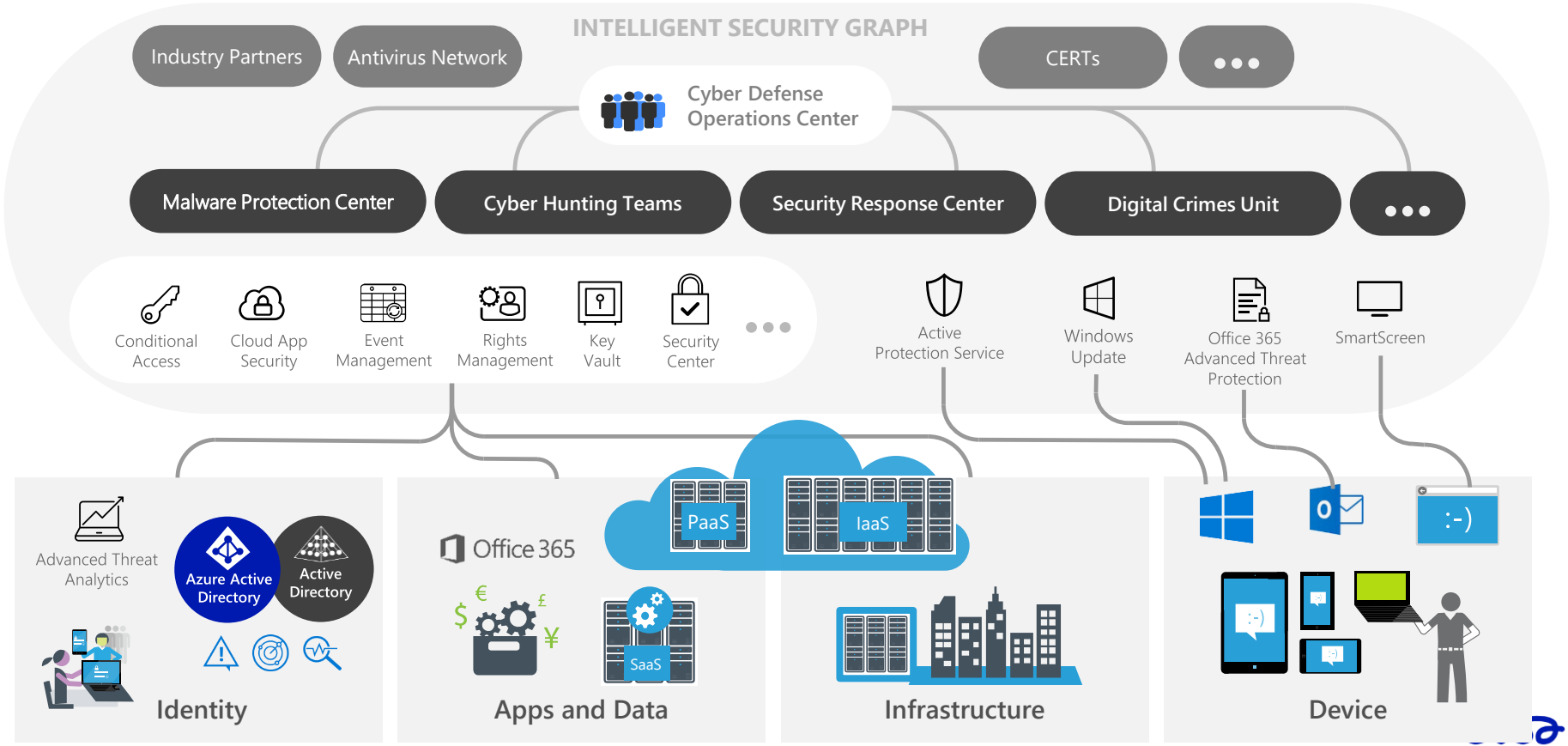
- Identiteettiin kohdistuvat hyökkäykset ovat kolminkertaistuneet viimeisen vuoden aikana
- Perinteiset tietoturvatyökalut eivät ole pysyneet muutoksen perässä
- Pelkät asiantuntijat eivät riitä kyberturvan kasvaviin tarpeisiin

Microsoft Intelligent Security Graph

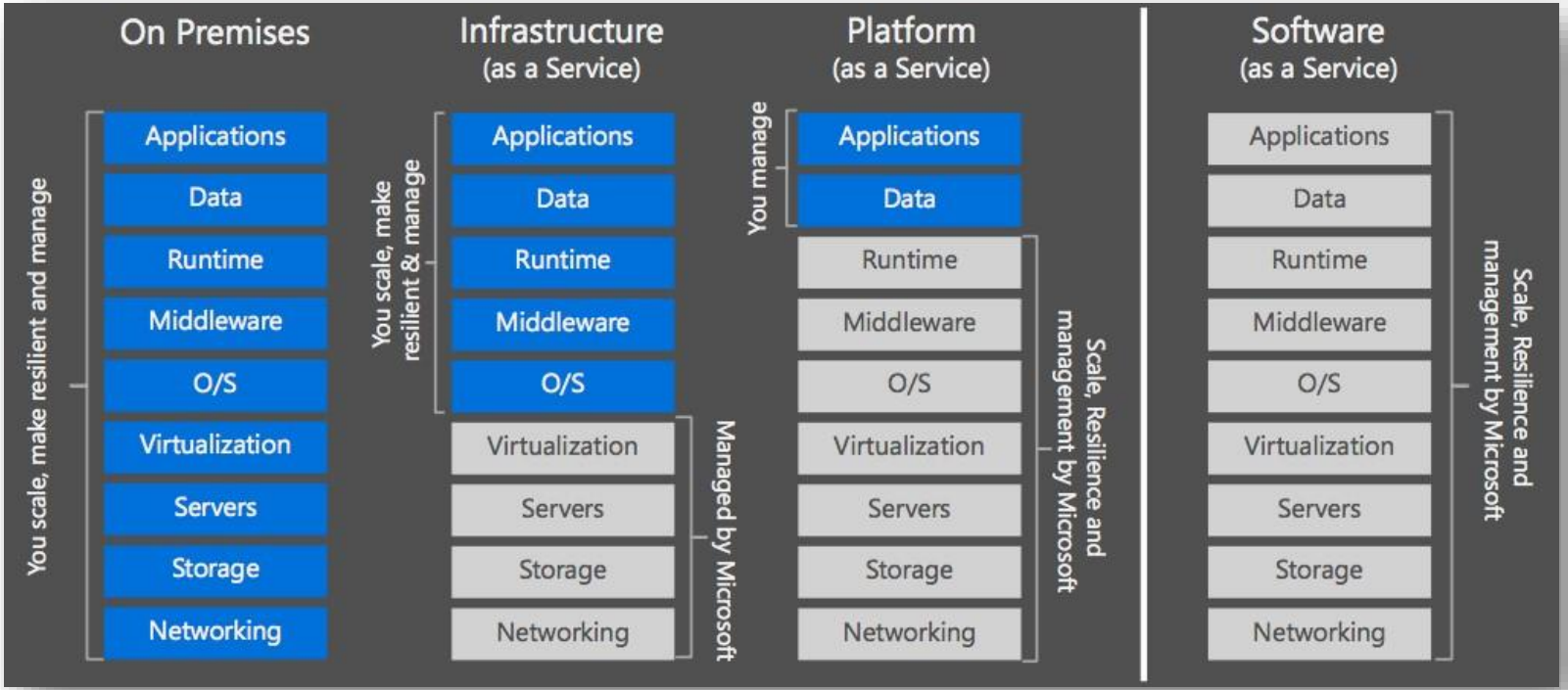
Unique insights, informed by trillions of signals



