PALVELUKUVAUS - TIETOTURVAPALVELUT

SISÄLLYS

Tietoturvapalvelut yleisesti 2

Laitteiden tietoturva (EDR ja XDR) 2

Sophos 2

Symantec 3

SOC (MDR) 4

Sähköpostin tietoturva 6

Tekninen kuvaus 6

Lisensointi 7

Tietoturvakoulutus ja hyökkäyssimulaatio 7

Miten palvelu toimii 7

Lisensointi 8

DDoS-suojaus 8

Verkkoskannaus 9

Lisensointi 9

ZTNA (Zero Trust Network Access) 9

Lisensointi 11

Secure Web Gateway (SWG) 12

Miten tuote toimii 12

Lisensointi 13

Lisätietoja 13

Tietoturvapalvelut yleisesti

Asiakkaan vastuulla on huolehtia sovellustensa, laitteistonsa ja henkilöstönsä tietoturvasta ja tietoturvakoulutuksesta. TNNet Oy tarjoaa kattavasti erilaisia tietoturvaan liittyviä lisäpalveluita, joita voi hankkia joko omina palveluinaan tai yhdessä muiden TNNetin palveluiden kanssa. Palveluiden skaala on hyvin laaja aina käyttäjien koulutuksesta tietoverkon tekniseen tietoturvaan asti.

Organisaation tietoturva on aina yhtä vahva kuin sen heikoin lenkki. Tyypillisesti on voitu ajatella, että riittää, kun käyttäjillä on antivirus asennettuna. Tietoturva ei kuitenkaan ole mikään yhden palvelun tai tuotteen kokonaisvaltainen ratkaisu, vaan tärkeintä on ns. kerrossuojautuminen.

Tietototurvapalveluissa hyödynnetään usein kolmannen osapuolen tuotteita (esimerkiksi Sophos, Symantec, Netscout, Tenable), joissa myös osa datasta on kolmannen osapuolen hallussa. Huolehdimme oman tietoturvapolitiikkamme mukaisesti, että kaikki käytettävät kolmannet osapuolet vastaavat TNNetin tietoturvavaadetta. Kaikki data säilytetään mahdollisuuksien mukaan omassa laitesaleissamme tai vähintään Euroopan sisällä. Jos data poistuu TNNetin laitesalista, on se erikseen mainittu tässä palvelukuvauksessa. Tällaisissa tapauksissa tarkemmat ja ajankohtaiset tiedot datan sijaintiin ja tietoturvaan liittyen löytyvät tapauskohtaisesti toimittajan omilta sivustoilta tai palvelukuvauksista.

Laitteiden tietoturva (EDR ja XDR)

Laitteiden tietoturvapalvelut sisältävät tietoturvasovelluksia niin käyttäjien laitteille kuin palvelimillekin. Vaihtoehtoina ovat joko Sophoksen tuoteperhe tai Symantecin tuotteet. Sophoksen ratkaisut tuovat lisäarvoa, mikäli organisaation käytössä on myös muita Sophoksen tuotteita (esimerkiksi palomuuri). Muutoin ominaisuuksissa on pieniä valmistajakohtaisia eroja, mutta isossa kuvassa tuotteet ovat lähtökohtaisesti tasavertaisia. Isoin ero valmistajien välille tulee hinnoittelumalleissa, joka voi vaikuttaa olennaisesti myös lopulliseen hinnoitteluun.

Käyttäjän laitteilla tarkoitetaan henkilökohtaisia työkoneita (Windows ja Mac) sekä tabletteja ja puhelimia (Android ja iOS). Palvelimilla tarkoitetaan kaikkia palvelinkäyttöjärjestelmiä, kuten Windows Serverit ja Linux-jakelut. Myös käyttäjien tietokoneille olevat Linuxit lasketaan palvelimiksi, vaikka ne olisivat työpöytäkäytössä.

Sophos

Sophoksen tietoturvapalvelu koostuu useista erillisistä pienistä komponenteista. Sophos-käyttäjän tietoturvapaketti sisältää seuraavat Sophoksen komponentit:

- Central Intercept X Endpoint Advanced (Tietokoneiden tietoturva)
- Central Intercept X for Mobile (Mobiililaitteiden tietoturva)
- Central Device Encryption (Tietokoneiden keskitetty salaushallinta)

Komponentit ovat myös erikseen tilattavissa, mutta uskomme, että tietoturvan on oltava kokonaisvaltaista ja katettava kaikki työssä käytettävät laitteet, jotta tietoturvatuotteista on oikeasti hyötyä.

Lisäksi käyttäjille on saatavilla *Central Mobile Advanced*, joka lisää mobiililaitteilla yksityiskohtaisempaa hallintaa pelkän haittaohjelmasuojauksen lisäksi. Central Mobile Advancedia voi käyttää esimerkiksi rajoittamaan mobiililaitteille asennettavia softia ja se mahdollistaa mobiililaitteiden käyttöönoton automaattisesti.

Palvelinlaitteille on myynnissä yksinkertaisuudessaan yksi komponentti *Central Intercept X Advanced for Server*. Palvelu tukee yleisimpiä Linux-ympäristöjä sekä kaikkia Microsoftin tukemia Windows Server -jakeluja. Lisämaksusta on saatavilla myös tuki Windows Servereille aina versioon 2008 asti. Tarkemmat ja

kattavat tuotetiedot mainituista komponenteista kannattaa lukea suoraan valmistajan sivuilta. Myös muut sivuilta löytyvät tuotteet ovat saatavilla TNNetin kautta, mutta tässä palvelukuvauksessa on listattu vain mielestämme tärkeimmät tietoturvaa parantavat tuotteet.

Miten palvelu toimii

Huolehdimme siitä, että jokaisella asiakkaalla on tietoturvalliset politiikat, joita ylläpidämme säännöllisesti. Kun tuotteisiin tulee uusia ominaisuuksia, huolehdimme siitä, että ne tulevat käyttöön sellaisille laitteille, jotka ovat TNNetin määrittämien politiikkojen piirissä.

Asiakkaan ylläpitäjien on mahdollista tehdä TNNetin määrittämistä politiikoista klooneja, joihin voidaan asettaa yrityskohtaisia erityissääntöjä. Erityissäännöt voidaan erillispyynnöstä tehdä myös meidän toimestamme, mutta erityispolitiikkojen ylläpitäminen on aina asiakkaan vastuulla. TNNet vastaa siis vain omien politiikkojensa ajantasaisuudesta.

Asiakkaan ylläpitäjillä on mahdollisuus käyttää itsepalveluportaalia kokonaisvaltaisesti lisenssien ja laitteiden hallintaan. Ongelmatilanteissa TNNetin tuki on aina saatavilla. Ratkaisemme useimmat ongelmat suoraan itse, mutta mikäli ongelma on laadultaan sellainen, että tarvitaan valmistajan tukea (esimerkiksi bugi sovelluksessa), hoidamme asioinnin veloituksetta Sophoksen suuntaan. Olemme myös Sophoksen platinakumppani, joka mahdollistaa asiakkaillemme ohituskaistan suoraan kakkostason tuelle.

