

Microsoft Dev Box

Securing your company's crown jewels

(Yrityksesi kruununjalokivien turvaaminen)



Not Bad Security

Me olemme **Not Bad Security** –
ketterä pilvitietoturvan ja datan
syväosaaja.



notbadsecurity.com

Joni Nieminen

Senior Security Architect

joni.nieminen@notbadsecurity.com



Työkokemus: 20 vuotta IT-alalla eri tehtävissä ja positioissa

Ennen: KONE, Elisa, SD Worx, Fujitsu

Osaaminen: Microsoft Azure, Microsoft 365, Entra ID, Cloud Security, Hybrid Infrastructure



Mediasta bongattua

Valioon laaja tietomurto, tuhansien tiedot ovat saattaneet vuotaa – it-kumppani Vincitin tunnukset murrettu

Tietomurron tekijä on voinut saada käsiinsä muun muassa työntekijöiden henkilötunnuksia ja palkkatietoja sekä vakuutusyhtiön asiakkaiden terveystietoja.

Valioon joulukuussa kohdistunut laaja tietoturvahyökkäys sai alkunsa ohjelmistoyhtiö Vincitin työntekijän henkilökohtaiselta koneelta vuotaneesta salasanasta.

Helsingin tietomurrossa vietiin mahdollisesti kymmeniä miljoonia dokumentteja – tietoa rikollisesta toiminnasta ei ole

Tähän mennessä kaupungilla ei ole tietoa, että tietoja olisi yritetty hyödyntää rikollisesti. Tietoja on vuotanut mahdollisesti noin 900:lta turvakiellon alaiselta asiakkaalta.


Mediakonserni Keskisuomalainen: Tietoturvahyökkäys pysäytetty, tietoja ei vuotanut

Keskisuomalainen-konsernista kerrotaan, että tällä viikolla havaittu tietoturvahyökkäys ei edennyt alkua pidemmälle. Tilaajien tiedot eivät vaarantuneet.

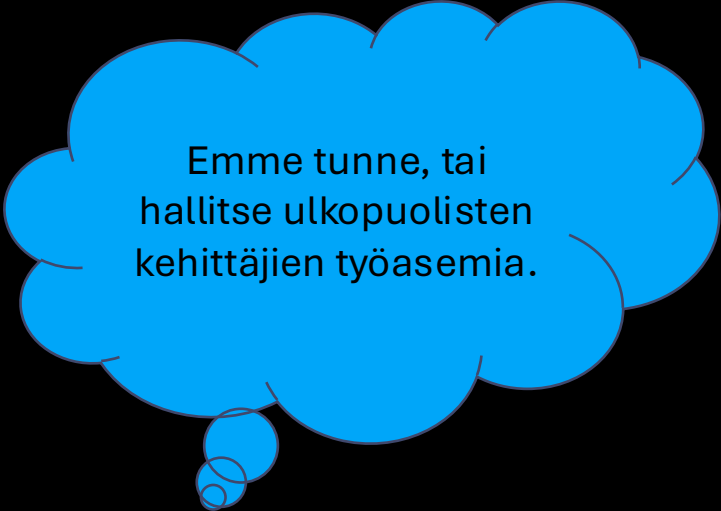
An aerial photograph of a winding, multi-lane road that curves through a landscape of snow and patches of green vegetation. Several cars are visible traveling along the road. The image is overlaid with a semi-transparent dark grey filter.