Miten Microsoft suojaa sinua ja ympäristöjäsi

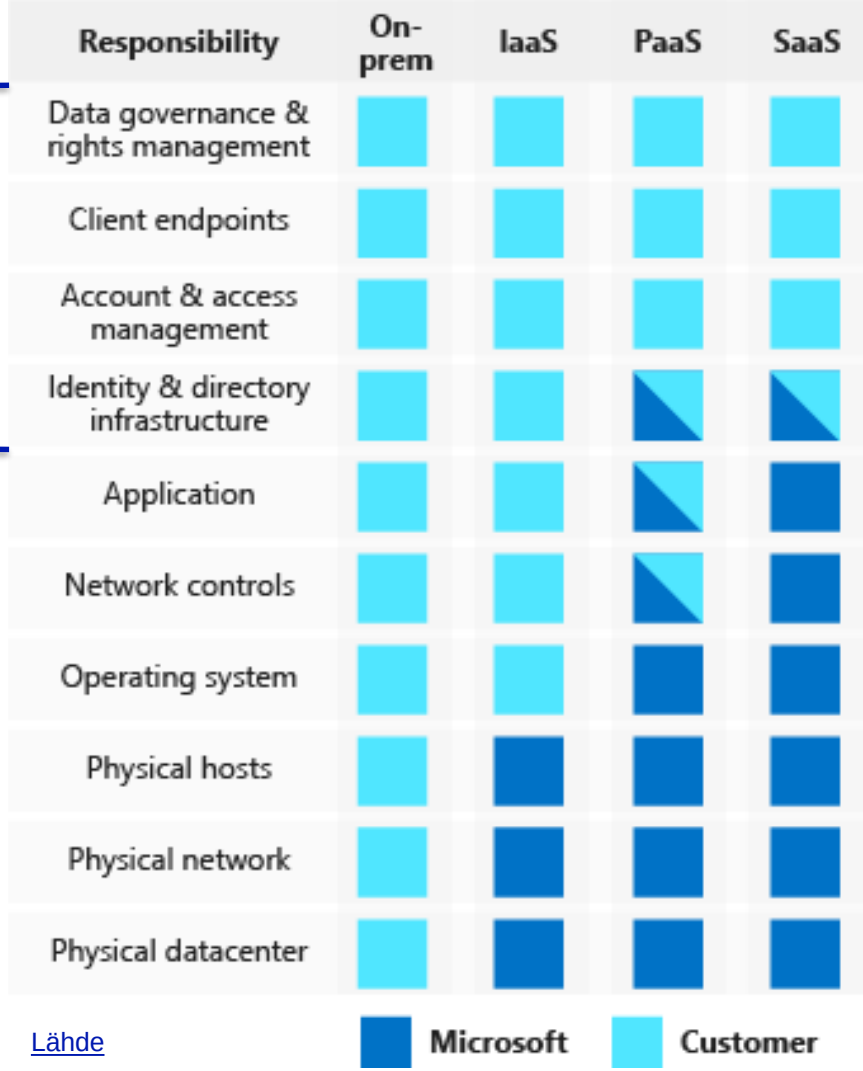


Hallintavastuu: On-premises > IaaS > PaaS > SaaS



Tietoturvavastuut

- Myös SaaS-mallilla hankittavissa liiketoimintasovelluksissa on merkittävää tietoturvavastuuta asiakkaan puolella
- Data, päätelaitteet, käyttäjähallinta, identiteetti vaativat kukin omat tarkkaan mietityt hallintakäytäntönsä
- …Ja tietoturvan toteutukseen kehitetyt omat SaaS-palvelunsa



Dynamics 365 tietoturvan ominaisuudet

Taustalla globaalin pilvipalvelun infrastruktuuri

Tieto replikoituu kahden palvelinkeskuksen välillä lähes reaaliaikaisesti

Fyysinen tietoturva palvelinkeskuksissa huippuluokkaa

Tieto aina kryptattua, palvelun työntekijöillä ei pysyvää pääsyä dataan

Yksi Region sisältää kymmenittäin Dynamics 365 –asennuksia (Scale Group)

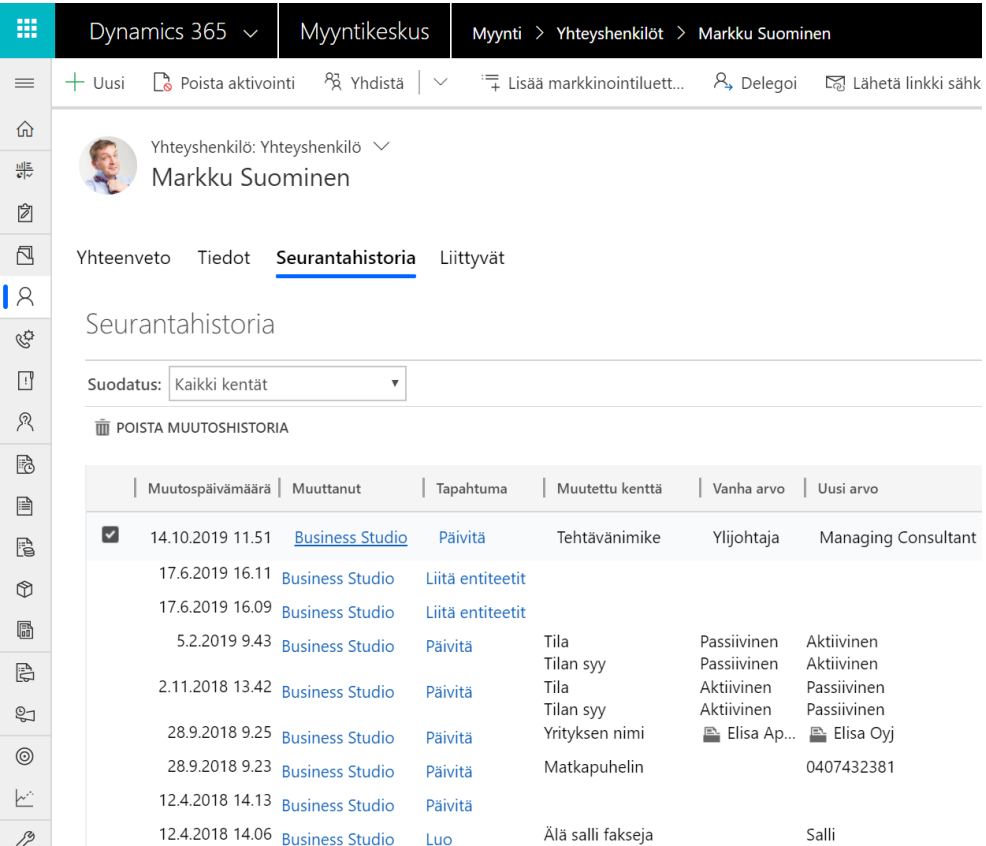
Yksi Scale Group sisältää kymmenittäin palvelimia, jotka palvelevat sen asiakasympäristöjä