Jos palvelussa havaitaan tietoturvauhka, ohjelmistot luonnollisesti pyrkivät poistamaan uhan automaattisesti ja jättävät siitä ilmoituksen asiakkaan ylläpitäjälle sekä Sophoksen portaaliin. Ilmoitusten huomaaminen ja niihin reagoiminen on kuitenkin asiakkaan vastuulla. TNNet auttaa erillisellä työpyynnöllä myös laitteiden jälkitarkastuksessa ja ilmoitusten tulkitsemisessa, mikäli niihin tarvitaan apua. Tietoturvauhkien löytäminen, havaitseminen ja reagointi on mahdollista ulkoistaa. TNNetillä on siihen erikseen oma palvelunsa (SOC), joka on kuvattu myöhemmin tässä palvelukuvauksessa.

Lisensointi

Kaikki Sophoksen käyttäjälisenssit laskutetaan käyttäjämäärän mukaan, jolloin käyttäjän laitemäärällä ei ole vaikutusta. Käyttäjällä tarkoitetaan oikeaa henkilöä, ei pelkkää käyttäjätunnusta. Sophoksen järjestelmä pyrkii erottelemaan käyttäjät laitteelle kirjautuneen käyttäjätunnuksen perusteella. Esimerkiksi jos käyttäjä kirjautuu laitteilleen kaksilla eri tunnuksilla, oletuksena tästä tulee kahden lisenssin kulu. Tunnukset voidaan kuitenkin liittää yhteen henkilöön joko ylläpitäjän toimesta (asiakas tai TNNet), jolloin lisenssejä kuluukin vain yksi. Liitoksen tekeminen tai sen tarpeen ilmoittaminen TNNetille on aina asiakkaan vastuulla. Käyttäjällä voi siis olla esimerkiksi Windows PC, Mac, puhelin ja tabletti, joista kertyy yhteensä yhden lisenssin kulu, jos laitteet on asetettu yhden käyttäjän alle.

TNNetin laskutusperuste on aina Sophoksen pilven raportoima lisenssimäärä. Kun lisensoitavia kohteita lisätään, lisenssimäärä päivittyy automaattisesti Sophoksen järjestelmään. Vastaavasti jos lisensoitava kohde on poistunut (esimerkiksi virtuaaliserveri poistetaan), kohde poistuu automaattisesti lisensoinnista, kun laite on ollut 30 vuorokautta offline-tilassa Sophoksen pilven suuntaan.

Sophoksen palvelussa data säilytetään Sophoksen pilvessä Euroopan rajojen sisällä. Tarkemmat spesifikaatiot datan regulaatiosta voi lukea Sophoksen sivuilta.

Symantec

Symantec käyttää samaa tuotetta kaikissa suojattavissa laitteissa riippumatta siitä onko kyseessä mobiililaite, tietokone vai palvelin. Symantecin tietoturvatuotteet ovat integroitavissa Symantecin muihin tuotteisiin (*ZTNA (Zero Trust Network Access)*, *Secure Web Gateway (SWG)* ja *SOC (MDR)*) tuoden mainittuihin palveluihin lisäominaisuuksia.

Symantecin laitteiden tietoturva on täysiverinen EDR-tuote (Endpoint Detection and Response), jota voidaan hallita keskitetysti pilvestä. Pilvi on Symantecin ylläpitämä ja sijaitsee fyysisesti Euroopassa. Datan

sijainnista ja käsittelystä voi lukea tarkemmin Symantecin sivuilta. Asiakas saa aina myös itselleen ylläpitotunnukset Symantecin pilveen, josta voi tarkastella laitteiden tietoturvan tasoa ja muokata tietoturvapolitiikkoja. EDR:stä saa parhaan hyödyn irti, kun kyberturvallisuuden asiantuntija käyttää sitä aktiivisesti. Tästä johtuen SOC-palvelu on erittäin suositeltava lisäpalvelu Symantecin turvan kanssa.

Vaihtoehtoina on ottaa Symantecin Endpoint Security (SES) tai Endpoint Security Complete (SESC). Suosittelemme SES-tuotetta mobiililaitteille, ja SESC-tuotetta muille laitteille, sillä suurin osa SESC:n mukana tulevista lisäominaisuuksista ei ole tuettuna mobiililaitteilla.

Miten palvelu toimii

Asiakkaan ylläpitäjien on mahdollista tehdä TNNetin esimäärittämiin politiikkoihin muutoksia. Muutokset voidaan erillispyynnöstä tehdä myös toimestamme, mutta pyydettyjen erityispolitiikkojen tietoturvallisuus on aina asiakkaan vastuulla. TNNet vastaa siis vain omien politiikkojensa tietoturvallisuudesta.

Asiakkaan ylläpitäjillä on mahdollisuus käyttää itsepalveluportaalia kokonaisvaltaisesti lisenssien ja laitteiden hallintaan. Ongelmatilanteissa TNNetin tuki on aina saatavilla. Ratkaisemme useimmat ongelmat suoraan itse, mutta mikäli ongelma on laadultaan sellainen, että tarvitaan valmistajan tukea (esimerkiksi bugi sovelluksessa), hoidamme asioinnin veloituksetta Symantecin suuntaan.

Jos palvelussa havaitaan tietoturvauhka, ohjelmistot luonnollisesti pyrkivät poistamaan uhan automaattisesti ja jättävät siitä vain ilmoituksen asiakkaan ylläpitäjälle ja Symantecin portaaliin. Ilmoitusten huomaaminen ja niihin reagoiminen on kuitenkin asiakkaan vastuulla. TNNet auttaa erillisille työpyynnöllä myös laitteiden jälkitarkastuksessa ja ilmoitusten tulkitsemisessa, mikäli niihin tarvitaan apua. Tietoturvauhkien löytäminen, havaitseminen ja reagointi on mahdollista ulkoistaa. TNNetillä on siihen erikseen oma palvelunsa *SOC (MDR)*, joka on kuvattu myöhemmin tässä palvelukuvauksessa.

Lisensointi

Tuotteet lisensoidaan aina per laite. Laite voi olla esimerkiksi mobiililaite, tietokone tai serveri. Mobiililaitteet eivät tue aivan kaikkia samoja tietoturvaominaisuuksia kuin muut laitteet, joten mobiililaitteille on suotavaa ottaa heikompi paketti. Lisenssit ovat voimassa kuukauden kerrallaan, joten lisenssimäärä on hyvin joustava laitemäärän muuttuessa.

