Cinia

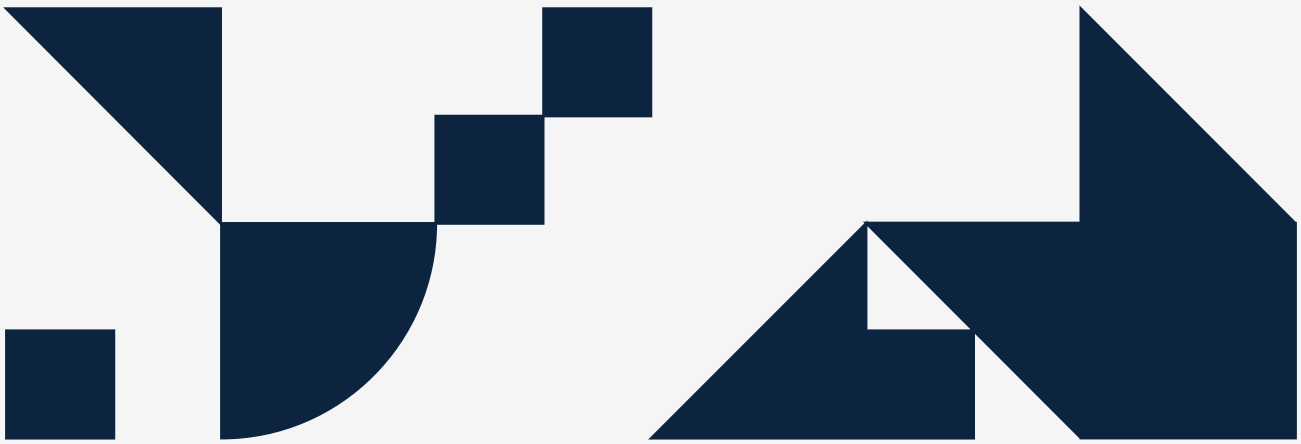
Opas:

# Monitorointi osana jatkuvuudenhallintaa

Varmista liiketoimintakriittisten digipalvelujen saatavuus

# Sisältö:





# Miten hyvin digitaaliset palvelusi toimivat?

Yllättävän moni ei tiedä vastausta otsikon kysymykseen. Näin on, vaikka liiketoiminta pyörii yhä enemmän digitaalisten ympäristöjen ja niiden käyttökokemuksen varassa. Samaan aikaan kyberhyökkäysten määrä on nousussa, ja IT-ratkaisuja rakennetaan entistä monimutkaisempien toimittajaverkostojen varaan.

Jos digitaalisten palveluiden reaaliaikainen monitorointi ei ole kunnossa, tieto viiveistä tai katkoksista saattaa tihkua IT-tiimille pikkuhiljaa pieniä puroja pitkin, esimerkiksi asiakaspalvelun yhteydenottojen kautta. Silloin on jo myöhäistä.

Millaisiin riskeihin organisaatiosi pitäisi varautua ja mitä kaikkea tulisi monitoroida kattavan tilannekuvan muodostamiseksi? Siihen saat vastauksia tästä oppaasta.

# Miksi digitaalisia ympäristöjä täytyy valvoa reaaliaikaisesti?

Kuluttajana on vaikeaa ajatella elämää ilman sähköisiä palveluja. Liian pitkät latautumisajat tai pätkivät yhteydet ovat kiusallinen vaiva kenelle tahansa. Käyttäjien odotukset saumatonta käyttökokemusta kohtaan kasvavat tulevaisuudessa entisestään.

Yritysten ja organisaatioiden näkökulmasta ongelma on vielä paljon kriittisempi. Miten oma liiketoimintasi kestäisi tilanteen, jossa kaiken ytimessä sykkivät digitaaliset palvelut tai niihin liittyvät alustat ja järjestelmät eivät toimikaan kuten pitää?

