PROTECTION BUILT FOR YOUR BUDGET AND STAFF:

Yrityksen tietoturvaopas

WatchGuard®

JOHDANTO

Teknologia muuttaa arkemme vääjäämättä. Viimeisimpinä esimerkkeinä pilvipalvelut ja koneoppiminen ovat vaikuttaneet viestintään, yhteydenpitoon ja liiketoimintaan lukemattomilla tavoilla.

Monet yritysten eivät enää tarvitse toimistotiloja, sillä työntekijät ja data ovat yhä useammin muualla kuin toimistossa. Näiden hajautettujen organisaatioiden työntekijät ja toiminnot ovat eri kaupungeissa ja jopa eri maissa, mikä tuo haasteita yritysten IT-tiimeille. Myös liiketoimintaan kohdistuu ennen näkemättömiä haasteita, joita aiemmin käytetyt ratkaisut eivät riitä ratkaisemaan.

Uudet haasteet edellyttävät uutta lähestymistapaa. Tarkastelemme tässä oppaassa lähemmin yrityksien kohtaamia haasteita sekä niihin vastaamista, unohtamatta ketteryyden ja kustannustehokkuuden vaateita.

jopa 60%

suomalaisista työntekijöistä siirtyi koronan rajoittamiseksi etätyöskentelyyn Euroopan kärkimaana.

Eurofound

TIETOTURVALLISUUS

Yritykset näkevät paljon vaivaa ”riittävän hyvän” turvatason varmistamiseksi ja löytääkseen vaihtoehdon sinällään tarpeellisille, mutta liian kalliille tai vaikeasti hallittaville tietoturvakokonaisuuksille.

Uhkien muuttuessa yhä monimutkaisemmiksi, yritykset tarvitsevat ratkaisuja, jotka mahdollistavat seuraavan sukupolven uhkien torjumisen. Tärkeää on huomata, että nämä uhat eivät valikoi kohdettaan koon mukaan.

Monipisteisyyteen ja työntekijöiden liikkuvuuteen liittyy omat turvallisuushaasteensa. Kattava suojaus kaikilla toiminnan alueilla on kriittisen tärkeää tällaisille organisaatiolle. Etätyöskentelyyn ja työntekijöihin liittyy aivan uudenlaisia riskejä, ja hakkerit käyttävät tätä väylää hyväkseen päästääkseen käsiksi varsinaiseen pääkohteeseen.

24%

yrityksistä mainitsi osaamisvajeen yhdeksi kolmesta suurimmista haasteista.

Gartner

RESURSSIT

Osaavan IT-henkilöstön rekrytointi on yhä haasteellisempaa, ja hyvien työntekijöiden säilyttäminen on vieläkin hankalampaa. 21 % keskisuurista yrityksistä kertoo, että suurin IT-toimintojen osaamisvaje liittyy nimenomaan turvallisuuteen.

Hyvistä työntekijöistä kilpaillaan jatkuvasti, sillä osaavista alan työntekijöistä on jatkuva pula. Spiceworkin vuosittain laatiman raportin “State of IT” mukaan 36 % IT-alan ammattilaisista olettaa saavansa palkankorotuksen 2019, ja 26 % suunnittelee vaihtavansa alan työpaikkaa lähivuosina. CIO:n raportin mukaan teknologiasektorilla on miljoona avointa työpaikkaa vuoteen 2020 mennessä, ja yliopistoista valmistuu vuosittain vain 400 000 alan osaajaa, eli noin 60 % teknologiasektorin työpaikoista jää täyttämättä.

BUDJETTI

Pienten ja keskisuurten organisaatioiden haasteet ja riskit ovat usein samankaltaisia kuin suuremmilla yrityksillä, mutta näillä yrityksillä ei ole suuryritysten resursseja. Tosiasiassa 34 % näistä yrityksistä ilmoitti, että budjetti on eräs kolmesta suurimmasta haasteesta 2019.