Tosielämän use case


| Asiakas-case X



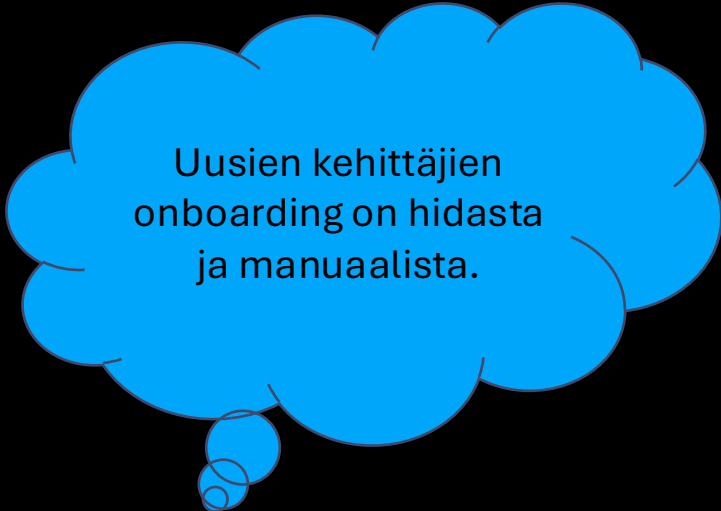
Kehityskäytäntömme
ovat hyvin
sirpaloituneet.



Emme tunne, tai
hallitse ulkopuolisten
kehittäjien työasemia.