## Vaakalaudalla raha, maine, yhteiskunnan toimivuus ja turvallisuus

Toimialojen erityispiirteet lisäävät panoksia jatkuvuudenhallinnan varmistamiseen. Tehokkaaksi viritetyssä teollisessa tuotannossa jokaisen sekunnin viivästys maksaa. Finanssialalla maineella ja asiakkaiden luottamuksella on suuri merkitys. Logistiikkaa ja liikennettä ohjaavan datan täytyy liikkua, jotta fyysinen maailma toimii kuten pitää. Energiasektorilla digitaalisten ympäristöjen ongelmat voivat pahimmillaan vaikeuttaa sähkön tai lämmön jakelua, sosiaali- ja terveysalalla taas ihmisten turvallista hoitoa.

## Ongelmien rajaaminen voi olla hidasta

Monimutkaisissa digitaalisissa ympäristöissä ongelmien selvitys ja rajaaminen ilman kunnollista valvontaa on hidasta ja hankalaa. Nopea diagnostiikka edellyttää useiden eri mittauspisteiden kytkemistä yhteen näkymään. IT-ympäristöjen laajan tilannekuvan ja jatkuvan monitoroinnin merkitys korostuu entisestään, kun puhutaan yhteiskunnalle kriittisistä palveluista, joiden toimivuus on varmistettava koko ajan.

## Huolena kyberuhkat ja toimitusketjujen tietoturva

Kaikki toimitusketjusi organisaatiot kohtaavat ympärillään saman uhkamaiseman: kyberhyökkäysten määrä on lisääntynyt viime vuosina huimasti. Yksi on varautunut ransomware-riskeihin tai palvelunestohyökkäyksiin hyvin, toinen ei niin luotettavasti.

Oma liiketoimintasi voi katketa, jos kumppani joutuu kyberhyökkäyksen kohteeksi. Silloin esimerkiksi integraatiot välillänne eivät enää toimi luotettavasti. Ilman omaa monitorointia olet täysin kumppanin ulkoisten viestintäkanavien varassa: mitä tapahtui, kenelle tapahtui, millaiset vaikutukset sillä on järjestelmiisi? Tarvitset tiedon, jotta voit rajata hyökkäyksen vaikutukset minimiin ja viestiä omille asiakkaillesi ennen kuin he hätääntyvät.

# Esimerkkejä jatkuvuudenhallinnan haasteista

## Case 1: Konesalitoimittaja ja asiakas ovat eri mieltä palvelujen saatavuudesta

Toimittajan mukaan konesalipalvelut toimivat hyvin, mutta asiakkaan mielestä palvelut eivät ole sopimuksen mukaisia. Niissä esiintyy hidastelua ja lyhyitä katkoja.

Pääsy konesaliin voi olla estynyt palomuuriongelman takia tai verkkoreitityksissä voi olla häiriöitä. Kokonaisuus ei siksi toimi sovitusti. Jos palvelun saatavuutta valvotaan vain konesalin sisältä, ei nähdä sitä, miten palvelu toimii ulkoapäin päästä päähän.

**Ratkaisu: Monitoroi palvelua mahdollisimman hyvin sieltä, mistä sitä käytetään.**

## Case 2: Työntekijät eivät pääse kirjautumaan potilastietojärjestelmään

Useampi hyvinvointialueen yksikkö on siirtynyt käyttämään samaa potilastietojärjestelmää, ja yhtäkkiä huomataan, etteivät kaikki työntekijät pääse kirjautumaan siihen sisään. Aiemmin aamulla töihin tulleet pystyvät jatkamaan käyttöä normaalisti.

Järjestelmätoimittajalta on jäänyt huomaamatta ominaisuus, joka estää uusia käyttäjiä kirjautumasta aina, kun tietojärjestelmän käyttäjämäärä ylittää tietyn rajan.

**Ratkaisu: Mittaa ja valvo järjestelmien kokonaisuutta niin, että pystyt rajaamaan ongelman nopeasti, ja pystyt pyytämään juuri oikeaa yhteyshenkilöä korjaamaan sen.**

## Case 3: Käyttökokemus hidastui ohjelmisto-päivityksen jälkeen

Asiakas päivittää verkkopalveluunsa uuden ohjelmistoversion. Testiympäristössä se on toiminut moitteettomasti, mutta tuotannossa vasteaika nousee.

