



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

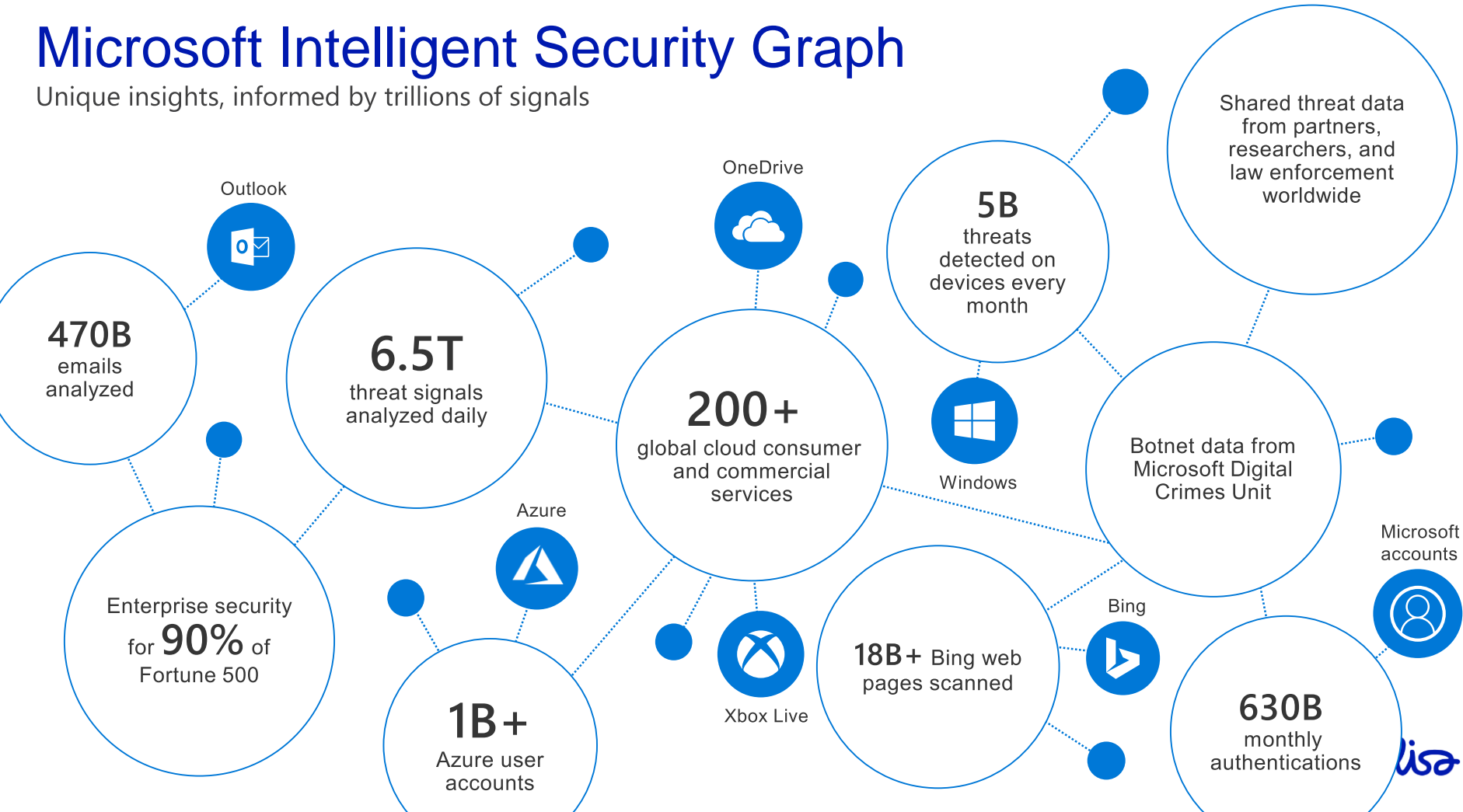
- Jokainen organisaatio on nyt teknologiaorganisaatio
- Työtä tehdään sijainnista riippumatta, yhä monipuolisemmalla sovellus- ja laitekirjolla
- Dataa on kaikkialla ja sitä syntyy kaikista älykkäistä laitteista