SOC (MDR)

Tuotamme SOC-palvelua 24/7 yhdessä Sophoksen kanssa. Sophoksen kyberasiantuntijat valvovat yhteistyössä ympäristöä seitsemällä eri aikavyöhykkeellä niin, että 24/7 valvonta toteutuu vuoden jokaisena päivänä virkeiden työntekijöiden toimesta. Ellei toisin sovita, toimii SOC-palvelu niin, että hälytyksen tultaessa SOC-tiimi tekee ensimmäisen arvion tilanteesta, jonka jälkeen he ovat yhteydessä TNNetiin. Jos tilanne vaatii välittömiä toimia, eikä SOC-tiimi saa TNNetin työntekijöitä kiinni, yrittää SOC-tiimi vielä mahdollisuuksien mukaan soittaa suoraan loppuasiakkaalle, ja viimeisenä vaihtoehtona tiimi voi itse tehdä tarvittavat toimenpiteet ympäristössä. Huomionarvoista on kuitenkin se, että TNNetillä on 24/7 vikapäivystys, josta saa aina jonkun kiinni. Kun SOC-tiimi on saanut kontaktin TNNetiin, teemme tarvittavat toimenpiteet parhaalla katsomallamme tavalla joko loppuasiakkaan kanssa yhteistyössä tai kriittisessä tilanteessa omatoimisesti. Edellä kuvattu toimintatapaa on mahdollista myös muokata asiakkaan tahtomalla tavalla: on mahdollista antaa SOC-tiimille suoraan lupa toimia parhaalla katsomallaan tavalla tai antaa ehdoton kielto, että he eivät missään tilanteessa saa tehdä muutoksia ympäristöön. **Hälytyksen vastaanottaminen ja kyberuhan torjuminen sisältyvät palvelun hintaan, joten tästä ei tule asiakkaalle lisäkustannuksia missään tilanteessa.**

SOC-tiimillä on oma SLT (Service Level Target), joka tarkoittaa sitä, että tavoitteena on muodostaa ensimmäinen hyökkäystä torjuva toimenpide 30 minuutin sisään ensimmäisestä hälyttävästä havainnosta. Tähän aikaan siis sisältyy jo havainnon analysointi ja korjaustoimenpiteiden suunnittelu. Historiallisesti SOC-palvelussa kyberhyökkäykset on torjuttu 38 minuutissa ensimmäisestä havainnosta koko casen sulkemiseen asti.

SOC-tiimiä on saatavilla kahdella eri tasolla, essentials ja complete. Complete vaatii, että organisaatiossa on käytössä Sophoksen EDR -tuotteet, jolloin saamme organisaatioon paremman näkyvyyden sekä hallinnan ja sitä kautta myös varmistettua paremmin tietoturvan tason. Jos käytössä on muita valmistajia, kuten esimerkiksi Symantecin tai Microsoftin EDR-tuotteet, voidaan ne tästä huolimatta ottaa SOC:n piiriin, mutta vain essentials -tasolla. SOC:iin on integroitavissa myös muita palveluita kuin pelkät EDR-tuotteet. Esimerkiksi monen valmistajan palomuurilaitteet ovat saatavissa SOC:in pariin.

SOC-palvelussa dataa säilytetään 90 vuorokautta ilman lisäkuluja, mutta palveluun on mahdollista ottaa lisäpalveluna pidennetty datan säilytysaika (yksi vuosi).

Essential ja Completen väliset erot ovat listattuna alla olevassa taulukossa. Erot johtuvat pääosin siitä, että ilman Sophoksen omia tietoturvasovelluksia SOC -iimillä ei ole täyttä hallintaa ja näkyvyyttä organisaation ympäristöön, jolloin aivan kaikkia ominaisuuksia ei myöskään pystytä lupaamaan. Tarkka kuvaus SOC-tiimin toiminnasta, datan sijainnista ja vastuista on luettavissa Sophoksen sivuilta. Koko organisaation on aina oltava samalla SOC-tasolla, eli ei ole mahdollista sekoittaa organisaation sisällä Essentials ja Complete -tasoja.

	Essentials	**Complete**
24/7 SOC-ammattilaisten monitorointi ja hälytyksiin reagointi	X	X
Integraatio muiden valmistajien tuotteisiin	X	X
Viikko- ja kuukausiraportointi tapahtumista	X	X
Kyberammattilaisten tekemä haavoittuvuuksien etsintä	X	X
Uhkien hallinta, hyökkäykset pysäytetään ja leviäminen estetään	X	X
Täydellinen uhan poistaminen, haittaohjelma poistetaan varmasti ympäristöstä		X
Juurisyyanalyysi (RCA)		X
1 000 000 € tietoturvatakuu (esim. ransomware-maksu, mainehaitta, lakikulut)		X

SOC-tiimin lisensointi on perustyypiltään käyttäjä- ja serverikohtainen. Muut ulkopuoliset integraatiot hinnoitellaan pääsääntöisesti myös sekä käyttäjä- että serverikohtaisesti, mutta integraatiokohtaisia eroavaisuuksia voi olla. Lisenssit ovat oletuksena kuukausilisenssejä, eli yhden kalenterikuukauden irtisanomisajalla ilman sitoutumista minimi- tai enimmäismäärään lisenssejä. Lisenssejä on kuitenkin mahdollista hankkia myös määräaikaisina (12,24 tai 36kk), jolloin on sitouduttava myös tiettyyn lisenssien lukumäärään. Sophoksen palomuuriin sisältyy SOC aina, kun palomuurilla on Xstream-tason lisenssi. Myös M365-ympäristö on integroitavissa lisämaksutta SOC:in piiriin, jos käyttäjillä on jo muun tuotteen kautta SOC-lisensointi.

Sähköpostin tietoturva

Yli 90% hyökkäyksistä organisaatioita vastaan alkaa haitallisesta sähköpostista, ja 75% kiristyshaittaohjelmahyökkäyksistä (ransomware) tulee sähköpostin kautta organisaation sisään. Koska sähköpostihyökkäykset yleensä liittyvät ihmistekijään, eli ihmisen tekemään virheeseen, Microsoft 365 ja Google Workspace -ympäristöt ovat organisaatioiden heikoin lenkki. Onnistuneet phishing- ja ransomwarehyökkäykset voivat aiheuttaa merkittävää taloudellista vahinkoa. Tämän tietoturva-aukon sulkeminen vaatii suojausta montaa eri uhkaa vastaan: tietojenkalastelua, haittaohjelmia sekä datan ja tunnusten varastamista.

Toteutamme sähköpostin tietoturvaa sekä Checkpointin että Symantecin tuotteilla hieman asiakastarpeen mukaisesti. Molemmissa tapauksissa data sijaitsee valmistajan pilvessä, joka on Euroopassa. Palvelukuvauksen toimintaperiaatteet ovat molemmilla valmistajilla samat myös teknisten vaatimusten osalta.