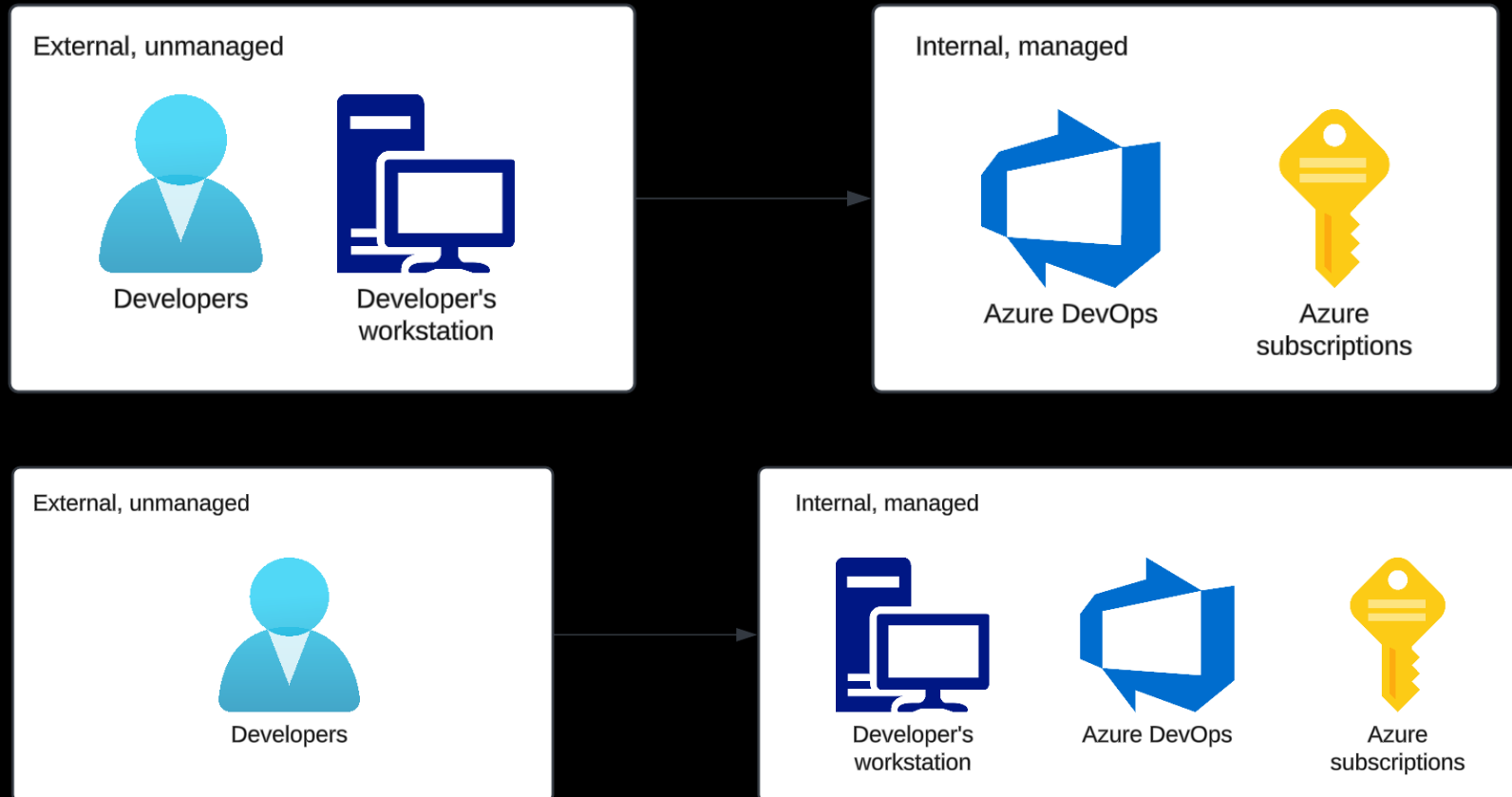


Emme tiedä missä
kaikkialla
lähdekoodimme on.



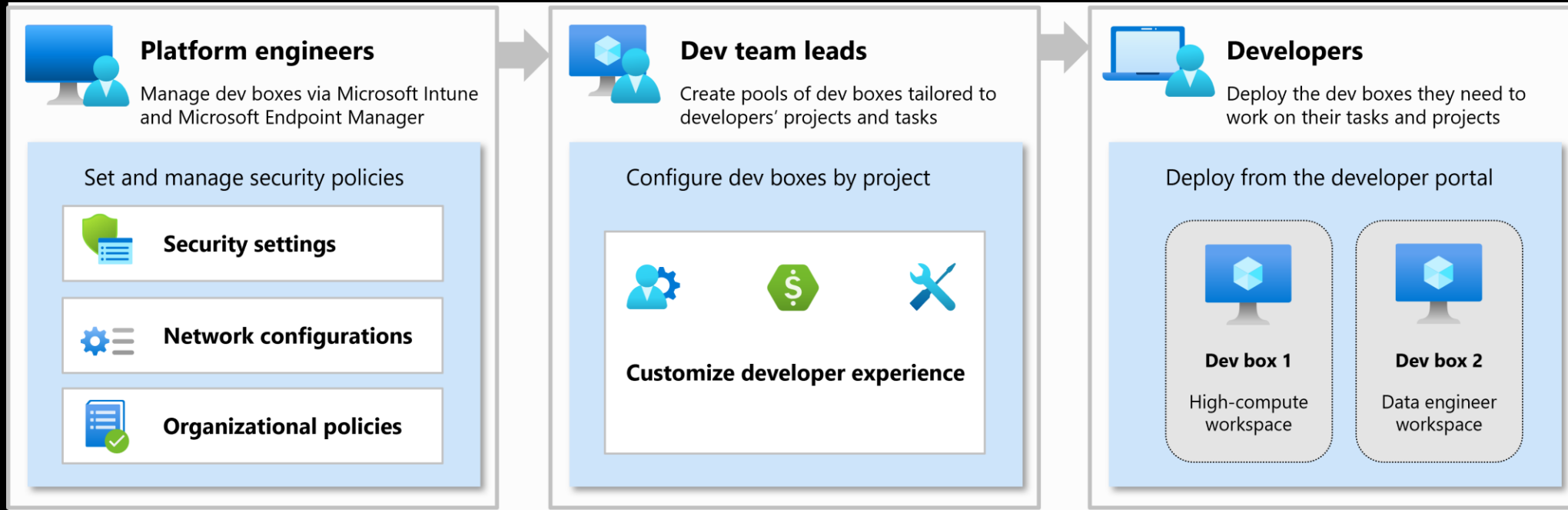
Uusien kehittäjien
onboarding on hidasta
ja manuaalista.