Uudet uhat

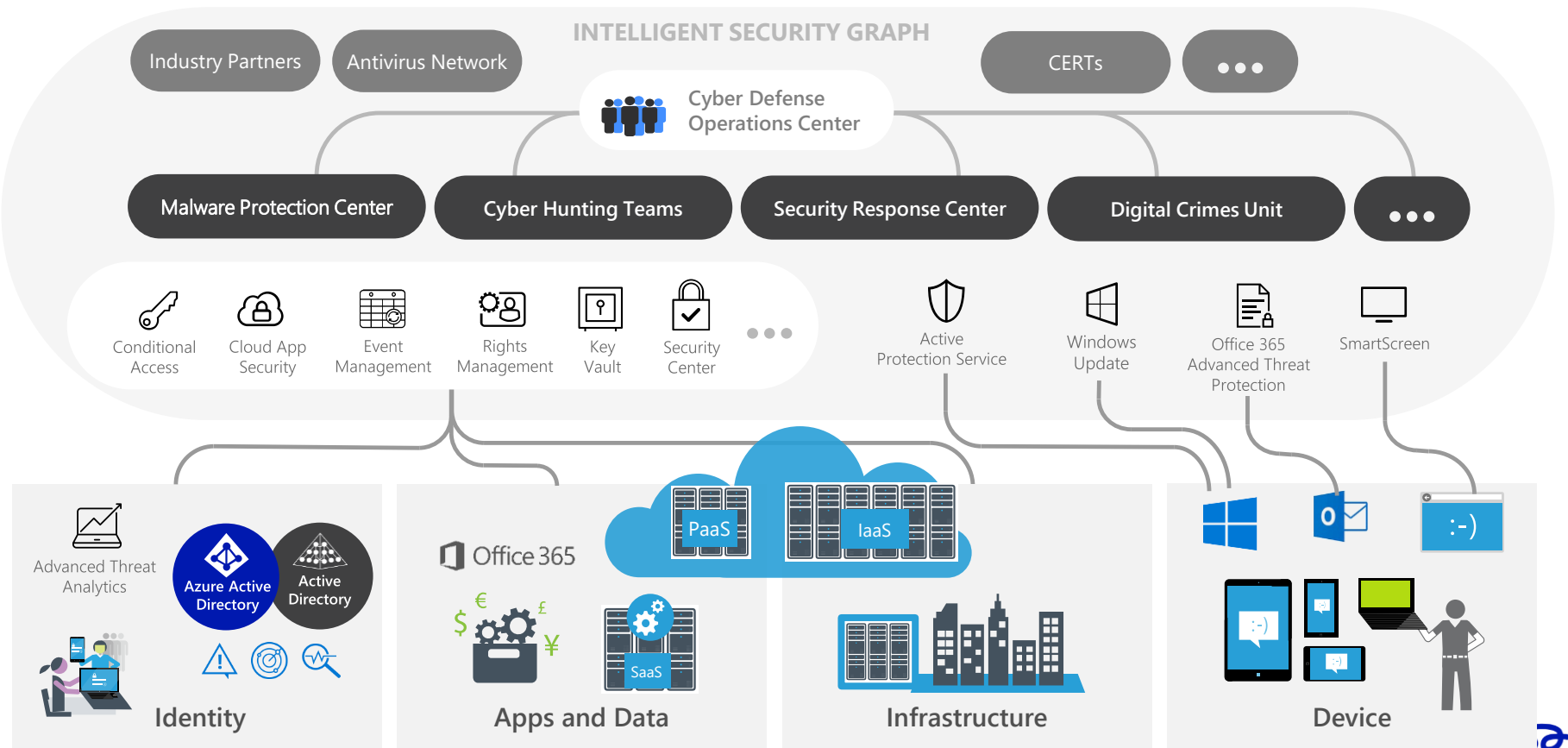
- Identiteettiin kohdistuvat hyökkäykset ovat kolminkertaistuneet viimeisen vuoden aikana
- Perinteiset tietoturvatyökalut eivät ole pysyneet muutoksen perässä
- Pelkät asiantuntijat eivät riitä kyberturvan kasvaviin tarpeisiin