Tekninen kuvaus

Sähköpostin tietoturva toimii API-rajapinnalla sähköpostitarjoajan (Google tai M365) ja sähköpostiturvan välillä. Kun sähköposti menee sähköpostipalvelimelle, sähköpostiturva ”kaappaa” viestin välistä omaan palveluunsa, jossa viestin tietoturva tutkitaan läpi. Viestistä voidaan AI:ta hyödyntäen tulkita esimerkiksi käytettyä kieltä (näyttääkö huijausviestiltä), skannata liitetiedostot virusten tai haitallisen ohjelmien varalta sekä tarkastella muita sähköpostiin liittyviä teknisiä parametrejä, kuten SPF ja DKIM -tietueiden oikeellisuus.

Järjestelmän käyttöönotto vaatii Microsoftilla Global Admin -rooliin kuuluvan tilin, jonka jälkeen tilin oikeudet voidaan rajata Exchange-adminiin. Vikatilanteissa kuitenkin Global Adminin olemassaolo voi helpottaa vian löytämistä. Googlen käyttöönotto vaatii integraatiotilille oman Googlen workspace-lisenssin ja Administrator-tason käyttäjän.

Kun sähköpostiturva on tarkistanut viestin, se joko välitetään sellaisenaan alkuperäiseen kohteeseen, tai viestiä voidaan muokata. Sisään tuleville viesteille voidaan laittaa esimerkiksi varoitus käyttäjälle, että viestissä oli jotakin epäilyttävää, mutta se päästettiin kuitenkin läpi. Viesti voidaan myös laittaa sähköpostiturvan karanteeniin, josta ylläpitäjä voi käydä viestin tarkastamassa ja vapauttamassa. Jos viesti on tarpeeksi varmasti haitallinen, se voidaan estää kokonaan. Estetytkin viestit ovat kuitenkin saatavilla jälkikäteen järjestelmästä, ja niiden avulla voidaan järjestelmää kouluttaa kunkin organisaation omiin tarpeisiin.

Lisensointi

Microsoftin sähköposteissa ei tarvitse lisensoida jaettuja ryhmälaatikoita, aliaksia tai muita Microsoftille lisensoimattomia sähköposteja. Nämä ovat kuitenkin saman suojan piirissä kuin normaalitkin käyttäjät. Hyvä nyrkkisääntö on, että jos Microsoft vaatii laatikosta lisenssin, niin lisenssi vaaditaan myös sähköpostiturvaan. Minimilisenssi, jota voidaan suojata, on Exchange Online plan 1. Jos Microsoftilta halutaan suojata ja tarkastella tietoja myös muissa sovelluksissa (Teams, Sharepoint, OneDrive), tulee käyttäjillä olla vähintään Microsoft E5 -lisenssi.

Googlen tapauksessa ryhmälaatikoita ei lisensoida tai suojata, vaan ainoastaan ryhmään kuuluvien jäsenien laatikot suojataan. Jos käyttäjä siis menee suoraan ryhmälaatikkoon lukemaan viestejä, ei viesti ole suojattu. Suojattavilla käyttäjillä tulee olla Googlelta sähköpostia varten mikä tahansa lisenssi, paitsi Essentials tai Business Starter. Google Driven suojaaminen vaatii vähintään Googlen Business Standard -lisenssin.

Molemmissa sähköpostipalveluissa käyttäjiä on mahdollista suojata myös ryhmä- tai jopa käyttäjäkohtaisesti, jolloin koko organisaation ei tarvitse olla suojattuna. Kannattaa kuitenkin aina muistaa, että tietomurtoon riittää yksikin suojaamaton laatikko, jos hyökkääjä onnistuu lähettämään suojaamattomalle henkilölle haittaohjelman.

Tietoturvakoulutus ja hyökkäyssimulaatio

Suurin osa kyberhyökkäyksistä saa alkunsa loppukäyttäjän tekemästä virheestä. Virheitä voidaan yrittää paikata erilaisilla teknologiaratkaisuilla, mutta varmin keino välttyä kyberhyökkäykseltä on kouluttaa käyttäjiä. Teknologiset ratkaisut ja koulutus eivät kuitenkaan ole toisiaan poissulkevat vaihtoehdot, vaan toisiaan erittäin hyvin tukevia. Mitä jos käyttäjä tekee koulutuksesta huolimatta virheen, tai mitä jos teknologiaratkaisu kohtaakin entuudestaan tuntemattoman hyökkäyksen eikä osaa torjua sitä?

Keskimäärin 18% haitallisista sähköposteista tulee klikatuksi, eli käytännössä joka viides työntekijä klikkaa huijaussähköpostissa olevia linkkejä. Vain kolmen kuukauden palvelun käytön jälkeen tämä prosentti saadaan laskettua alle kahteen. Vastaavasti jos palvelun käyttö lopetetaan, paluu alkuperäisen 18% lukemaan tapahtuu noin parissa kuukaudessa, eli jatkuva ja säännöllinen koulutus on äärimmäisen tärkeää.

Miten palvelu toimii

Toteutamme loppukäyttäjiin kohdistuvia hyökkäyssimulaatioita, eli huijaussähköpostikampanjoita, sekä käyttäjien mikrokoulutuksia tietoturvaan liittyen Nimblr:n järjestelmää hyödyntäen. Järjestelmä on monikielinen, mutta esimerkiksi Suomi, Ruotsi ja Englanti ovat täysin tuettuja kieliä.

Palvelussa organisaation käyttäjille lähetetään siis kalasteluviestejä, jotka ovat AI:n kustomoimia hyödyntäen esimerkiksi loppukäyttäjän titteliä tai organisaation toimialaa. Näin hyökkäykset ovat realistisia ja verrattavissa jokapäiväisiin kalasteluviesteihin. Viestejä lähetetään säännöllisen epäsäännöllisesti, jotta käyttäjä ei voisi ajankohdasta päätellä, onko viesti aito vai tämän palvelun viesti.

Hyökkäyssimulaation lisäksi käyttäjälle luodaan muutaman minuutin mittaisia mikrokoulutuksia tietoturvaan liittyen. Koulutukset ovat kokonaisvaltaisesti tietoturvaan liittyviä, eli kyseessä ei ole pelkästään huijaussähköpostien tunnistamista, vaan myös ihan perinteistä fyysistä tietoturvaa, haittaohjelmia, webin käyttöä ja ajankohtaisia pinnalla olevia kyberuhkia. Koulutusten aiheet muokkautuvat organisaatio- ja käyttäjäkohtaisesti sen mukaan, kuinka ihmiset katsovat koulutuksia ja toimivat hyökkäyssimulaatioissa.

Jos käyttäjät eivät syystä tai toisesta tee heille määrättyjä koulutuksia, käyttäjille menee kerran viikossa muistutusviesti koulutuksesta. Lisäksi organisaation pääkäyttäjä pääsee portaalista näkemään, miten käyttäjät ovat käyneet koulutuksia ja suoriutuneet hyökkäyssimulaatioista.

