LAUREA

F-Secure Client Security 9 -asennus ja testaus työasemissa

Tanninen, Marko

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

F-Secure Client Security 9 -asennus ja testaus työasemissa

Tanninen, Marko
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tanninen, Marko

F-Secure Client Security 9 -asennus ja testaus työasemissa

Vuosi 2011 Sivumäärä 68

Tämän opinnäytetyön tarkoituksena on selvittää soveltuuko F-Secure Client Security 9 paremmin yrityksen tietoturvaksi kuin vanha F-Secure Client Security versio 8. Opinnäytetyö sisältää ohjelman asennuksen, konfiguroinnin ja testaamisen. Tämän lisäksi opinnäytetyössä käsitellään myös tietoturvallisuuden historiaa ja sen kehitystä vuosien varrella.

Opinnäytetyön aihe ja toimeksianto tuli suoraan asiakkaalta ja toimeksiantajalta, joten vaihtoehtoisten virustentorjuntaohjelmien vertailu ei tullut kyseeseen tässä työssä.

Opinnäytetyössä oli tarkoituksena mitata työasemien käynnistyksen kestoa, ohjelman täystarkistuksen kestoa, muistin käyttöä sekä yleisesti käyttäjien mielipiteitä ohjelmasta. Työasemien testaamiseen käytettiin Microsoftin valmiita raportointityökaluja, F-Securen Policy Manager hallintatyökalua sekä Hewlett-Packard Operation Manager for Windows-ohjelmaa.

Kysely käyttäjille toteutettiin sähköpostin välityksellä. Kysymykset toteutettiin suurimmaksi osaksi avoin kommentti tyylillä. Kyselyn perusteella käyttäjät tuntuivat olevan tyytyväisiä uuteen ohjelmaan. Suurin osa käyttäjistä ei ollut huomannut oikeastaan mitään muutosta tai muutosta ainakaan huonompaan suuntaan käytettävyydessä. Palautteita tuli yhteensä 22 kappaletta.

Asiasanat F-Secure, F-Secure Client Security 9, tietoturva, virus,

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Business Information Technology

Tanninen, Marko

F-Secure Client Security 9 installing and testing in workstations

Year 2011 Pages 68

The purpose of this thesis is to discover whether the F-secure Client Security 9 adapts better to being the main information security program than the earlier version F-secure Client Security 8. The thesis includes installing the program, as well as configuring and testing it. Additionally it includes retrospection into the history of information security and its development over the years.

The subject and assignment were directly commissioned by the client and employer, so comparing various alternative antivirus programs could not be considered.

The purpose of this thesis was to measure the duration of starting workstations, the duration of program full scans and the general opinion of the users regarding the program. The workstations were tested by using Microsoft's complete reporting tools, F-Secure's Policy Manager management tool and also Hewlett-Packard's Operation management for Windows program.

The survey was conducted via email and the form of the questions used was mainly open comments. On the basis of the survey it was concluded that the users seemed to be content with the new program. The majority of users had not actually noticed any difference or at least any turn for the worse. A total of 22 feedback items were received.

Keywords F-Secure, F-Secure Client Security 9, information security, virus

Sisällys

1 Johdanto

Virustorjunnan jatkuva päivittäminen on välttämätöntä nykyaikana, koska uusia viruksia ja haittaohjelmia syntyy jatkuvasti lisää. Virusten muuntautumiskyky lisää haasteita virusten torjunnalle. Yhteiskunnan haavoittuvuus on lisääntynyt, koska tietotekniikka ulottuu niin monille alueille. Tietokoneiden sisältämän tiedon määrä kasvaa jatkuvasti. Ilman ajan tasalla olevaa virustorjuntaa tietojärjestelmät eivät tunnista mahdollisia uusia viruksia ja ne saattavat aiheuttaa vakavia ongelmia yrityksen toiminnalle.

Nykyinen virustentorjuntajärjestelmä oli yrityksessä todettu varsin raskaaksi. Ohjelman oli todettu hidastavan ja jopa estävän työaseman normaalin käytön virustorjunnan täystarkistuksen aikana. F-Secure oli markkinoinut, että uusi F-Secure Client Security 9 on nopeampi ja kevyempi kuin edellinen F-Secure Client Security 8. Uuden version suorituskykyä yrityksen ympäristössä päätettiin testata. (F-Secure 2010.)

Jos uusi versio testauksen tuloksena osoittautuisi paremmaksi, niin yritys ottaisi sen käyttöön. Yritys odottaa, että uuden virustorjuntaohjelman käyttöönotolla säästetään työaikaa ja työaseman käytettävyys lisääntyy.

Opinnäytetyössä syvennytään F-Secure Client Security 9 asentamiseen, konfigurointiin ja testaamiseen. Työssä käydään läpi myös virusten ja virustorjunnan historiaa sekä ympäristössä tällä hetkellä olevaa F-Secure Client Security 8 versiota. Vanhaa versiota käytetään työssä vertailukohteena uuteen versioon.

2 Testausprojektin tavoitteet

2.1 Yritys ja testiympäristö

Yrityksellä on Suomessa 1830 työasemaa, 360 palvelinta, 140 trukkipäätettä, 445 tuotannon työasemaa ja 135 erilaista Windows-päätettä. Työasemissa käytetään pääsääntöisesti käyttöjärjestelmänä Windows XP:tä, mutta myös Windowsin 7 versio on käytössä muutamassa työasemassa. Suurimmassa osassa palvelimia on käytössä Windows Server 2003, mutta myös Windows 2008 ja eri Linux-versiot on käytössä osassa palvelimista. Virustorjunta hoidetaan F-Secure 8-ohjelmistolla.

Yrityksen pääkonttori on Helsingissä ja sillä on toimipaikkoja noin 20 paikkakunnalla Suomessa. Lisäksi myyntipisteitä on useilla pienemmillä paikkakunnilla. Ulkomailla yrityksellä on yhteensä 400 työasemaa ja 30 palvelinta. Toimipisteitä on muun muassa Venäjällä, Ruotsissa ja Virossa, mikä aiheuttaa lisää haasteita virustorjunnalle.

Työasemia ja palvelimia on sekä tuotanto että toimistokäytössä. Erikseen on asennettu erillinen virustorjuntapalvelin, jonka tehtävänä on hoitaa sekä ulos että sisääntulevan sähköpostiliikenteen virustorjuntaa. Koska tuotantoympäristöt on erotettu palomuureilla toimistoverkoista, virustorjuntaa varten on avattu palomuuriin portit virustorjuntapalvelimeen. Sieltä jaetaan keskitetysti virustorjuntapäivitykset tuotantoverkon palvelimille ja työasemille. Palvelimien kriittisyysaste on huomioitu toimittajan palvelusopimuksissa. Testaukseen valittiin mukaan 40 normaalissa toimistokäytössä olevaa työasemaa.

2.2 Työn rajaus ja projektin vaiheet

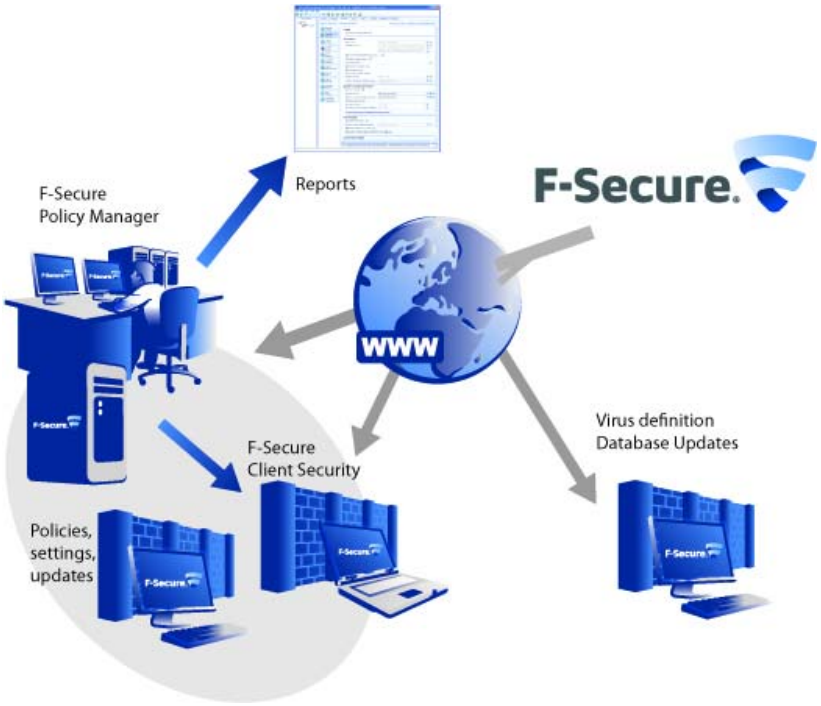
Projektin tavoitteena oli testata F-Secure Client Security 9:n suorituskykyä työasemissa. Projektissa verrataan vanhan F-Secure Client Security 8:n ja uuden F-Secure Client Security 9:n kuormitusta laitteille. Ohjelman asetuksien, tarkistuksien ja muiden ominaisuuksien hallintaan käytetään F-Securen Policy Manager konsolia. Työasemat ovat laitetehoiltaan erilaisia. Tästä syystä vertailuja tehdään vain työasemakohtaisesti, eikä niitä voida vertailla keskenään. Ohjelman palvelinversiota ei tässä testattu.

Projektin vaiheisiin kuului ohjelman asennus, konfigurointi ja testaus. Projektin aikataulu oli kolme kuukautta. Se jaettiin kolmeen osaan eli ohjelman asennukseen, konfigurointiin ja testaukseen. Jokaisen vaiheen oli tarkoitus kestää noin kuukauden. Asennus ja konfigurointi saatiin toteutettua hyvin aikataulussa, mutta testausvaihe kesti odotettua pidempään.

Asennusvaiheen tarkoitus oli asentaa palvelin, F-Secure Policy Manager konsoli, tarvittava määrä OMW-agentteja sekä laittaa UserEnvDebuglevel -lokitus työasemiin. Konfigurointivaiheessa taas oli tarkoitus määritellä tarvittavat asetukset Policy Manager konsolilla, jotta työasemiin voitaisiin asentaa Client Security. Ennen uuden Client Securityn asentamista täytyi suorittaa suorituskykymittaukset vanhalla versiolla. Näistä otettiin tiedot talteen dokumentteihin myöhempää tarkastelua varten. Asetusten määrittämisen jälkeen suoritettiin F-Secure Client Security 9:n asennus. Tämän jälkeen suoritettiin suorituskykymittaukset uudella F-Secure Client Security versiolla. Viimeisenä vaiheena tehtiin suorituskykyvertailut versioiden välillä sekä toteutettiin käyttäjäkysely. Lopuksi esitettiin tulokset asiakkaalle.

3 F-Secure–ohjelmistot

Seuraavassa kuvassa käydään läpi F-Secure ohjelmistojen toimintamallia yleisellä tasolla ja sitä miten kukin komponentti toimii kokonaisuuden kannalta.



Kuva 1: F-Secure tuotekaavio (F-Secure 2009)

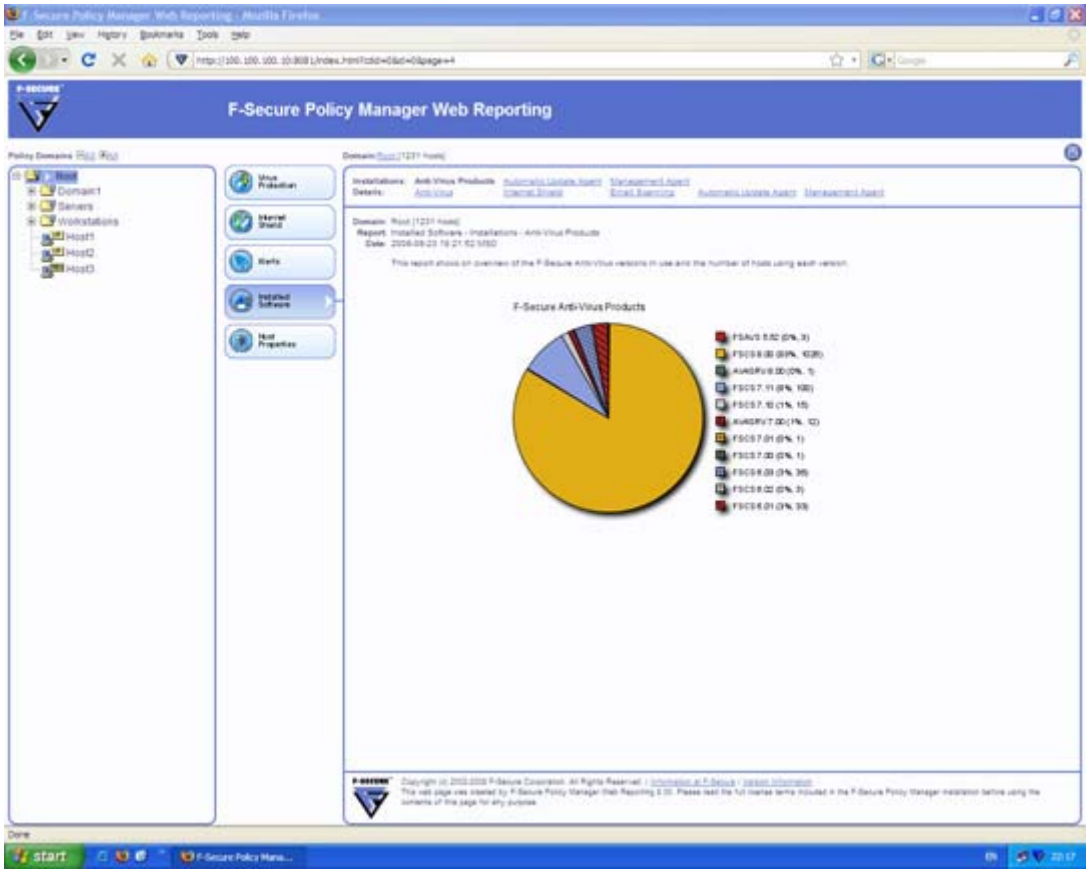
3.1 F-Secure Policy Manager

F-Secure Policy Manager on hallinta- ja jakelutyökalu, jonka avulla voidaan hoitaa yrityksen tietoturvaa. Sen avulla voidaan toteuttaa helposti erilaisten määritysten jakaminen sekä ohjelmien asentaminen ja ylläpito. Policy Manager on myös erittäin hyvä väline tietoturvan valvomiseen. Ohjelman avulla yritys säästää myös menoissa, koska tietoturvasta vastaavat henkilöt voivat valvoa ja tehdä muutoksia suoraan toimipisteeltään eikä heidän tarvitse käydä paikan päällä käsin asentamassa virustentorjuntaa tai sen päivityksiä yms. laitteille. Hallintaohjelmalla voidaan myös lukittaa asetuksia, mikä estää käyttäjiä muuttamasta kriittisiä asetuksia. Tämä helpottaa huomattavasti tietoturvasta vastaavien henkilöiden työtä, koska heidän ei tarvitse pelätä, että käyttäjät muuttaisivat mitään asetuksia. Uusien määritysten tekeminen ja jakaminen koko yrityksen laitteille on helppoa ja nopeaa.

F-Secure Policy Managerin versio 9 sisältää itse Policy Manager server ohjelmiston sekä sen hallintaan kehitetyn konsolin. Konsolin avulla ylläpitäjät voivat määrittää asetuksia, asentaa ohjelmia, muuttaa niiden versiota sekä poistaa laitteilta ohjelmia.

Konsolin avulla hoidetaan kaikki tarvittavat asennus/valvonta-tehtävät. Halutut asetukset määritellään Policy Manager konsolilla, josta ne sitten jaetaan kaikille laitteille. Ohjelma tarkistaa automaattisesti onko uusia määrityksiä tullut ja asentaa ne löydettyään.

Ohjelma myös luo erilaisia raportteja, joiden avulla on helppo valvoa ja tutkia esimerkiksi saastuneita objekteja sekä yleisesti ympäristön tietoturvallisuutta. Sen avulla pystytään helposti huomaamaan mahdolliset haittaohjelmat laitteissa. Raporttien avulla voidaan myös tarkastella mitä ohjelmia laitteille on asennettu. Kuvassa 1 näkyy ympäristön laitteille asennetut ohjelmat ja niiden versiot.



Kuva 2: F-Secure ohjelmien versiot työympäristössä (F-Secure 2009)

3.2 F-Secure Client Security

F-Secure Client Security on tietoturvapaketti, jossa yhdistyy, erilaiset innovatiiviset tekniikat. Tietoturvaongelmat käsitellään automaattisesti ja käyttöliittymä on uudistettu mukavammaksi ja helpommaksi käyttää. Selaussuojaus on uusi ominaisuus, joka ilmaisee turvalliset sivustot ja estää haitallisille sivustoille pääsyn.

Ohjelmisto on vaivaton asentaa ja sitä on helppo käyttää, joten käyttöönottokustannukset eivät kohoa. Järjestelmänvalvojat voivat hallita työasemien ja etätoimistojen tietoturvaa keskitetysti yhdellä valvontapäätteellä. Keskitetyn hallinnan ansiosta verkon määrittäminen, seuranta ja tietoturvan tilan raportoiminen on helppoa. (F-Secure 2011)
Techait yhtiö on tehnyt seuraavanlaisen listan F-Secure Client Security 9 uusista ominaisuuksista.

F-Secure Client Security 9 -ominaisuudet:

- Tuki Microsoft Windows 7 -käyttöjärjestelmälle
- Suorituskyvyn parannukset sisältävät pienemmän järjestelmäresurssien käytön ja nopeamman haittaohjelmien suojauksen
- Uusi selauksen suojaus ja Exploit Shield – ominaisuus estävät pääsyn uhkia sisältäville sivuille ja suojaavat haavoittuvuuksia hyväksikäyttäviltä haittaohjelmilta
- F-Securen Real-time Protection Network reagoi välittömästi uusiin tietoturvauhkiin
- Helppokäyttöinen, uudistettu käyttöliittymä ja keskitetty hallinta vähentävät ylläpidon tarvetta
- Automatisoitu toiminta säästää aikaa ja vähentää työmäärää
- Epäilyttävien tiedostojen poisto tai vapautus karanteenista hallintakonsolista
- Sähköpostin ja verkkoliikenteen skannaus
- Palomuuri sisältäen hyökkäyksen eston
- Keskitetty hallinta F-Secure Policy Managerilla.

(techait 2009)

4 Haittaohjelmat ja virustorjunta

4.1 Haittaohjelman määritelmä

Haittaohjelma on tietokoneohjelma, jonka tarkoituksena on aiheuttaa harmia tietokoneen käyttäjälle. Haittaohjelmat voivat poistaa koneelta tiedostoja tai ruuhkauttaa tietoliikennettä niin, että koneella tai koko työympäristössä työskenteleminen voi olla lähes mahdotonta. Haittaohjelmien avulla myös salasanat voivat päätyä vääriin käsiin, jolloin esimerkiksi sähköpostiviesteissä olevat tiedot voivat joutua kenen tahansa luettavaksi. (Tietoturvaopas 2008.)