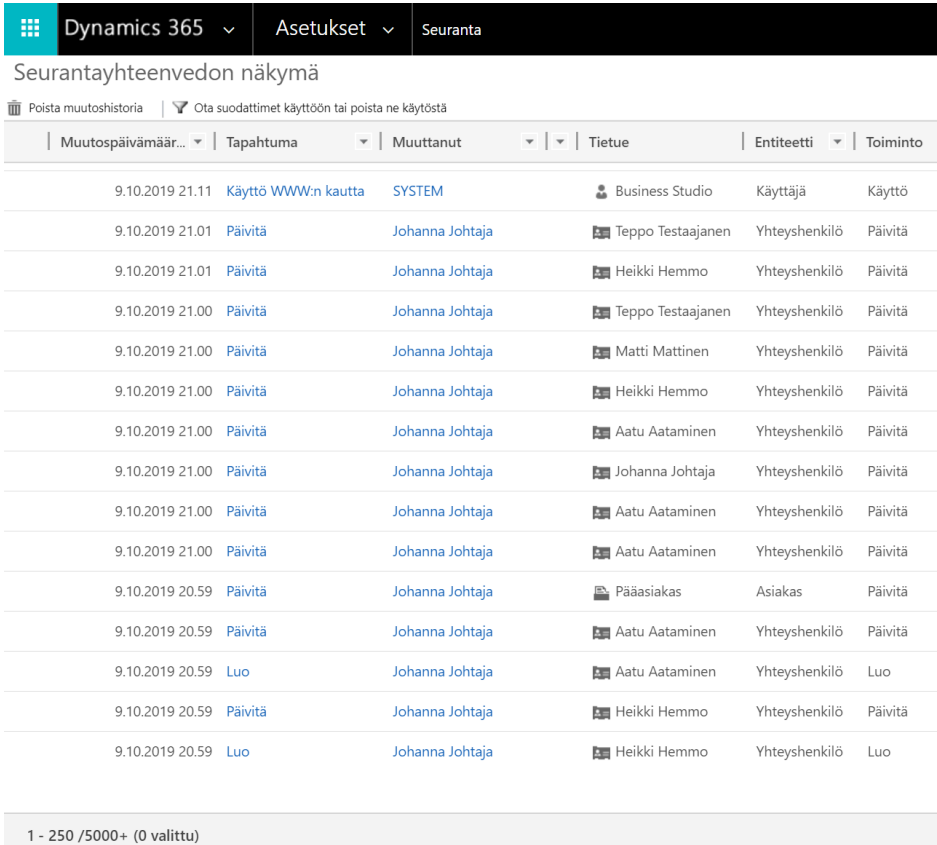
Versiopäivitykset ajetaan viikoittain pienimmästä Regionista suurimpaan (Oceania -> Europe/NAM)

Käyttöoikeushallinta Dynamics 365 -sovelluksessa

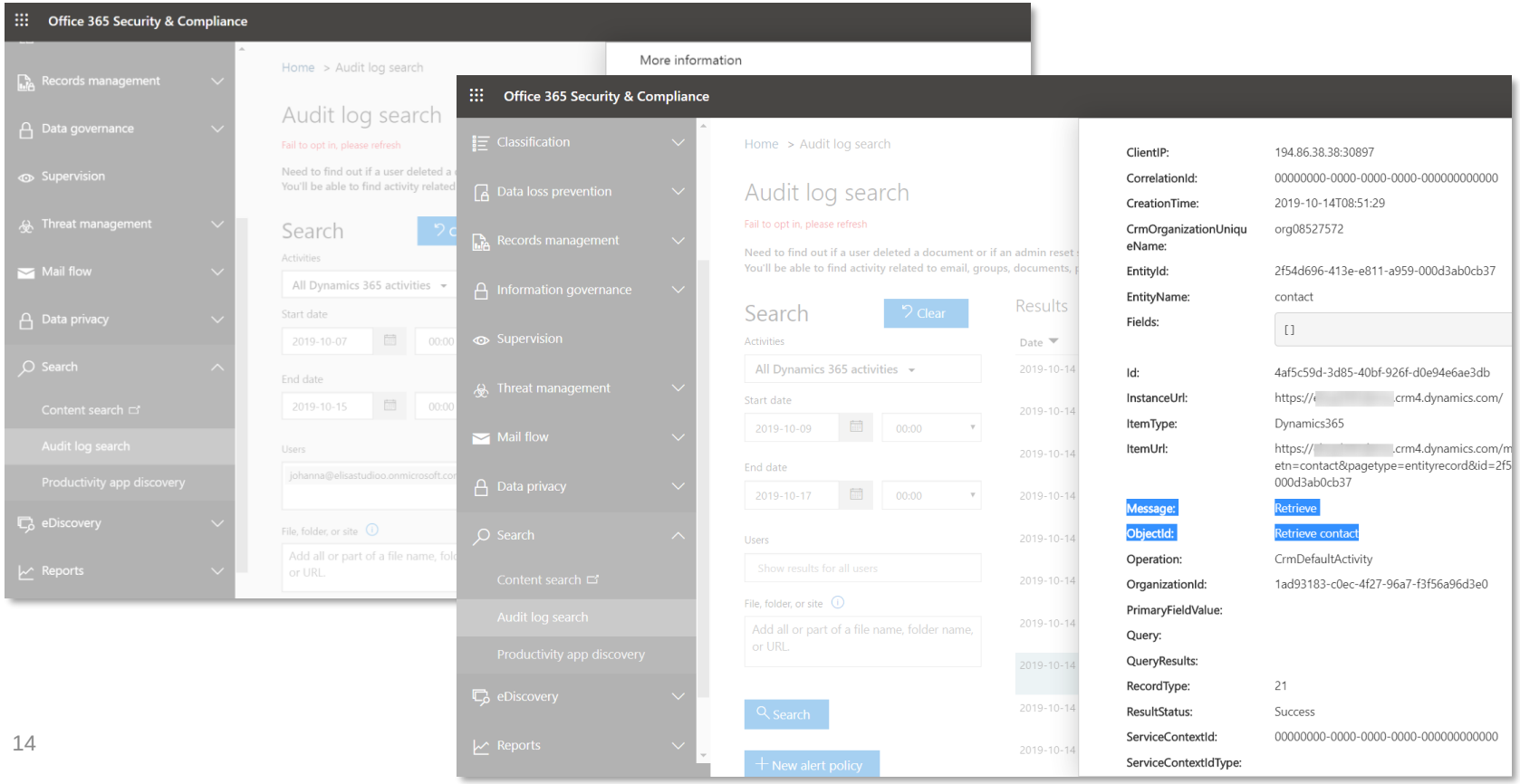
- Mihin sovelluksiin käyttäjä saa kirjautua?
- Mitkä toiminnot & tietuetyypit ovat saatavilla?
- Mitä tietueita käyttäjä näkee?
- Mitä tietuelomakkeen kenttiä käyttäjä näkee?
- Mitä muutoksia/lisäyksiä käyttäjä saa tehdä tietueille?