Palvelu sisältää TNNetin toimesta palvelun käyttöönoton yhdessä asiakkaan kanssa ja asiakkaan pääkäyttäjän koulutuksen portaaliin sekä tuen mahdollisissa ongelmatilanteissa. Käyttöönotossa tyypillisesti pitää sähköpostipalveluntarjoajalle sallia Nimblr:n käyttämät IP-osoitteet, jotta viestit eivät mene roskapostiin. TNNet voi tehdä tämän, jos tarvittavat oikeudet omaava käyttäjätunnus on saatavilla. Käytännössä palvelu ei vaadi asiakkaan pääkäyttäjältä käyttöönoton jälkeen toimenpiteitä, vaan oikein käyttöönotettuna palvelu havaitsee itse uudet ja poistuneet työntekijät tarpeen mukaan.

Kaikki palvelun data on Nimblr:n konesalissa (Hetzner), joka sijaitsee Euroopassa.

Lisensointi

Palvelu lisensoidaan käyttäjäkohtaisesti. Käyttäjät voidaan määritellä erikseen, ja kaikkia organisaation käyttäjiä ei tarvitse lisensoida. Palvelu on aluksi vuoden määräaikainen, ja jatkuu sen jälkeen toistaiseksi voimassa olevana yhden kalenterikuukauden irtisanomisajalla, ellei toisin ole sovittu asiakaskohtaisessa sopimuksessa.

DDoS-suojaus

TNNetin verkkoyhteyksiä hyödyntäviin palveluihin on mahdollista ostaa lisäpalveluna DDoS-suojauspalvelu. Palvelu vaatii toimiakseen TNNetin IP-osoitteen, eli käytännössä palvelulla voidaan suojata palvelinympäristöjä, palomuureja ja nettiliittymiä. Kaikissa Hosting-tuotteissa palvelu on oletuksena päällä.

Palvelu toteutetaan Arborin Sightline with Sentinel -tuotteella, johon myös asiakkaalle on mahdollista antaa oma pääsy joko hallinta- tai raportointiportaaliin. Hallintaportaalista on mahdollista jopa itse suorittaa hyökkäyksen torjuntatoimenpiteitä, jos niin haluaa. Raportointiportaalista on mahdollista koostaa itselleen kattavia raportteja verkon liikenteestä niin normaali- kuin poikkeustilanteissakin. Portaalinäkymä vaatii, että suojattavat IP-osoitteet ovat omasta verkkoblokista eikä jaetusta IP-verkosta. Näin ollen esimerkiksi tavallisella julkisella IP-osoitteella olevaa Openstack-virtuaalipalvelinta ei voida näyttää raportoinnin puolelta. Jaetuissa IP-verkoissa olevat palvelutkin voidaan kuitenkin suojata DDoS-suojauspalvelulla, mutta ilman portaalinäkymää.

DDoS-suojaus toimii BGP Flowspec-teknologialla siten, että Sentinel pyrkii tunnistamaan DDoS-hyökkäyksiä erilaisilla parametreilla kuten liikenteenmäärä, tunnetusti haitalliset lähdeosoitteet ja liikenneprofiili. Tämän jälkeen BGP Flowspeciä hyödyntäen voidaan TNNetin reitittimille kertoa, että liikennettä ei vastaanoteta TNNetin reunalta sisään kohdistuen suojattuun palveluun. Sentinel on maailman johtava tuote hyökkäysten tunnistamisessa, mutta se ei kuitenkaan takaa kaikkien hyökkäyksien havaitsemista. Mikäli asiakas kokee hyökkyäksen, jota Sentinel ei tunnista, voidaan vastaavat torjuntatoimenpiteet tehdä asiantuntijan analyysin perusteella joko asiakkaan itsensä toimesta hallintaportaalista tai asiantuntijoidemme avulla.

Kun TNNet havaitsee hyökkäyksen, hyökkäys pestään ensi tilassa pois, jotta mahdollinen häiriö palveluille loppuu. Hyökkäyksen loppumisen jälkeen, tai tarvittaessa jo hyökkäyksen aikana, asiakasta raportoidaan tapahtumien kulusta. Jos hyökkäys kohdistuu sellaiseen palveluun, joka ei ole suojauksen piirissä, ja hyökkäys haittaa TNNetin muiden asiakkaiden palveluita, laitamme kaiken palveluun kohdistuvan liikenteen mustaan aukkoon. Tämä tarkoittaa sitä, että hyökkäys käytännössä loppuu, mutta palveluun ei myöskään pääse ulkopuolelta edes luvallinen liikenne. Hyökkääjä on siis saavuttanut tavoitteensa. Jos hyökkäys on niin pieni, että TNNetin muut palvelut eivät siitä koe haittaa, ei hyökkäykselle tehdä mitään.

Jos halutaan suojata yksittäinen laite, joka on sellaisen palomuurin takana, jonka takana on myös muita laitteita, tulee suojata koko palomuuri ja kaikki sen takana olevat laitteet. Jos näin ei toimittaisi, voisi suojattavan palvelun kaataa hyökkäämällä vierekkäiseen palveluun, joka sivuvaikutuksena kaataisi myös palomuurin. Sama analogia pätee myös muissa palveluissa, joissa suojattava palvelu on riippuvainen muista palveluista.

Verkkoskannaus

Verkkoskannauspalvelussa TNNet skannaa julkiverkkoon näkyviä IP-osoitteita pyrkien löytämään tunnettuja haavoittuvuuksia ja liian avoimia palomuurin sallintasääntöjä. Tyypillisesti mikään ei ole yhtä pysyvää, kuin hetkellinen muutos. Hetkellinen muutos voi olla esimerkiksi huoltotoimenpiteen vuoksi avattu pääsy palomuurille tai testimielessä asennettu lisäosa kotisivuille. Skannauspalvelua voi yksinkertaisuudessaan hyödyntää siihen, että säännöllisesti testaa, onko palomuurin rajaukset sellaisessa kunnossa kuin on kuvitellut niiden olevan tai onko verkkosivujen kaikki komponentit päivitetty haavoittuvaisista versioista uusimmaksi.

Palvelussa skannaamme turvallisesti erikseen määritetyt palvelut siten, että skannauksesta ei koidu muuta haittaa skannattavalle ympäristölle. Liian aggressiivinen testaus voisi aiheuttaa esimerkiksi palvelunestohyökkäyksen kaltaisen tilanteen skannattavaan ympäristöön. Skannaukset voidaan tehdä aina täsmällisesti sovittuun aikaan, jolloin skannattavassa ympäristössä on mahdollista valmistautua skannaukseen. Asiakkaan on myös hyvä ilmoittaa omalle palveluntarjoajalleen skannauspalvelun käyttöönotosta, mikäli palveluntarjoaja on joku muu kuin TNNet, sillä palveluntarjoajalla saattaa olla omia sääntöjä verkkoskannauksen osalta.

