E-Opas

360 Secure Fabric
Kohti tietoturvallisia ja älykkäitä verkkoja

aruba
a Hewlett Packard Enterprise company

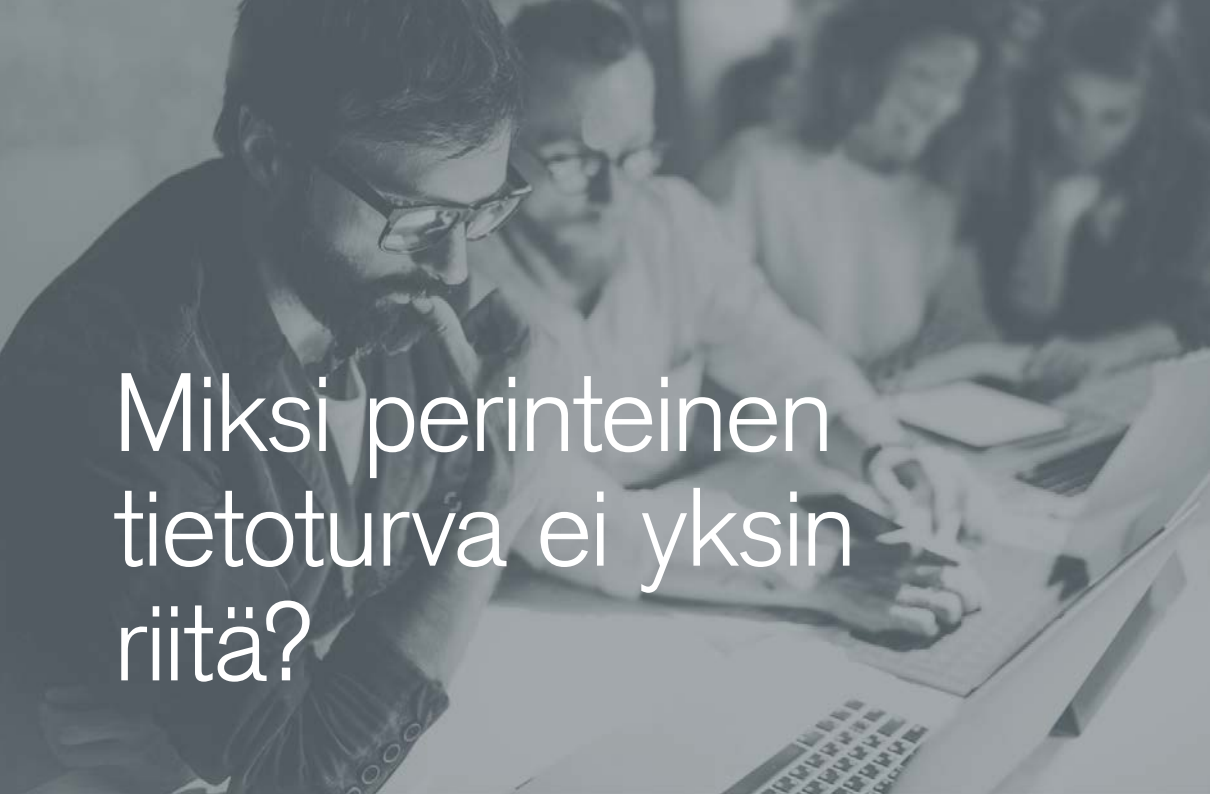
ATEA

Miten suojaat liiketoimintaasi ja verkkoasi digiajassa?

Kerromme tässä oppaassa yritysten liiketoiminnasta ja digitalisaatiosta vastaaville ammattilaisille miksi verkkojen kokonaisvaltainen suojaaminen on niin tärkeää ja miten se on tehtävissä uusimmalla teknologialla. Palveluiden, sovellusten ja ohjelmistojen on toimittava tehokkaasti, ja niiden pitää olla aina käyttäjien saatavilla. Tuotanto, prosessit ja palvelut eivät toimi, mikäli verkoissa ilmenee haasteita. Mobiliteetti, IoT ja hajautetut sovellukset (Esim. Hybridi, Pilvi jne.) asettavat verkkojen tietoturvalle uusia vaatimuksia!

Miten varmistat yrityksellesi suorituskykyiset ja tietoturvalliset verkot? Miten suojaat liiketoimintaasi ja dataasi tekoälyllä? Miten kannattaisi nyt edetä?

Gartner ennustaa*: Maailmassa on vuonna 2020 yli 20 miljardia verkkoon kytkettyä IoT-laitetta.



Miksi perinteinen tietoturva ei yksin riitä?

Tietomurto voi lamaannuttaa organisaatiosi koko liiketoiminnan. Kyberhyökkäykset lisääntyvät nopeasti, ja verkkoon kytketyt laitteet voivat avata hakkereille uusia kanavia toteuttaa yhä ovelampia hyökkäyksiä. Liiketoiminnan jatkuvuuden, kehittämisen ja kasvun turvaaminen vaativat tietoturvallisia verkkoja.

Tietomurtojen havaitsemiseen tarvitaan edistyksellistä analytiikkaa ja tekoälyä sekä identiteettipohjaista ja sovellustietoista verkkoratkaisua. On havaittava myös tilanteet, joissa tietoturvariskin aiheuttaja onkin organisaation verkkoon tunnistettu ja autentikoitu käyttäjä tai laite!

Gartner*: Lähes kaikki CIO:t odottavat kyberuhkien kasvavan lähivuosina.