Muutosseuranta Dynamics 365 -sovelluksessa

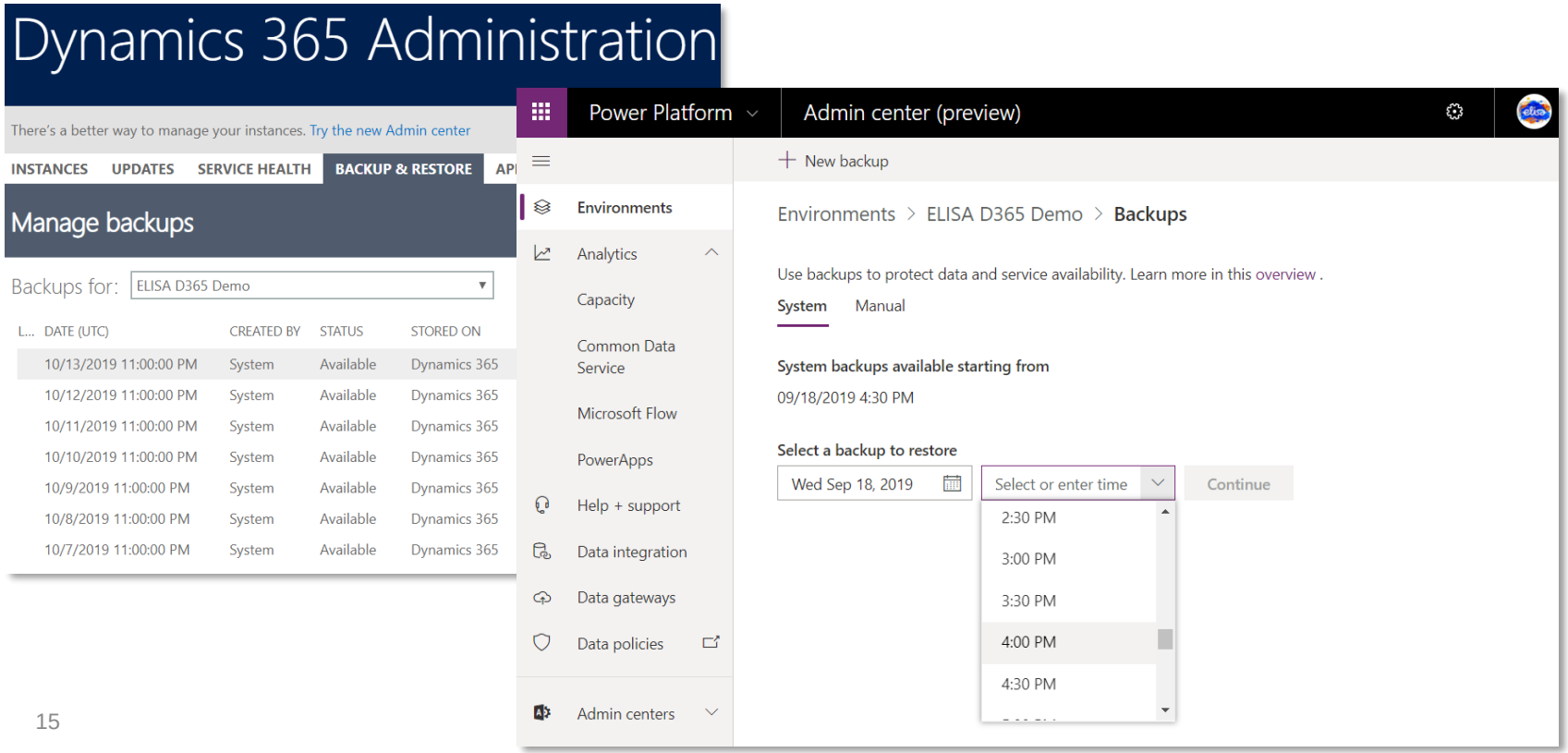




Lukuseuranta Microsoft 365 -hallintakeskuksessa



Varmuuskopiot (backup) ja ympäristöt



Microsoft 365 tietoturvan palvelut

Yleisimmät uhat pilvipalveluissa

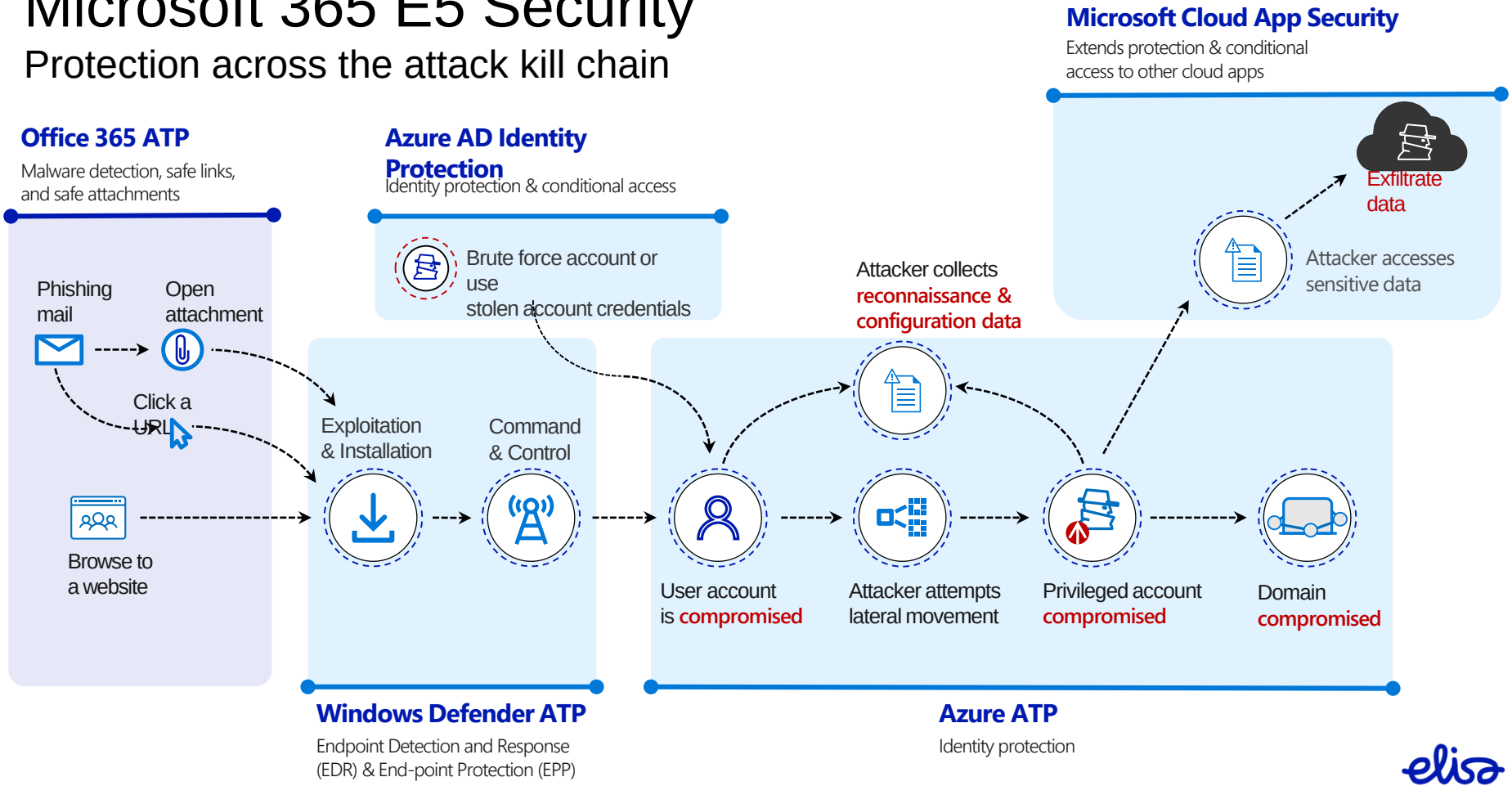
Identiteetin varkaus / murtaminen	• Väärinkäyttäjä saa haltuunsa käyttäjän tunnuksen & salasanan ja kirjautuu käyttäjän tunnuksella pilvipalveluihin • Väärinkäyttäjä pystyy esiintymään käyttäjänä • Pääsy resursseihin
Informaation väärinkäyttö	• Nykyiset työkalut mahdollistavat sujuvan jakamisen ja ryhmätyöskentelyn • Haasteena informaation leviäminen ei-tarkoitetuille henkilöille ja informaation väärinkäyttö
Varjo IT	• Epämääräiset sovellukset • Haitallinen toiminta murtautumisen jälkeen • Lateraalinen siirtyminen

Yleisimmät uhat – Microsoftin ratkaisut

Identiteetin varkaus / murtaminen	• Ehdollinen pääsynhallinta (Azure AD Conditional Access) • Mahdollisuus vahvaan tunnistautumiseen (MFA) • Intune
Informaation väärinkäyttö	• Azure Information Protection (AIP)
Varjo IT	• Advanced Threat Protection ja Cloud App Security