Asiakas saa jokaisesta skannauksesta yksityiskohtaisen raportin löydetyistä laitteista, avoimista porteista ja niistä löydetyistä haavoittuvuuksista. Raportin lukeminen on aina asiakkaan vastuulla, mutta erillisestä lisäpyynnöstä on mahdollista pyytää apua raportin tulkintaan ja havaintojen korjaamiseen asiantuntijoiltamme.

Skannaus suoritetaan Tenablen Nessus -työkalua hyödyntäen, mutta palvelu on toimintaperiaatteeltaan on-premin tapainen, eli kaikki skannaukset ja datan säilöntä tapahtuvat TNNetin ylläpitämällä laitteistolla.

Lisensointi

Palvelu lisensoidaan asset-määrän mukaan. Assetilla tarkoitetaan joko verkkosivua (FQDN) tai IP-osoitetta. Jos verkkosivu sijaitsee samassa IP-osoitteessa kuin mikä on jo määriteltynä asseteihin, lisensoidaan kaksi assetia. Jos skanneriin määritetään esimerkiksi kokonainen IP-verkko, niin asseteiksi lasketaan koko verkon koko (/28 maskilla laskutetaan 16 assetia).

ZTNA (Zero Trust Network Access)

ZTNA ei ole yksittäinen teknologia, vaan tapa toimia. ZTNA:lla tarkoitetaan yleisesti sitä, että verkkoon päästääkseen käyttäjän tulee olla teknologisesti tunnistettu, käyttäjällä on mahdollisimman vähän pääsyjä ja käyttäjän mahdolliset oikeudet tehdä muutoksia ovat mahdollisimman vähäiset. Tämän lisäksi edellä mainittuja ehtoja tarkkaillaan jatkuvasti, ja mikäli tilanne muuttuu, voidaan pääsy estää. Tuotamme ZTNA palvelua Symantecin ZTNA-tuotteella, jonka data sijaitsee Symantecin palvelimilla Googlen eurooppalaisissa konesaleissa.

ZTNA toimii teknisesti siten, että muurin taakse asennetaan ZTNA-connectori, joka soittaa HTTPS-yhteyden ZTNA-pilveen. Vastaavasti käyttäjä ottaa HTTPS-yhteyden ZTNA-pilveen, jossa nämä yhteydet yhdistetään. Yhteyttä monitoroidaan koko ajan ja se voidaan katkaista heti, kun käyttäjä lopettaa applikaation käytön tai tietoturva sitä vaatii. Jokaisesta ZTNA:n läpi kulkevasta liikenteestä jää kattavat lokitiedot talteen, jotta jälkikäteenkin on mahdollista tarkastella, kuka on käyttänyt sovelluksia miten ja milloin. Havainnollistava kuvaus toiminnasta on kappaleen lopussa olevassa kuvassa.

ZTNA portaali tukee käytännössä kaikkia TCP protokollia, jos käyttäjällä on asennettuna Symantecin agentti, joka mahdollistaa esimerkiksi tietokantayhteydet konesaliin erillisillä ohjelmistoilla. Jos käyttäjän ei ole

mahdollista asentaa Symantecin agenttia koneelleen, ZTNA tukee selaimen kautta käytettäväksi seuraavia applikaatioita:

- Web-applikaatio (HTTP ja HTTPS, TCP -porttia voidaan muuttaa)
- SSH-applikaatio tai SSH-gateway (Porttia voidaan muuttaa, salasana ja avainkirjautuminen)
- RDP-applikaatio (Porttia voidaan muuttaa)

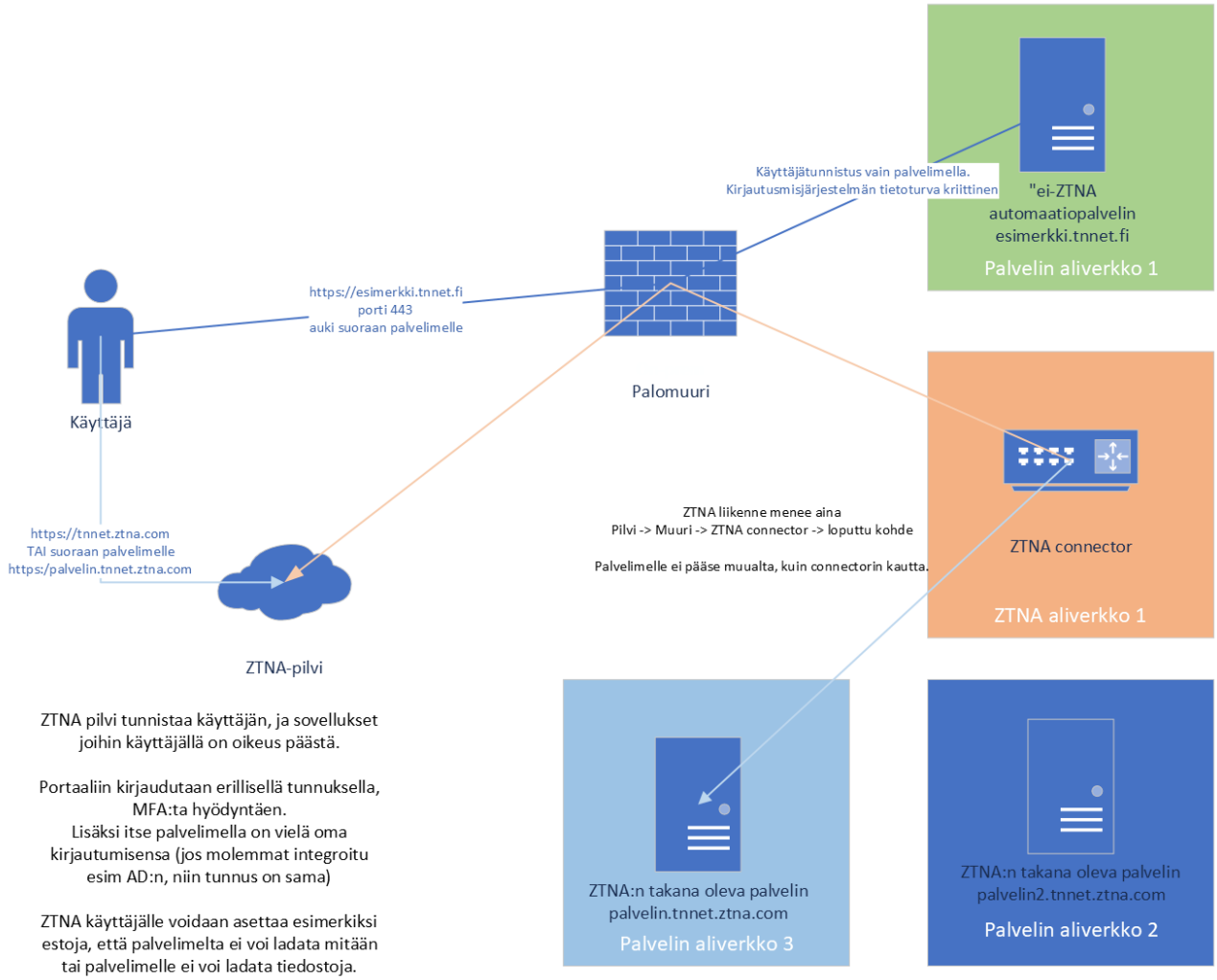
ZTNA palveluun on mahdollista määrittää sovelluksille lisävaateita tietoturvan osalta. Esimerkkejä tällaisista rajoituksista:

- Mistä lähdeosoitteesta yhteydet sallitaan.
- Mistä GeoIP:stä yhteydet sallitaan, esimerkiksi vain Suomesta, vain Euroopasta, kaikkialta paitsi Aasiasta.
- Pitääkö käyttäjällä olla MFA päällä ZTNA-pilveen.
- Mihin vuorokauden aikaan palvelua voi käyttää.
- Onko laitteen tietoturva halutulla tasolla (vaatii Symantecin laiteturvan, kts. Kappale *Symantec*)

Lisäksi on saatavilla applikaatiokohtaisia erityissääntöjä, esimerkiksi Web-applikaatiolle voidaan määrittää, voiko palveluun tehdä ainoastaan GET -requesteja, vai sallitaanko esim POST ja PUT -requestit, jolloin voitaisiin estää palveluun tiedostojen lataaminen tai palvelusta tiedostojen lataaminen. SSH-applikaatiossa taas voidaan estää tiettyjen käyttäjänimien käyttäminen kokonaan.

Asiakkaalla on mahdollisuus saada ZTNA-portaaliin omat ylläpitäjätunnukset, joilla portaalia pystyy hallinnoimaan täysin itsenäisesti. Palveluun sisältyy TNNetin toimesta palvelun käyttöönotto ja tapauskohtaisesti sovittujen asetusten ja politiikkojen määrittäminen yhdessä asiakkaan kanssa. Portaali on varsin yksinkertainen, joten käyttöönoton jälkeen itsenäinen ylläpito on helppoa, jos muutoksia tarvitsee tulevaisuudessa tehdä. Erillisestä työpyynnöstä voimme myös voi auttaa myöhempien asetusten tekemisessä.

ZTNA palvelun vaatima connectori on ilmainen, mutta vaatii oman Docker-ympäristön, jossa connectoria voidaan ajaa. Connectori on mahdollista ostaa TNNetiltä lisäpalveluna täysin avaimet käteen periaatteella, tai hoitaa sen ylläpito itse. Yksi connectori vaatii virallisen dokumentaation mukaan 4vCPU ja 16GiB RAMia, jolla pystytään palvelemaan noin 70 yhtäaikaista yhteyttä. Kokemuksemme mukaan kuitenkin pienemmälläkin palvelimella palvelu toimii, jos yhteyksiä ei ole yhtäaikaisesti paljoa.



1 Periaatekuva ZTNA:n toiminnasta palomuurin kanssa.

Lisensointi

ZTNA palvelu lisensoidaan käyttäjäkohtaisesti perustuen viimeisen kuukauden aikana olleisiin aktiivisiin käyttäjiin. Lisensointi on luottamuspohjaista, mutta lisenssimääriin tehdään pistotarkastuksia. Asiakas on vastuussa ilmoittaa TNNetille oikeasta lisenssimäärästä, mikäli hankittu lisenssimäärä ei olekaan riittävä. ZTNA lisenssit ovat aina vuoden määräaikaisia ensimmäisestä ostosta alkaen, mutta esimerkiksi 6kk myöhemmin ostetut lisenssit voidaan hankkia vain sopimuskauden viimeiseksi kuudeksi kuukaudeksi. Jos palvelu halutaan lopettaa, se tulee irtisanoa kirjallisesti vähintään 2kk ennen sopimuskauden päättymistä. Muussa tapauksessa, sopimus jatkuu automaattisesti uudella vuoden määräaikaisuudella. TNNetin ylläpitämä connectori voidaan toteuttaa 1kk irtisanomisajalla, mutta on huomioitava, että palvelua ei voi käyttää ilman yhtään olemassa olevaa connectoria.

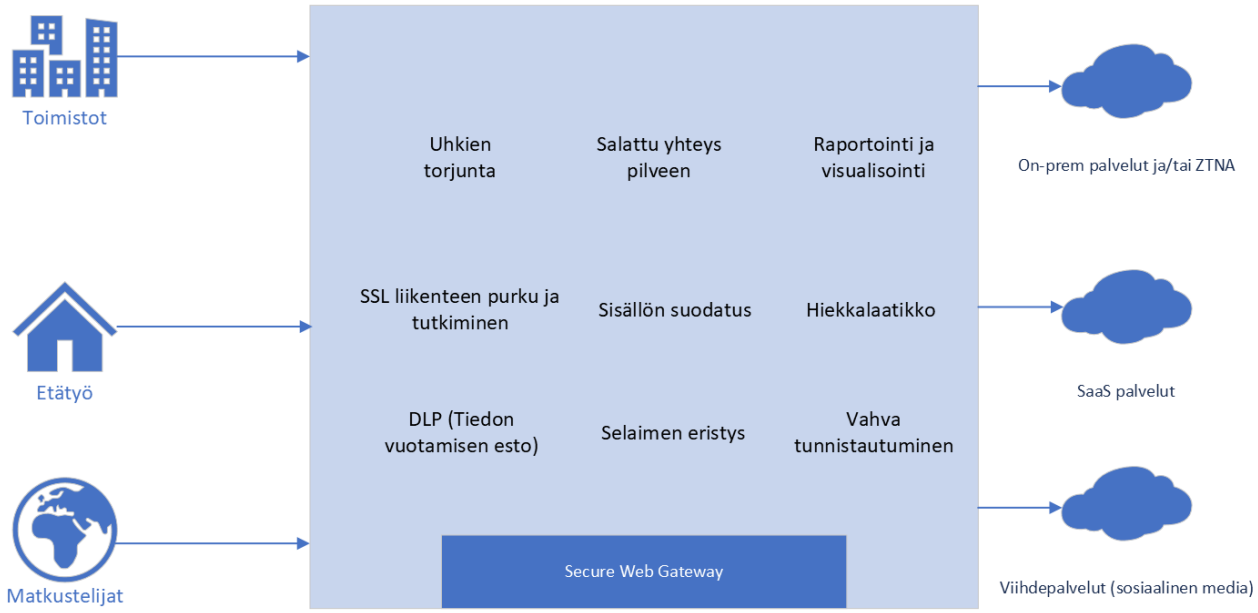
Portaalin käyttäjät on mahdollista integroida useita eri auth-providereita vasten (esimerkiksi Okta, AD, ja EntraID). Kaikkia integroituja käyttäjiä ei tarvitse lisensoida, vaan ainoastaan palvelua käyttäneet, aktiiviset käyttäjät lisensoidaan.