Uuden ohjelmistoversion tietokanta ei kykene vastaamaan kyselyihin, kuten pitäisi, ja käyttäjäkokemus kärsii. Testeissä ajetut käyttäjämäärät ovat olleet paljon alhaisempia kuin oikeassa elämässä.

**Ratkaisu: Ilman reaaliaikaista monitorointia vasteajan nousu olisi jäänyt havaitsematta. Ohjelmiston hidastelusta ja katkoista olisi tullut tieto IT-tiimille vasta, kun asiakaspalveluun alkaisi tulla valituksia.**

## Case 4: Selittämättömiä katkoja sovellusten toiminnassa

Liiketoimintakriittiset sovellukset lakkaavat ajoittain toimimasta ilman selvää syytä. Ongelmat osuvat samoihin ajankohtiin, jolloin yrityksen verkkoon suuntautuu päivityksiä toimittajan konesalista. Mittareiden mukaan yritysverkko toimii hyvin ja laadukkaasti, mutta liiketoiminta on silti jumissa.

Lopulta valvontaratkaisu osoittaa, että toimittajan palomuurista ei pääse läpi kuin tietty määrä liikennettä. Päivitysten aikaan liikennemäärä ylittyy. Kun ongelma korjataan, sovellukset toimivat taas luotettavasti.

**Ratkaisu: Monitoimittajaympäristöissä ongelmien juurisyiden selvittely voi olla hyvin hankalaa, vaikka aikaa ei olisi hukattavaksi. Hyvin toteutettu, kattava valvonta on erittäin tärkeä apuväline ongelmien ratkaisussa.**

# Monitoroi ainakin näitä asioita, kun haluat varmistaa palvelun laadun

# 1. Käyttökokemus päästä päähän

Palvelun laatua pohtiessa lähde liikkeelle siitä, kuka, mistä ja miten käyttää yrityksen digitaalisia palveluja. Käyttäjäryhmien tunnistamisen jälkeen voit määritellä, miten monitorointi tulee toteuttaa, jotta palvelun laatua ja saatavuutta seurataan oikein.

Palvelun ketju palvelimilta loppukäyttäjälle toimii juuri niin hyvin kuin sen heikoin lenkki. Nykyaikainen valvontaratkaisu simuloi järjestelmien käyttöä, kuten oikea käyttäjä niitä käyttäisi. Näin saadaan selville todellinen käyttökokemus, joka kertoo miten hyvin IT-ratkaisu toimii päästä-päähän (end-to-end).

# 2. Monitoimittajaympäristöt ja rajapinnat

Monitoimittajaympäristöissä vaatimus palvelujen saumattomuudesta korostuu entisestään. Kyky ongelmista palautumiseen ja liiketoiminnan jatkuvuuteen on aiempaa kovemmalla koetuksella, ellei monitorointi ulotu mahdollisimman kattavasti eri rajapintoihin ja integraatioihin.

Kumppanisi voi kertoa, että heidän järjestelmässään on kaikki kunnossa, ja samaa voit sanoa omistasi. Palvelun käyttäjän kannalta on kuitenkin yhdentekevää, missä kohtaa ongelma on, ja se voi löytyä rajanpinnasta, joka ei palauta sisältöä kuten pitää.

Jokainen toimija valvoo useimmiten vain omalla vastuullaan olevaa aluetta eikä sitäkään välttämättä kovin tarkasti. Perusteelliseen vianselvitykseen eivät eri palveluntarjoajien valvonnat välttämättä riitä.

Jos hoidat oman monitorointisi riittävän kattavasti, pystyt paikantamaan vian ja ohjaamaan korjaustoimenpiteet heti oikealle vastuutaholle.

# 3. Pilvipalvelut

Pilviympäristöjen hyödyntäminen ja monipilviratkaisut ovat yleistyneet sitä mukaa kun legacy-järjestelmiä on uudistettu ja uutta rakennettu. Monipilviratkaisuilla tarkoitetaan ICT-järjestelmiä, jotka on hajautettu useamman pilvipalvelun ja/tai konesalin välillä.