Microsoft 365 E5 Security

Protection across the attack kill chain

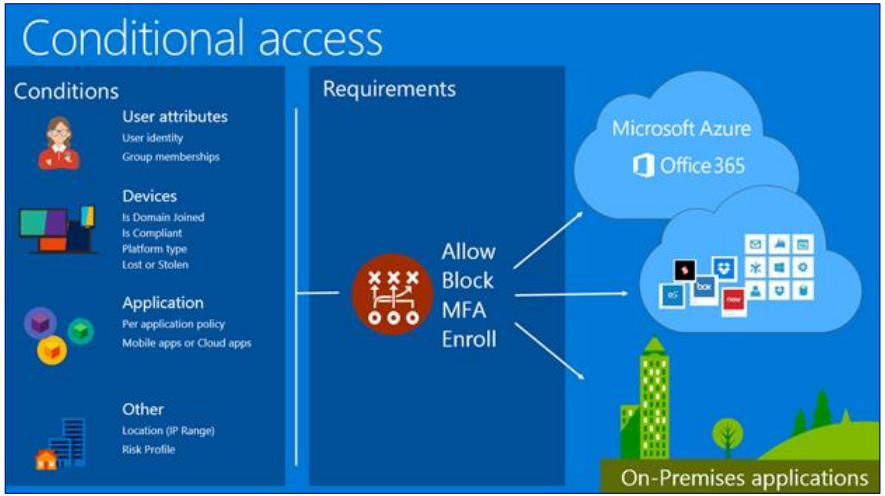


Identiteetin suojaaminen

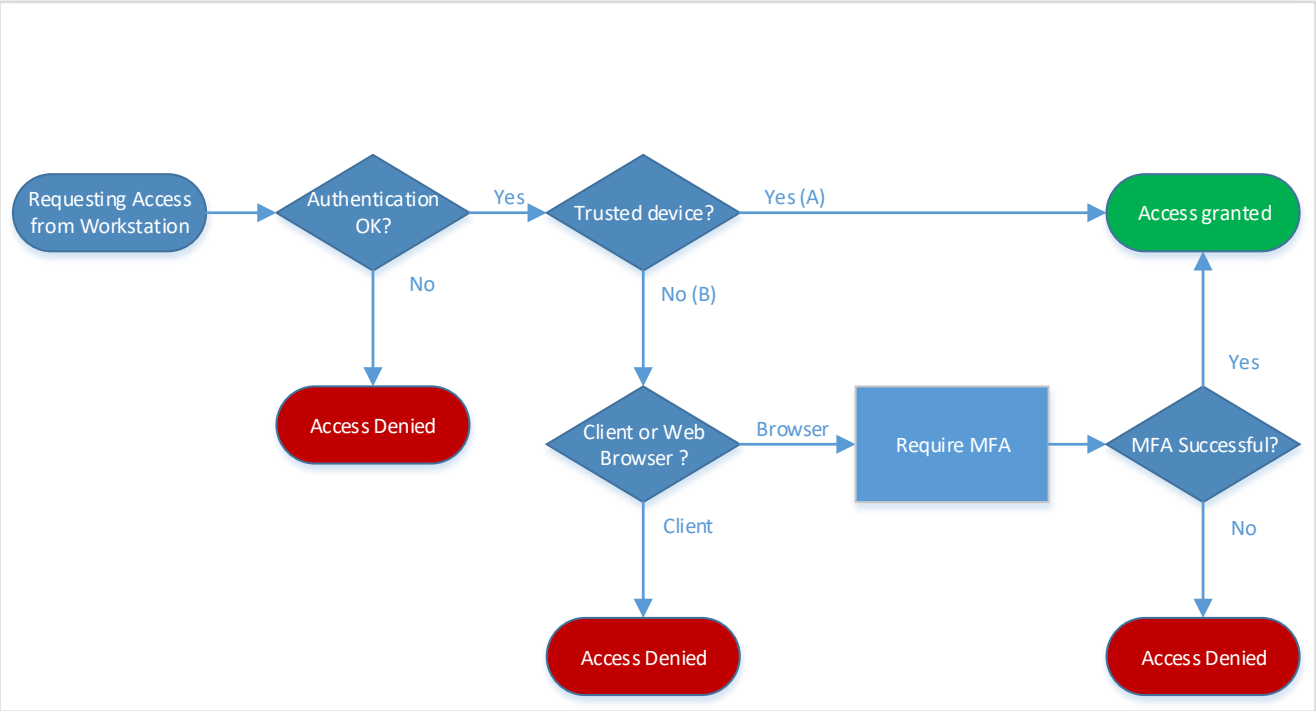
- Loppukäyttäjä on aina tietoturvan heikoin lenkki
  - Tapoja saada käyttäjän tunnukset tietoon on useita. Yleisin ja konkreettisin esimerkki sähköpostin kalasteluviestit
- Identiteetin suojaamisella hankaloitetaan väärinkäyttöä
  - Vaikka varas saisi tunnuksen ja salasanan tietoonsa, ei niillä pääse kirjautumaan ellei laite ole luotettu
- Vahva tunnistautuminen (MFA) vs ehdollinen pääsynhallinta (Conditional Access)
  - MFA:lla ei pystytä _estämään_ kirjautumista
  - MFA pystytään kiertämään vanhakantaisella kirjautumisella (legacy authentication)
    - https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/09/ttn201809261243.html
  - MFA on loppukäyttäjälle ”rasittavampi”
- Asianmukaisesti toteutettu moderni pääsynhallinta on loppukäyttäjälle lähes näkymätön, mutta estää tietomurrot tehokkaasti

Modernin pääsynhallinnan periaate

- Määritellään pääsyehdot
  - Ryhmäjäsenyys
  - Luotettu laite (Työasema / Mobiili)
  - Sovellustyyppi (Client / Selain)
  - Verkkosijainti
- Määritellään pääsymekanismi
  - Sallitaan käyttö
  - Estetään käyttö
  - Sallitaan, mutta vaaditaan vahva tunnistautuminen (MFA)
  - Vaaditaan laitteen rekisteröinti Intuneen
- Ehtoja ja mekanismeja yhdistelemällä voidaan luoda haluttuja skenaarioita