Haittaohjelmat voidaan luokitella seitsemään eri ryhmään. Tunnetuimpia haittaohjelmia ovat virukset, erilaiset madot ja vakoiluohjelmat. Yleisin tapa saada viruksia koneelle on sähköpostin välityksellä. Myös erilaisten siirrettävien medioiden avulla voidaan saastuttaa koneita esimerkiksi cd- ja dvd-levyjen sekä muistitikkujen avulla. Muita haittaohjelmia ovat Troijan hevoset, takaporttiohjelmat, mainosohjelmat sekä botit. Troijan hevonen on erittäin vaikea huomata, koska se voi naamioitua vaikkapa peliksi tai joksikin muuksi ohjelmaksi.

Takaporttiohjelmien avulla koneeseen avautuu ulkoinen yhteys, jonka kautta sitten ohjelman tekijä voi halutessaan varastaa tiedostoja tai salasanoja. (Tietoturvaopas 2008.)Mainosohjelmat eivät yleensä tee mitään varsinaista haittaa koneen tiedostoille tai muullekaan käytölle. Niiden tarkoituksena on vain saada käyttäjä ohjautumaan halutulle sivulle normaalien mainoksien tapaan. Tämän takia niitä ei edes aina luokitellakaan haittaohjelmiksi. Botit leviävät automaattisesti ja voivat myös sisältää muitakin ominaisuuksia esimerkiksi takaportteja tai vakoiluohjelmia. Bottien avulla konetta voidaan hallita käyttäjän huomaamatta. Niiden avulla konetta voidaan käyttää laittomiin asioihin kuten tiedostojen tai roskapostin lähettämiseen. Bottien avulla voidaan myös toteuttaa ns. botverkko-hyökkäyksiä, joiden tarkoituksena on yleensä ruuhkauttaa jonkin yrityksen verkkoliikenne tai muulla tavoin sabotoida yrityksen toimintaa. (Tietoturvaopas 2008.)

4.2 Haittaohjelmien ja virusten torjuntakeinoja

Virustentorjunta on erittäin tärkeä osa tietojärjestelmien ylläpitoa. Virusten torjuntaan on kehitetty monia erilaisia tekniikoita kuten haittaohjelmien poistajia, palomuureja ja virustentorjuntaohjelmia. Nykyään useasti myydään ohjelmistopaketteja, jotka sisältävät nämä kaikki tuotteet yhdessä. Tämä helpottaa ylläpitoa ja päivityksien sekä kokonaan uusien versioiden käyttöönottoa. (Cknow 2009.)

Palomuurit pyrkivät estämään viruksien pääsyn koneelle estämällä esimerkiksi protokollia ja sulkemalla tiettyjä portteja, joita mahdolliset haittaohjelmat käyttävät. Palomuuri voidaan myös asettaa tutkimaan yrityksestä lähtevää tietoa. Näin voidaan paremmin suojata yrityksen salaisia tietoja.

Virustentorjunta- ja haittaohjelmien torjuntaohjelmat ovat seuraavana vuorossa, mikäli haittaohjelmat läpäisevät palomuurit. Virustorjuntaohjelmat ja haittaohjelmien torjuntaohjelmat perustuvat pääasiassa jo kerättyyn tietoon viruksista. Tämän kerätyn tiedon perusteella on tehty niin sanottu virustietokanta, johon aina verrataan tiedostoja. Mikäli tiedosto löytyy tietokannasta, sen toiminta pyritään estämään joko poistamalla tiedosto tai asettamalla se karanteeniin, jolloin sen ei pitäisi voida toimia.

4.3 Haittaohjelmien ja virustorjunnan historiaa

4.3.1 Historiaa vuosilta 1970–1990

Ensimmäinen löydetty haittaohjelma oli mato nimeltään Creeper. Se löydettiin ARPANETIstä vuonna 1970 ja sen tehtävänä oli levitä modeemeista toiseen lähettäen viestiä "I'm the creeper, catch me if you can!". Heti tämän jälkeen ilmestyi Reaper-haittaohjelma, jonka tarkoituksena oli löytää ja tuhota Creeper. 1974 ilmestyi haittaohjelma nimeltä Rabbit, joka aiheutti huomattavasti enemmän ongelmia edellisiin verrattuna, koska se monistautui niin nopeasti sekä kaatoi järjestelmiä. (Piekkola 2005.)

Ensimmäinen varsinainen virus ilmestyi 1981. Se oli nimeltään Elk Cloner ja se levisi Apple 2 käyttöjärjestelmälevykkeiden kautta. Virus tarttui myös jokaiseen levykkeeseen, joka laitettiin laitteen sisälle. Tämän takia virus levisi helposti laitteesta toiseen. (Piekkola 2005.)

Virallisesti tietokonevirus-termi syntyi vuonna 1983 Etelä-Kalifornian yliopistossa, jossa Len Adleman kutsui oppilaansa tekemään ohjelmaa tietokonevirusta. Ensimmäistä kertaa kyseistä termiä käytettiin akateemisessa julkaisussa seuraavana vuonna 1984, jolloin Fred Cohen julkaisi artikkelin nimeltä ”Experiments with Computer Viruses”. Artikkelin mukaan tietokonevirus oli ohjelma, jotka on tehty aiheuttamaan haittaa tai tuhoa ohjelmille tai järjestelmille. (Piekkola 2005.)

IBM PC–tietokoneiden kanssa yhteensopiva virus havaittiin ensimmäistä kertaa 1986. Tämä virus oli nimeltään Brain. Se oli käynnistyslohkovirus, joka tartutti arvioiden mukaan yli 300 000 levykettä. Isot tartuntamäärät johtuvat siitä, että juuri tuohon aikoihin MS-DOS-käyttöjärjestelmän suosio kasvoi, jota mm. IBM PC käytti tuolloin. (Piekkola 2005.)

Samana vuonna esitettiin tietokonevirus VirDem, joka pystyi kopioitumaan itsestään liittymällä muihin ajettaviin tiedostoihin. Se tarttui pääasiassa .COM-tiedostoihin. Hakkereiden keskuudessa kyseinen ohjelma herätti suurta kiinnostusta. Myös ensimmäinen Troijan hevonen havaittiin kyseisenä vuonna. Se esitti olevansa ilmainen tekstinkäsittelyohjelma ja olikin, mutta käytettäessä tuhosi ja korruptoi tietoa koneelta. (Piekkola 2005.)

Seuraava vuosi 1987 oli erittäin huono tietokoneiden käyttäjien kannalta. Silloin ohjelmoijat kiinnostuivat tekemään haitallisia ohjelmia oikein kunnolla. Suurin osa hyökkäyksistä kohdistui IBM PC–koneisiin, mutta myös Apple-, Amiga- ja Atari ST–koneille tehtyyn jonkin verran hyökkäyksiä. (Piekkola 2005.)

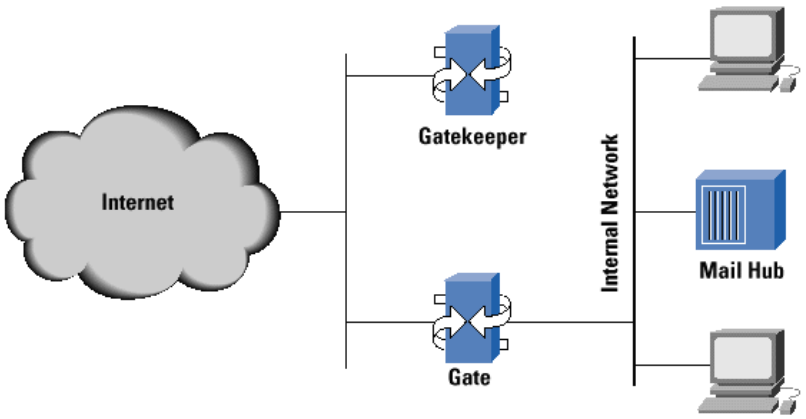
Virustorjuntaohjelmat saivat alkunsa Ralf Burgerin julkaisemasta teoksesta vuonna 1987. Teoksessa ”Computer Viruses: A High-Tech Disease” kerrottiin tarkasti miten tietokonevirus nimeltä Vienna tehtiin toimintakyvyttömäksi. Teos ei valitettavasti ollut ainoastaan virustentorjuntaohjelmien alku, vaan siitä hyötyivät myös virusten tekijät. Teoksessa nimittäin kerrottiin tarkasti miten tietokoneviruksia tehdään.(Piekkola 2005.)

Ensimmäinen varsinainen virustorjuntaohjelma tehtiin vuonna 1988. Sen toiminta perustui tunnettujen merkkijonojen etsintään ja ohjelmien muuntamiseen niin, että virukset luulivat koneen olevan jo saastunut. Tämän tarkoituksena oli estää viruksen tarttuminen koneelle. Samana vuonna syntyi myös ensimmäinen virustentorjuntaan perehtynyt keskustelupalsta nimeltä VIRUS-L. Keskustelupalstan käyttäjinä olivat muun muassa Eugene Kaspersky ja John McAfee, jotka perustivat myöhemmin omat tietoturvayhtiönsä kaspersky Anti-Virus sekä McAfee Anti-Virus.(Piekkola 2005.)

4.3.2 Historiaa vuosilta 1990–2000

Vuonna 1990 löydettiin ensimmäinen polymorfinen virus, joka aiheutti erittäin paljon ongelmia virustentorjuntaohjelmille. Tämä johtui siitä, että virus kykeni muuntautumaan joka käynnistyskerralla. Näin merkkijonoihin perustunut virustentorjunta ei enää riittänyt. Tämän jälkeen aloitettiin ensimmäisten palomuurien käyttö, jotka suodattivat tietoliikennettä. Nämä kyseiset palomuurit olivat pääasiassa IP-reitittimiä, johon oli määritelty erilaisia sääntöjä. Säännöt olivat hyvin yksinkertaisia esimerkiksi päästä kaikki liikenne läpi tai estä kaikki. Tästä lähtien palomuureja alettiin käyttää ja kehittämään

1991 kehitettiin ensimmäinen kaupallinen palomuuriratkaisu nimeltä DEC SEAL. Tämä ratkaisu toteutettiin tietylle yritykselle räätälöitynä palveluna.



Kuva 3: DEC SEAL palomuuri (Frederic Avolio 2011)

Vuonna 1992 ilmestyivät ensimmäiset virustentorjuntaohjelmia häiritsevät virukset sekä ensimmäinen virus Windows-käyttöjärjestelmälle. Tästä lähtien Windows oli ensisijainen viruksien kohde.

Vuonna 1994 CD-levyjen käyttö lisääntyi huomattavasti, joka aiheutti sen, että viruksia alkoi levitä reilusti aikaisempaa enemmän. CD-levyissä oli se ongelmallinen asia, että virusta ei voinut poistaa mitenkään muuten kuin tuhoamalla levyn.

Vuonna 1997 tuli ensimmäinen sähköpostin liitetiedostona leviävä virus. Jos käytössä oli Microsoft Mail–sähköpostiohjelma, virus yritti lähettää sähköpostiviestin liitetiedostona saastunutta Word-dokumenttia. Sähköpostin liitetiedostona leviävä virus antoi mahdollisuuden levitä entistä helpommin koneesta toiseen, koska enää ei tarvinnut fyysistä mediaa kuten cd-levyä levittyäkseen koneesta toiseen. Tämän uuden leviämistavan myötä virustorjuntaohjelmien tuli jatkossa toimia jo ennen työasemaverkkoa. Samana vuonna ilmestyivät myös ensimmäiset virukset Linux-käyttöjärjestelmälle ja IRC-keskusteluohjelmalle.

Vuonna 1998 ilmestyivät ensimmäiset virukset, jotka käyttivät hyväkseen HTML ja Java-koodia. Virukset käyttivät hyväkseen koodien bugeja sekä esimerkiksi HTML-viestiin voi olla kätkettynä viruksia. Yleisimmin ne levisivät joko sähköpostin tai internetsivujen avulla. Näiden avulla tietokonetta pystyttiin hallitsemaan haitallisesti etäkoneesta käsin
Vuonna 1999 ilmestyi ensimmäinen sähköpostimato, joka pystyi tarttumaan koneelle pelkästään sähköpostin avaamisella. Tämä oli erikoista siinä mielessä, että aikaisemmin madon tarttumiseen oli tarvittu aina sähköpostissa olevan liitetiedoston avaaminen aktivoimaan mato.

Saman vuoden lopulla ilmestyi ensimmäinen tietokonevirus, joka pystyi päivittämään itseään verkkoyhteyden avulla. Viruksen nimi oli Babylonia ja se yritti päivittää itseään japanilaisen palvelimen kautta. Päivityksen tarkoituksena oli muuttaa viruksen muotoa niin, että viruksentorjuntaohjelmat eivät huomaisi sitä. (Piekkola 2005.)

4.3.3 2000-luvun virustorjunnan historiaa

Vuonna 2000 ilmestyi ensimmäiset matkapuhelimia ja kämmentietokoneita hyväksikäyttävät madot. Timofonica-niminen mato ei varsinaisesti ollut haitallinen millekään, koska sen tarkoituksena oli vain lähettää tekstiviestejä erään palveluntarjoajan puhelinnumeroihin. (Piekkola 2005.)

Vuodet 2001–2004 olivat läpimurto tiedon urkinta- ja vakoilumenetelmien saralla. Nämä olivat erittäin ongelmallisia siksi, että nykyiset virustentorjuntaohjelmat eivät tunnistaneet tällaisia uhkia. Onneksi markkinoille syntyi nopeasti juuri tällaisten uhkien torjumiseen tarkoitettuja ohjelmia. (Piekkola 2005.)

Viime vuosikymmenen aikana virustorjuntaohjelmien lisäksi on tullut muita tapoja ehkäistä haittaohjelmien pääsyä koneelle. Tällaisia ovat esimerkiksi palomuurit joita nykyään tulee jo käyttöjärjestelmän mukana, mutta löytyy myös monipuolisempia ilmaisia sekä kaupallisia versioita. Tämän lisäksi on myös rootkittien poisto-ohjelmia esimerkiksi F-Secure Blacklight sekä erilaisten haittaohjelmien poistoon tarkoitettuja ohjelmia.

4.4 F-Secure

Petri Allas ja Risto Siilasmaa perustivat Data Fellows yrityksen vuonna 1988. Yrityksen toiminta perustui silloin käyttäjien kouluttamiseen ja tietokantojen rakentamiseen. Vuonna 1991 yhtiö kehitti ensimmäisen heuristisen skannerin virustorjuntatuotteita varten. Data Fellows oli ensimmäinen yritys maailmassa, joka loi tietokoneiden turvallisuutta käsittelevän web-sivuston vuonna 1994. Web-sivustolla oli kattava virusluettelo, millaista ei ollut aiemmin internetissä. Vuonna 1999 Data Fellows muutti nimensä F-Secure Oyj:ksi ja yhtiö listautui Helsingin pörssiin. Vuonna 2000 yritys laajensi toimintaansa matkapuhelimien tietoturvaan. (F-Secure 2010)

Vuonna 2001 F-Secure julkaisi paljon uusia tuotteita. Näitä oli Pocket PC – salausratkaisu tallennetuille sähköposteille, yhteistiedoille ja kalentereille. Yritys julkaisi myös tietoturvahälytysjärjestelmän, joka ilmoittaa hakulaitteelle tai matkapuhelimelle yms. vakavista viruksista. (F-Secure 2010)

Vuonna 2002 F-Secure päätti keskittyä liiketoiminnassaan pelkästään virustentorjuntaan. Samana vuonna julkaistiin myös ensimmäinen langattomasti päivittyvä virustorjuntatuote. Vuonna 2004 F-Secure julkaisi ensimmäiset virustentorjuntaohjelmat ja – ratkaisut mobiililaitteille. Seuraavien vuosien aikana F-Secure otti käyttöön mm. DeepGuard-teknologiaa hyödyntävän F-Secure Internet Security 2007 tuotteen. F-Secure tarjoaa myös varmennustilaa Online Backup nimisenä palveluna, joka toimii internet-palveluntarjoajien kautta. Tällä hetkellä F-Securen tuotteisiin kuuluu tietokoneiden lisäksi myös älypuhelimien tietoturva sekä verkkolevyt jonne voidaan varmuuskopioida yrityksen tärkeitä tietoja esimerkiksi palvelimilta. Älypuhelimien suosio kasvaa kokoajan, joten niiden tietoturvaa muun tietotekniikan ohella täytyy ylläpitää yhä paremmin. (F-Secure 2010.)

F-Securen markkinat myös laajentuivat ja toimipisteitä perustettiin Singaporeen, Intiaan ja Malesiaan. Vuonna 2009 F-Securen liikevaihto oli 125.1 milj. euroa.
(F-Secure 2010) Tässä yrityksessä F-Securen virustorjuntaohjelmat ovat olleet laajassa käytössä jo pitkään, mutta tiettävästi tämänkaltaista yhteistä testaushanketta ei ole toteutettu toimittajan kanssa aiemmin.

5 Nykyisen ympäristön testaus

5.1 Menetelmät

Ensimmäinen asia projektissa oli työasemien käynnistysaikojen mittaus, mutta menetelmästä ei ollut vielä siinä vaiheessa tietoa. Aluksi aiottiin pyytää käyttäjiä ottamaan sekuntikellolla aikaa johonkin tiettyyn pisteeseen saakka. Se olisi kuitenkin ollut huono vaihtoehto, koska siinä olisi mennyt käyttäjien aikaa, eivätkä ajat välttämättä olisi olleet luotettavia.

Pienen etsinnän jälkeen löydettiin Microsoftin kehittämä rekisterimuutos, jonka avulla käynnistymisestä syntyisi log-tiedosto, johon kirjautuisi kaikki käynnistyksen yhteydessä tapahtuvat prosessit. Päätimme kokeilla tätä vaihtoehtoa, koska se vaikutti tarkemmalta ja käyttäjäystävällisemmältä. Windows-rekisteriin lisättiin avain UserEnvDebugLevel. Tämä avain luotiin polkuun HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon. Avainta luodessa sille piti määrittää erilaisia arvoja. Avaimen nimeksi piti määritellä UserEnvDebugLevel, avaimen tyypiksi DWORD-arvo ja arvon dataksi 10002. Tämän jälkeen .log tiedostoon alkoi kerääntyä tietoa erilaisista prosesseista mitä koneella ajettiin. Mikäli lokituksen halusi ottaa pois päältä, siihen oli kaksi eri tapaa. Ensimmäinen on yksinkertaisesti poistaa kyseinen UserEnvDebugLevel-avain, jolloin lokia ei enää syntynyt. Toinen tapa on muuttaa määritetty arvon data 00000:ksi, jolloin lokitus loppuu, mutta arvon muuttamalla takaisin 10002:ksi sen saa suoraan uudelleen käyttöön. Tämä tapa on hyvä silloin, jos tietää tarvitsevansa lokitusta uudelleen myöhemmin.

5.1.1 Virustorjunnan täystarkistuksen kesto

Virustorjunnan täystarkistuksen keston mittaus suoritettiin F-Secure Policy Managerin konsolin raportointityökalujen avulla. Täystarkistukset asetettiin päälle Policy Managerin konsolin kautta toimintaohjeiden (policyjen) avulla. Client Security 8 oli määritetty tarkistamaan toimintaohjeet 30 minuutin välein, jolloin kaikki siihen määrätyt toiminnot suoritettiin. Ohjelma loi jokaisen täystarkistuksen päätteeksi raportin, jossa näkyi tarkistuksen kesto, viruksien lukumäärä sekä muita tarkistukseen liittyviä tietoja. Raporttien perusteella kerättiin tarkistuksien kestot dokumenttiin, jotta niitä voitaisiin uuden version asennuksen jälkeen vertailla keskenään.