| Ratkaisuehdotus

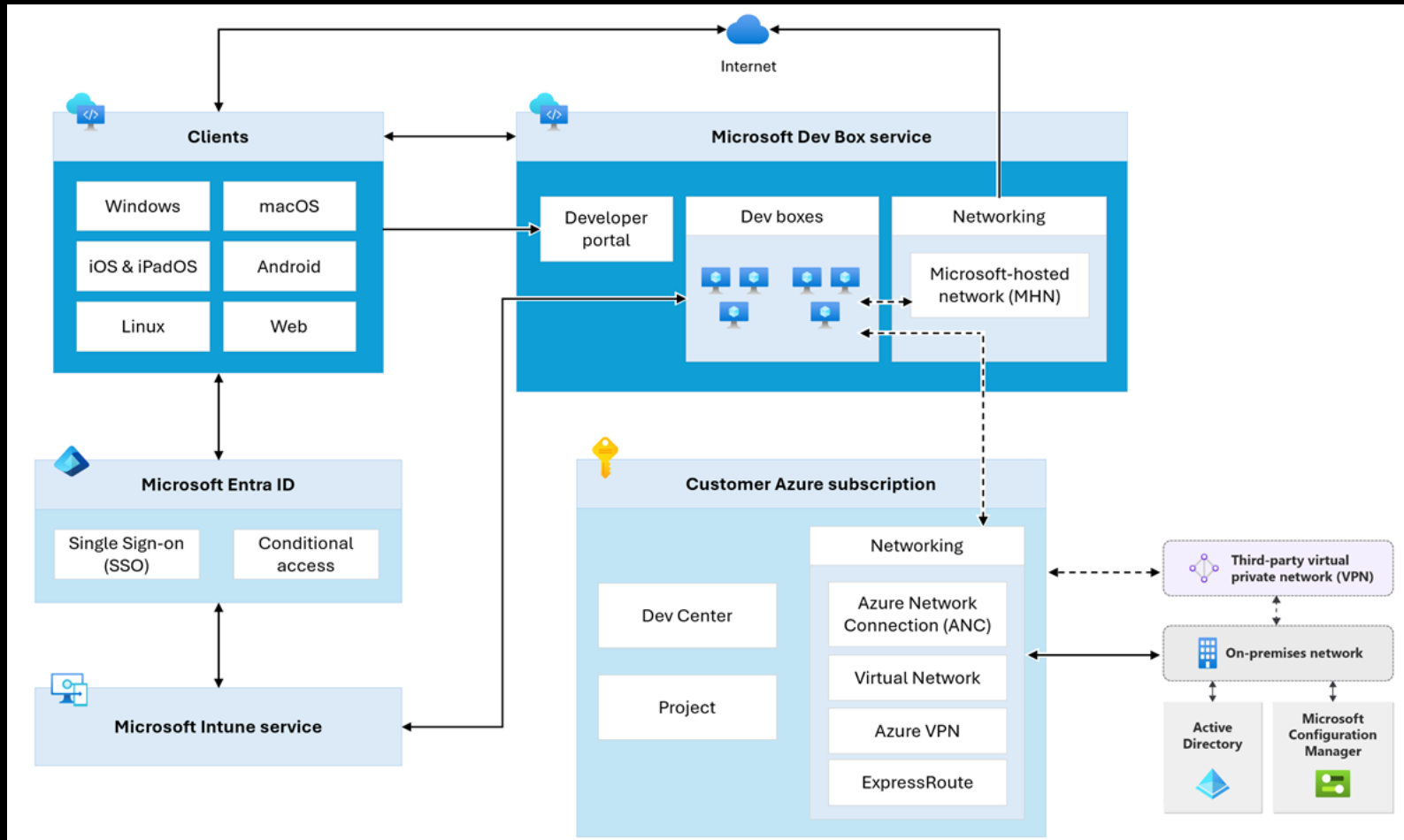


Mikä on Microsoft Dev Box?