Työaseman pääsynhallinta vuokaaviona



(A) = Yrityksen toimialueeseen liitetty työasema

(B) = Muu työasema, esim. Kotikone

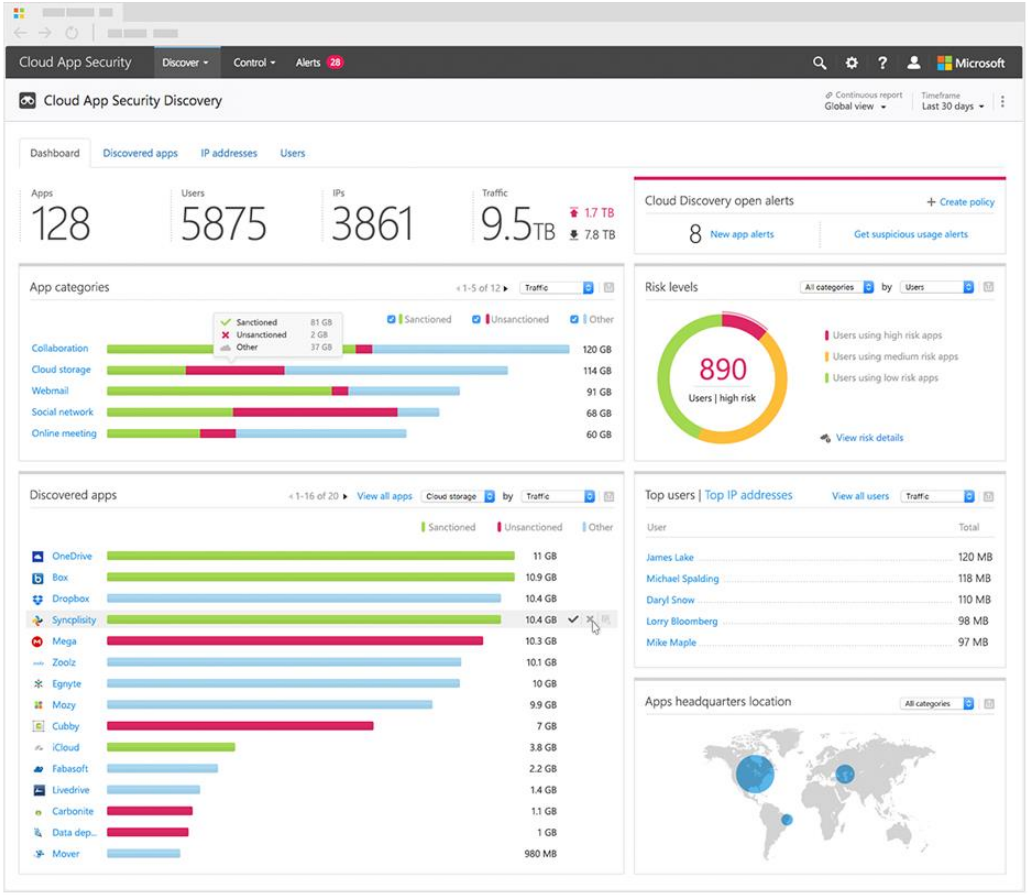
Azure Information Protection

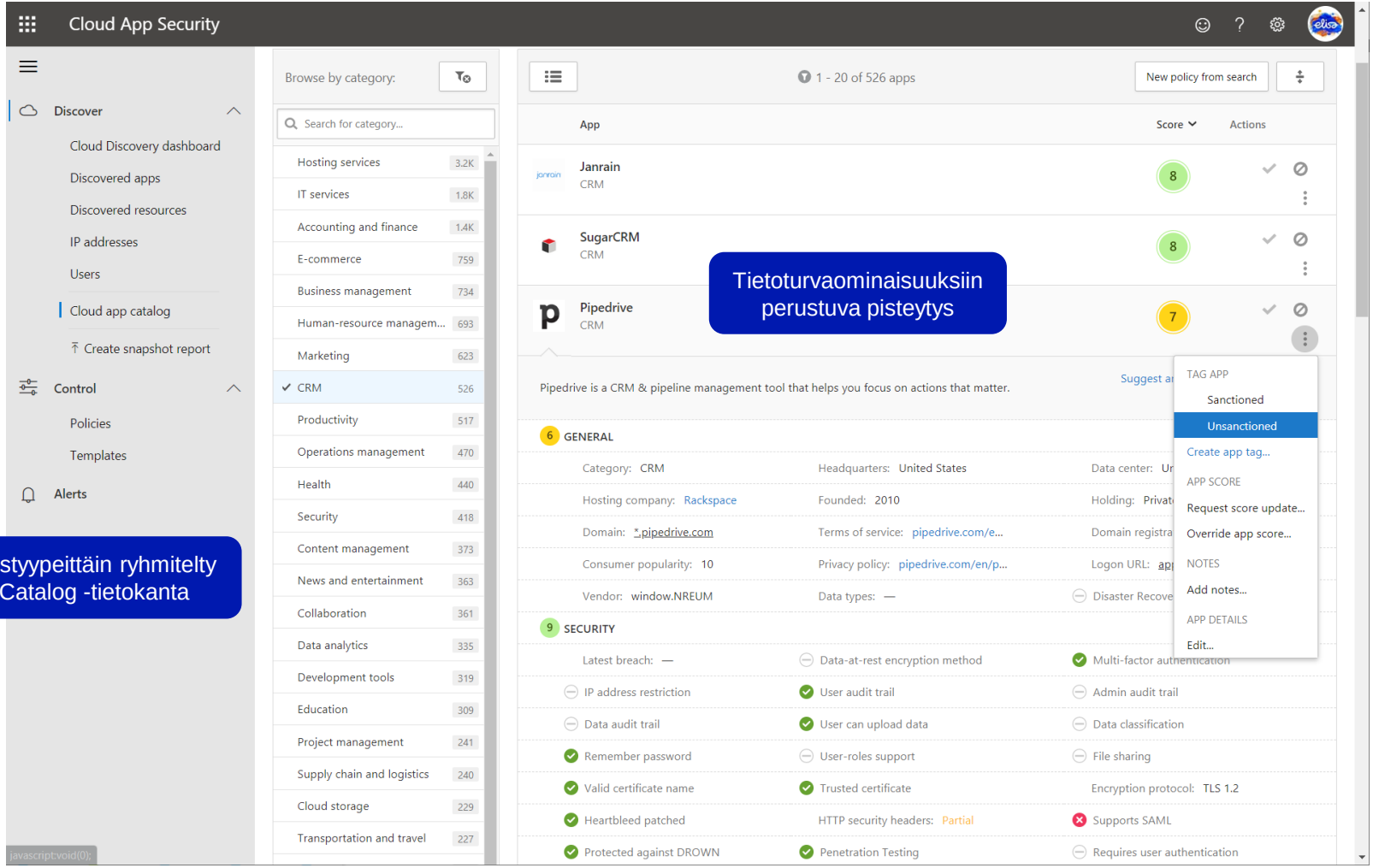
- Tiedostojen luokittelu, merkintä ja suojaaminen
- Luokittelu voi olla käyttäjävalintainen tai automaattinen
  - Elisa suosittelee käyttäjäpohjaista luokittelua kulttuurin jalkauttamiseksi
- Tiedostojen seuranta
  - Käyttäjät ja ylläpitäjät voivat seurata (tracking site) suojaamiaan tiedostoja
  - Voidaan estää paikallinen kopiointi, tulostus, kuvakaappaus, postin jatkolähetys
  - Oikeuksien peruuttaminen
- Suojaus kulkee dokumentin mukana
  - USB – tikut, Sähköpostin liitteet

- Käyttöönotto hallitusti PoC – mallisesti
  - Tehdään määritykset
  - Julkaistaan säännöt ainoastaan halutulle käyttäjäryhmälle
  - Voidaan toteuttaa asiakastyöpajana
- Mahdollista kohdistaa eri sääntöjä eri käyttäjäryhmille
- Mahdollista määrittää super user (saa auki kaikki tiedostot)