5.1.2 Työasemien käynnistyksen keston mittaus

Rekisteriavaimen UserEnvDebuglevel lisäämistä kokeiltiin ensiksi kahdella työasemalla varmistaaksemme sen toimivuuden halutulla tavalla. Työaseman käynnistyksen yhteydessä hakemistoon x syntyi tiedosto y, jossa näytti olevan paljon käynnistymiseen liittyvää tietoa.

Käyttäjiä ei pyydetty erikseen käynnistämään työasemaansa uudelleen vaan odotettiin käyttäjien normaalia työaseman käynnistystä.

Lokia tarkemmin tutkittua huomattiin, että lokista löytyi erittäin paljon yksityiskohtaista ja tarkkaa tietoa kellonaikoineen. Lokissa näkyi esimerkiksi menivätkö työasemalle ja käyttäjälle määritellyt ryhmäkäytännöt (group policies) läpi vai eivät. Lokissa oli myös todella paljon ns. turhaa informaatiota projektiamme varten. Useiden koneiden lokeissa näkyi paljon saman prosessin toistoa, joka ei jostain syystä mennyt läpi. Joissakin tilanteissa tällaiset tapaukset saattoivat kasvattaa log-tiedoston kokoa erittäin paljon.

Log tiedostosta kuitenkin näki selvästi milloin F-Secure-ohjelmien prosessit ovat käynnistyneet, joka oli tässä opinnäytetyössä erittäin tärkeä osa. Käynnistymisen keston mittaaminen siis oli ajoitettava varmuudella näiden prosessien käynnistymisen jälkeen. Lokista löydettiin userinit.exe-ohjelma, joka toistui useamman kerran lokin aikana. Userinit.exe on Windowsin käynnistymiseen liittyvä avainprosessi, jonka aikana muun muassa verkkoyhteys pystytetään. Kyseisen ohjelma käynnistyi myös ryhmämääritysten jälkeen. Tämän johtopäätöksen ansiosta mittaus päätettiin suorittaa jokaisesta loki-tiedostosta ryhmämääritysten jälkeen olevasta userinit.exe-tiedostosta. (Processlibrary 2010)

Seuraavaksi piti tehdä päätös sen suhteen, mikä prosessi laskettaisiin viimeiseksi prosessiksi käynnistymisen suhteen eli mihin prosessiin käynnistyminen loppuisi.

5.1.3 Esimerkki käynnistyslokista

USERENV(2c0.2c4) 06:28:18:265 InitializePolicyProcessing: Initialised Machine Mutex/Events
USERENV(2c0.2c4) 06:28:18:265 InitializePolicyProcessing: Initialised User Mutex/Events
USERENV(2c0.2c4) 06:28:18:265 LibMain: Process Name:
\??\C:\WINDOWS\system32\winlogon.exe
USERENV(2c0.2c4) 06:28:18:937 Entering CUserProfile::Initialize ...

USERENV(9d8.9dc) 06:29:07:390 LibMain: Process Name: C:\Program Files\F-Secure\FSAUA\program\fsaua.exe
USERENV(2ec.7c4) 06:29:07:421 LoadUserProfile: Yes, we can impersonate the user. Running as self
USERENV(2ec.7c4) 06:29:07:421 LoadUserProfile: Calling DropClientToken (as self) succeeded
USERENV(2c0.3f8) 06:29:07:421 IProfileSecurityCallBack: client authenticated.
USERENV(2c0.3f8) 06:29:07:421 In LoadUserProfileP
USERENV(2c0.3f8) 06:29:07:421 LoadUserProfile: Running as client

USERENV(2c0.738) 06:29:09:453 ProcessGPOs: Computer Group Policy has been applied.
USERENV(2c0.738) 06:29:09:453 ProcessGPOs: Leaving with 1.
USERENV(2c0.738) 06:29:09:453 ApplyGroupPolicy: Leaving successfully.
USERENV(6d4.9d0) 06:29:09:515 LibMain: Process Name: C:\Program Files\F-Secure\Anti-Virus\FSGK32.EXE
USERENV(c68.c6c) 06:29:09:562 LibMain: Process Name: C:\WINDOWS\system32\userinit.exe
USERENV(a24.a68) 06:29:19:156 LibMain: Process Name: C:\Program Files\F-Secure\FWES\Program\fsdfwd.exe
USERENV(2c0.858) 06:30:19:889 ProcessGPOs: User Group Policy has been applied.
USERENV(2c0.858) 06:30:19:889 ProcessGPOs: Leaving with 1.
USERENV(2c0.858) 06:30:20:606 ApplyGroupPolicy: Leaving successfully.
USERENV(9d4.9fc) 06:30:29:515 LibMain: Process Name: C:\Program Files\F-Secure\Anti-Virus\fssm32.exe
USERENV(cf4.d10) 06:31:14:760 LibMain: Process Name: C:\WINDOWS\system32\userinit.exe

5.2 Testaus

Suorituskyvyn mittaus päätettiin suorittaa noin puolelle koneista. Nykyisestä ympäristöstä pyrittiin mittaamaan työasemien suorituskyky, täystarkistuksen kesto sekä työasemien käynnistymisen kesto. Suorituskyvyn mittaamiseen käytettiin HP Operations Manager for Windows (OMW) valvonta- sekä performance agenttia. Ohjelmaa oli aikaisemmin käytetty vain palvelimien valvontaan eikä ollut tietoa, kuinka hyvin se soveltuisi työasemien suorituskyvyn mittaamiseen. Sen takia agentti asennettiin aluksi vain parille työasemalle, jolla sitten testattiin ohjelman toimivuutta haluttuun tehtävään. Testauksessa huomattiin ohjelman toimivan, joten kyseinen agentti asennettiin 25 työasemalle, joista sitten pyrittiin mittaamaan suorituskyky. Ohjelman avulla pystyttiin luomaan erilaisia graafeja, jonka perusteella voitiin verrata haluttuja tietoja. Tässä projektissa päädyttiin käyttämään ohjelman Global History parametria, joka loi graafin prosessorin käytöstä, muistin käytöstä, verkon liikenteen määrästä yms. Graafien avulla saatiin hyvin selville tarkistuksen aikana tapahtuva prosessorin kuormitus sekä muistin käyttö.

Suorityskykykaavioita kerätessä huomattiin, että agentti ei toiminutkaan jokaisessa työasemassa oikein. Osasta puuttui dataa välistä tai agentti ei ollut kerännyt sitä ollenkaan.

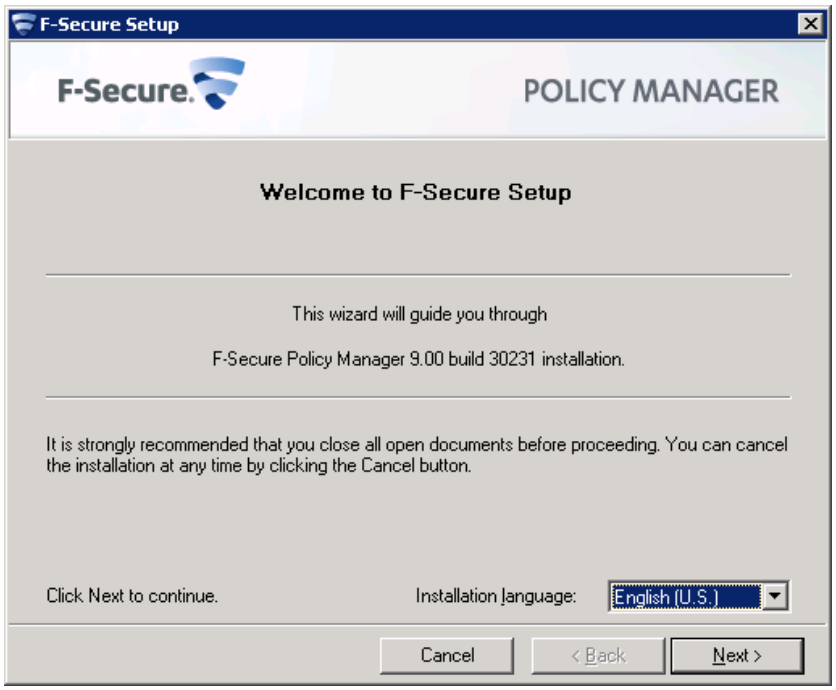
6 F-Secure Policy Manager console-palvelin

Projektin alkaessa piti päättää mille palvelimelle Policy Manager asennetaan. Aluksi piti päättää millä käyttöjärjestelmällä kyseinen ohjelma toimisi parhaiten. Vaihtoehdot olivat tässä tapauksessa Windows Server 2003 sekä Windows Server 2008. Projektissa pohdittiin myös Windows 7 työasemien testaamista, jolloin Windows Server 2008 olisi ollut hyvä ratkaisu. Windows 7 testaamisesta kuitenkin päätettiin luopua joten käyttöjärjestelmäksi päätettiin ottaa Windows Server 2003. Yrityksen tiloista löytyikin jo valmiiksi juuri tähän tehtävään sopiva palvelin, joten projektia varten ei tarvinnut alkaa erikseen pystyttämään palvelinta. Palvelimessa oli jo valmiiksi käyttöjärjestelmä ja muut tarvittavat ohjelmistot vain Policy Manager puuttui. Seuraavassa kappaleessa kerrotaan tarkemmin miten asennus toteutettiin.

6.1 F-Secure Policy Manager 9 – asennus

Tässä kappaleessa kerrotaan kuvankaappauksien avulla, miten F-Secure Policy Manager versio 9 asennetaan palvelimeen ja mitä asetuksia ensimmäisen käynnistyskerran aikana täytyy määrittää. Jokaisen kuvankaappauksen yhteydessä kerrotaan, mitä kyseisessä ikkunassa kysytään ja mitä määrityksiä kussakin vaiheessa on tehtävä.

Käynnistettäessä asennustiedoston ensimmäisenä ruudulle ilmestyy kuvan 4 kaltainen ikkuna, jossa määritellään asennuksen kieli.

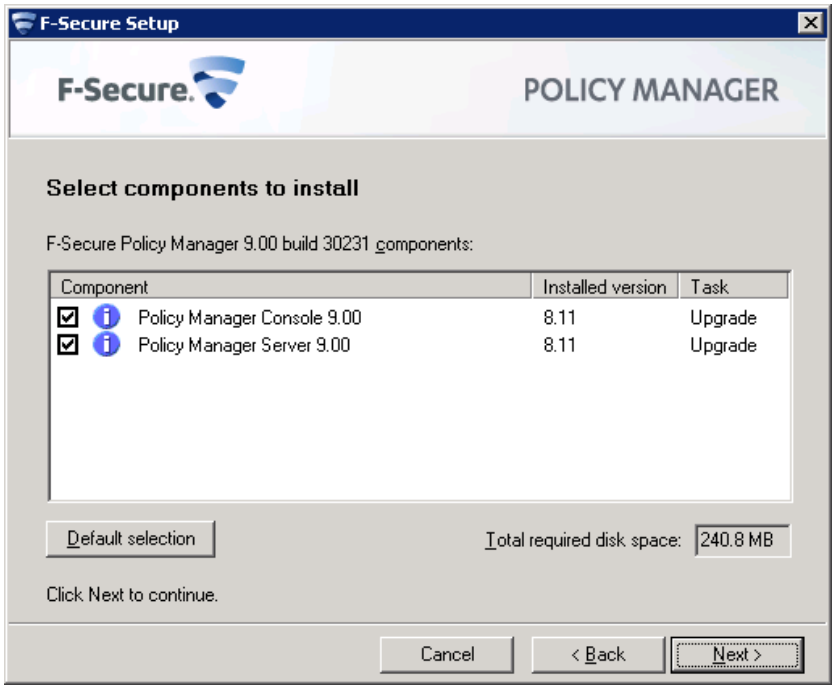


Kuva 4: F-Secure Policy Managerin kielivalinta

Kuvassa 5 on F-Securen laatimat lisenssiehdot ohjelman asentamista varten. Ne täytyy hyväksyä, mikäli haluaa jatkaa asennusta.

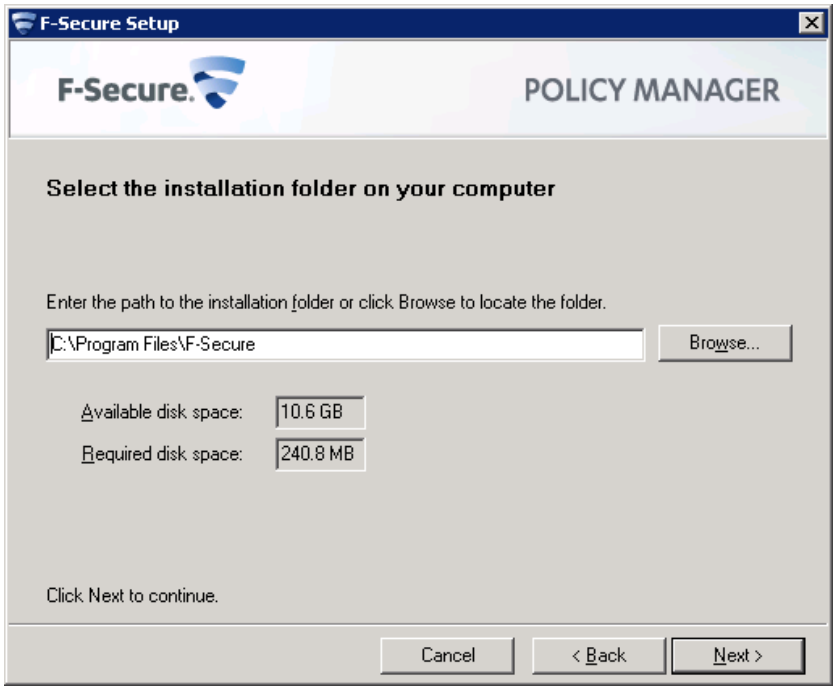
Kuva 5: Lisenssiehtojen lukeminen ja hyväksyminen

Seuraavassa kuvassa 6 valitaan mitkä ohjelman komponentit haluat asentaa. Ikkunassa lukee myös versionumerot ohjelmista sekä kuinka paljon ne vaativat vapaata tilaa kovalevyltä asentuakseen.



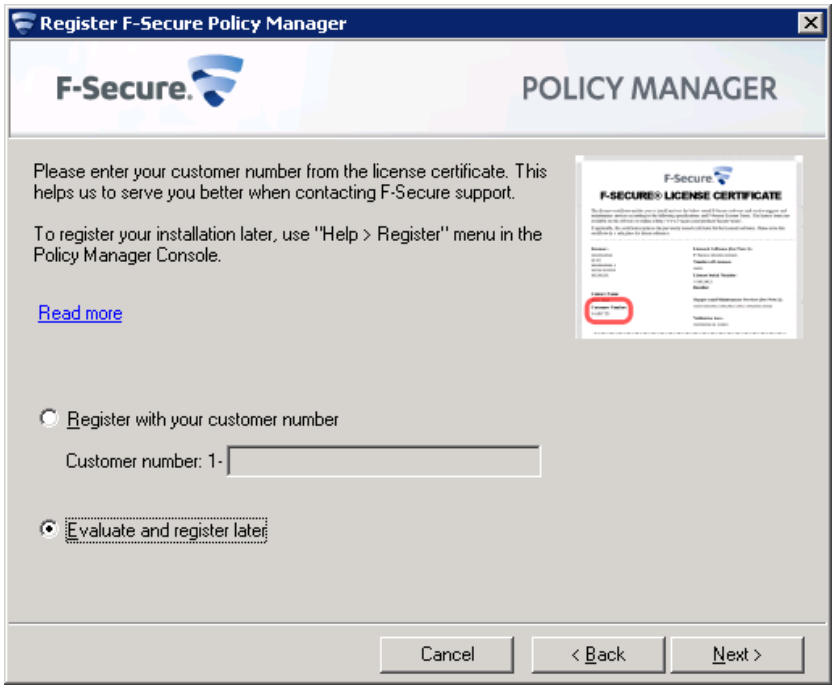
Kuva 6: Asennettavien komponenttien valinta

Kuvassa 7 voi valita minne kansioon haluaa ohjelman asentaa. Oletuksena ohjelma asentuu kansioon c:\Program Files\F-Secure. Tässä ikkunassa kerrotaan myös miten paljon ohjelma vaatii tilaa toimiakseen sekä miten paljon tilaa asemalla on. Mikäli ohjelma asennetaan jonkin paketin avulla, tätä ikkunaa ei tule, sillä asennuspolku on jo määritetty pakettia tehdessä. Tämän takia tulee muistaa varmistaa ennen asennusta, että kovalevyllä on tarpeeksi tilaa ohjelman asennusta varten.



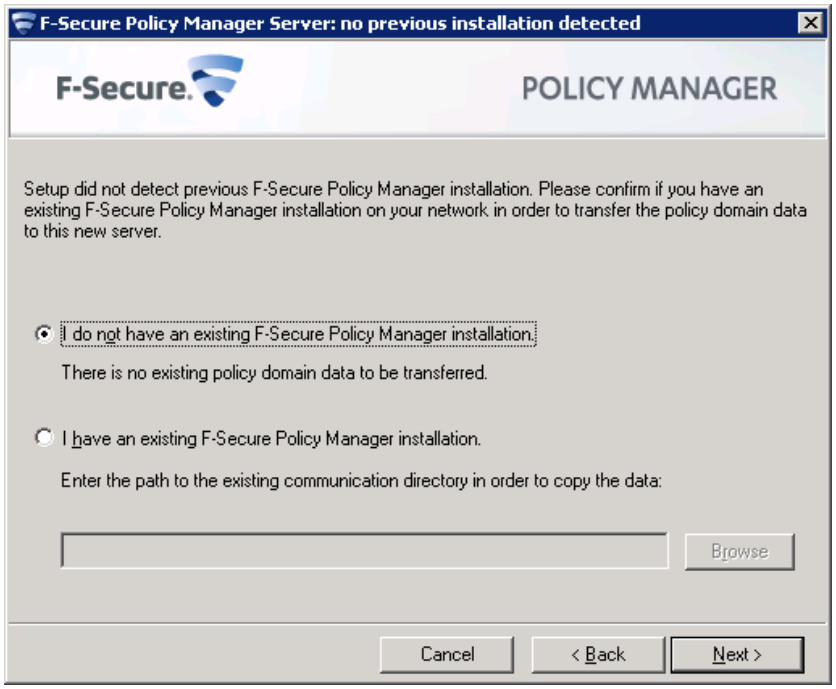
Kuva 7: Asennuksen tiedostopolku

Tuotteen voi joko rekisteröidä asennuksen yhteydessä tai halutessaan vasta myöhemmin. Ohjelmaan kuuluu 30 päivän kokeiluversio, joten rekisteröintiä ei ole pakko suorittaa välittömästi.