| Pilvityöasema (VDI) developer twistillä



Arkkitehtuurista



Windows 365 vs. Azure Virtual Desktop vs. Microsoft Dev Box

Kategoria	Windows 365	Azure Virtual Desktop	Microsoft Dev Box
<i>Infrastrukturi</i>	<ul style="list-style-type: none">Microsoft ylläpitää	<ul style="list-style-type: none">Asiakas ylläpitää	<ul style="list-style-type: none">Microsoft ylläpitää
<i>Verkot</i>	<ul style="list-style-type: none">Anna Microsoftin ylläpitääVoit myös itse ylläpitää	<ul style="list-style-type: none">Asiakas ylläpitää	<ul style="list-style-type: none">Anna Microsoftin ylläpitääVoit myös itse ylläpitää
<i>Identiteetit</i>	<ul style="list-style-type: none">Vain oman yrityksen identiteetit (Entra ID)Tukee federoitua IDP:a	<ul style="list-style-type: none">Vain oman yrityksen identiteetit (Entra ID)Tukee ADFS	<ul style="list-style-type: none">Vain oman yrityksen identiteetit (Entra ID)Vain work & school -tilit
<i>Tietoturva</i>	<ul style="list-style-type: none">Voit konfiguroida MFA:n (Conditional Access)Voit käyttää omaa reititystä & palomuuria	<ul style="list-style-type: none">Voit konfiguroida MFA:n (Conditional Access)Voit käyttää omaa reititystä & palomuuria	<ul style="list-style-type: none">Voit konfiguroida MFA:n (Conditional Access)Voit käyttää omaa reititystä & palomuuria
<i>Kulut</i>	<ul style="list-style-type: none">Lisensoidaan erikseen alkaen 31,30€/käyttäjä/kkSubscription-malli	<ul style="list-style-type: none">Kulutus Azure-infrastruktuurin käytön mukaanKäyttöjärjestelmä lisensoitava joko PAYG, tai BYOLEniten optimoitavissa	<ul style="list-style-type: none">Microsoft IntuneMicrosoft Entra ID P1Microsoft Windows 10/11 EnterpriseDev Box –kapasiteetista maksetaan päälläolon mukaan tuntihintaa
<i>Käyttötapaudet</i>	<ul style="list-style-type: none">Perinteisen toimisto- ja frontline-työntekijän PCPalvelu, infrastrukturi ei kustomoitavissa pl. käyttöjärjestelmä & verkot	<ul style="list-style-type: none">Perinteisen toimisto- ja frontline-työntekijän PCDIY, “kaikki”(infrastrukturi) kustomoitavissa	<ul style="list-style-type: none">Eryyisesti kehittäjille suunnattu työasema, ei niinkään tavallisille käyttäjillePalvelu, infrastrukturi ei kustomoitavissa pl. käyttöjärjestelmä & verkotItsepalvelu kehittäjille

Dev Boxin lisensointi



Microsoft Azure
Microsoft Entra ID
Microsoft Intune.



Microsoft Windows 10/11 Enterprise
Microsoft Intune
Microsoft Entra ID P1.



Microsoft 365 F3
Microsoft 365 E3 / Microsoft 365 E5
Microsoft 365 A3 / Microsoft 365 A5
Microsoft 365 Business Premium / Microsoft 365 Education Student Use Benefit.