  - Kassakaappitunnus, tai splitattu salasana parille taholle

Cloud App Security

- Tunnista ja hallitse ”Varjo IT” – sovelluksia ja niiden riskitasoja
- Suojaa ja valvo sensitiivistä informaatiota missä tahansa pilvipalvelussa
- Suojaudu kyberuhkia vastaan ja tunnista epäilyttäviä käytöksiä

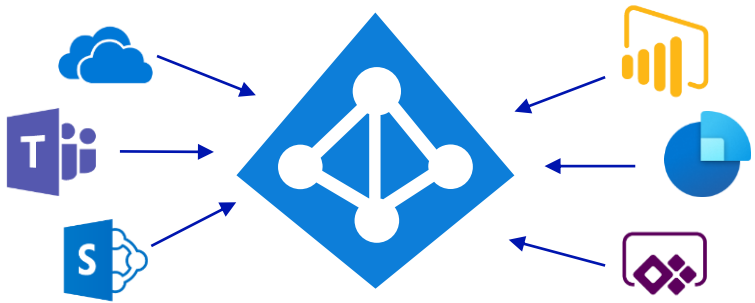




Sovellustyypeittäin ryhmitelty App Catalog -tietokanta

Azure AD B2B ja ulkoiset identiteetit

- Liiketoimintasovellusten käyttäjät eivät ole enää vain talon sisältä tulevia työntekijöitä vaan kasvavassa määrin muita osapuolia (asiakas, kumppani)
- Azure AD B2B erottaa autentikoinnin ja auktorisoinnin toisistaan
- Ulkoiset tahot kuten kumppanit tai asiakkaat voivat käyttää omaa identiteettiään palveluissa
  - Azure AD:ssa hallinnoidaan globaalisti jo yli miljardi identiteettiä
- Itsepalvelutoiminnot rekisteröintiin tai automaattinen provisiointi
- Elinkaaren hallinta (esim. poistuvat kumppanin työntekijät)
- Käytön seuranta