45 % yli 500 työntekijän yrityksistä odottaa IT-budjetin kasvavan 2019, mutta se ei silti riitä kattamaan kaikkia tarpeita (Spiceworks). Riittävien turvallisuusratkaisujen on sisällettävä kaikki laitteiston päivittämisestä uusien pilvipalvelujen käyttöönottoon, ja entistä suurempi budjetti voidaan myös käyttää usealla eri tavalla.

HAASTEISIIN VASTAAMINEN

Tarkastellaan lähemmin kolmea suurinta haastetta.

HAASTE #1:

ETÄTYÖSKENTELY JA MONIPISTEINEN TOIMINTA

Olipa kyseessä organisaatio, jolla on useita toimipisteitä eri puolilla maata, tai vaikka oppilaitos useine rakennuksineen, on pääpalomuurin ulkopuolelle jäävät kohteet pystyttävä suojaamaan. Tämä voi osoittautua erityisen tärkeäksi, sillä tällaiset kohteet ovat usein hakkereille helpompia hyökkäyksen kohteita ja avaavat väylän varsinaisiin pääkohteisiin.

Suojaus on näin ollen ulotettava laajemmalle – vaikka se vääjäämättä tarkoittaa sekä kustannusten nousua että toteutuksen kompleksisuutta.

Käyttöönottokustannukset

Monipisteisille organisaatioille on ominaista, ettei kaikissa sijaintipaikoissa ei ole omia IT-resursseja. Vaihtoehtoina on rajallisen tiimin käyttäminen eri pisteiden paikan päällä tehtävissä toteutuksissa tai käyttöönoton suorittaminen pääkonttorista käsin, joka tarkoittaa todennäköisesti runsaasti aikaa vievää etäkäyttöönottoa. Kumpikaan näistä tavoista ei ole erityisen kustannustehokas vaihtoehto.

Käyttökustannukset

Monipisteisen yrityksen on varmistettava, että kaikissa sijainneissa voidaan tehokkaasti hyödyntää erityisesti liiketoiminnan kannalta kriittisiä sovelluksia. Myös verkko- ja MPLS-palvelujen kustannukset voivat karata käsistä, joten yritykset tarvitsevat ratkaisuja, jotka pitävät kustannukset kurissa ja varmistavat samalla verkon toimivuuden sijainnista riippumatta.

Kompleksisuus

Hallinnointiin liittyy aina haasteita valitusta toteutusvaihtoehdosta riippumatta. Tietoa tarvitaan siitä, mitä missäkin sijaintipaikassa tapahtuu ja toisaalta tarvitaan kokonaiskuva suojauksen tasosta ja toimivuudesta. Edellyttäkö se kirjautumista jokaiseen sijaintipaikkaan erikseen omalla hallintatyökalulla? Tarvitaanko turvallisuuden perusteellisempaan tarkasteluun erillinen SIEM-toteutus? Kaikki nämä voivat hankaloittaa turvallisuuden hallintaa huomattavasti.

RATKAISU #1:

ETÄKÄYTTÖÖNOTTO JA KESKITETTY HALLINTA

Säästä käyttöönotossa

Mitäpä jos käyttöönotto etäkohteissa onnistuisi suoraan pääkonttorista käsin? **WatchGuard RapidDeployn** avulla kaikkien **Firebox-**palomuurien asetukset voidaan määrittää valmiiksi ja lähettää sitten sinne, missä niitä tarvitaan. Kaikki asetukset ladataan automaattisesti, ja **Firebox** on käyttövalmis, kun laite kytketään sähköverkkoon ja internetiin paikan päällä!

Samoin toimii langattoman verkon **Secure Cloud Wi-Fi** hallintaan. Kirjaudu pilvipalvelun hallinta-alustaan ja määritä tarpeelliset asetukset, kuten langaton verkko, turvallisuus, raportointiaikataulut ja kaikki muu päivittäiseen toimintaan tarvittava. Laite täytyy vain yhdistää verkkoon, ja kaikki asetukset ladataan suoraan laitteelle täsmälleen sellaisina kuin ne alun perin tehtiin.

WatchGuard AuthPoint -monivaihetunnistautuminen hyödyntää mobiilisovelluksesta saatavaa tunnistetta, ja mahdollistaa myös toimipisteiden ulkopuolelta yrityksen verkkoon kirjautumisen turvallisesti ja vaivatta. Työntekijöiden tulee pelkästään ladata mobiilisovellus, vastaanottaa aktivointiviesti ja skannata QR-koodi.

