Datasheet

WithSecure™ Elements

Enemmän joustavuutta, vähemmän monimutkaisuutta. Yksi alusta kaikkiin tietoturvatarpeisiin.

Nykypäivän yritysympäristöt muuttuvat jatkuvasti ja nopeasti. Niin myös kyberuhat. Yritykset siirtyvät kaikilla toimialoilla hyödyntämään pilvipalveluita ja omaksuvat uusia digitaalisia työskentelytapoja, mikä saa hyökkääjät hyödyntämään laajentuvia hyökkäyspintoja entistä kehittyneemmillä ja tehokkaammilla menetelmillä.

Yleinen tapa vastata uusiin uhkiin on koota monimutkainen joukko erikoistuneita teknologioita ja ratkaisuja useilta eri toimittajilta. Tällainen monitahoinen kokoelma työkaluja on haastava jo pelkästään käytännöllisyyden kannalta, puhumattakaan tietoturvaan jäävistä porsaanrei'istä.

- Useiden tällaisten ratkaisujen tehokas käyttö edellyttää spesifistä (ja harvinaista) osaamista.
- Hajautetut ratkaisut eivät integroidu keskenään eivätkä jaa tietoja toisilleen. Tämä luo siiloja ja heikentää tunnistusominaisuuksia.

WithSecure™ Elements on kattava ja kokonaisvaltainen tietoturva-alusta, joka sopeutuu niin liiketoiminnassa kuin uhkakentällä ilmeneviin muutoksiin. Se on yhtenäinen, täysin pilvessä toimiva alusta, joka kattaa kaikki kriittiset tietoturvan arvoketjun osa-alueet: Vulnerability Management, Endpoint Protection, Endpoint Detection and Response ja Collaboration Protection. Voit käyttää yksittäisiä ratkaisuja tiettyihin tarpeisiin tai hanki kokonaisvaltainen kyberturva yhdistämällä ne kaikki – valinta on sinun.

- **Täysi tilannekuva:** vertaansa vailla oleva näkyvyys ja kattava tilannekuva ympäristöösi.
- **Saumaton integrointi:** ratkaisut toimivat saumattomasti yhdessä ja jakavat tietoa keskenään hyökkäyksistä ja uhista – näin tunnistusominaisuudet ovat poikkeuksellisen hyvät.
- **WithSecure™ Elements Security Center:** keskitetty kyberturvan hallinta nopeuttaa toimintojasi.
- **Täysin pilvessä toimiva SaaS-alusta:** valitse kulloinkin tarvitsemasi ratkaisut ja skaalaa palveluiden käyttöä tarpeidesi mukaan.
- **Hallinnoituna palveluna tai itse hallittavana:** Tee yhteistyötä sertifioitujen kumppaneidemme kanssa tai hoida hallinnointi itse. Olemme tukenasi valinnastasi riippumatta.

Miksi WithSecure™ Elements?

Joustava. Modulaarinen. Skaalautuva.
Käytä yksittäisiä ratkaisuja tarpeidesi mukaan tai hanki kokonaisvaltainen kyberturva-alusta yhdistämällä ne kaikki. Joustavilla lisensointivaihtoehdoilla sopeudut muuttuviin tarpeisiin nopeasti.

All-in-One. Yhtenä pakettina.
Minimoi riskit yhdistetyllä huipputason suojauksella, joka kattaa koko tietoturvan arvoketjusi.

Kokonaisvaltainen tilannekuva.
Havainnollista merkitykselliset tiedot ja ymmärrä kriittiset riippuvuussuhteet kyberhyökkäyksissä.