Dev Boxin infrastruktuurin hinta

SKU	Pricing per Dev Box Instance		
	Max Monthly Price	Hourly Compute	Monthly Storage
8 vCPU, 32 GB RAM, 256 GB Storage	€143.21	€1.55	€19.69
8 vCPU, 32 GB RAM, 512 GB Storage	€162.90	€1.55	€39.38
8 vCPU, 32 GB RAM, 1,024 GB Storage	€202.28	€1.55	€78.76
8 vCPU, 32 GB RAM, 2,048 GB Storage	€281.03	€1.55	€157.51
16 vCPU, 64 GB RAM, 256 GB Storage	€266.73	€3.09	€19.69
16 vCPU, 64 GB RAM, 512 GB Storage	€286.42	€3.09	€39.38
16 vCPU, 64 GB RAM, 1,024 GB Storage	€325.79	€3.09	€78.76
16 vCPU, 64 GB RAM, 2,048 GB Storage	€404.55	€3.09	€157.51
32 vCPU, 128 GB RAM, 512 GB Storage	€533.45	€6.18	€39.38
32 vCPU, 128 GB RAM, 1,024 GB Storage	€572.83	€6.18	€78.76
32 vCPU, 128 GB RAM, 2,048 GB Storage	€651.58	€6.18	€157.51

Konfiguroi automaattinen sammutus päivittäin ja maksat vain esim. 8h päivässä.

Konfiguroi lepotila (hibernation), kun käyttäjä on inaktiivinen, tai sulkee yhteyden Dev Boxiin.

Monitoroi Dev Boxien utilisaatiota ja käytä pienempiä kokoja (CPU, RAM, storage).

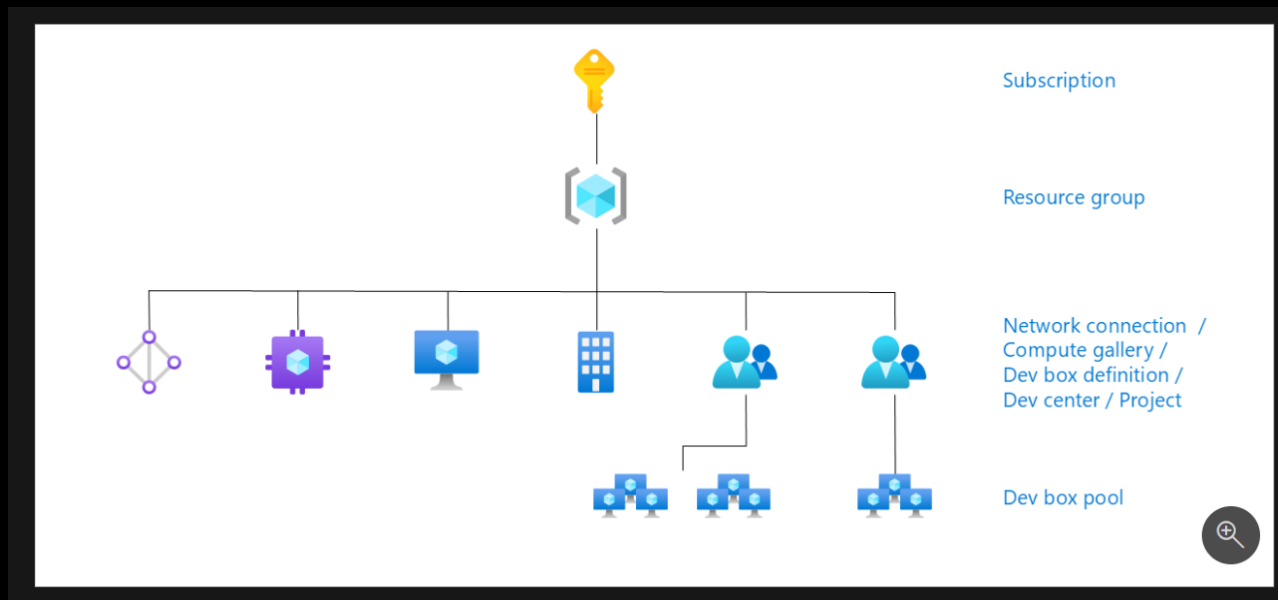
Muista poistaa käyttämättömät Dev Boxit ja et maksa storagesta turhaan!