Microsoft Intelligent Security Graph

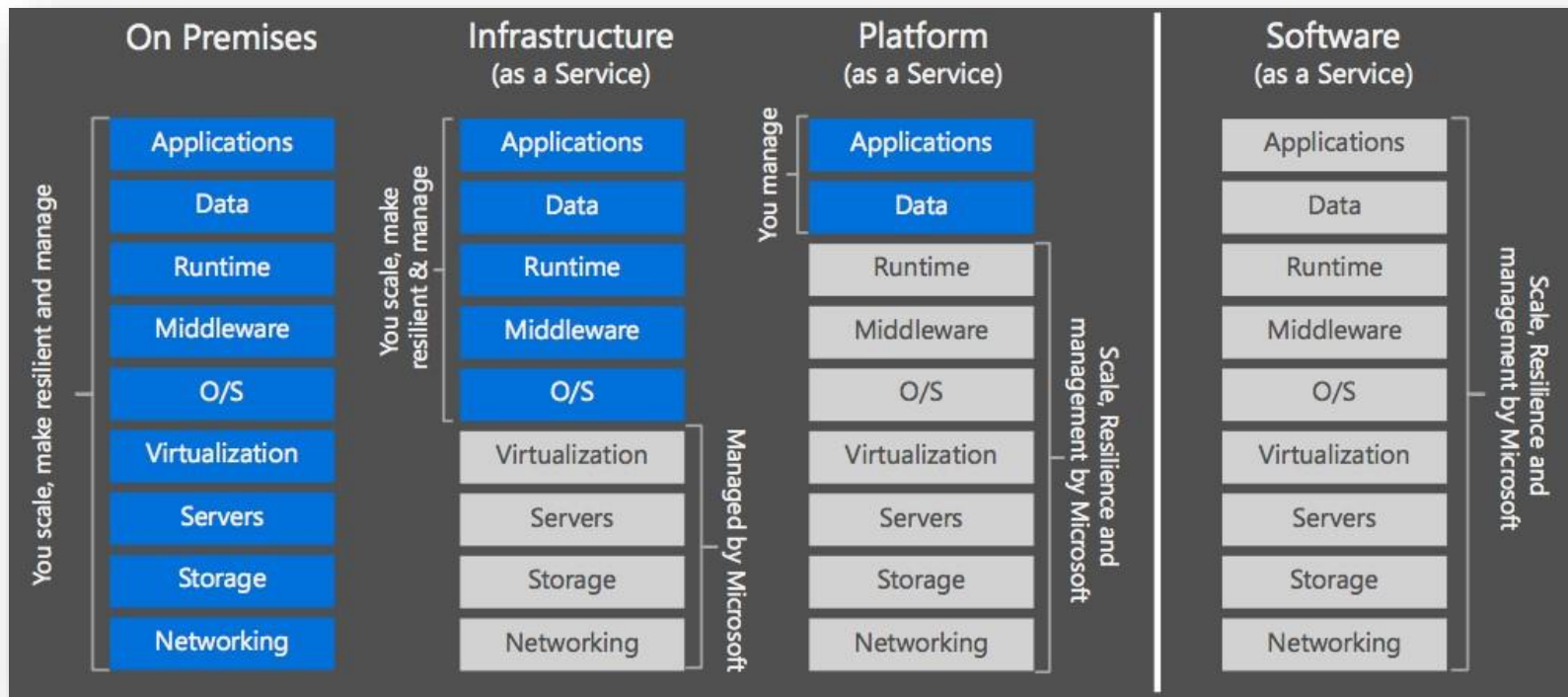
Unique insights, informed by trillions of signals



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

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Microsoft	Microsoft
Application	Customer	Customer	Microsoft	Microsoft
Network controls	Customer	Customer	Microsoft	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