Lisää suorituskykyä

SD-WAN sisältyy kaikkiin Firebox-palomuureihin, eli ylimääräisiä kustannuksia ei tule. Palomuurit mittaavat useiden WAN-vaihtoehtojen tehokkuutta (myös hajonta, viive ja pakettihävikki) ja valitsevat automaattisesti optimaalisen vaihtoehdon sijainnista riippumatta.

Hallitse uhkia

WatchGuard Dimension sisältyy kaikkiin Fireboxeihin ja varmistaa selkeän kuvan saamisen verkon turvallisuusuhista, ongelmista ja trendeistä kaikkialla organisaatiossasi sijainnista riippumatta. WatchGuard Wi-Fi Cloud tarjoaa älykkään kokonaiskuvan uhista ja langattomaan verkkoon kytketyistä laitteista, joten tuttuun kysymykseen ”Miksi verkko ei taaskaan toimi !?” on aina helppo vastata. Myös AuthPoint - on täysin pilvipohjainen; lisenssien jakaminen, hylättyjen varmennuspyyntöjen seuranta sekä SSO-portaalien hallinnointi ja integroinnit sujuvat helposti.

HAASTE #2:

ETÄTYÖSKENTELYN RISKIT

Etätyöntekijöiden suojaaminen voi olla etätyöpisteen turvallisuuden varmistamistakin haasteellisempaa. Etätyötä tekevät ovat harvemmin palomuurin suojassa ja käyttävät usein turvattomia avoimia verkkoja. Etätyöntekijät ovat alttiimpia haittaohjelmahyökkäyksille, jos suojana on ainoastaan työaseman virustorjuntaohjelmisto. Myös virukset voivat levitä yrityksen verkkoon etätyöntekijöiden pistäytyessä toimistolla ja liittäessään työasemansa verkkoon.

Etätyöskentelyn suosion kasvaessa on myös sen turvallisuus varmistettava tavalla, joka on sekä helposti käyttöön otettavissa että kustannustehokas.

Muuta huomioitavaa

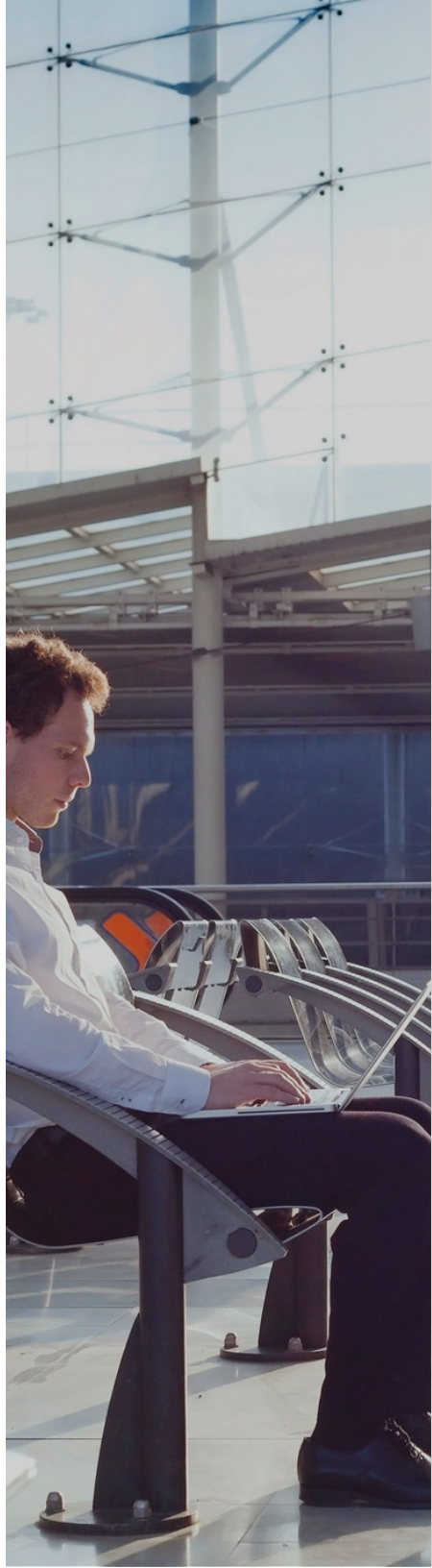
Etätyöntekijöiden suojaaminen voi olla haasteellista myös siksi, että he ovat usein alttiimpia kiristysohjelma- ja tietojenkalasteluhyökkäyksille palomuurin puuttumisen vuoksi.