Pilvimaailma ja hajautetut ympäristöt tuovat lisää haasteita palvelutason ja jatkuvuuden hallintaan. Monitoroinnin avulla pystyt vastaamaan muun muassa näihin kysymyksiin: Miten yhteydet pilvipalveluihin toimivat? Entä pilvien väliset yhteydet? Miten toimivat itse sovellukset ja niihin liittyvät teknologiat?

# 4. Sovittujen palvelutasojen seuranta (SLA)

Saatko todellisuudessa sitä, mitä tilasit? Reaaliaikainen monitorointi antaa mitattua, puolueetonta tietoa, joka auttaa keskusteluissa toimittajan kanssa. Mittarien antamista luvuista on hyötyä varsinkin silloin, jos palveluntarjoaja kiistää ongelmat ensin kokonaan.

Toisaalta jatkuva valvonta auttaa huomaamaan, jos olet tilannut tarpeeseen nähden liikaa. Voit tehdä dataan nojaavia päätöksiä ja maksaa vain siitä, mitä tarvitset.

## Lokienhallinta on tärkeä osa it-ympäristöjen ylläpitoa

Lokien tarjoamaa tietoa ei kannata jättää hyödyntämättä. Sitä voi kerätä tänä päivänä helposti ja kustannustehokkaasti.

Keskitetty lokienhallinta on sitä oleellisempaa, mitä kriittisempiä palvelut ovat. Lokitiedostot sisältävät tärkeää tietoa muun muassa verkkolaitteiden, ohjelmistojen ja järjestelmien

hyvinvoinnista ja vikatilanteista. Lokitietojen avulla voidaan seurata myös tapahtumaketjuja, eli sitä, kuka on käyttänyt mitäkin laitetta, mihin aikaan ja mitä laitteella on tehty.

Reaaliaikaista ympäristöjen monitorointia täydentävän SIEM-palvelun (Security Information Event Management) avulla havainnoit tietoturvapoikkeamat, reagoit niihin viipymättä ja selvität, mitä tapahtui. Mikä arvokkainta: lokitietojen avulla voi ennakoida myös tulevaisuudessa tapahtuvia vikatilanteita.

# Koska valvontaan kannattaa kiinnittää erityistä huomiota?

# 1. Digitaaliset palvelut ovat liiketoiminta-kriittisiä

Ei ole väliä, käytätkö itse kehitettyä palvelua vai ulkopuolista SaaS-ohjelmistoa, kuten ERP-järjestelmää. Jos koko liiketoimintasi pyörii ydinpalvelujen varassa, tarvitset proaktiivista valvontaa, joka simuloi käyttäjän todellista kokemusta. Siten ehdit reagoida ongelmiin ennen kuin on myöhäistä.

# 2. Palvelusi on riippuvainen ketjun muista toimijoista

IT-ympäristöjen kompleksisuus lisää ylläpidon haasteita. Pätkimisen tai hidastelun juurisyyn selvittely voi viedä kohtuuttoman paljon aikaa. Onko toimittajakumppanin järjestelmissä viivettä, toimivatko rajapinnat kuten pitää? Ongelman rajaamista helpottaa, jos tieto virtaa useista eri lähteistä yhteen tilannekuvaan.

# 3. Toimittaja vaihtuu

Organisaatioiden murros- ja muutosvaiheet asettavat omat haasteensa palveluiden laadulle. Toimittajan vaihtuminen on hyvä esimerkki ajankohdasta, jolloin valvonnasta on erityisen paljon hyötyä. Esiintyykö katkoksia ja jos, niin kuinka pitkiä? Palautuvatko palvelut, kuten pitää? Monitoroinnin avulla varmistat sovitun palvelutason toteutumisen heti alussa.

# 4. “Mutun” sijaan tarvitset mitattua tietoa

Käyttäjien antama palaute voi hämärtää käsitystä palvelun todellisesta laadusta. Vain mitattu ja täsmällinen tieto auttaa arvioimaan, mikä todella toimii, ja mitä on järkevää parantaa seuraavaksi.