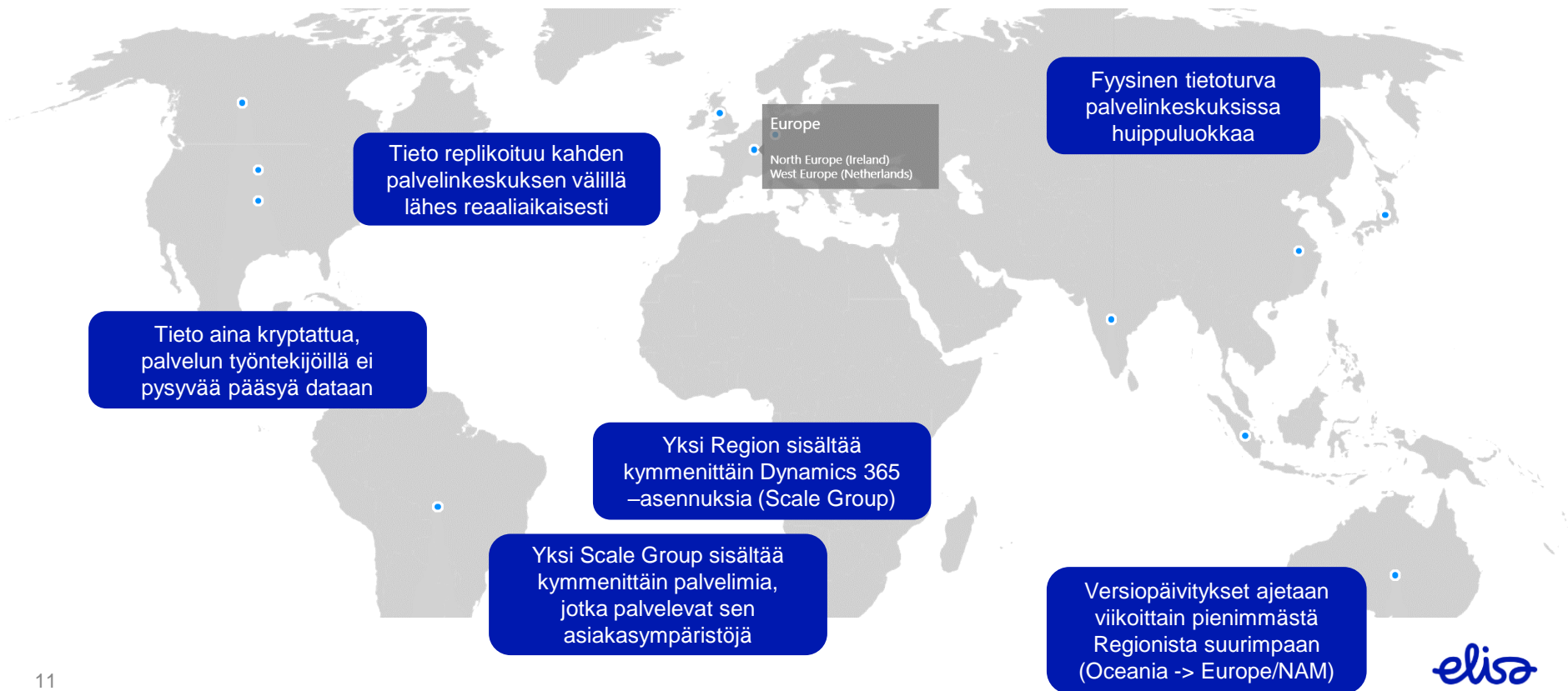
Lähde

 **Microsoft**  **Customer**

Dynamics 365 tietoturvan ominaisuudet



Taustalla globaalin pilvipalvelun infrastruktuuri



Käyttöoikeushallinta Dynamics 365 -sovelluksessa




- Mihin sovellukseen 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


 Dynamics 365 ▾


Myyntikeskus


Myynti > Yhteyshenkilöt > Markku Suominen


 Uusi

 Poista aktivointi

 Yhdistä ▾

 Lisää markkinointiluett...

 Delegoi

 Lähetä linkki sähkö





Yhteyshenkilö: Yhteyshenkilö ▾
Markku Suominen

Yhteenveto Tiedot **Seurantahistoria** Liittyvät

Seurantahistoria

Suodatus: Kaikki kentät ▾
















 POISTA MUUTOSHISTORIA

	Muutospäivämäärä	Muuttanut	Tapahtuma	Muutettu kenttä	Vanha arvo	Uusi arvo
<input checked="" type="checkbox"/>	14.10.2019 11.51	Business Studio	Päivitä	Tehtävänimike	Ylijohtaja	Managing Consultant
	17.6.2019 16.11	Business Studio	Liitä entiteetit			
	17.6.2019 16.09	Business Studio	Liitä entiteetit			
	5.2.2019 9.43	Business Studio	Päivitä	Tila	Passiivinen	Aktiivinen
				Tilan syy	Passiivinen	Aktiivinen
	2.11.2018 13.42	Business Studio	Päivitä	Tila	Aktiivinen	Passiivinen
				Tilan syy	Aktiivinen	Passiivinen
	28.9.2018 9.25	Business Studio	Päivitä	Yrityksen nimi	 Elisa Ap...	 Elisa Oyj
	28.9.2018 9.23	Business Studio	Päivitä	Matkapuhelin		0407432381
	12.4.2018 14.13	Business Studio	Päivitä			
	12.4.2018 14.06	Business Studio	Luo	Älä salli fakseja		Salli

Seurantayhteenvedon näkymä

 Poista muutoshistoria

 Ota suodattimet käyttöön tai poista ne käytöstä

	Muutospäivämäärä...	Tapahtuma	Muuttanut	Tietue	Entiteetti	Toiminto
	9.10.2019 21.11	Käyttö WWW:n kautta	SYSTEM	 Business Studio	Käyttäjä	Käyttö
	9.10.2019 21.01	Päivitä	Johanna Johtaja	 Teppo Testaajanen	Yhteyshenkilö	Päivitä
	9.10.2019 21.01	Päivitä	Johanna Johtaja	 Heikki Hemmo	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Teppo Testaajanen	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Matti Mattinen	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Heikki Hemmo	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Aatu Aataminen	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Johanna Johtaja	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Aatu Aataminen	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Aatu Aataminen	Yhteyshenkilö	Päivitä
	9.10.2019 21.00	Päivitä	Johanna Johtaja	 Pääasiakas	Asiakas	Päivitä
	9.10.2019 20.59	Päivitä	Johanna Johtaja	 Aatu Aataminen	Yhteyshenkilö	Päivitä
	9.10.2019 20.59	Luo	Johanna Johtaja	 Aatu Aataminen	Yhteyshenkilö	Luo
	9.10.2019 20.59	Päivitä	Johanna Johtaja	 Heikki Hemmo	Yhteyshenkilö	Päivitä
	9.10.2019 20.59	Luo	Johanna Johtaja	 Heikki Hemmo	Yhteyshenkilö	Luo