Usein organisaatiot yrittävät suojata etätyöntekijät VPN:n avulla. VPN voi parantaa turvallisuutta, mutta samalla sen käyttäminen voi olla myös haaste loppukäyttäjälle, sillä yhteys katkeaa usein ja toistuvia uudelleenkäynnistyksiä tarvitaan.

Uusien ratkaisujen käyttöönotto ja turvallisuuskäytäntöjen juurruttaminen voi olla haasteellista etätyöntekijöille. Etätyöntekijät osallistuvat koulutuksiin ja vaikuttavat noudattavan ohjeita, mutta parhaiden turvallisuuskäytäntöjen noudattaminen voi käytännössä olla varsinainen koetinkivi etätyötä tekeville.

Ylimääräiset kustannukset

Kaikkien etätyötä tekevien kustannustenhallinta voi osoittautua hyvinkin haasteelliseksi. Esimerkiksi käyttäjäkohtaisia tunnistevälineitä edellyttävä monivaiheinen todennus voi aiheuttaa merkittäviä kustannuksia. Ratkaisujen on oltava helppokäyttöisiä ja kustannustehokkaita käyttöönoton KAIKISSA vaiheissa



RATKAISU #2:

TURVAA ETÄTYÖSKENTELY

Palomuurin laajennus työasemaan

WatchGuard Total Security Suite suojaa myös etätyöntekijät tehokkaasti ja sisältää myös kiristysohjelmien eston (Host Ransomware Prevention), joka tunnistaa toiminnan ja estää tiedostojen salaamisen käynnistymisen.

Helppokäyttöisyys

Jos turvallisuusratkaisut ovat liian monimutkaisia käyttää tai niistä aiheutuu liikaa ylimääräistä työtä niitä ei todennäköisesti käytetä tai niitä yritetään kiertää. Käytäntöjä voidaan yrittää juurruttaa, mutta aina löytyy joku, joka jättäytyy pois joukosta. WatchGuard ratkaisut on suunniteltu nimenomaan helppokäyttöisyyttä silmällä pitäen. Kaikki palvelumme auttavat suojaamaan työntekijät sijainnista riippumatta VPN-yhteyden ongelmattoman käytön varmistavasta IPSec VPN:stä ja tietojen kalasteluviesteiltä suojaavaan DNSWatchiin, joka kertoo kaiken tarvittavan heti hyökkäyksen ilmetessä.

Kustannustehokkuus

AuthPoint-monivaihetunnistus hyödyntää mobiilisovellusta, joka on helppo ladata suoraan sovelluskaupasta ja ottaa käyttöön skannaamalla QR-koodi. Erillisiä laitteita tai avaimia ei enää tarvita, vaan kaikki toimii helposti työntekijän omalla puhelimella. Näppärä käyttää työntekijöille, ja samalla myös kustannukset pysyvät kurissa!

HAASTE #3:

VAATIMUSTENMUKAISUUDEN VARMISTAMINEN

Vaatimustenmukaisuus on varmistettava toimialasta riippumatta, ja osa näistä säännöksistä vaatii enemmän työtä. Turvallisuusvaatimukset kasvavat ja uusia säännöksiä tuntuu tulevan jatkuvasti. Vaatimustenmukaisuuden varmistaminen on osa työtä, mutta siihen voi kulua myös paljon aikaa.