OPAS: MONITOROINTI OSANA JATKUVUUDENHALLINTAA

# Kokemuksia digitaalisten ympäristöjen monitoroinnista

# Pohjantähti: Valvontaratkaisu tuo varmuutta liiketoiminnan jatkuvuuteen

Yli 120 vuotta toimineessa vakuutusyhtiö Pohjantähdessä on viety viime vuosina läpi isoja uudistuksia vakuutus-, korvaus- ja asiakaspalvelujärjestelmiin. Yhtiön IT-infrastruktuuri kattaa kymmeniä sovelluksia ja tietoliikenneyhteyksiä sekä yli sata palvelinta.

Asiakkaat odottavat, että verkkopalvelut toimivat laadukkaasti vuorokauden ympäri. Jokaisen IT-ratkaisun, joka vaikuttaa käyttäjän kokemukseen, pitää toimia ilman häiriöitä. Siksi ympäristöjä monitoroidaan proaktiivisesti.

**”**

**Näkyvyys IT-ympäristöömme, sovelluksiin ja tietoliikenteeseen on parantunut selvästi, ja tiedämme tarkasti mitä ympäristössämme tapahtuu.**

Lue lisää

# Säteilyturvakeskus: Nopeaa reagointia häiriötilanteisiin

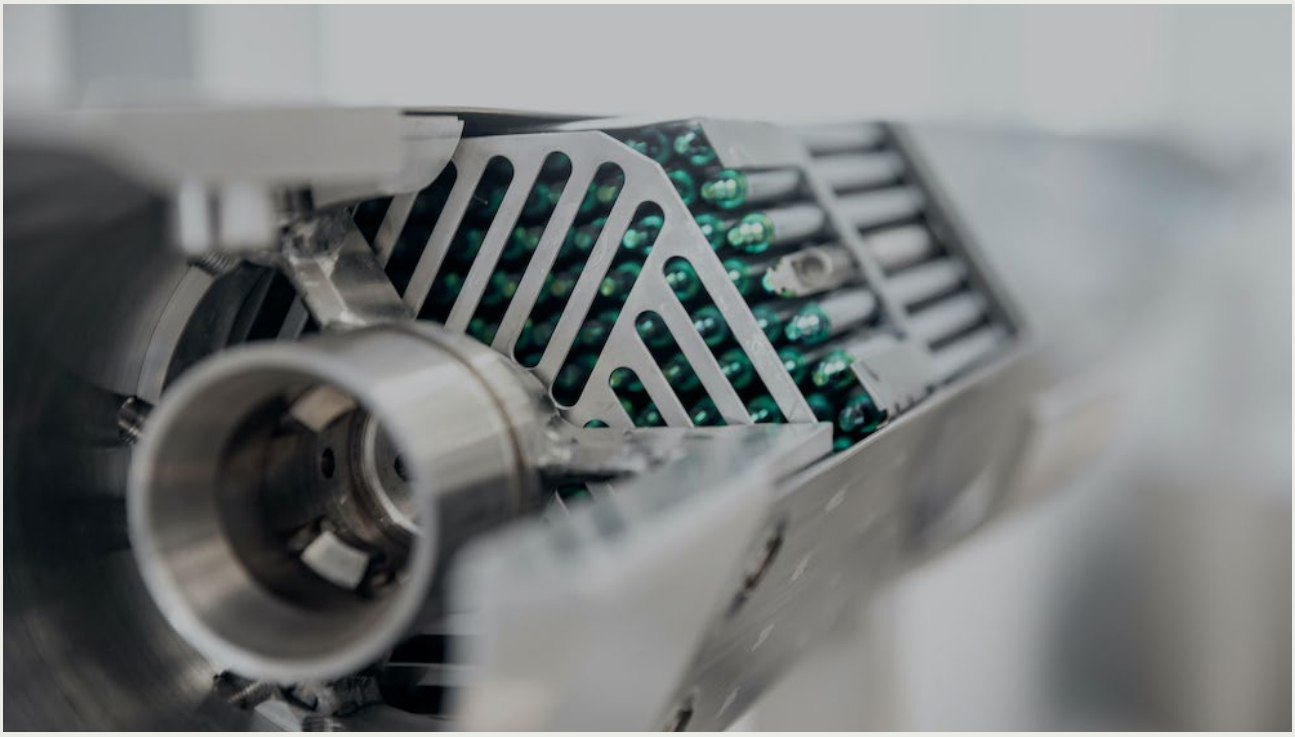
Valvovana viranomaisena Säteilyturvakeskus tekee töitä koko Suomen turvallisuuden eteen.  Siksi STUKin ICT-järjestelmien valvonnan täytyy toimia 100 % varmuudella vuorokauden ympäri.