Identiteettien hallinta

Vain yrityksesi identiteetillä

ⓘ Note

Microsoft Dev Box supports work and school accounts. It doesn't support the use of guest accounts or personal accounts.



Ehdollinen pääsynhallinta (Conditional Access)

Dev Box on automaattisesti Intuneen liitetty ja yrityksesi hallitsema laite.



Kun yrityksesi policyt sallivat resurssien käytön vain hallituilta laitteilta, niin kolmannen osapuolen laitteilla ei voi käyttää palveluitanne (Microsoft Azure, Azure DevOps, ym., ym.).



Omat yrityksen käyttäjät kirjautuvat SSO:lla, MFA ulkopuolisille.



Rajoita tarvittaessa lokaation ja/tai IP-osoitteen perusteella.



Verkon
tietoturva



Hostaa Dev Boxeja omassa virtuaaliverkossasi Azuressa.

Voit tällöin käyttää Network Security Groupeja, omaa reititystä, Azure Firewallia, tai NVA:ta.

Mahdollistaa yhteydet on-premiseen (VPN, ExpressRoute).

Kontrolloi internetyhteyksiä ulospäin. Sisään tullaan turvallisesti vain Microsoftin Windows 365 -palvelun kautta.


Laitehallinta

Hallitset Dev Boxeja Intunessa kuin mitä tahansa muuta laitetta.

Jakele ja päivitä Dev Boxien sovellukset automaattisesti.

Kovenna Dev Boxit configuration policyilla ja baselineilla.

Käytä Intunen Endpoint Privilege Managementia (EPM) antamaan kehittäjille oikeudet asentaa sovelluksia ilman local administrator -oikeuksia.

An aerial photograph of a winding, multi-lane road with several cars driving on it. The road is surrounded by a mix of green grass and patches of snow. The text "Datan hallinta" is overlaid in the center of the image.

Datan hallinta

Dev Boxit ovat *hosted-on-your-behalf*, eli niitä ajetaan Microsoftin subscriptioneissa ja sinulla ei ole pääsyä virtuaalikoneeseen.

Voit käyttää Azure Marketplace imageja, joissa on valmiina esim. Microsoft 365 Apps, Visual Studio jne.

Voit vaihtoehtoisesti tehdä omia custom imageja Azure Compute Galleryyn.

Levyt ovat kryptattuja oletuksena, ei tarvitse säätää BitLockeria erikseen.

Tuottavuus

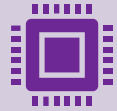
Dev Boxit ovat henkilökohtaisia ja niitä voi olla useita eri käyttötarpeisiin (dev, staging, prod).

Team leadina voit kustomoida oman tiimisi dev boxit tarpeen mukaan.

Yksittäinen kehittäjä voi kustomoida oman dev boxinsa WinGetillä ym. ja jakaa kustomoinnin muille.

Kloonaa git repositorysi valmiiksi Dev Boxiin sen käynnistyttyä.

Dev Boxin hallinta ja etäyhteys



Osoitteessa <https://aka.ms/devbox-portal> kehittäjä luo ja hallitsee Dev Boxejaan.



Selaimella voi myös ottaa etäyhteyden Dev Boxiin (demo).



Paras käyttökokemus Windows App:lla, joka toimii mm. Windowsilla, macOS:lla, iOS:lla, Androidilla/ChromeOS:lla (demo).



Myös Remote Desktop App:lla voi ottaa etäyhteyden.

Rajoitukset ja muut huomiot

Vain Windows-työasemat, WSL Linux-käyttäjille.

Dev Boxin provisiointi kestää ~30-60 minuuttia. (voi ei!)

Kulttuurishokki kehittäjälle, sillä perinteisesti on totuttu paikalliseen kehittämiseen omalla työasemalla.

| Demo





Kiitos!



Not Bad
Security

We are Not Bad Security, a nimble company focused on securing the clouds. Contact us via notbadsecurity.com