1 - 250 / 5000+ (0 valittu)

Lukuseuranta Microsoft 365 -hallintakeskuksessa

The screenshot displays the Office 365 Security & Compliance center. The left-hand navigation pane includes sections for Records management, Data governance, Supervision, Threat management, Mail flow, Data privacy, Search, Content search, Audit log search (which is highlighted), Productivity app discovery, eDiscovery, and Reports. The central pane shows the 'Audit log search' interface, featuring a search bar, a filter for 'All Dynamics 365 activities', and date range selectors for start and end dates. Below these are user filters and a search button. The right-hand pane displays the search results in a table format. The table has columns for 'Date', 'Message', and 'Objectid'. A single result is shown for the date 2019-10-14, with the message 'Retrieve contact' and the objectid '2f54d696-413e-e811-a959-000d3ab0cb37'.

Date	Message	Objectid
2019-10-14	Retrieve contact	2f54d696-413e-e811-a959-000d3ab0cb37

Varmuuskopiot (backup) ja ympäristöt

Dynamics 365 Administration

There's a better way to manage your instances. [Try the new Admin center](#)

INSTANCES UPDATES SERVICE HEALTH **BACKUP & RESTORE** API

Manage backups

Backups for:

L...	DATE (UTC)	CREATED BY	STATUS	STORED ON
	10/13/2019 11:00:00 PM	System	Available	Dynamics 365
	10/12/2019 11:00:00 PM	System	Available	Dynamics 365
	10/11/2019 11:00:00 PM	System	Available	Dynamics 365
	10/10/2019 11:00:00 PM	System	Available	Dynamics 365
	10/9/2019 11:00:00 PM	System	Available	Dynamics 365
	10/8/2019 11:00:00 PM	System	Available	Dynamics 365
	10/7/2019 11:00:00 PM	System	Available	Dynamics 365

Power Platform Admin center (preview)

+ New backup

Environments > ELISA D365 Demo > Backups

Use backups to protect data and service availability. Learn more in this [overview](#).

System Manual

System backups available starting from
09/18/2019 4:30 PM

Select a backup to restore

Wed Sep 18, 2019

2:30 PM
3:00 PM
3:30 PM
4:00 PM
4:30 PM

Continue

Environments
Analytics
Capacity
Common Data Service
Microsoft Flow
PowerApps
Help + support
Data integration
Data gateways
Data policies
Admin centers

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

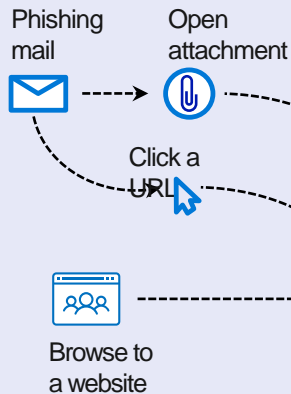
- Advanced Threat Protection ja Cloud App Security