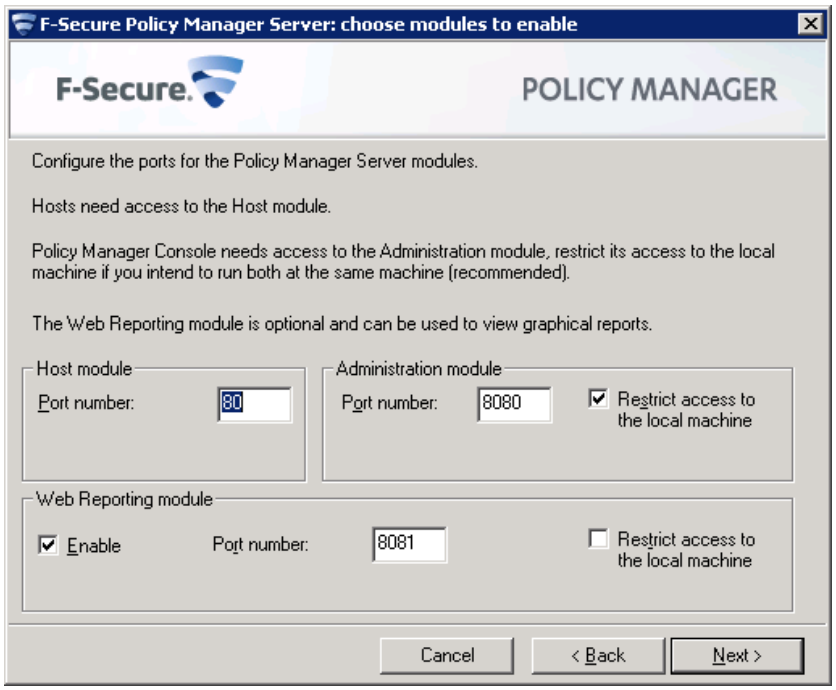
Kuva 8: Tuotteen rekisteröinti

Mikäli palvelimeen on jo asennettu jokin aikaisempi versio F-Secure Policy Managerista, voidaan sen asetukset kopioida suoraan uuteen. Mikäli palvelimella ei ole aikaisempaa versiota ohjelmistosta, se asentuu F-Securen määrittelemillä oletusasetuksilla.

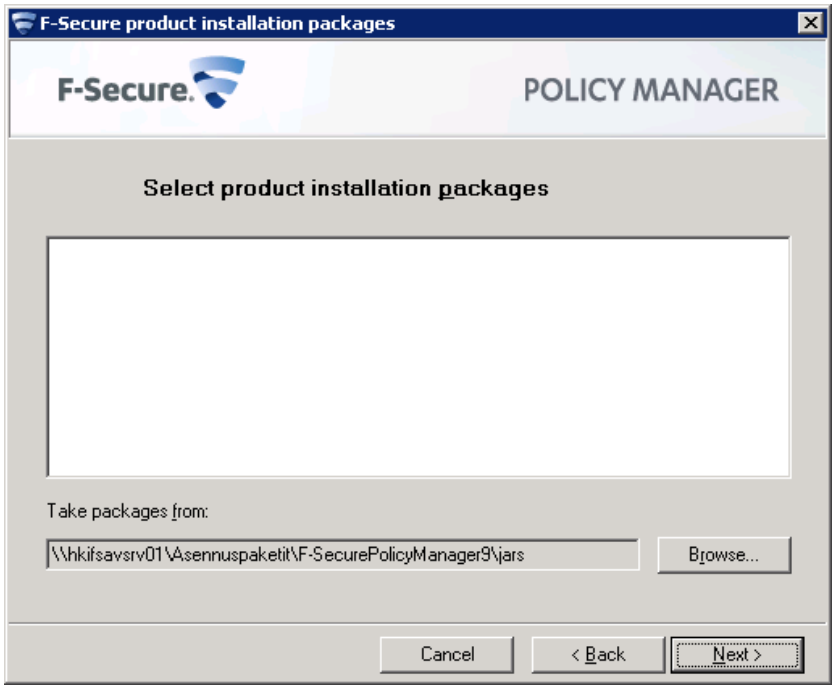


Kuva 9: Vanhan F-Secure version asetusten kopioiminen uuteen

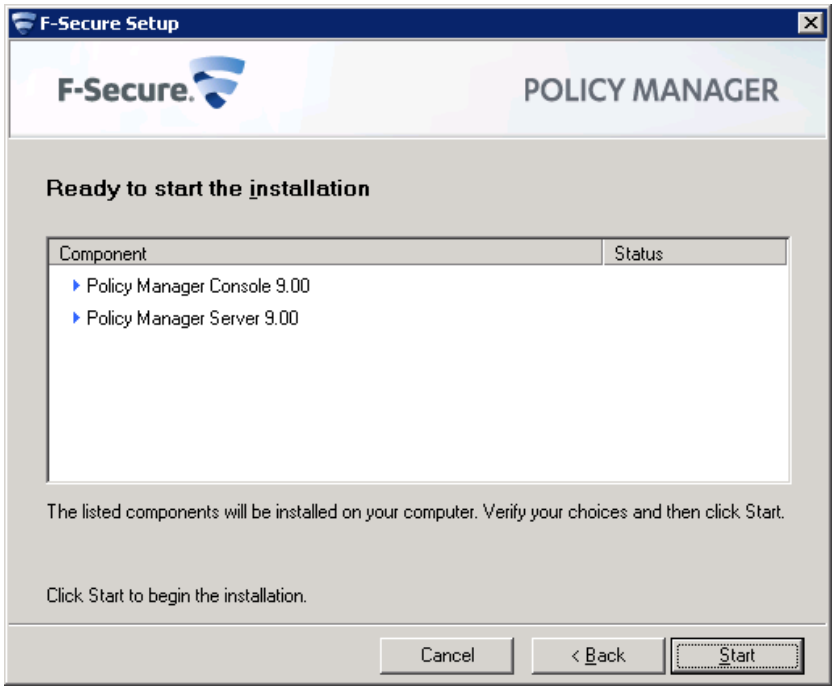
Seuraavassa kuvassa 10 määritellään mitä portteja ohjelman osat käyttävät. Oletusasetukset näkyvät kuvassa.



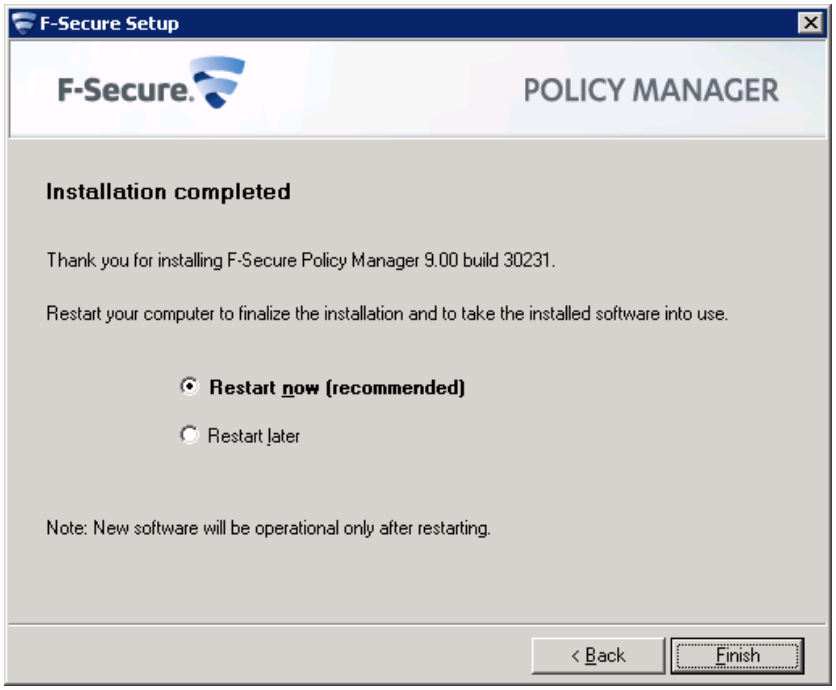
Kuva 10: Porttien määrittäminen



Kuva 11: Asennuspakettien lähteen määrittäminen



Kuva 12: Asennuksen käynnistäminen

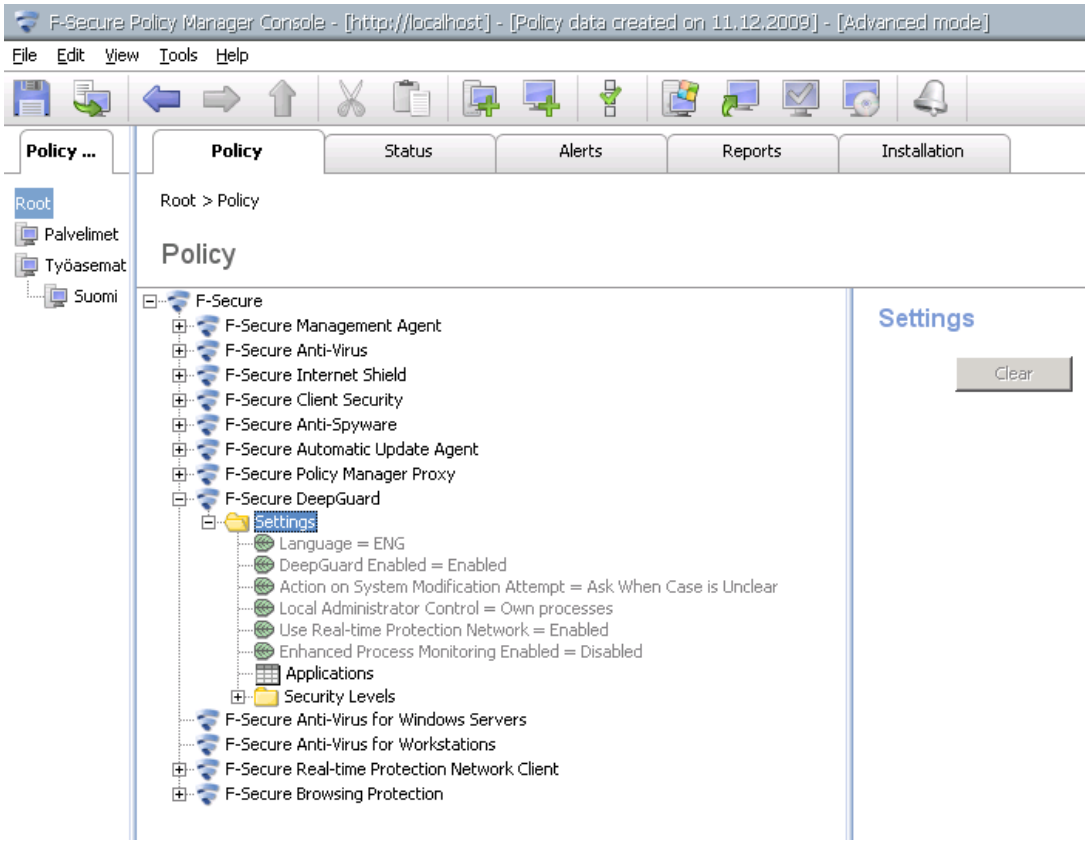


Kuva 13: Asennuksen viimeistely

7 F-Secure Client Security 9 asennus ja konfigurointi

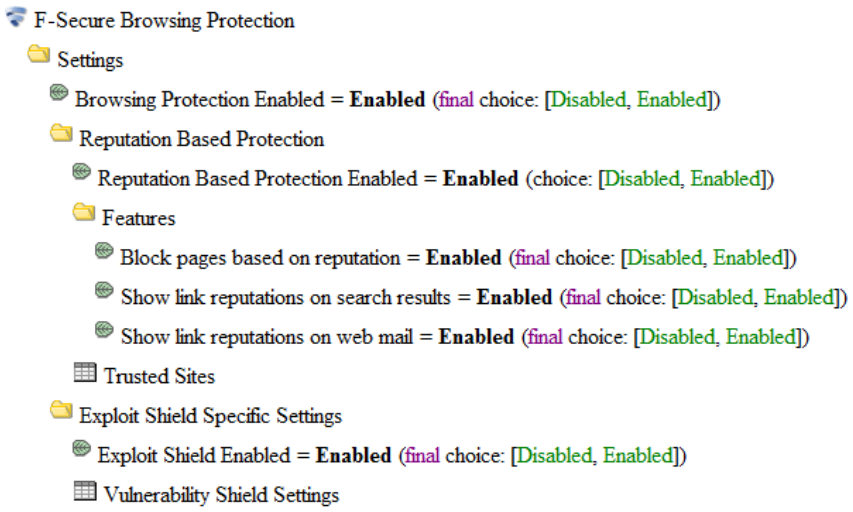
F-Secure Client Security versio 9:n asennus toteutettiin luomalla Policy Manager konsolilla msi-asennuspaketti. Asennus työasemiin tehtiin komentorivikehotetta käyttäen Active Directoryn käyttäjäoikeusryhmiä apuna. Client Securityä varten tarvittavat asetukset määriteltiin Policy Manager konsolilla ennen paketin tekoa. Uuteen versioon päätettiin ottaa asetuksiin mallia vanhasta versiosta, koska ne oli todettu kyseisessä versiossa toimiviksi ja hyviksi. Tietenkin uutta versiota säätäessä piti jokainen asetus tarkistaa kuitenkin ja määrittää yksitellen. Tähän kuluikin suhteellisen paljon aikaa, koska jokainen asetus piti määrittää käsin konsolille.

Uudessa Policy Manager versiossa oli myös uusia komponentteja, jotka olivat Deep Guard ja Browsing Protection. Näiden kanssa piti miettiä otetaanko ne käyttöön ja mikäli otetaan niin millä asetuksilla. Deep Guard komponentti antaa reaaliaikaisen tietosuojan. Komponentti toimii uuden ns. pilviteknologian avulla, joka päivittää reaaliajassa uudet viruslöydökset kaikille laitteille, jossa kyseinen toiminto on käytössä. Näin uudet virukset eivät pääse tarttumaan koneelle. Tämä teknologia antaa paljon nopeamman reagointimahdollisuuden uusille viruksille vanhaan päivitystekniikkaan verrattuna (F-Secure 2011).



Kuva 14: DeepGuard asetukset

Browsing protection taas suojelee käyttäjää menemästä epäilyttäville sivuille, josta saattaisi mahdollisesti tulla haittaohjelmia laitteelle. Tekniikka toimii niin, että F-Securella on tiedossaan WWW-osoitteita, josta mahdollisesti voi koneelle tulla haittaohjelmia. Mikäli käyttäjä yrittää mennä tällaiselle sivulle, joka on F-Securen mukaan todettu saastuneeksi, se estää käyttäjää menemästä sinne. Käyttäjä voi myös itse ilmoittaa mahdollisista saastuneista sivuista F-Securelle, jonka toimesta sivu tarkastetaan ja lisätään saastuneiden sivujen listaan, mikäli siihen nähdään aihetta. Komponenttien asetuksien tutkimisen jälkeen päätettiin ottaa ne käyttöön oletusasetuksilla.



Kuva 15: Browsing Protection asetukset

8 F-Secure Client Security 9 testaus

8.1 Käynnistyslokien kerääminen

Asennuksen jälkeen aloitettiin välittömästi uuden version testaus. Ensimmäinen vaihe oli käynnistyslokien kerääminen. Tämä vaihe oli suhteellisen helppo toteuttaa, koska tarvittavat muutokset oli jo tehty rekisteriin. Nyt täytyi vain kerätä lokit talteen ja aloittaa niiden analysointi ja vertailu vanhaan versioon nähden. Lokit saatiin kerättyä suhteellisen vaivattomasti ja niiden tarkastelu voitiin aloittaa. Tässä vaiheessa huomattiin, että aikojen vertailu oli joissain koneissa mahdotonta. Tämä siitä syystä, että projektin alkuvaiheessa emme vielä tienneet, mikä olisi se arvo käynnistyslokissa, jota lähtisimme vertailemaan. Vertailukelpoinen tiedosto löytyi vasta projektin loppuvaiheilla. Tästä syystä vanhalla versiolla kerätyt lokit analysoitiin vasta uuden kanssa samaan aikaan. Tarkastelun yhteydessä ilmeni, että kaikki vanhat lokit eivät olleetkaan täydellisiä tai niissä oli jotain muuta vikaa, jonka takia lokit eivät olleet vertailukelpoisia.

8.2 Täystarkistuksen keston mittaus

Tämän jälkeen laitettiin virustorjuntaohjelman täystarkistus päälle. Tarkistuksen johdosta kahdella koneella oli niin paljon hitautta, että tarkistus jouduttiin keskeyttämään. Nämä koneet kuitenkin myöhemmin saatiin myös täystarkistettua. Hitaus todennäköisesti johtui koneiden heikosta suorituskyvystä. Kyseisissä työasemissa oli vanhemmat komponentit kuin muissa ympäristön työasemissa. Kaikissa muissa työasemissa täystarkistus meni läpi, eikä niistä tarkistuksen aikana tullut valituksia. Seuraavaksi kerättiin täystarkistuksen kestot dokumenttiin myöhempää tarkastelua varten.

8.3 Suorituskykykaaviot

Tämän jälkeen kerättiin OMW:n avulla suorituskykykaaviot ja prosessilistat talteen. Kaavioiden keräämisessä oli jonkin verran ongelmia. Kaavioita ei saatu kerättyä aivan jokaisesta työasemasta, koska Jostain syystä agentti ei ollut saanut kerättyä kaikista työasemista dataa tarpeeksi pitkään. Osassa työasemista dataa saattoi olla parin päivän ajalta, kun taas osassa oli viikoittain. Syitä datan puuttumiselle ei löytynyt, mutta yksi vaihtoehto saattoi olla esimerkiksi työaseman pois päältä oleminen. Tiedon analysoinnin kanssa oli ongelmia, koska tietojen paikkansa pitävyyttä ja laatua ei ollut tarkastettu ennen uuden version asennusta. Tämän johdosta osasta koneista on olemassa vain tiedot uuden version kanssa. Ennen uuden version asentamista olisi pitänyt tarkastaa, että kaikista työasemista vanhalla versiolla on saatu tiedot talteen.

Saatujen tietojen mukaan uusi versio nopeutti jokaista työasemaa huomattavasti. Osassa työasemista käynnistys nopeutui yli puolella ja täystarkistus kesti myös kolmanneksen vähemmän. OMW ei toiminut niin hyvin kuin odotettiin. Käyttöliittymä oli hankala ja hidas, jonka takia tiedon tallentamiseen ja analysointiin meni paljon odotettua kauemmin. Kaikki saatavilla oleva tieto kerättiin dokumenttiin, joka on kokonaisuudessaan liitteenä opinnäytetyön lopussa. (liite 2.)

9 Käyttäjien palaute

Käyttäjäpalaute päätettiin toteuttaa avoimien kysymyksien avulla, jolloin käyttäjät voisivat kertoa monipuolisesti mielipiteitään. Kysymykset päätettiin luoda yhdessä eri projektin toimihenkilöiden kanssa. Kyselyn oli tarkoitus olla melko lyhyt, jotta mahdollisimman moni käyttäjä jaksaisi vastata siihen. Kysymyksiä kyselyssä oli kuusi. Seuraavaksi pitikin päättää miten kysely jaettaisiin käyttäjille. Vaihtoehtoina oli luoda käyttäjäkyselylomake nettiin esimerkiksi Microsoft Accessin avulla, johon jokainen sitten olisi voinut vastata.

Toinen vaihtoehto oli lähettää kysymykset sähköpostilla, johon käyttäjät sitten vastaisivat halutessaan. Tässä projektissa päädyttiin jälkimmäiseen vaihtoehtoon, joka osoittautui erittäin toimivaksi. Käyttäjille annettiin vastausaikaa viikko, joka riitti hyvin tässä projektissa. Lähes jokainen käyttäjä teki kyselyn alusta loppuun ja kysymyksiin vastattiin nopeasti.