Secure Web Gateway (SWG)

SWG:t toimivat yrityksen työntekijöiden ja Internetin välissä, suodattavat epävarman sisällön verkkoliikenteestä, estävät kyberuhkia ja tietomurtoja, ja estävät riskialttiin tai luvattoman käyttäjäkäyttäytymisen. SWG:tä voisi ajatella eräänlaisena käyttäjäkohtaisena palomuurina, joka toimii pilvessä käyttäjän sijainnista riippumatta.

SWG:t ovat erityisen hyödyllisiä etätyöntekijöiden hallinnassa. Vaatimalla etätyöntekijöitä käyttämään Internetiä turvallisen verkkoyhdyskäytävän kautta, voivat yritykset, jotka luottavat hajautettuun työvoimaan, estää paremmin tietomurtoja. Tämä onnistuu, vaikka heillä ei olisi suoraa hallintaa työntekijöidensä laitteista tai verkoista, tai käyttäjiä ei voida suojata yrityksen omilla palomuurilaitteilla.

Kun asiakaslaitteelta lähetetään pyyntö verkkosivustolle tai sovellukseen Internetissä, pyyntö kulkee ensin SWG:n kautta. Porttina toimiva SWG todentaa käyttäjän ja tarkastelee pyyntöä varmistaen, että se ei riko hyväksyttäviä käyttöpolitiikkoja. SWG sallii pyynnön jatkua vain, jos se on todettu sopivaksi ja turvalliseksi. Havainnollistava kuva tästä toimintaperiaatteesta on tämän kappaleen lopussa.



2 Periaatekuva SWG:n toiminnasta.

Miten tuote toimii

Toteutamme SWG:n Symantecin järjestelmällä. Jos käytetään Cloud SWG:tä, data sijaitsee Symantecin pilvessä Euroopassa sijaitsevissa laitesaleissa. Pilven kautta toteutuvat tietoliikennenopeudet ovat maksimissaan noin 500 Mbps, mutta vaihteluväli on ruuhkan mukaan 100 – 500 Mbps. Jos nämä mainitut nopeudet eivät riitä, on SWG mahdollista toteuttaa myös omilla palvelimilla (Edge Gateway) TNNetin omasta laitesalista. Tarjoamme erillisenä lisäpalveluna myös täysin ylläpidetyn SWG-ympäristön Kanavuoren laitesalista.

Tarkemmat kuvaukset ja kattavammat ominaisuudet kannattaa lukea suoraan Symantecin omilta sivustoilta. Alla vielä listattuna tärkeimmät ominaisuudet, jotka SWG mahdollistaa:

- Uhkien torjunta – Tunnistetaan sivuilta ja ladattavista tiedostoista mahdollisia haittaohjelmia tai muita tietoturvauhkia ja reagoidaan niihin.

- Salattu yhteys pilveen – Käyttäjällä on aina salattu yhteys pilveen.
- SSL liikenteen purku ja tutkiminen – Voidaan purkaa HTTPS liikenteestä salaus, jotta liikenne pystytään tarkistamaan tietoturvauhkien varalta.
- Sisällön suodatus – Tunnistetaan sivustolla näytettävä sisältö ja voidaan asettaa sen mukaisia tietoturvapolitiikkoja.
- Tiedon vuotamisen esto – Nettiin ladattavista tiedostoista pystytään tunnistamaan erilaisia merkintöjä, esim. Salainen tai Julkinen ja niiden mukaan tiedoston lataus voidaan estää.
- Selaimen eristys[1] – Halutut sivut, joko kaikki tai tietyt kriteerit täyttävät, voidaan ajaa todellisuudessa pilvessä ja käyttäjälle näytetään vain ”videokuvaa” sivusta. Näin sivuston tietoturvauhkat eivät vaikuta käyttäjään.
- Hiekkalaatikko[1] – Nettisivuilta ladattavat tiedostot ajetaan ”hiekkalaatikossa” ennen kuin ne päätyvät käyttäjille. Näin voidaan varmistua ladattavien tiedostojen tietoturvallisuudesta.
- Vahva tunnistautuminen – Integroitavissa useaan eri auth-provideriin, MFA mahdollisuus.
- Raportointi ja visualisointi – Kattavat raportit ja muokattavat visuaaliset kuvaajat tietoturvatapahtumista.

Mikäli käytössä on myös Symantecin laitteiden tietoturva, voi sen tuomia tarkistusmahdollisuuksia integroida mukaan SWG:n turvaominaisuuksin. Tietoturva-agentti voi hoitaa myös SWG:n yhdistämisen, jolloin käyttäjältä ei vaadita mitään toimenpiteitä.

1. Vain Core Network Protection bundlen mukana ostetussa SWG:ssä (Sisältää ZTNA:n ja merkatut ominaisuudet).

Lisensointi

SWG palvelu lisensoidaan käyttäjäkohtaisesti perustuen viimeisen kuukauden ajan aktiivisiin käyttäjiin. Lisensointi on luottamuspohjaista, mutta lisenssimääriin tehdään pistotarkastuksia. Asiakkaalla on vastuu ilmoittaa TNNetille oikeasta lisenssimäärästä, mikäli hankittu lisenssimäärä ei olekaan riittävä**. ZTNA lisenssit ovat aina vuoden määräaikaisia** ensimmäisestä ostosta alkaen, mutta esimerkiksi 6kk myöhemmin ostetut lisenssit voidaan hankkia vain sopimuskauden viimeiseksi kuudeksi kuukaudeksi. Jos palvelu halutaan lopettaa, se tulee irtisanoa kirjallisesti vähintään 2kk ennen sopimuskauden päättymistä. Muussa tapauksessa, sopimus jatkuu automaattisesti uudella vuoden määräaikaisuudella. Mahdollisen Edge Gatewayn lisensointi sisältyy käyttäjien lisenssiin, mutta laskentakapasiteetti ja palvelimien ylläpito on hankittava erikseen. Palvelua voi kuitenkin käyttää täysin pilvinatiivina, jolloin ylimääräisiä lisäkuluja ei tule.

Lisätietoja

Lue myös TNNet yleinen palvelukuvaus.

Suosittelemme lukemaan myös muut TNNetin palvelukuvaukset, sillä tietoturvapalvelut ovat liitettävissä käytännössä kaikkiin TNNetin tuottamiin palveluihin.