Microsoft 365 E5 Security

Protection across the attack kill chain

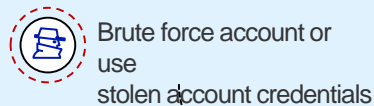
Office 365 ATP

Malware detection, safe links, and safe attachments



Azure AD Identity Protection

Identity protection & conditional access



Exploitation & Installation



Command & Control



Windows Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

Attacker collects **reconnaissance & configuration data**

User account is **compromised**

Attacker attempts lateral movement

Privileged account **compromised**

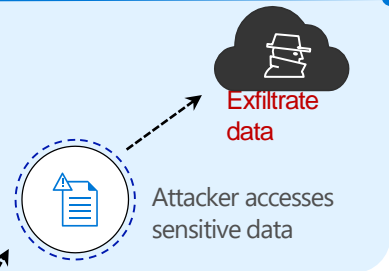
Domain **compromised**

Azure ATP

Identity protection

Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



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

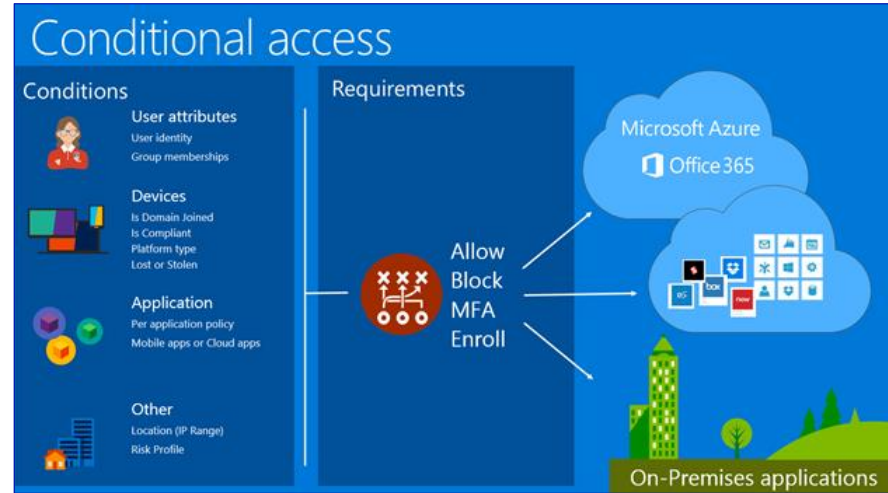
- Määritellään pääsyehdot

- Ryhmäjäsenyys
- Luotettu laite (Työasema / Mobiili)
- Sovellustyyppi (Client / Selain)
- Verkkosijainti

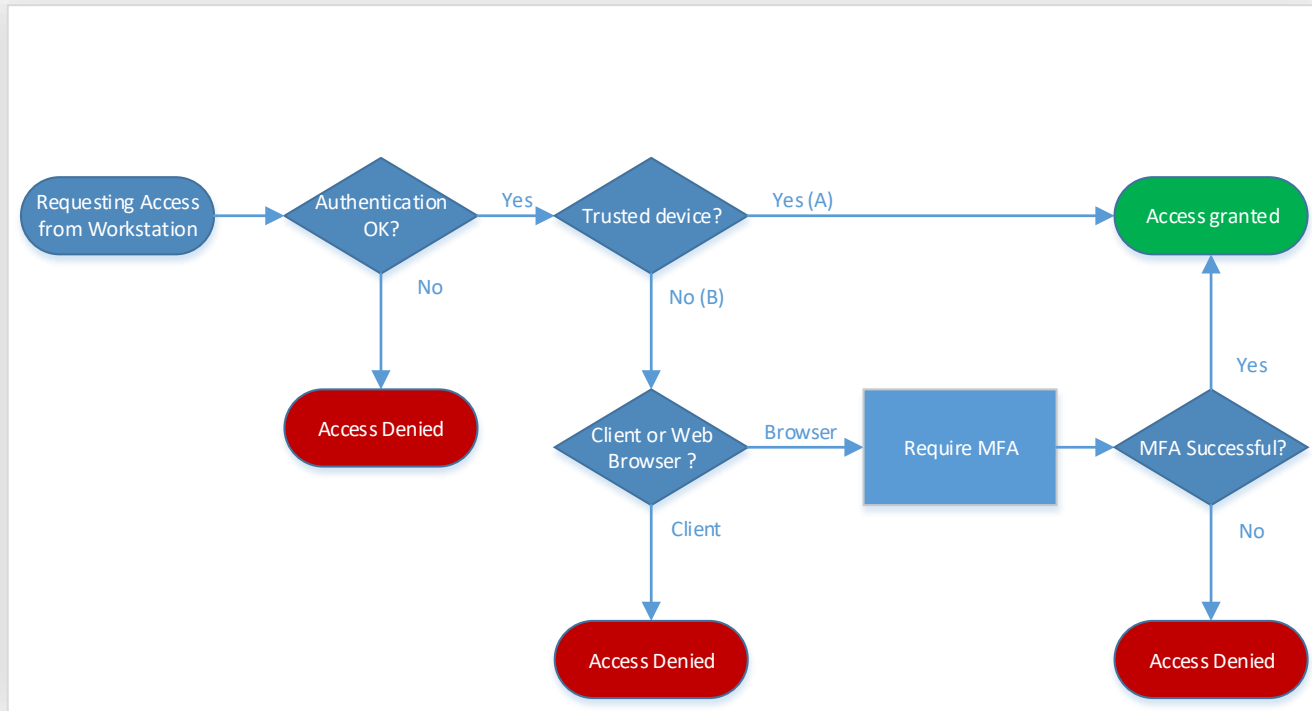
- Määritellään pääsymekanismi

- Sallitaan käyttö
- Estetään käyttö
- Sallitaan, mutta vaaditaan vahva tunnistautuminen (MFA)
- Vaaditaan laitteen rekisteröinti Intuneen