Kokonaisuudessaan palautteita tuli 22, joista suurin osa oli positiivisia. Palautteen perusteella käyttäjät tuntuivat olevan tyytyväisiä uuteen versioon eikä se aiheuttanut heille erityisemmin ongelmia. Käyttäjien mukaan käyttöliittymä oli selkeä sekä helppokäyttöinen. Osa käyttäjistä huomasi täystarkistuksen aikana hitautta, mutta suurimman osan mukaan käytössä ei ollut muutosta tai eivät ainakaan huomanneet hitautta työasemassa verrattuna vanhaan. Käyttäjäpalaute ja kyselylomake ovat kokonaisuudessaan liitteenä raportin lopussa (liite 1).

10 Yhteenveto

Kokonaisuudessaan projektilla saavutettiin sille asetetut tavoitteet ja asiakas oli lopputulokseen tyytyväinen. Ongelmia projektissa oli suhteellisen paljon mittaukseen liittyvissä asioissa. Osan ehkä olisi voinut ennaltaehkäistä, osaa taas ei. Olisi ehkä pitänyt tarkastella enemmän vaihtoehtoisia suorituskykymittaukseen soveltuvia ohjelmia, eikä luottaa siihen mikä ensisilmäyksellä vaikutti hyvältä. Tämä olisi saattanut kokonaisuudessaan nopeuttaa työntekoa paljonkin. OMW ei toiminut odotetulla tavalla ja kaavioiden kerääminen vei projektista huomattavan suuren osan aikaa.

Mittaustuloksia kerätessä huomattiin ongelma sekä lokien että OMW:n tekemien kaavioiden kanssa. Ryhmämäärityksiä ei löytynytkään jokaisesta lokitiedostosta. Tämä oli siinä määrin ongelmallinen tilanne, että tiedostojen kerääminen suoritettiin sekä uudella että vanhalla versiolla ennen tiedostojen tarkempaa analysointia. Vanhan version käynnistyslokeja ei voitu enää kerätä uudelleen, joten kaikista koneista ei saatu vertailukelpoista dataa käynnistymisestä. Jouduttiin tyytymään pelkästään uudella versiolla tehtyyn käynnistyksen keston mittaukseen.

Aikataulullisesti projektissa pysyttiin suhteellisen hyvin ja mitään suurempia ongelmia ei ilmennyt. Yhteistyökumppanit olivat tyytyväisiä projektiin ja sen tuloksiin.

Projektin aika olen oppinut paljon uutta tietoturvallisuudesta sekä saanut käsityksen siitä miten yritysmaailmassa projekteissa toimitaan. Olen perehtynyt F-Securen tuotteisiin ja oppinut niiden toiminnasta enemmän. Uskon tästä olevan hyötyä tulevaisuudessa oman kehittymisen ja työn kannalta. Projektin jälkeen yritys päätti aloittaa työasemapäivitykset uuteen F-Secure Client Security 9:n versioon.

Lähteet

Cknow, Virus History Summary. Viitattu 25.3.2010.
http://www.cknow.com/cms/vtutor/virus-history-summary.html

Frederic Avolio, Firewalls and Internet Security, the Second Hundred (internet Years). Viitattu 24.3.2011.
http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

F-Secure. F-Secure product training for endpoint security level 2 course. Viitattu 25.3.2010.

F-Secure, Policy manager. Viitattu 7.4.2010. http://www.f-secure.com/fi_FI/products/business/centralized-management/policy-manager/

F-Secure, Policy-manager. Viitattu 7.4.2010. http://www.f-secure.com/fi_FI/about-us/pressroom/gallery/image-library/policy-manager/index.html

F-Secure, Quick-Facts. Viitattu 9.6.2010. http://www.f-secure.com/fi_FI/about-us/pressroom/quick-facts/

F-Secure, Deepguard. Viitattu 19.1.2011. http://www.f-secure.com/fi_FI/products/technologies/deepguard/

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampereen Yliopistopaino Oy

Techait, F-Secure Client Security 9. Viitattu 24.2.2011.
http://www.techait.com/yritys/ajankohtaista/50-fscs9.html

F-Secure, helpompi, turvallisempi ja kevyempi suojaus. Viitattu 24.2.2011. http://www.f-secure.com/fi_FI/products/business/desktops-laptops/client-protection/

F-Secure, Client-security_522x448.jpg. Viitattu 21.3.2011. http://www.f-secure.com/system/fsgalleries/diagrams/client-security_522x448.jpg

Microsoft, How to enable user environment debug logging in retail builds of Windows . Viitattu 25.3.2010. http://support.microsoft.com/kb/221833

Piekkola, Tietokonevirusten ja muiden haitallisten ohjelmien historia. Viitattu 1.6.2010.
http://www.cs.helsinki.fi/u/kerola/tkhist/k2005/alustukset/haittaohj/Haitalliset_Ohjelmat.pdf

Processlibrary, userinit.exe. Viitattu 27.5.2010.
http://www.processlibrary.com/directory/files/userinit

tietoturvaopas, Haittaohjelmat. Viitattu 29.4.2010.
http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html

Kuvat ja kuviot

Liitteet

KÄYTTÄJÄPALAUTTEET FSCS 9-versiosta

Oletko huomannut koneen käynnistyvän nopeammin / hitaammin?

- Ehkä hieman nopeammin
- On ollut nopeampi
- En
- Näppituntumana käynnistys ehkä hieman nopeammin. Muuten kuormittaa aiempaa vähemmän tämän huomaa siitä että aiemmat pienet jumimiset jotka näkyivät hetken odotteluna (niin odottavan aikanhan on aina pitkä) ovat poistuneet
- Ei havaintoa eroista
- Käynnistyy nopeammin.
- Eipä juuri merkittävää muutosta
- En ole huomannut
- Ei se ainakaan ole nopeutunut. Tosi hidas, mahdollisesti vielä hitaampi kuin ennen. Saattaa tietysti johtua myös uudesta Office-paketista.
- F-Secure käynnistyy hieman nopeammin kuin vanha
- Nopeudessa en ole huomannut eroa (vaihtui juuri uusi kone enne testauksen alkua)
- Kone on aina päällä "valvomokäytössä"
- Ei eroa
- En
- Ei ole ollut merkittävää muutosta.
- Ehkä nopeammin - ei ainakaan hitaammin
- Käynnistys on aika ajoin hidasta, mutta ei voi sanoa onko se virustorjunnasta johtuvaa
- Mielestäni koneen nopeudessa on ollut havaittavissa hitautta. Tämä ei ole merkittävästi näkynyt käynnistymisessä.
- ehkä vähän
- Sanoisin että hiukan nopeampi nyt
- hieman nopeammin
- En

25.2. laitettiin virustorjunnan hallinnasta työasemille täystarkistus päälle pakotetusti. Huomasitko työaseman käytössä hitautta tarkistuksen aikana?

- En muista huomanneeni
- Olin lomalla, kone mukana, joten ei tainnut tarkistus mennä koneellani
- En
- En muista huomanneeni
- En
- Muistaakseni Weetin sivulle pöytäkirjaa laittaessa huomasin hitautta.
- En muista hitautta olleen
- En ole huomannut
- En muista.

- Jumitti koko koneen, vei prosessoriaika yli 90 %, tunnin pyörimisen jälkeen soitin Helppariin joka keskeytti tarkastuksen
- 25.2 lomalla
- En ole huomannut
- En
- En, olin lomalla tuohon aikaan.
- Ei ole ollut merkittävää muutosta.
- En
- ei havaintoa
- En huomannut pakotettua täystarkistusta, jote sen osalta kaikki OK
- kyllä, välillä ”jäi odottelemaan” välillä ei huomannut mitään
- Nyt en ole varma, mutta voi olla ettei ollut vielä tuolloin uusi F-securen ohjelma minun koneella. Tai sitten en vain muista koko juttua.
- työasema ei ollut käytössä
- En

Oletko kokeillut virustorjunnan käyttöliittymää? Osaatko erikseen virustarkistaa tietyn hakemiston/tiedoston/USB-tikun tarvittaessa?

- Olen kokeillut ja osaan.
- Olen kokeillut, liittymä on tuttu kotikoneesta (Internet Security 2010)
- Kyllä osaan
- On kokeiltu. Tarkistukset sujuvat
- En
- En ole kokeillut, mutta osaisin tarvittaessa tarkistaa.
- En ole kokeillut
- En osaa
- Jep, osaan
- Vähän vilkuillut. Kohteiden tarkastaminen onnistuu.
- Kyllä
- Kyllä
- En
- En ole, en osaa
- Noup
- Olen - helppo juttu.
- en ole käyttänyt, tarkistin, miten toimii, ei ongelmia
- Mielstäni kohtalaisen selkeä ja yksinkertainen käyttää, en ainakaa haukua osaa.
- kyllä
- Kyllä osaan – ja on muuten helppo tehdä
- onnistuu
- En

Miltä uusi käyttöliittymä näyttää? Löydätkö sieltä tarvitsemasi tiedot, esimerkiksi onko virustorjunnan päivitykset ajan tasalla?

- Käyttöliittymä ok, kaikki tarpeellinen löytyy.
- Liittymä on parempi kuin aiemmin
- Selkeä. Hyvin löytyy
- Löytyy – mielestäni selkempi kuin aiemmin
- Selkeä. Löydän ja on ajan tasalla.

- Ok. Löydän.
- En tiedä
- En ole sitä käyttänyt??
- Ok
- Käyttöliittymä on selkeä, sieltä kyllä löytyy tarvittavat tiedot.
- Löytyy
- Kyllä
- En
- En tiedä
- No helposti löytyi.
- Liittymä näyttää loogiselta ja helpolta
- kotikoneella on samanlainen, olen tottunut tähän eikä se ole hankala
- Vähän aikaa näppäiltyä löytyy. Normaalia uuden käyttöön totuttelun tuskaa.
- ihan ok, tiedot löytyvät
- Käyttöliittymä on tosi yksinkertainen ja sen vuoksi käyttäjäystävällinen - uusi logo vaan on vähän sellainen että sitä ei tahdo tuosta erottaa käynnistyspalkista. Helposti näkee virustorjunnan tilan.
- käyttöliittymä on selkeä, tunnisteiden tila löytyy helposti
  En

Onko uuden version kanssa ollut ongelmia?

- Ei
- Ei
- Ei ole
- Ei
- En ole havainnut
- Ei ole.
- Power point aukeaa hitaasti mutta ongelma saattoi olla jo ennen päivitystä.
- Heittää roskapostiin joitain asioita, jotka ovat selvästi OK
- Ei
- Laskujen tarkastus ei toiminut enne kuin teki ilmoitetut toimenpiteet. Muuten ei ole ongelmia ollut.
- Laskujen tarkastus ei toiminut ilman lisäasetuksia
- Ei asentunut kunnolla. Tästä tieto Kirsi Kankkosella, johon olin yhteydessä
- Ei
- Ei
- Ei ole ollut.
- Ei
- ei
- Ei
- laskujen tarkistus vaatii asetusten muuttamisen, muuten ei mitään ongelmia
- Ei
- laskujen tarkastus tökki aluksi, mutta selaimen asetusten muutos auttoi
- Ei

Muita kommentteja tuotteesta:

- Tarkempi kuin aiemmin.
- Vaikuttaa paremmalta ja käytettävämmältä kuin aikaisempi versio.
- Vaikuttaa aivan toimivalta.

- Olen tottunut koneeni hitauteen, on sen verran vanha. En juuri hitauksiin kiinnitä huomiota ☺
- Hyvin pelaa.
- koko ajan näkyvä ”yläpalkin ilmoitus” tai hakusivuilla näkyvä ”luotettava sivu” ilmoitus sekä varoitus epäluotettavasta sivusta on hyvä – mikäli siihen voi luottaa
- Parempi kuin edeltäjänsä
- fiksu

Liite 1: Käyttäjäkysely

Suorituskykytestit – Työasemat

Suorituskykytestit seuraavien Työasemien osalta:

computer1
computer2
computer3
computer4
computer5
computer6
computer7
computer8
computer9
computer10
computer11
computer12
computer13
computer14
computer15
computer16
computer17
computer18

Työaseman tiedot

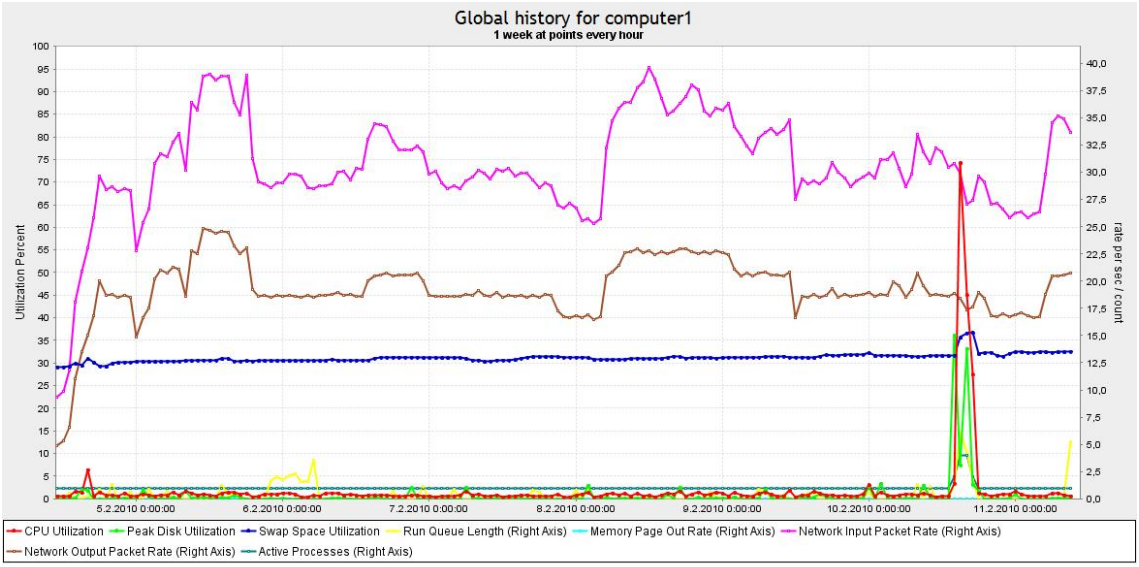
Työaseman nimi	**computer1**
Malli	HP Compaq DC7800SFF
Prosessorityyppi	Intel(R) Pentium(R) D CPU 3.00GHz
Muistin määrä MB	999
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 173min

käynnistyksen kesto 2.56min

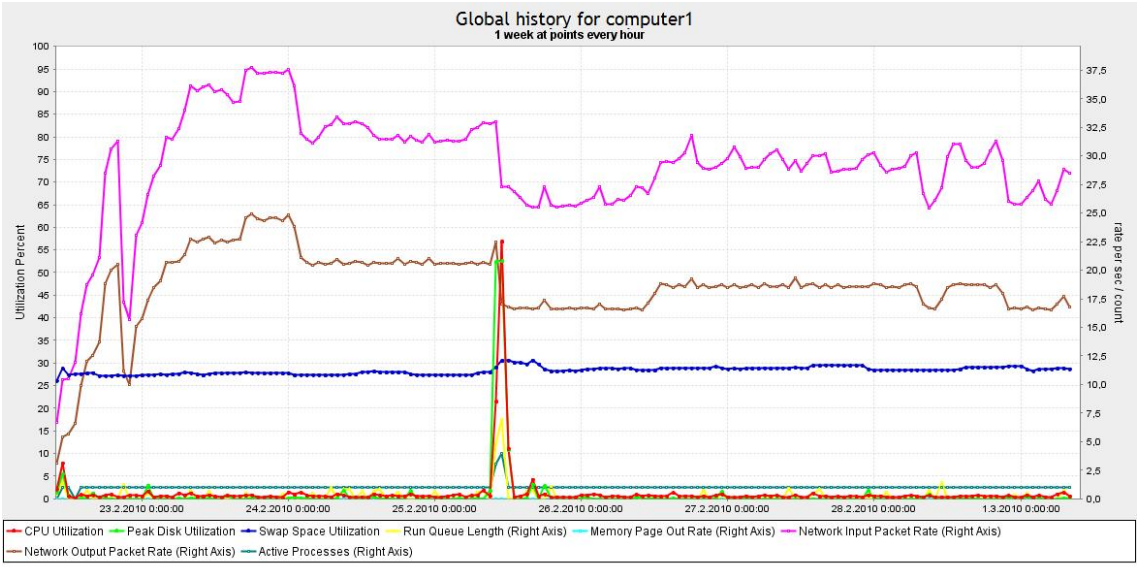


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 113min

käynnistyksen kesto 1.52min



Työaseman tiedot

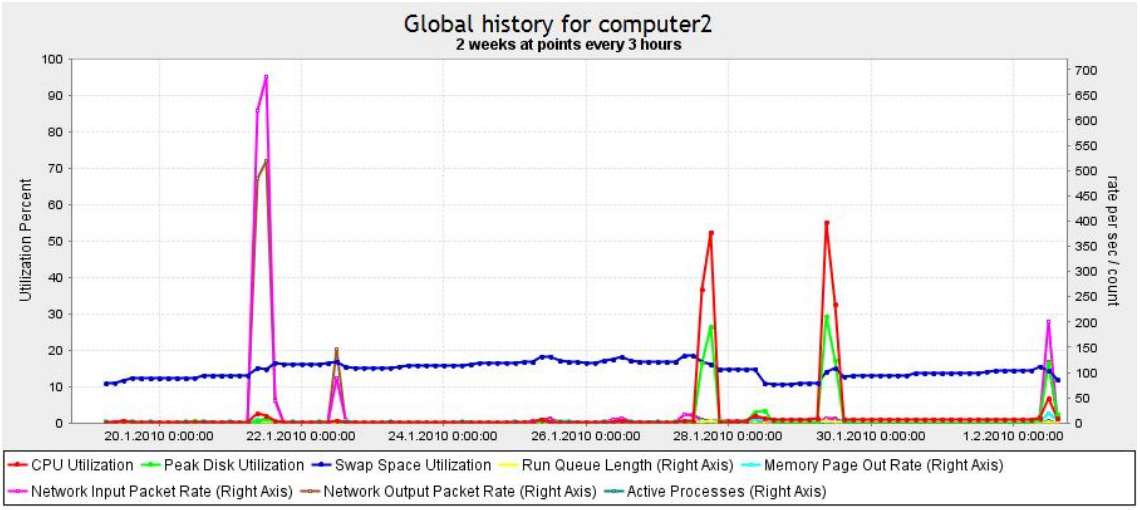
Työaseman nimi	**computer2**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz
Muistin määrä MB	3543
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 270min