Vaatimustenmukaisuuden varmistaminen voi lisätä myös kustannuksia ja rasittaa muutenkin rajallista budjettia. Säännösten päivittyessä ja muuttuessa on selvitettävä, miten tarvittavat uudet teknologiat sisällytetään budjettiin, ja miten niiden käyttöönottaminen varmistetaan tekemättä yrityksen tietoteknisestä infrastruktuurista entistäkin monimutkaisempaa.

Kustannukset

Vaatimustenmukaisuuden varmistamiseen on useita vaihtoehtoja. Turvallisuuteen voidaan käyttää siekailematta rahaa vaatimusten mukaisuuden varmistamiseksi tai vaihtoehtoisesti voidaan ottaa riski mittavista sakoista. Kumpikaan näistä ei ole luonnollisesti tavoiteltava vaihtoehto, eivätkä varmasti noudata budjettikuria.

Kompleksisuus

Infrastruktuurin on pysyttävä mukana uusien määräysten seuratessa toisiaan ja nykyisten muuttuessa jatkuvasti. Mitä enemmän ratkaisuja etätyössä tarvitaan, sitä haastavampaa niiden tehokas hallinnointi voi olla.

RATKAISU #3:

VAATIMUSTENMUKAISUUDEN HALLINTA

Vaatimustenmukaisuus

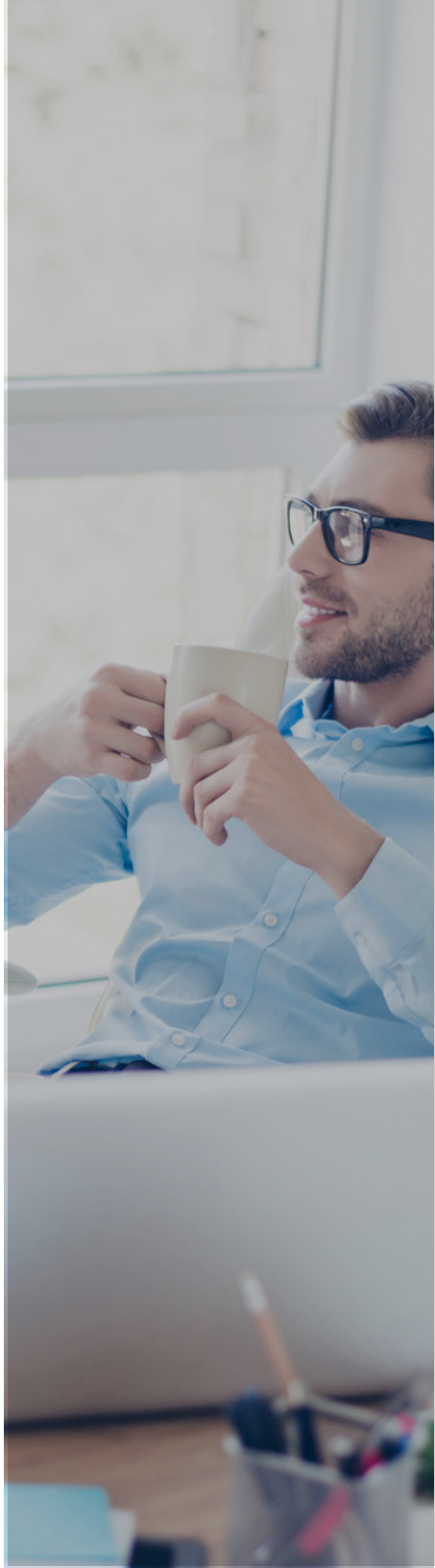
Tarvitaan ratkaisu, jolla voidaan tehdä useat tarkastukset yhdellä kertaa. WatchGuard Total Security Suiten avulla saat yli 10 turvallisuuteen liittyvää palvelua yhdessä kokonaisuudessa, eli varmistat useamman säännöksen noudattamisen samalla.

WatchGuard varmistaa myös Secure Wi-Fi ja MFA-sovellusten turvallisuuden. Vaatimukset edellyttävät yhä useammin, että langaton verkko ja salasanat suojataan kehittyneellä teknologialla. Saat kaiken tarvittavan samalta palveluntarjoajalta.