- Ehtoja ja mekanismeista yhdistelemällä voidaan luoda haluttuja skenaarioita



Työaseman pääsynhallinta vuokaaviona



(A) = Yrityksen toimialueeseen liitetty työasema

(B) = Muu työasema, esim. Kotikone

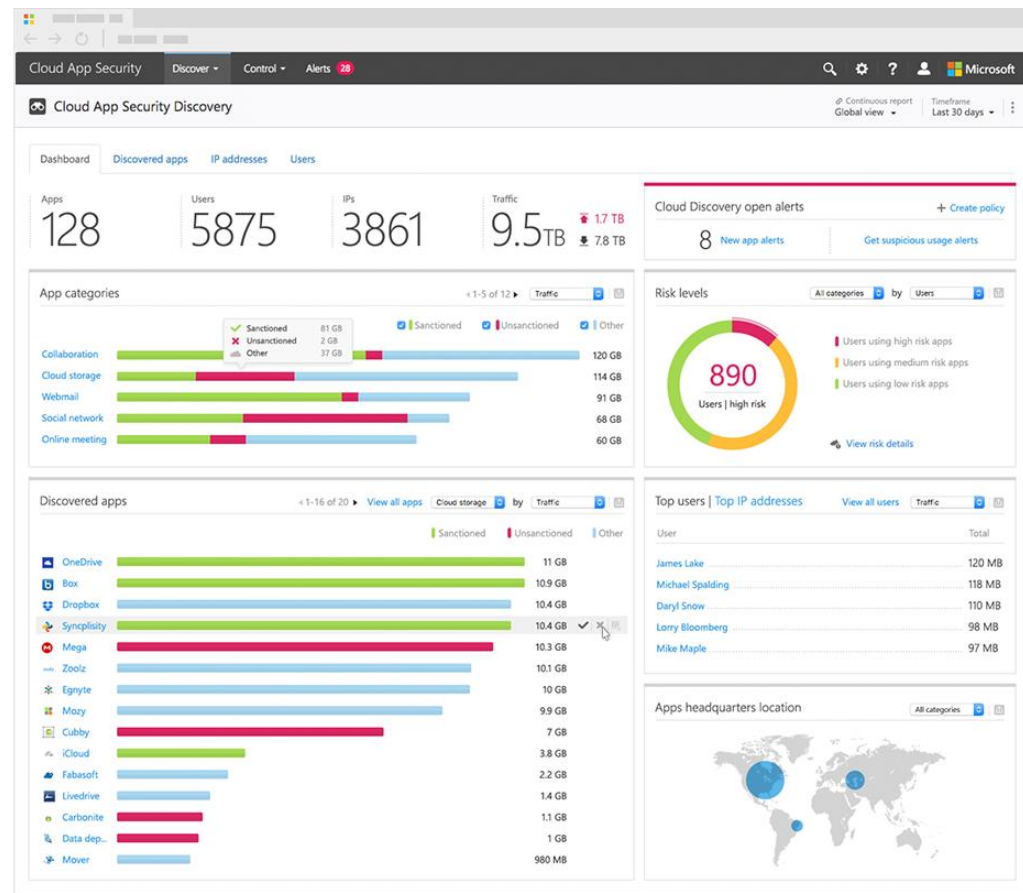
Azure Information Protection



- 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) suojaamia 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





- Discover
 - Cloud Discovery dashboard
 - Discovered apps
 - Discovered resources
 - IP addresses
 - Users
 - Cloud app catalog
 - Create snapshot report
- Control
 - Policies
 - Templates
- Alerts

Sovellustyypeittäin ryhmitelty
App Catalog -tietokanta

Browse by category:



Search for category...













Hosting services	3.2K
IT services	1.8K
Accounting and finance	1.4K
E-commerce	759
Business management	734
Human-resource managem...	693
Marketing	623
CRM	526
Productivity	517
Operations management	470
Health	440
Security	418
Content management	373
News and entertainment	363
Collaboration	361
Data analytics	335
Development tools	319
Education	309
Project management	241
Supply chain and logistics	240
Cloud storage	229
Transportation and travel	227