käynnistyksen kesto

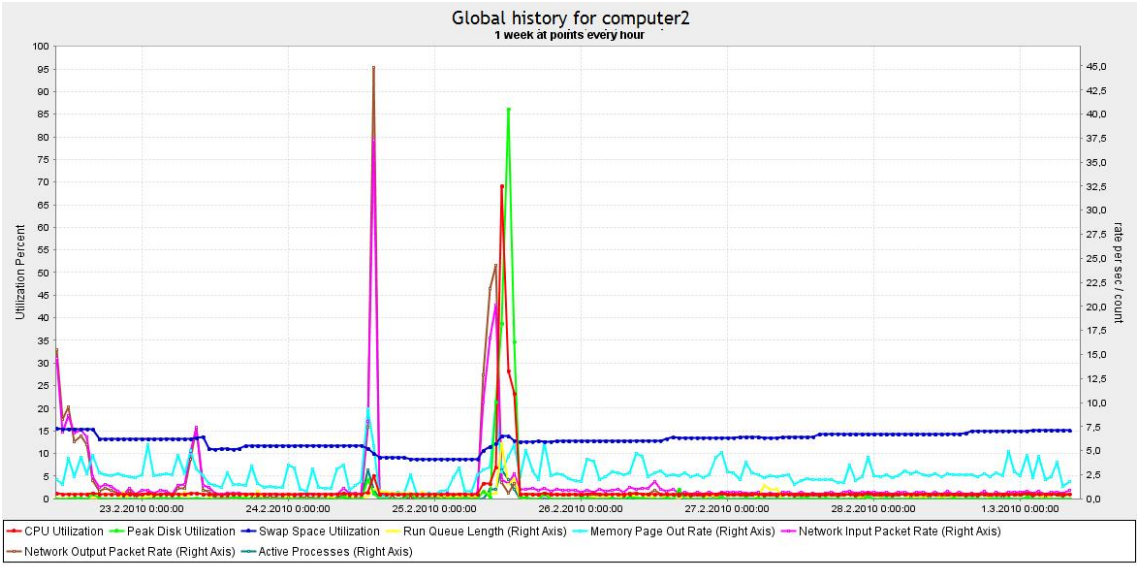


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 165min

käynnistyksen kesto 27.17min



Työaseman tiedot

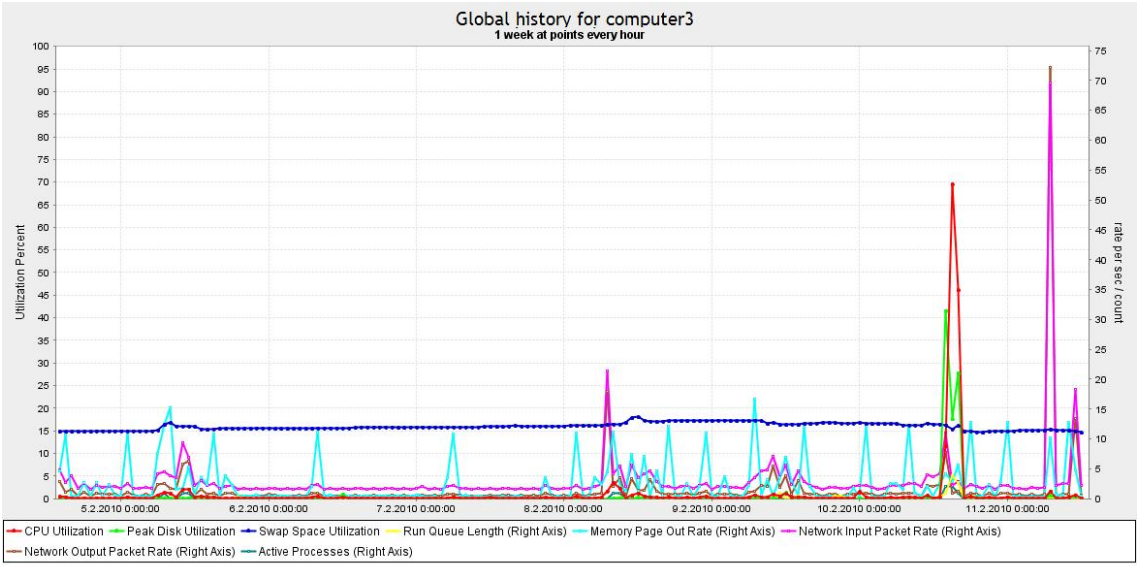
Työaseman nimi	**computer3**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz
Muistin määrä MB	4096
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto minuutteja: 34min

käynnistyksen kesto

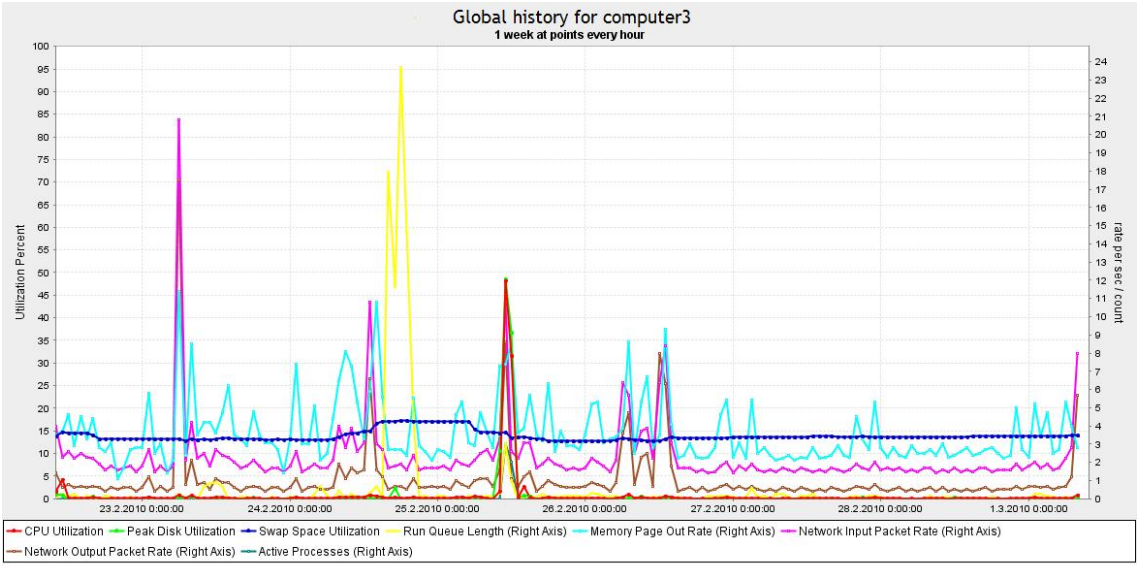


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 111min

käynnistyksen kesto 8.40min



Työaseman tiedot

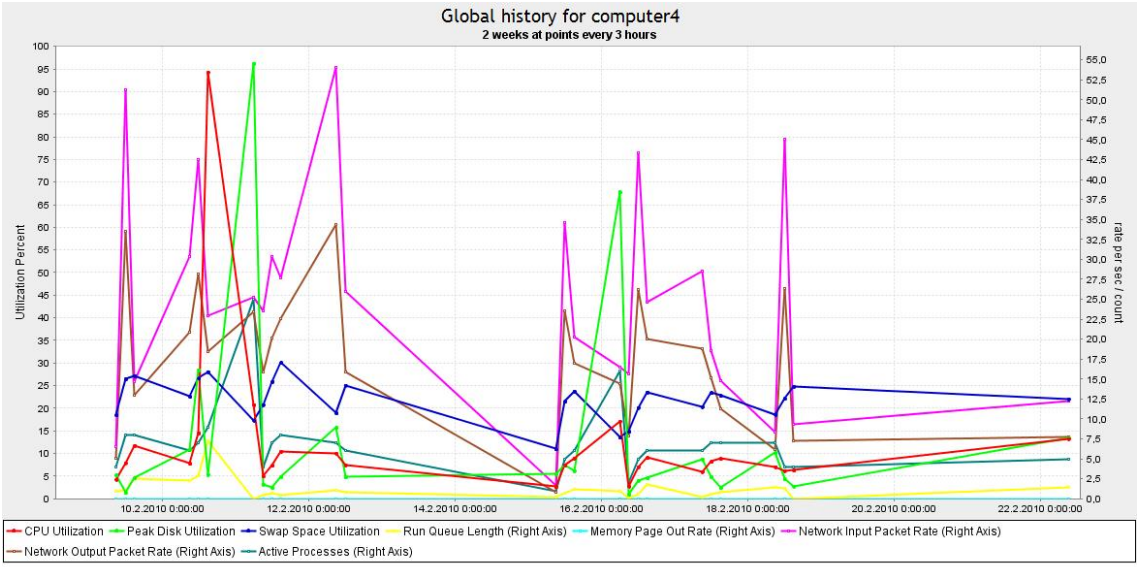
Työaseman nimi	**computer4**
Malli	HP Compaq 2510p
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU U7600 @ 1.20GHz
Muistin määrä MB	2048
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto minuutteja:

käynnistyksen kesto 4.32min

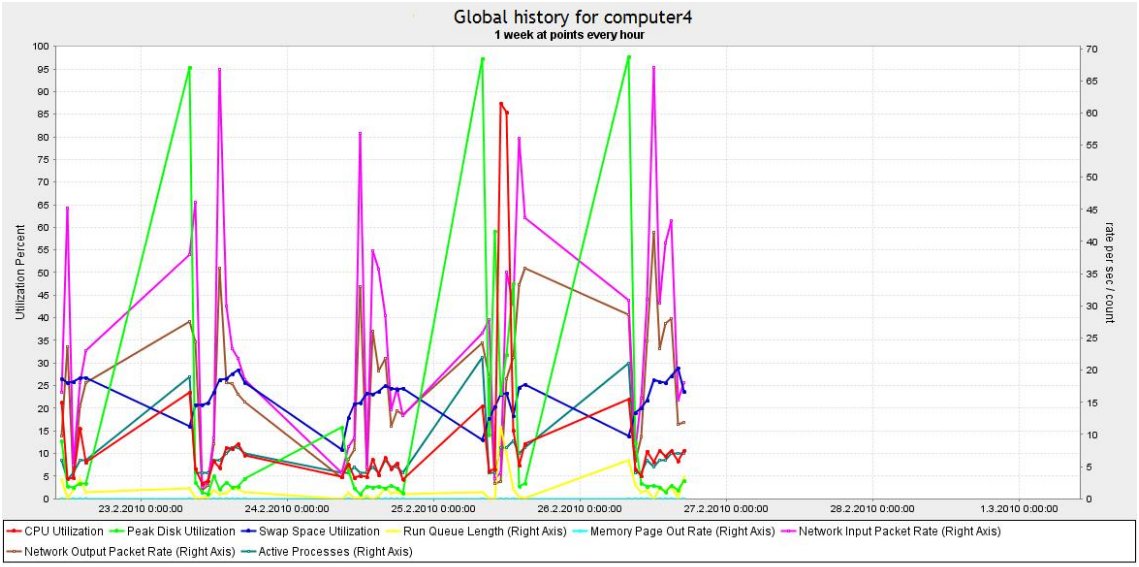


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 176min

käynnistyksen kesto 3.46min



Työaseman tiedot

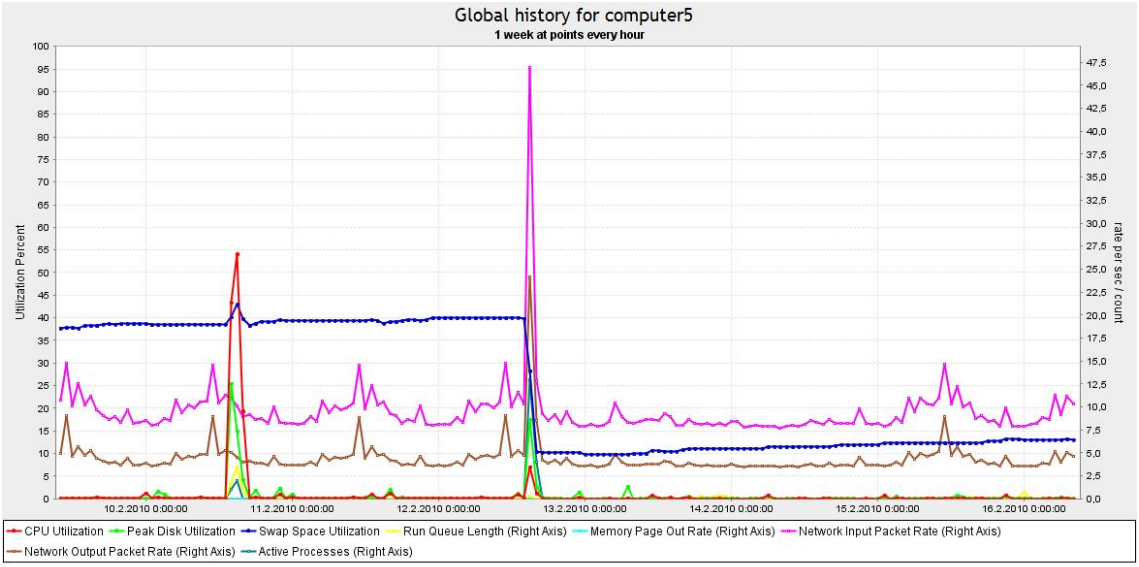
Työaseman nimi	**computer5**
Malli	HP Compaq DC7800SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz
Muistin määrä MB	2048
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 130min

käynnistyksen kesto

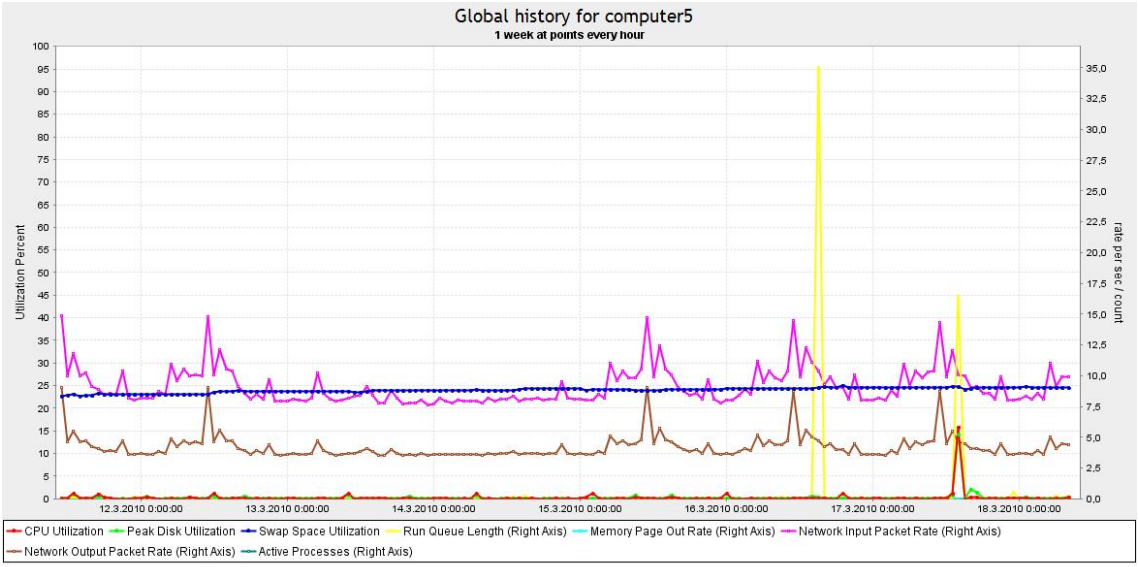


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 16min

käynnistyksen kesto 25sek



Työaseman tiedot

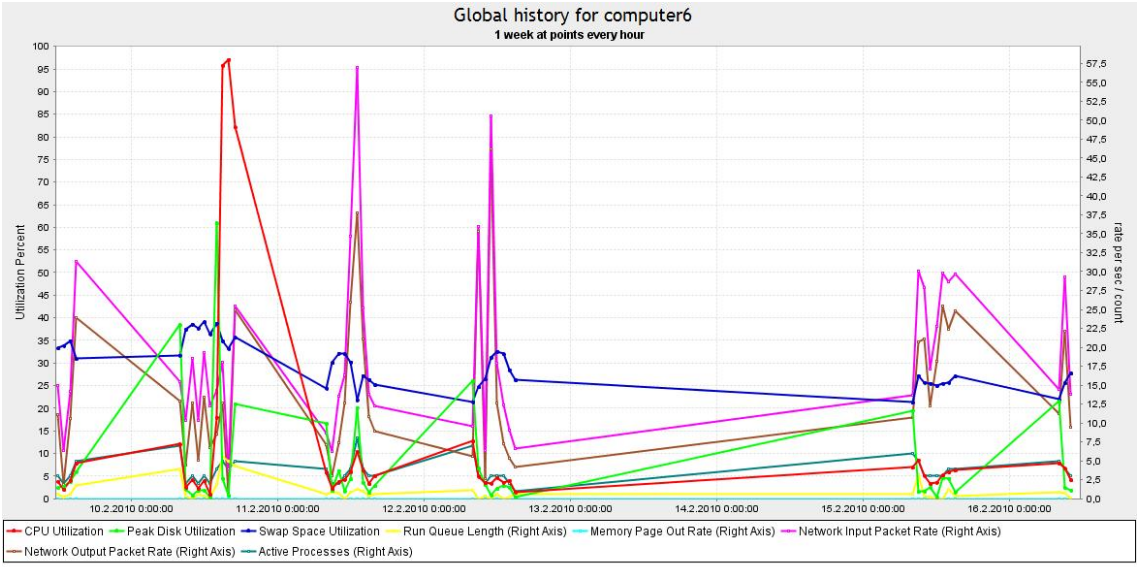
Työaseman nimi	**computer6**
Malli	HP Compaq nc6400
Prosessorityyppi	Intel(R) Core(TM)2 CPU T5500 @ 1.66GHz
Muistin määrä MB	1024
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 393min

käynnistyksen kesto 1.48min

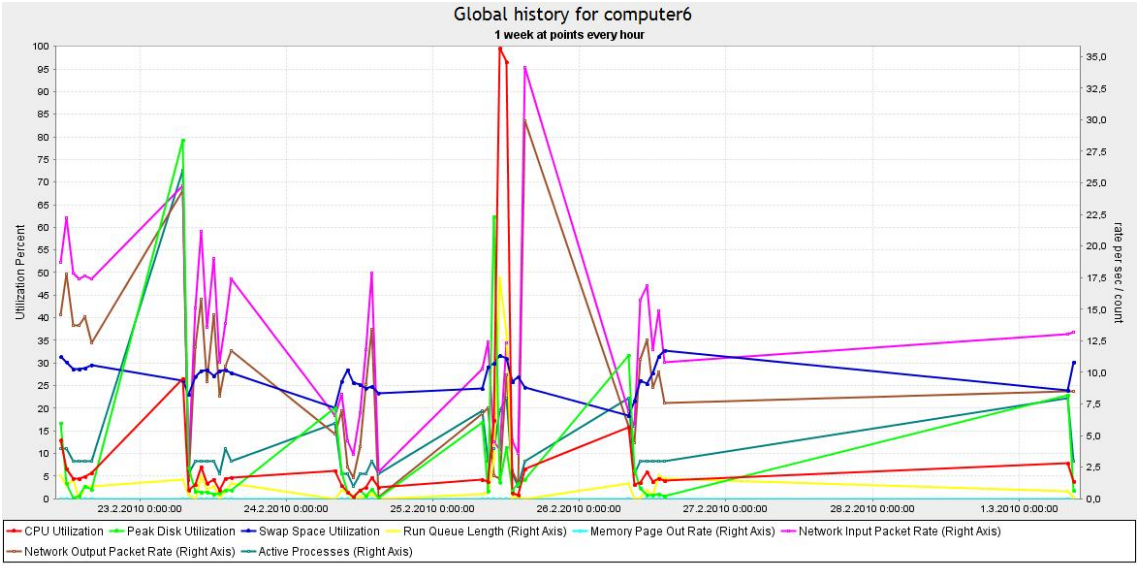


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 165min

käynnistyksen kesto 42sek



Työaseman tiedot

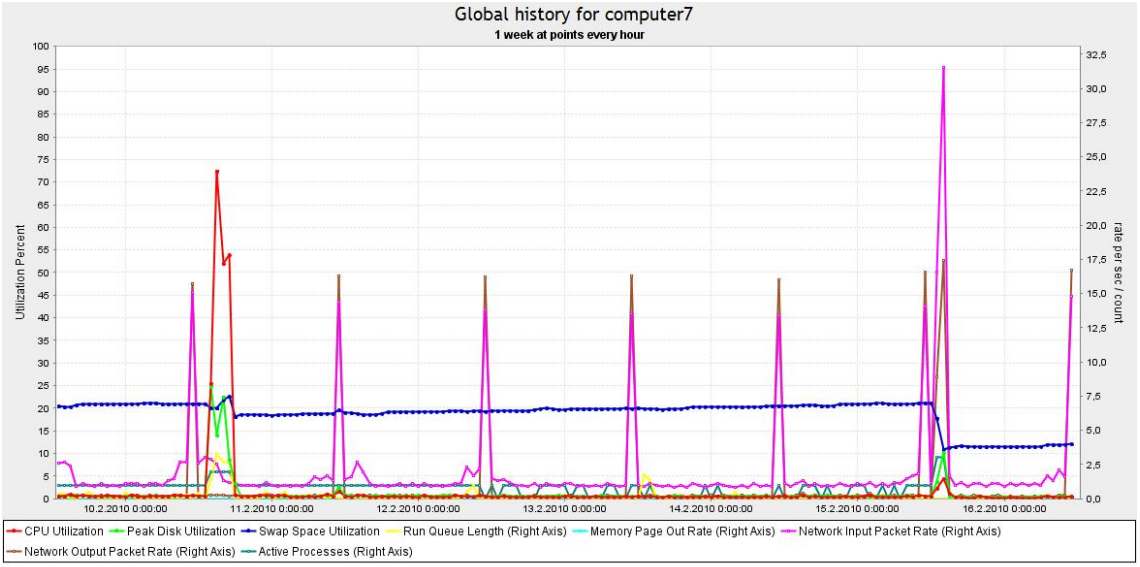
Työaseman nimi	**computer7**
Malli	HP Compaq DC7800SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E4500 @ 2.20GHz
Muistin määrä MB	2048
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 208min