STUK valvoo ja mittaa palvelinten ja palveluiden saatavuutta Cinian valvontaratkaisulla. Sama tilannekuva antaa tietoa myös ulkoisten toimittajien palvelujen laadusta.

**”**

**Cinian valvontaratkaisua on helppo suositella oikeastaan kaikille yrityksille. Nykypäivänä valvontajärjestelmät ovat välttämättömiä kaikille. Jos valvontaa ei ole, se tarkoittaa, että silloin on jotain pielessä.**

**Lue lisää**



# Vastuu Group: Monta pilveä, monta toimittajaa

Vastuu Group Oy:n digipalvelut varmistavat, että rakennusalan eri tahot noudattavat tilaajavastuu- ja veronumerolakia. Loppukäyttäjät odottavat saavansa palvelua reaaliajassa, nopeasti ja luotettavasti.

Palveluiden kriittisyys, monipilvi- ja monitoimittajaympäristö sekä eri järjestelmien keskinäinen riippuvuus vaikuttivat siihen, että Vastuu Group tarvitsi monipuolisen työkalun, joka on valmis kasvamaan liiketoiminnan mukana.

**"**

**Kahvipöydässä voi aina keskustella palvelun nopeudesta tai hitaudesta, mutta ilman mittaustuloksia kyse on "mutu" -tiedosta eikä oikeasta datasta. Cinian ratkaisun kautta saamme täsmällistä dataa. Kun nykytilanne on tiedossa, voidaan laatua parantaa tarpeen mukaan.**

Lue lisää

# Näin saat valvontaratkaisun käyttöösi

**Cinia cEye** on reaaliaikainen valvontaratkaisu, joka antaa kattavan näkyvyyden IT-ympäristöihisi. Sen selkeä dashboard esittää kuvan kokonaisuuden toimintakunnosta aina infrasta sovellustasolle asti.

Valvontaratkaisua käytetään useilla eri toimialoilla, mutta yksi tekijä yhdistää kaikkia asiakkaitamme: he haluavat tarjota omille asiakkailleen mahdollisimman laadukasta palvelua. Kuulutko joukkoon?

1. **Ota yhteyttä, niin varataan tapaaminen.** Käymme yhdessä läpi, millaisista elementeistä IT-ympäristösi muodostuu.
2. **Saat tarjouksen.** Palvelun sisältö ja kuukausimaksu määräytyy tarpeidesi mukaan.
3. **Autamme sinua listaamaan tekniset vaatimukset ja määrittelyt.** Niiden perusteella voit pyytää tarvittavat tiedot ja konfiguraatiot IT-toimittajiltasi.
4. **Kytkemme Cinia cEyen käyttöösi** avaimet käteen -palveluna.
5. **Nimetyt asiantuntijat auttavat saamaan Cinia cEyesta täyden hyödyn irti.** Tiimin osaaminen on käytössäsi koko asiakkuuden ajan, ja kehitämme valvontaasi jatkuvasti.

**Ota yhteyttä**

Cinia

# Cinia tuo varmuutta monimutkaistuvaan digitaaliseen maailmaan

Cinia on suomalainen digitaalisten toimintaympäristöjen turvaaja ja kriittisten, korkean toimintavarmuuden yhteyksien ja ohjelmistojen asiantuntija.

Yhdistämällä laaja-alaisen osaamisemme sekä uusimman teknologian toteutamme julkishallinnon ja yksityisen sektorin asiakkaillemme laadukkaat tietoverkko-, kyberturvallisuus- ja ohjelmistoratkaisut, jotka toimivat tänään ja huomenna.

Painimme kokemuksen tuomalla varmuudella digitaalisten haasteiden raskaassa sarjassa niin kotimaassa kuin kansainvälisesti yli 400 asiantuntijan voimin.