1 - 20 of 526 apps

New policy from search



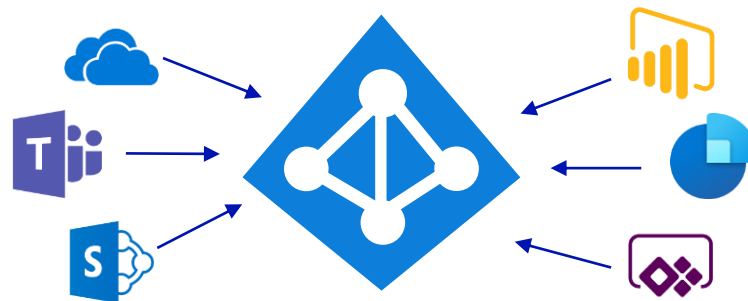
App	Score	Actions
 Janrain CRM	8	  
 SugarCRM CRM	8	  
 Pipedrive CRM	7	  
Pipedrive is a CRM & pipeline management tool that helps you focus on actions that matter. Suggest app		
6 GENERAL		
Category: CRM	Headquarters: United States	Data center: Ur
Hosting company: Rackspace	Founded: 2010	Holding: Privat
Domain: pipdrive.com	Terms of service: pipdrive.com/e...	Domain registra
Consumer popularity: 10	Privacy policy: pipdrive.com/en/p...	Logon URL: ap
Vendor: window.NREUM	Data types: —	Disaster Recove
9 SECURITY		
Latest breach: —	Data-at-rest encryption method	Multi-factor authentication
IP address restriction	User audit trail	Admin audit trail
Data audit trail	User can upload data	Data classification
Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.2
Heartbleed patched	HTTP security headers: Partial	Supports SAML
Protected against DROWN	Penetration Testing	Requires user authentication

Tietoturvaominaisuuksiin
perustuva pisteytys

- TAG APP
- Sanctioned
- Unsanctioned
- Create app tag...
- APP SCORE
- Request score update...
- Override app score...
- NOTES
- Add notes...
- APP DETAILS
- Edit...

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

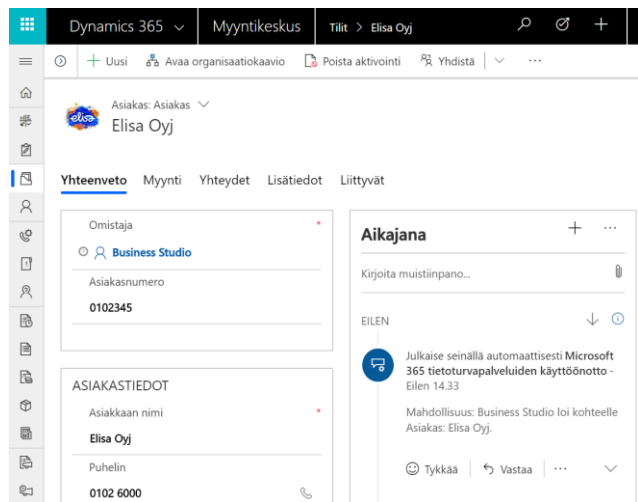
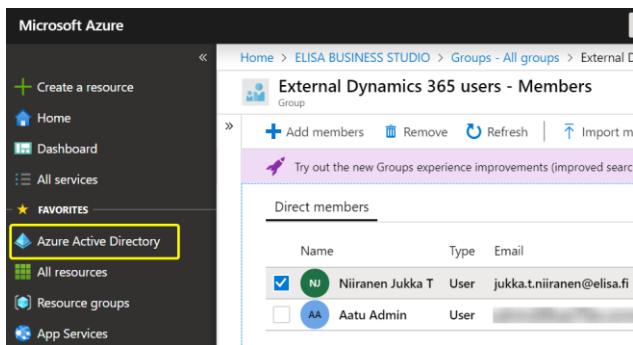


Ulkoisen käyttäjän kutsuminen Dynamics 365:een

1. Käyttäjän työ sähköpostiosoite 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

The top screenshot shows the 'Contoso Ltd' portal registration page. It has a navigation bar with 'Home', 'Services', 'About us', 'Orders', and a search icon. Below the navigation bar are links for 'Sign in', 'Register', and 'Redeem invitation'. The main content area has two sections: 'Register for a new local account' with fields for Email, Username, Password, and Confirm password, and a 'Register' button; and 'Register using an external account' with an 'Azure AD' button. An orange arrow points from the 'Azure AD' button to the user profile dropdown in the bottom screenshot.

The bottom screenshot shows the 'Contoso Ltd' portal 'Orders' page. The navigation bar is the same, but the user profile dropdown is open, showing 'Jukka Niiranen', 'Profile', and 'Sign out'. The main content area shows 'Home > Orders' and 'Here's the list:'. Below this is a table of 'Active Orders'.

Order Number ↓	Customer	Order Date	Order Status	Created On	Notes
0938	Company F	6/23/2006	Closed	6/19/2019 3:21 PM	▼
0937	Company CC	6/5/2006	Closed	6/19/2019 3:21 PM	▼
0936	Company Y	6/5/2006	Invoiced	6/19/2019 3:21 PM	▼
0935	Company I	6/5/2006	Shipped	6/19/2019 3:21 PM	▼
0934	Company BB	6/7/2006	Closed	6/19/2019 3:21 PM	▼

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)



Kiitos!

<https://yrityksille.elisa.fi/tyopajat>