käynnistyksen kesto

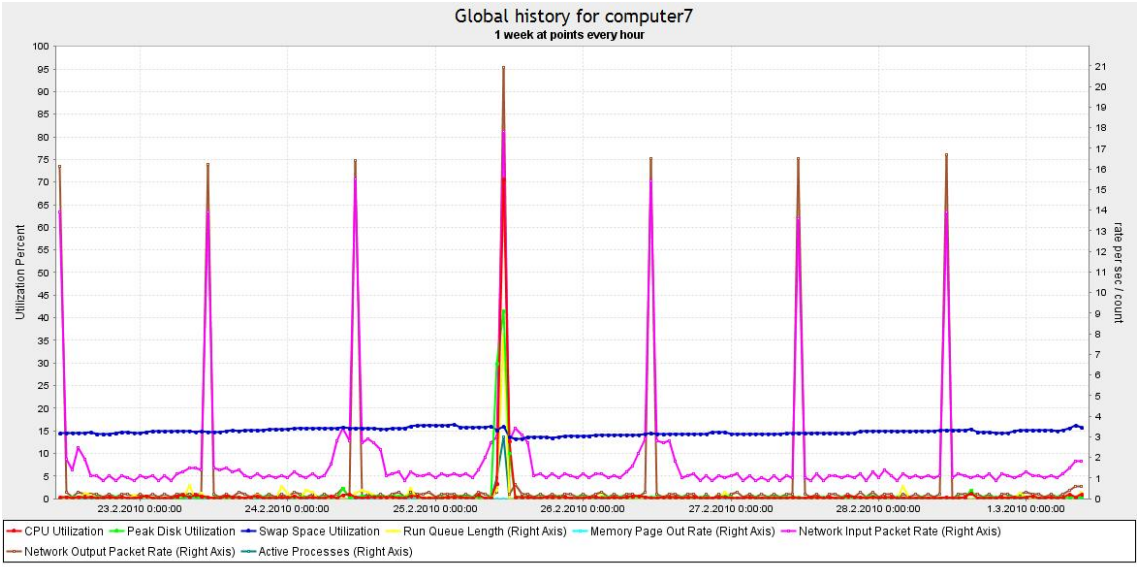


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 10:41:24 - 12:13:40 93min

käynnistyksen kesto 1.46min



Työaseman tiedot

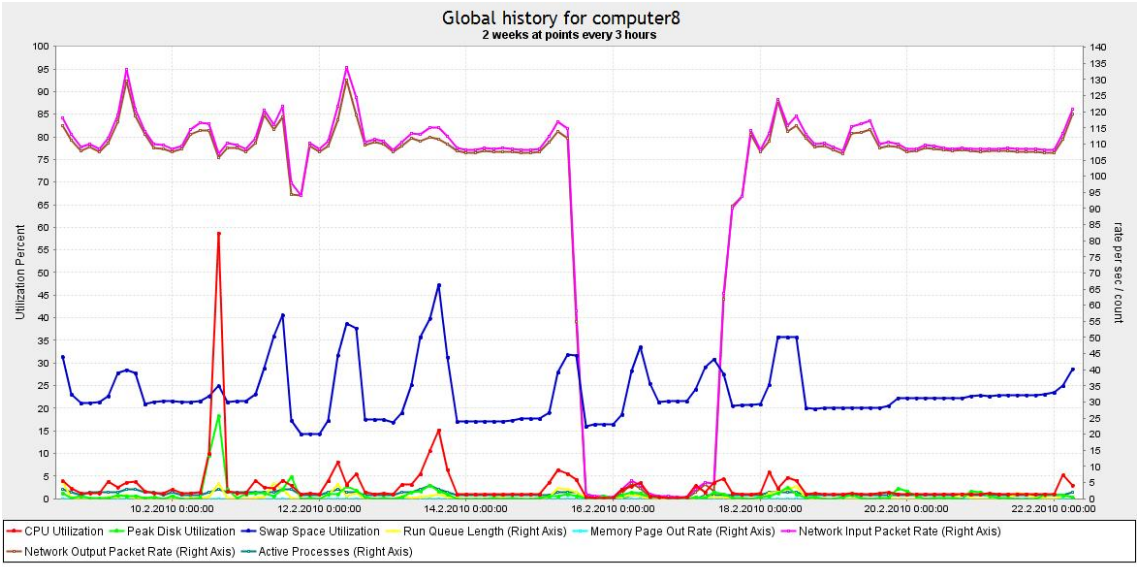
Työaseman nimi	**computer8**
Malli	HP Compaq DC7800SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz
Muistin määrä MB	2048
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 210min

käynnistyksen kesto 1.58min

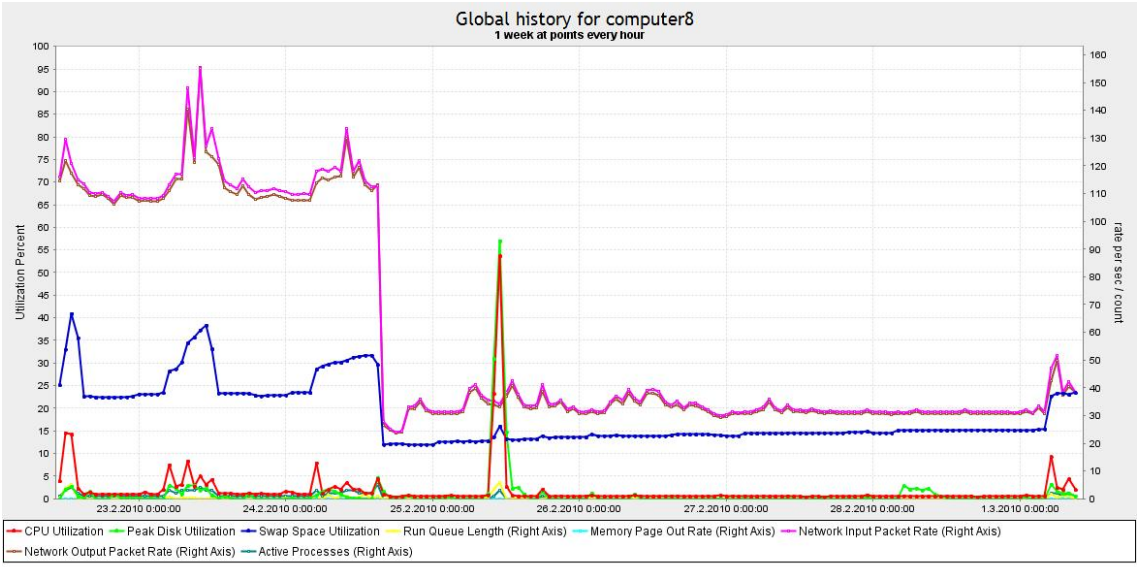


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 100min

käynnistyksen kesto 1.36min



Työaseman tiedot

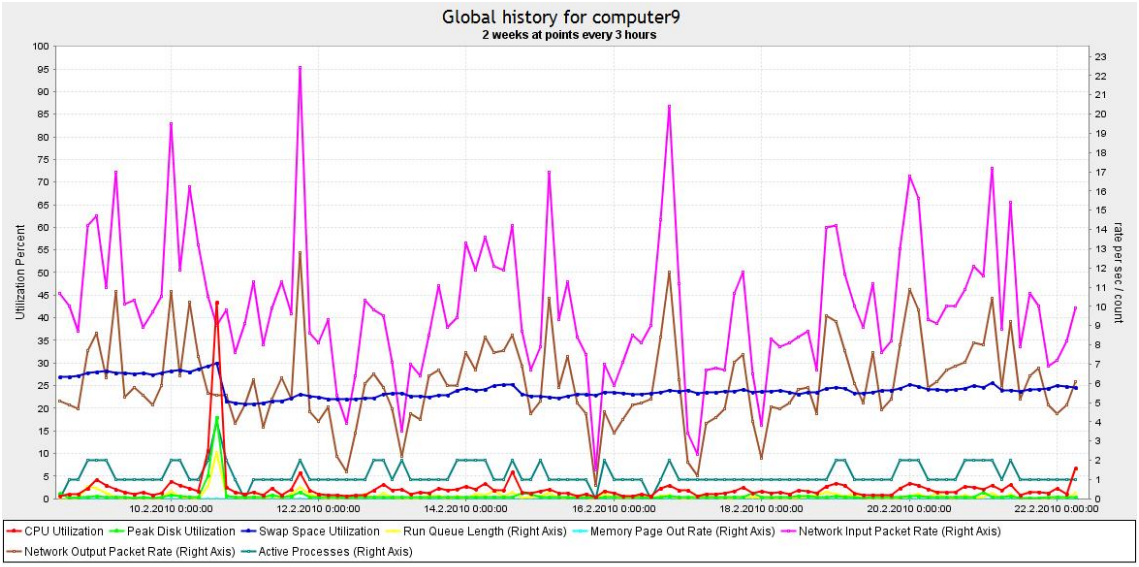
Työaseman nimi	**computer9**
Malli	HP Compaq DC7800CMT
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz
Muistin määrä MB	2048
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 186min

käynnistyksen kesto 1.04min

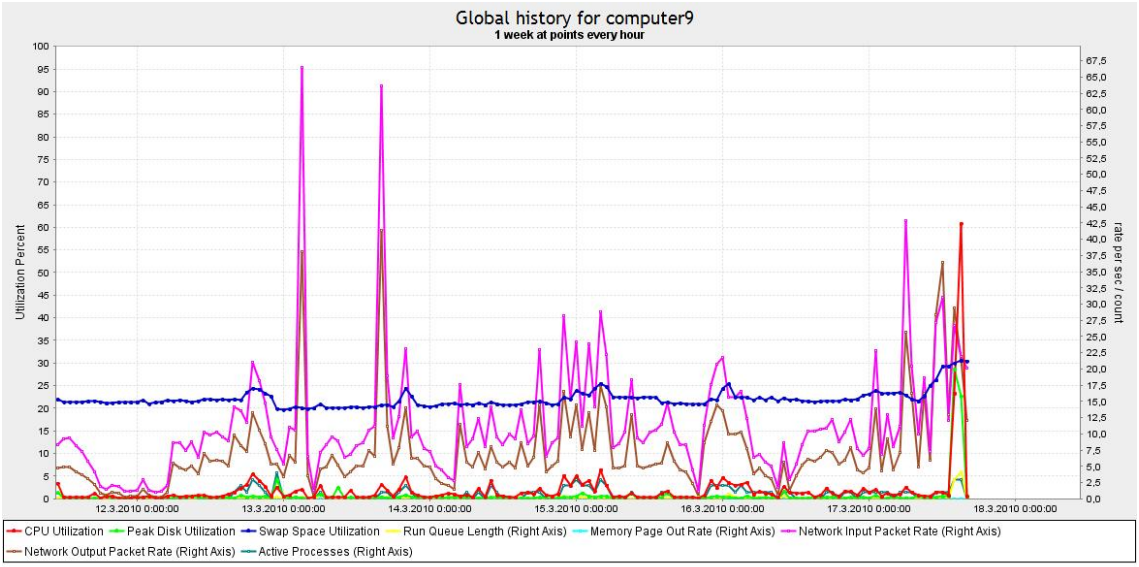


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 109min

käynnistyksen kesto 1.39min



Työaseman tiedot

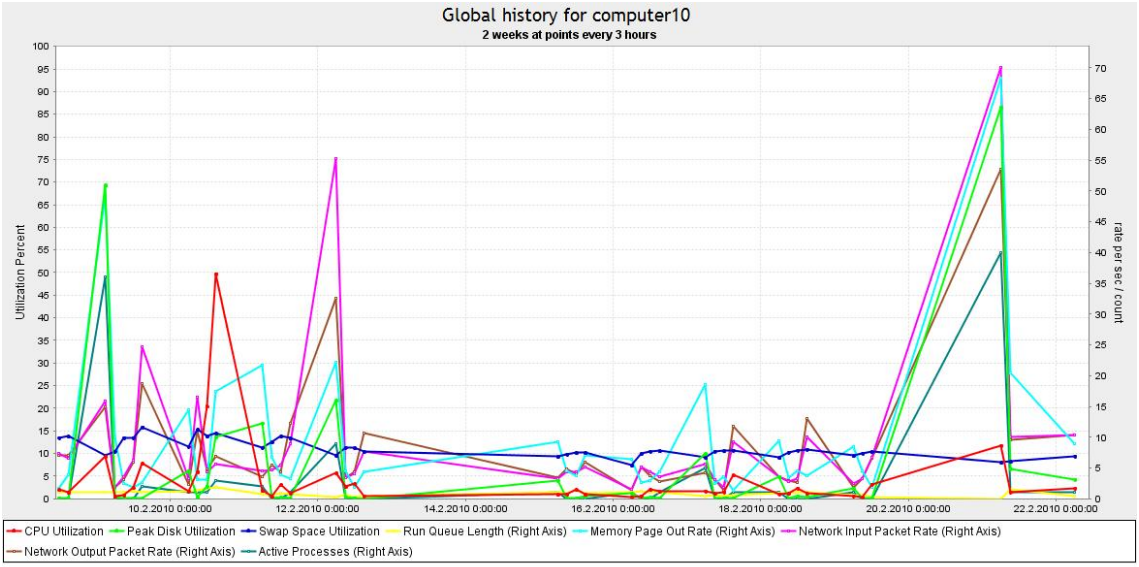
Työaseman nimi	**computer10**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz
Muistin määrä MB	4096
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 86min

käynnistyksen kesto 2.58min

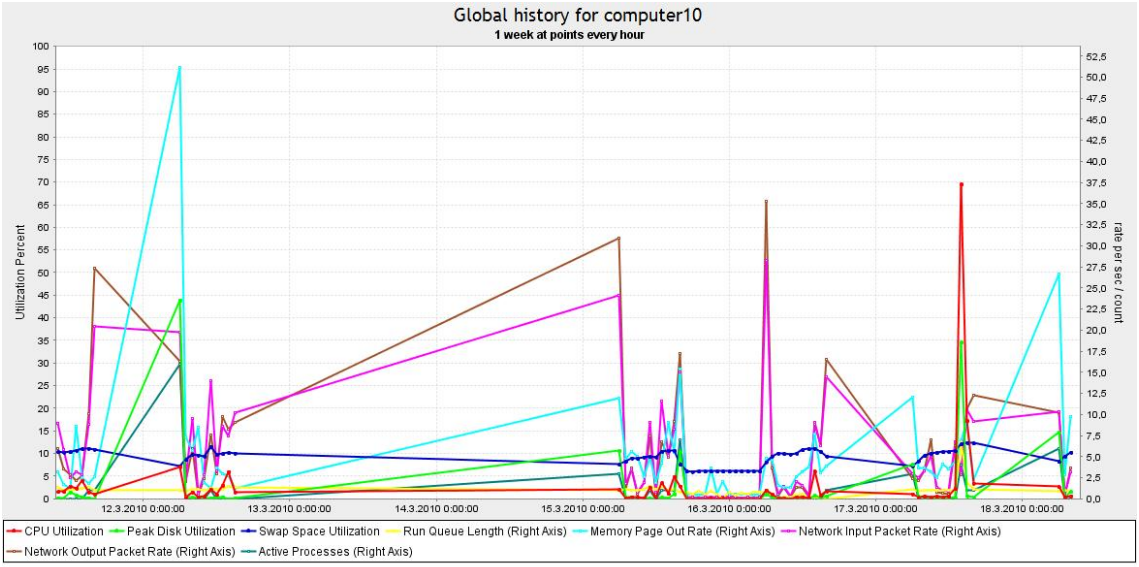


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 69min

käynnistyksen kesto 1.40min



Työaseman tiedot

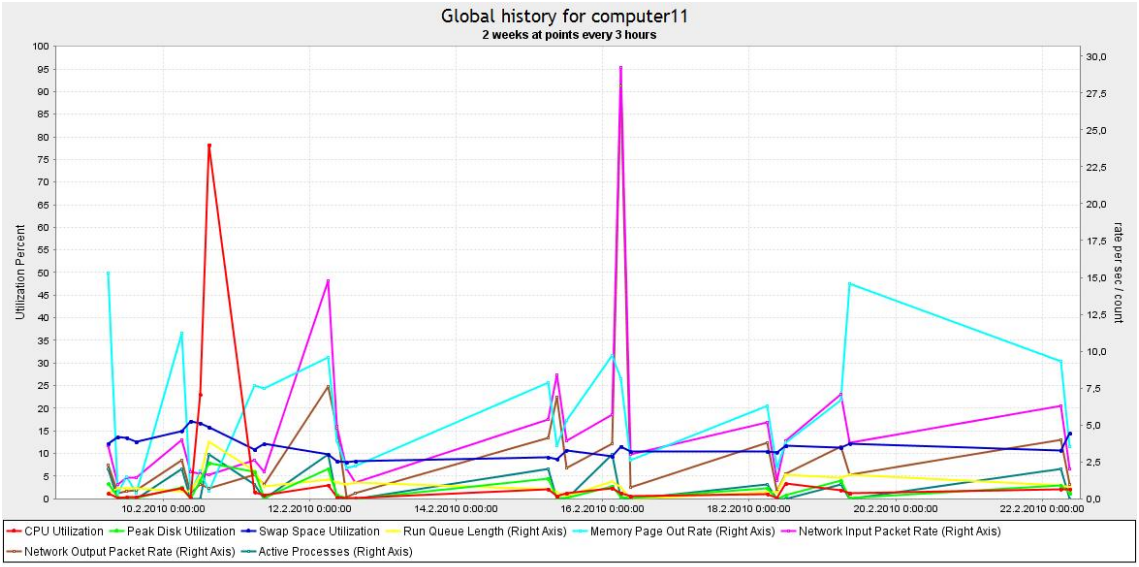
Työaseman nimi	**computer11**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz
Muistin määrä MB	4096
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto

käynnistyksen kesto 32sek

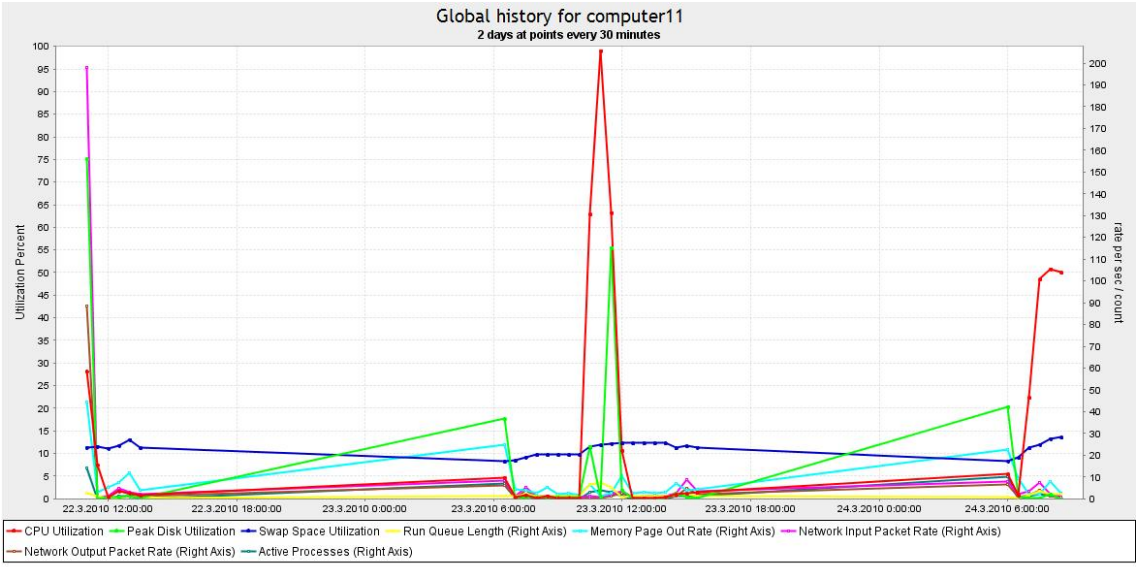


Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 90min

käynnistyksen kesto 2.36min



Työaseman tiedot

Työaseman nimi	**computer12**
Malli	HP Compaq nc4400
Prosessorityyppi	Intel(R) Core(TM)2 CPU T5500 @ 1.66GHz
Muistin määrä MB	1024
Käyttöjärjestelmä	Windows XP