Mitkä ovat tietoturvallisen verkon tärkeimmät elementit?

1. **Läpinäkyvyys.** Verkkoon, laitteisiin sekä niiden tapahtumiin.

2. **Hallittavuus.** Tehokas pääsynhallinta sekä autentikointi eri laitteille, käyttäjille ja rooleille.

3. **Monitorointi.** Yksinkertainen ja proaktiivinen tapa monitoroida verkon tapahtumia sekä havaita ja torjua poikkeamia eri laitteiden tai käyttäjien toiminnassa.

4. **Reaktiokyky.** Nopea ja automatisoitu kyky reagoida tietoturvariskeihin.

Aruba 360 Secure Fabric

Aruba 360 Secure Fabric mahdollistaa kaikki nämä elementit, ja tarjoaa kattavaa 360 asteen tietoturvaa suurtenkin organisaatioiden vaativiin tarpeisiin. Tehokas suojaustaso saavutetaan roolipohjaisella pääsynhallinnalla (Aruba ClearPass) sekä valvomalla tietoverkossa operoivia käyttäjiä, päätelaitteita ja tietojärjestelmiä hyödyntämällä myös edistyksellistä analytiikkaa ja tekoälyä (Aruba IntroSpect).

Tietoturva on vahvana osana HPE Aruban koko ratkaisu- ja tuotetarjontaa aina laitteista ohjelmistoihin. Aruba 360 Secure Fabric -ratkaisu on yhteensopiva eri laitevalmistajien ratkaisujen kanssa.

Mitä hyötyjä tekoäly tarjoaa?

Tekoäly oppii tunnistamaan tietomurrosta indikoivia kirjautumisyrityksiä, haavoittuvuuksia sekä haittaohjelmia yhä tehokkaammin. Se tarjoaa kykyä ennakoida riskejä, ja hälyttää poikkeamista tietoturvatiimiä. Hyökkäyksestä toipumiseen ei saa mennä liikaa aikaa. Tekoälyä hyödyntämällä hyökkäyksen vastatoimenpiteisiin ja normaalitilan palauttamiseen voidaan ryhtyä tuntien tai päivien sijaan minuuteissa.

Tekoälykäs ratkaisu oppii yhä fiksummaksi, kun tarjolla on reaaliaikaista dataa mm. laitekategorioista, valmistajista ja käyttöjärjestelmäversioista. Historia- ja lokitiedot, sekä tiedot mahdollisen hyökkäyksen tai tietomurron laajuudesta ovat visuaalisen käyttöliittymän kautta heti saatavilla.

Mitä kaikkea organisaatioltasi vaaditaan?

Liiketoiminnalle olennaisen tietopääoman, kuten asiakas- ja henkilödatan sekä tuotekehitystiedon, laitteiden, liiketoiminnan sekä yrityksen maineen suojaaminen edellyttävät digiajassa mm. näitä kyvykkyyksiä!

- Tunnistat ja valvot kaikkia verkkoon kirjautuvia käyttäjiä, laitteita ja tietojärjestelmiä. Tiedät reaaliaikaisesti, kuka on kirjautunut ja millä laitteella mihinkin tietojärjestelmään sekä milloin.
- Analysoit ja monitoroit käyttäjien käyttäytymistä sekä havaitset tietomurrosta indikoivia kirjautumisyrityksiä, haavoittuvuuksia sekä haittaohjelmia.
- Saat hälytyksiä tietoturvariskeistä sekä automaattisen kyvyn reagoida sisäverkostakin tuleviin tietoturvariskeihin.
- Luot soveltuvat pääsyoikeudet verkkoon ja resursseihin, kuten tietojärjestelmiin.

Miten sinun kannattaisi toimia?

Suosittelemme kartoittamaan verkkoympäristösi nykytilanteen, riskit ja miten verkkosi vastaavat käyttäjien tarpeita. Tässä viisi hyväksi todettua vinkkiä!

- Kartoita ympäristösi, ja selvitä verkkojen tietoturvataso. Tunnista heikkoudet ja kehityskohteet.
- Nosta verkkojen tietoturvatasoa suunnitelmallisesti.
- Valitse pätevä kumppani, jolla on kokemusta verkoista, tietoliikenteestä ja tietoturvasta sekä riittävät osaamisresurssit ja kattavat palvelut. Tarvitset monipuolista osaamista ja hyvää tiimiä.
- Vaadi oikeat työkalut ja edistyksellistä teknologiaa, joka palvelee liiketoimintasi ja käyttäjiesi tarpeita myös tulevaisuudessa. *Onko ratkaisu optimaalinen meille ja mitä ominaisuuksia se tarjoaa?*
- Varmista, että verkkoa ja tietoturvaa kehitetään maailman muuttuessa.

Mistä saat apua?

Atean ammattilaiset kertovat minkälainen verkko palvelisi parhaiten liiketoimintasi jatkuvuutta! Atea hyödyntää teknologiariippumattomana toimijana markkinoiden parhaita verkkoratkaisuja. On yhä tärkeämpää, että yritystäsi uhkaavat riskit tunnistetaan tehokkaasti. HPE Aruba tarjoaa uutta teknologiaa laadukkaampien verkkojen ja arkkitehtuurien rakentamiseen. Atea on HPE Aruban kumppani.

*Gartner, Press Release, February 2017
**Gartner, CIO Agenda Survey 2018

aruba
a Hewlett Packard Enterprise company

ATEA

www.atea.fi
customercare@atea.fi
010 613 611