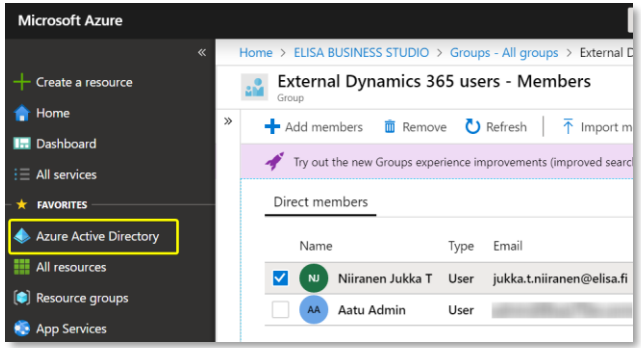


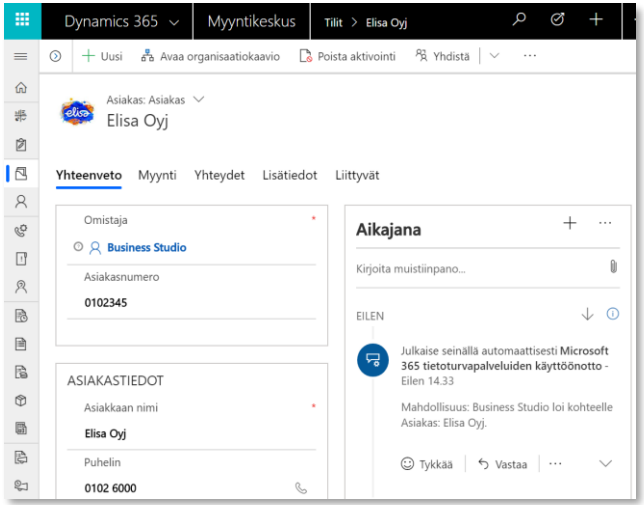
Ulkoisen käyttäjän kutsuminen Dynamics 365:een

1. Käyttäjän työsähköpostiosoite kutsutaan mukaan Azure AD -ryhmään

2. Ulkoinen käyttäjä saa sähköpostiinsa kutsuviestin organisaatioon liittymiseen

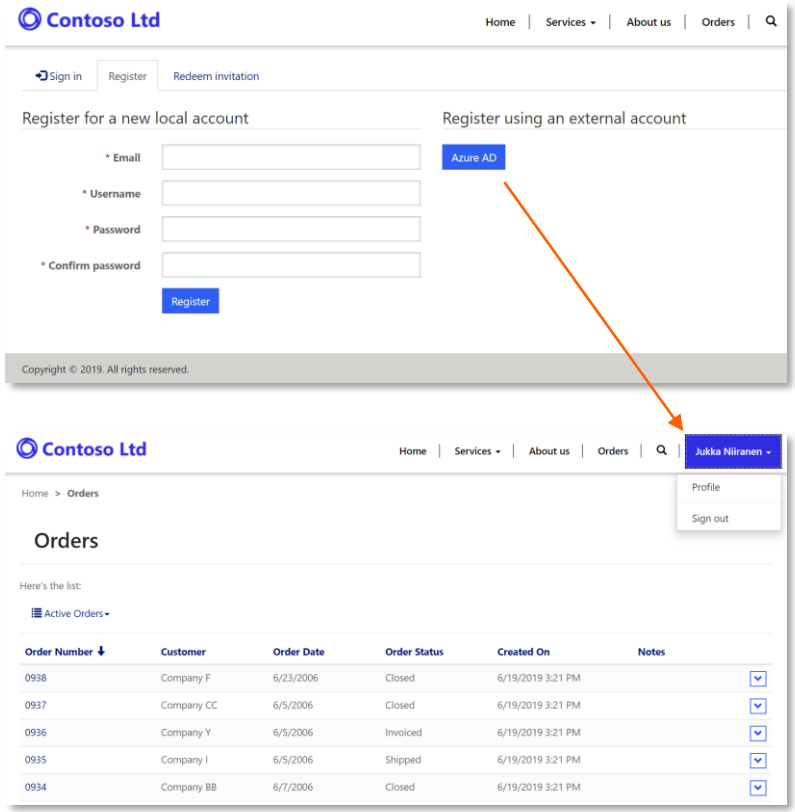
3. Ryhmälle luvitetut ja lisensoidut sovellukset ovat käytettävissä





Dynamics 365 Portals ja ulkoiset käyttäjät

- Julkisen portaalin kautta tarjottava näkyvyys asiakkaan tai yhteistyötahon omiin tuotteisiin, palveluihin, tietoihin
- Uuden käyttäjän rekisteröinti itsepalveluna, tämän omassa Office 365 –käytössä olevalla tunnuksella
- Ei erillisiä tunnuksia hallittavaksi
- Azure AD:n tarjoamat palvelut hyödynnettävissä identiteetin suojaamiseen



Yhteenveto

- Moderneissa pilvipohjaisissa SaaS-sovelluksissa on paljon valmiita toimintoja liiketoimintatiedon turvaamiseen
- Asiakkaalla on kuitenkin vastuu varmistaa, että suojautuminen uhkia vastaan kattaa identiteetit ja päätelaitteet
- Microsoft 365:stä löytyy laaja valikoima tuotteita tietoturvan hallintaan pilviympäristössä
- Elisan tietoturvatyöpajat auttavat alkuun: https://yrityksille.elisa.fi/tyopajat

Tietoturvatyöpajat

Office 365 tietoturva kuntoon Elisan monipuolisten työpajojen avulla

Tietoturva työpaja 1: Identiteetin ja informaation suojaaminen

- Ehdollinen pääsynhallinta ja vahva tunnistautuminen (Azure AD Conditional Access, MFA)
- Datan ja dokumenttien luokittelu ja suojaaminen (Azure Information Protection)
- Identiteettien käytön ja kirjautumisten monitorointi ja valvonta (Advanced Threat Analytics)
- Office 365 – tietoturvaominaisuudet (Message Encryption, Data Loss Prevention)
- Windows 10 – tietoturvaominaisuudet (mm. Credential Guard)

Tietoturva työpaja 2: Kehittyneiltä uhkilta suojautuminen ja monitorointi

- Sähköpostin ja dokumenttien suojaaminen (Office 365 Advanced Threat Protection)
- Pilvi-identiteettien käytön ja kirjautumisen suojaaminen (Azure Advanced Threat Protection)
- Työaseman suojaaminen (Microsoft Defender Advanced Threat Protection)
- Sovellusten suojaaminen (Cloud App Security)
- Uhkien monitorointi ja valvonta (Office 365 ATP Plan 2)
- Julkipilven SIEM (Azure Sentinel)

elisa

Kiitos!

https://yrityksille.elisa.fi/tyopajat