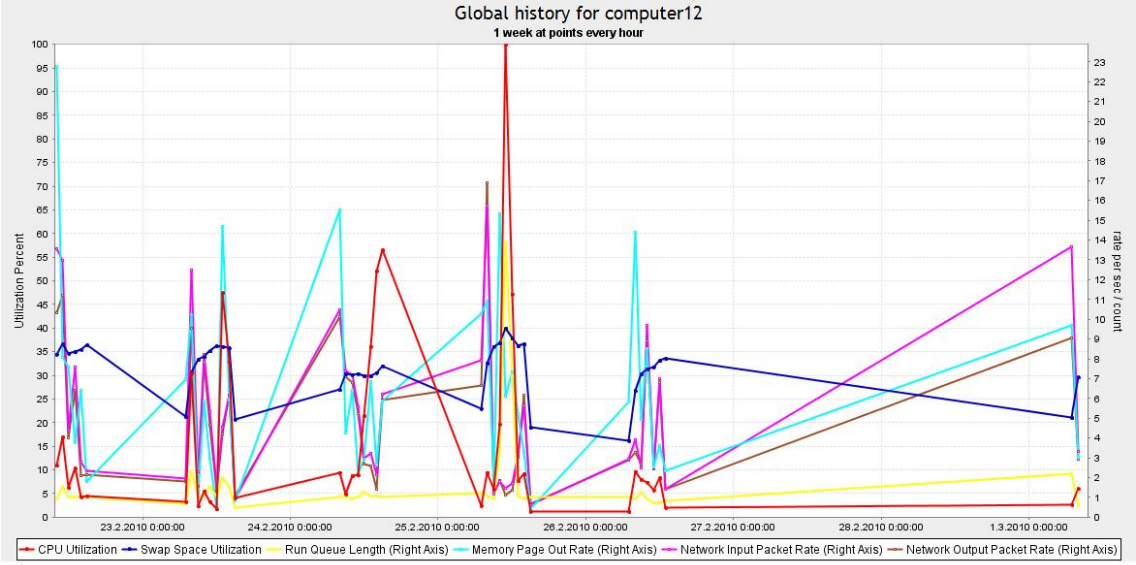
Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 132min

käynnistyksen kesto ennen asennusta 2.26min

käynnistyksen kesto asennuksen jälkeen 2.20min



Työaseman tiedot

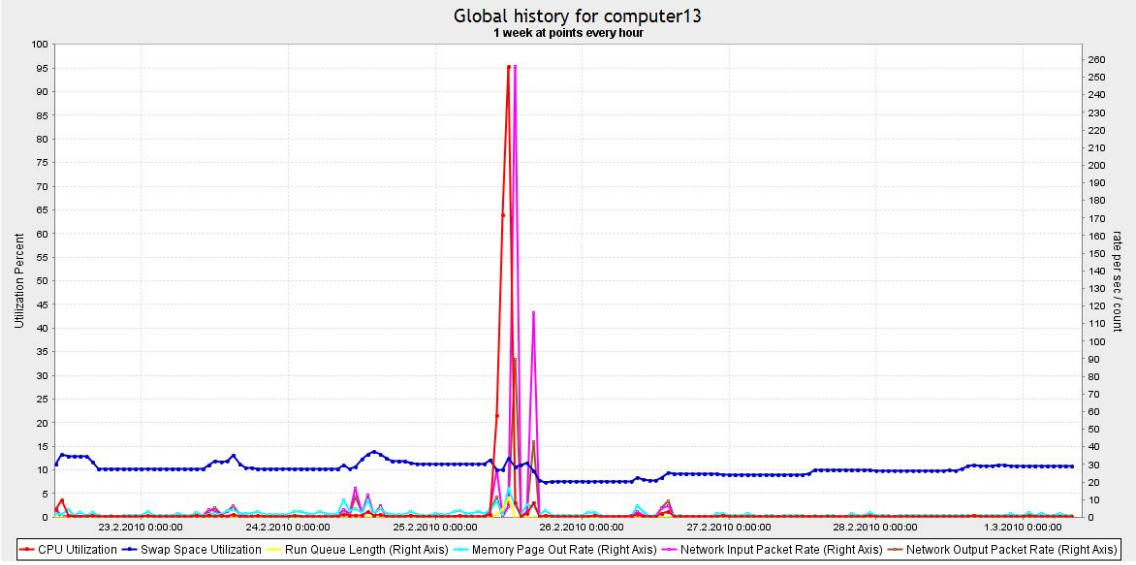
Työaseman nimi	**computer13**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz
Muistin määrä MB	3543
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 139min

käynnistyksen kesto 2.01min



Työaseman tiedot

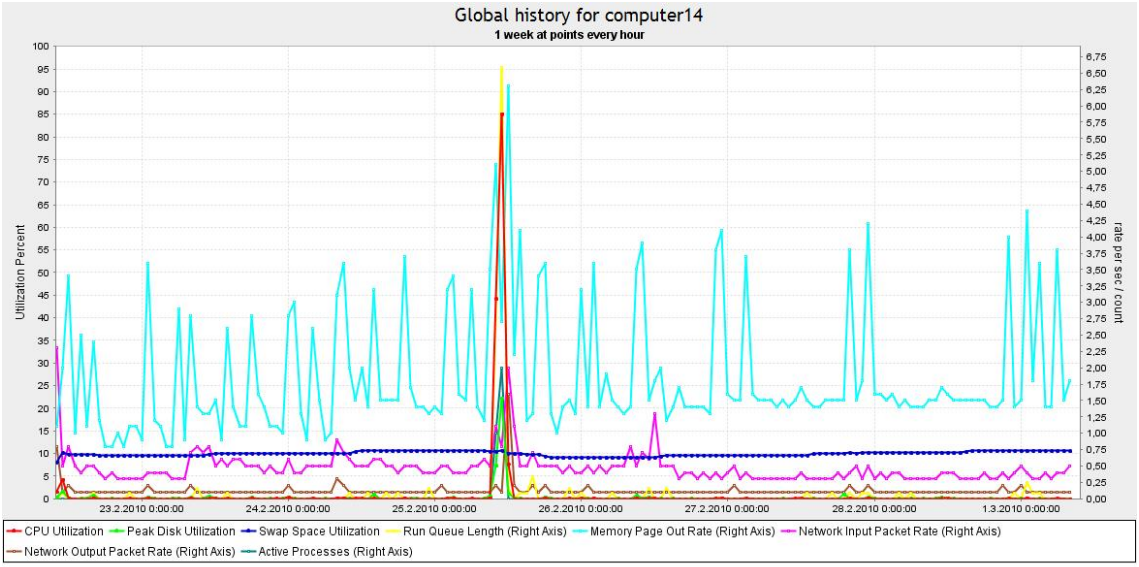
Työaseman nimi	**computer14**
Malli	HP Compaq dc7900 usdt
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7300 @ 2.66GHz
Muistin määrä MB	4096
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 95min

käynnistyksen kesto 1.25min



Työaseman tiedot

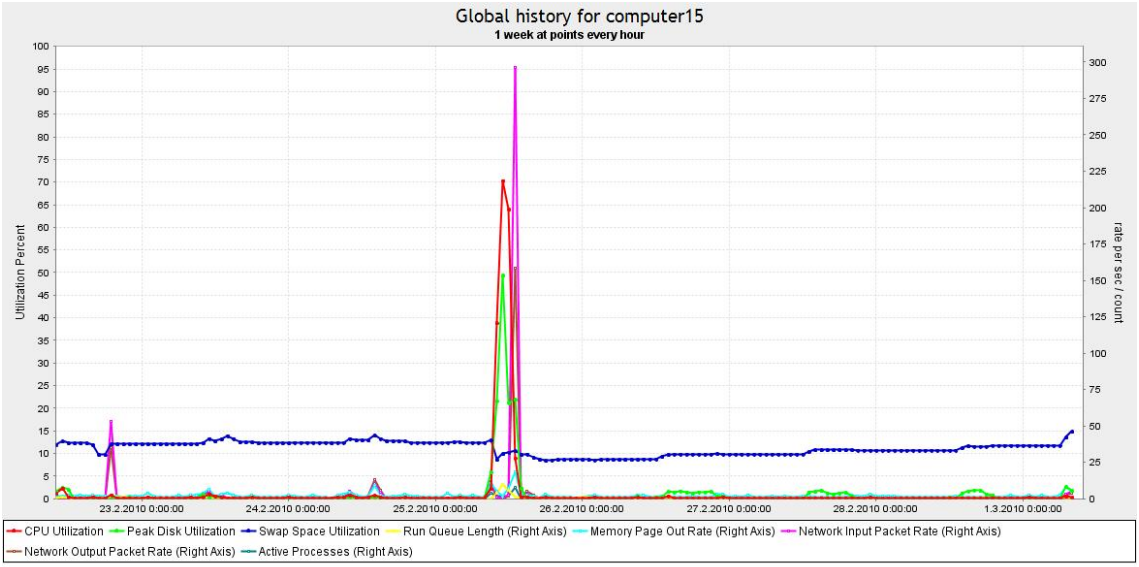
Työaseman nimi	**computer15**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz
Muistin määrä MB	2790
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 141min

käynnistyksen kesto 15.06min



Työaseman tiedot

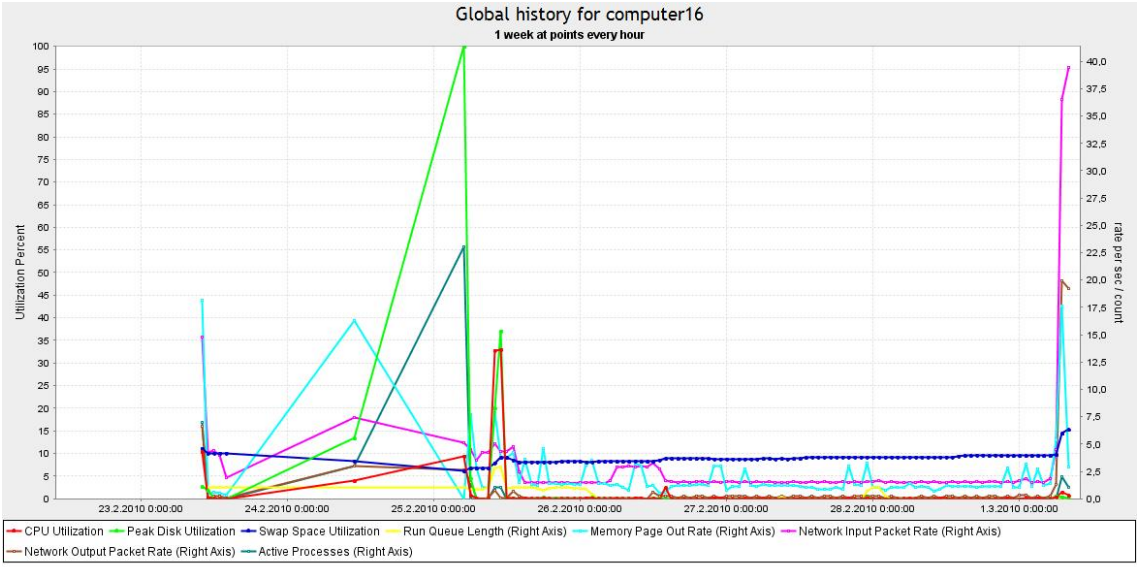
Työaseman nimi	**computer16**
Malli	HP Compaq dc7900 SFF
Prosessorityyppi	Intel(R) Pentium(R) 4 CPU 3.00GHz
Muistin määrä MB	1024
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 70min

käynnistyksen kesto 2.20min



Työaseman tiedot

Työaseman nimi	**computer17**
Malli	HP Compaq DC7600SFF
Prosessorityyppi	Intel(R) Pentium(R) 4 CPU 3.00GHz
Muistin määrä MB	1024
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 240min

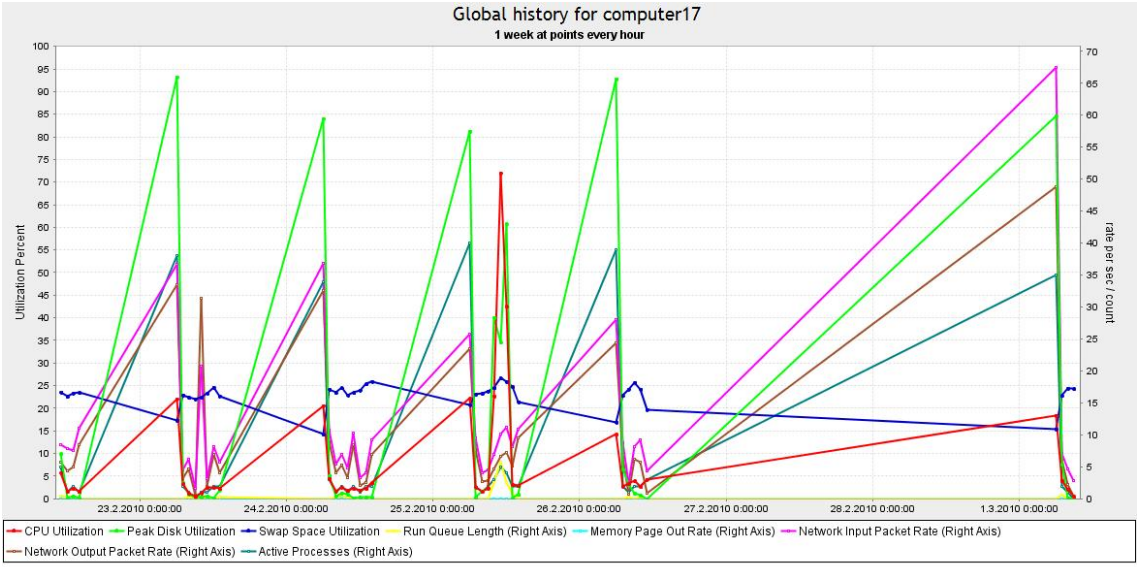
käynnistyksen kesto 4.57

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 155min

käynnistyksen kesto 5.29



Työaseman tiedot

Työaseman nimi	**computer18**
Malli	HP Compaq DC7700P CMT
Prosessorityyppi	Intel(R) Core(TM)2 CPU 6400 @ 2.13GHz
Muistin määrä MB	1024
Käyttöjärjestelmä	Windows XP

Suorituskykytiedot ennen F-Secure for workstations versio 9: n asennusta

Full Scan-tarkistuksen kesto

- kesto 178min

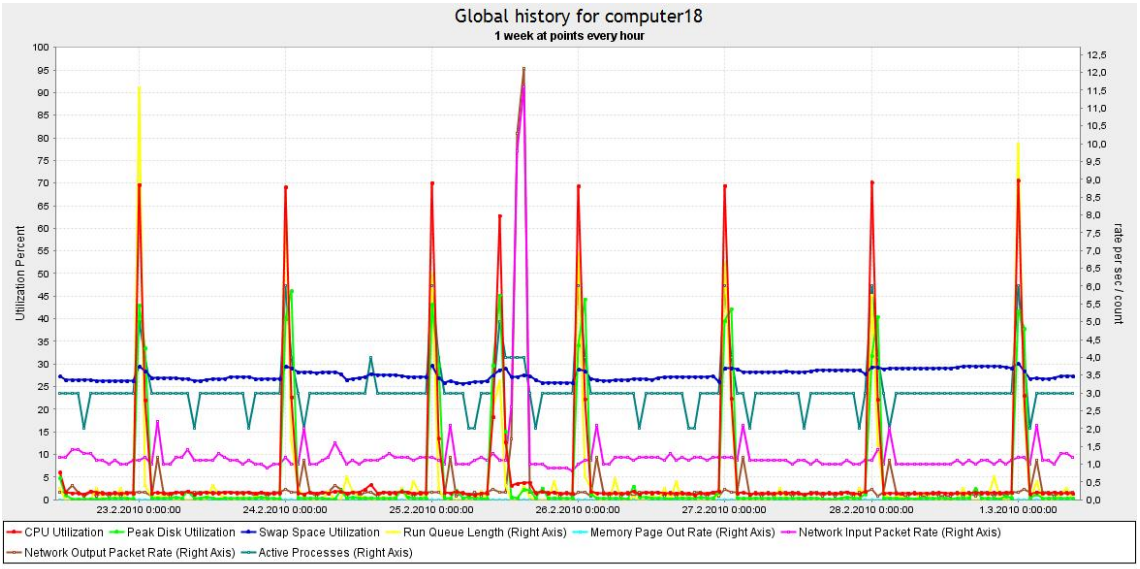
käynnistyksen kesto

Suorituskykytiedot F-Secure for workstations versio 9: n asennuksen jälkeen

Full Scan-tarkistuksen kesto

- kesto 91min

käynnistyksen kesto



Liite 2: Suorituskykymittaukset