Yksinkertainen keskitetty hallinta

WatchGuardin pilvipohjainen alusta tekee kaikkien kohteiden hallinnoinnista todella helppoa. WatchGuard System Manger (WSM) on saatavilla kaikkiin Firebox-muureihin ja se mahdollistaa kaikkien Firebox-muurien keskitetyn hallinnoinnin yhdellä helppokäyttöisellä konsolilla. Seuranta - ja hallinnointityökaluja hyödyntävä WSM mahdollistaa välittömät muutokset reaaliajassa tai aikataulutetusti. Dimension mahdollistaa myös raportoinnin tärkeimmistä vaatimustenmukaisuuksista (PCI DSS ja HIPAA).

Myös Secure Wi-Fi ja AuthPoint ovat hallinnoitavissa suoraan pilvipalvelusta, joten turvallisuusratkaisujen käyttöönotto, hallinnointi ja raportointi on sujuvaa paikasta ja tilanteesta riippumatta.



Yritysten keskeisempiä haasteita, eli tietoturvallisuutta, resursseja ja budjettia yhteenvedettäessä selviää, miksi WatchGuard on varteenotettava vaihtoehto:

Tietoturva

WatchGuard tarjoaa tarpeelliset turvallisuusratkaisut ilman tarpeettomia lisäominaisuuksia. Firebox-palomuurit Total Security Suite - palveluilla suojaavat sisäverkon tunnetuilta, tuntemattomilta ja piileviltä uhilta. WatchGuard Secure Wi-Fi on markkinoiden ainoa ratkaisu joka havaitsee ja estää kuusi tunnettua liiketoimintaa uhkaavaa langattomien verkkojen uhkatyyppiä. Heikot ja vääriin käsiin joutuneet salasanat voidaan suojata WatchGuardin monivaiheisella AuthPoint-todennuksella.

Resurssit

Kaikki WatchGuardin tuotteet on helppo ottaa käyttöön, käyttää ja hallinnoida. Esim. Mm. Firebox-palomuurien asetusten muuttaminen onnistuu helposti mistä päin maailmaa tahansa. Ratkaisujemme käyttöönotto ja hallinnointi onnistuu ilman turvallisuusasiantijoitakin. Pilvipohjaisten hallinta-välineiden avulla IT-tiimisi toimii saumattomasti tarjoten reaaliaikaista näkyvyyttä ja analytiikkaa. Raportointia varten on ennalta määritettävät sekä yksilölliset valmiit raporttipohjat

Haluatko tehdä yhteistyötä MSSP-palveluntarjoajan (Managed Security Service Provider) kanssa? WatchGuardin kattavan kumppanuusverokoston ansiosta saat juuri yrityksellesi sopivan MSSP:n, ja IT:n hallinnointi on helpompaa kuin koskaan aikaisemmin!

Budjetti

WatchGuardin tuotteet ovat suunniteltu ja hinnoiteltu pienempiäkin yrityksiä silmällä pitäen. Meiltä saat yksilölliset ratkaisut yrityksellesi maksamatta mistään tarpeettomasta.

TARTU TILAISUUTEEN!

Pyydä Sinun toimintaasi tukeva tarjous WatchGuard jälleenmyyjältäsi

PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

WatchGuard® Technologies, Inc. on johtava maailmanlaajuinen verkkoturvallisuuden, turvallisten langattomien verkkojen, varmennuksen ja älykkäiden verkkopalvelujen tarjoaja. Yrityksen palkittuja tuotteita ja palveluja myy miltei 10 000 alan jälleenmyyjää ja palveluntarjoajaa maailmanlaajuisesti yli 80 000 asiakkaalle. WatchGuardin missiona on tuoda yritystason turvallisuus helposti kaikkien yritysten ulottuville koosta ja toimialasta riippumatta. WatchGuard on ihanteellinen ratkaisu erityisesti keskisuurille ja hajautetuille yrityksille. WatchGuardin pääkonttori on Seattlessa, ja yrityksellä on toimipisteet kaikkialla Pohjois-Amerikassa, Euroopassa, Aasian ja Tyynenmeren alueella ja Latinalaisessa Amerikassa. Lisätietoja WatchGuard.com.

Part No. WGCE671405_010219