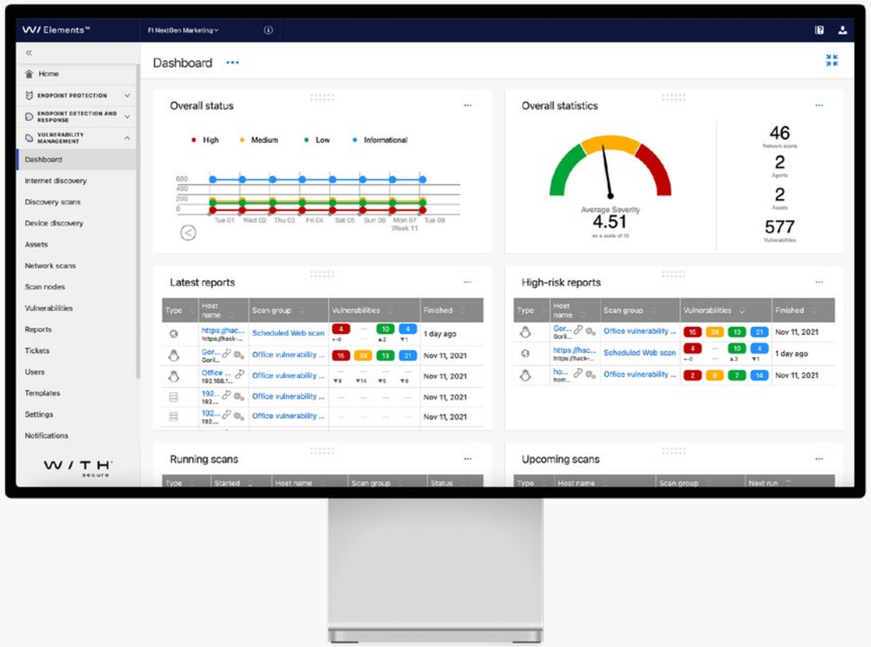
Nopea reagointi.
astaa erilaisiin hyökkäystapoihin päätelaitteissa ja pilviympäristöissä.

Yksinkertaistettu hallinta.
Tehosta tuottavuutta helppokäyttöisellä, keskitetyllä hallinnalla.

Pilvinatiivi alusta.
Pilvipalvelun nopeaa käyttöönoton ja tehokkaan ylläpidon ansiosta pienennät kustannuksia koontiversiolla.

WithSecure™ Elements on kokonaisvaltainen alusta, jossa kaikki toimii saumattomasti yhdessä:

- **Riskipohjainen näkymä hyökkäyspinta-alastasi** tuo potentiaaliset haavoittuvuudet esiin – mikään ei jää piiloon siiloihin.
- **Automatisoitu korjaustiedostojen hallinta** suojaa haavoittuvuuksien hyödyntämiseltä.
- **Ennakoiva suojaus** moderneilta haittaohjelmilta ja kiristyshaittaohjelmilta.
- **Kehittynyt pilvitietoturva** Microsoft 365 -ympäristöön.
- **Nopea ja tarkka havainnointi** kaikkein kehittyneimmille uhille ja hyökkäyksille
- **Hyökkäykset kuriin nopeasti** opastetuilla ja automatisoiduilla reagointitoimilla, saatavilla myös tukea eliittitason uhkien metsästäjiltä ympäri vuorokauden tarpeen mukaan.
- Tukena reaaliaikaiset uhkatiedot ja -analytiikka, joilla voidaan tunnistaa uudet uhat muutaman minuutin sisällä niiden ilmenemisestä.



WithSecure™ Elements Endpoint Protection

Markkinoiden johtava suojaus moderneilta haittaohjelmilta ja kiristyshaittaohjelmilta.

Hakkerit etsivät verkkoon kytketyistä laitteista jatkuvasti potentiaalisia haavoittuvuuksia, eivätkä epäröi mahdollisuuden ilmetessä. Useimmat kyberuhat voidaan estää tehokkaalla päätelaitesuojauksella ja toistuvalla haavoittuvuuksien korjauksella.

WithSecure™ Elements Endpoint Protection on todella kattava, palkittu suojausratkaisu, joka pysäyttää modernit uhat kiristyshaittaohjelmista ja ennennäkemättömistä haittaohjelmista nollapäivähaavoittuvuuksien hyödyntämiseen. Saat kattavan tietoturvan mobiililaitteille, tietokoneille ja palvelimille. Ylivertainen tarkkuus tarkoittaa vähemmän keskeytyksiä liiketoiminnalle ja palautumiseen tarvittavaa IT-työtä. Suodatetut hälytykset ja korkean tason automaatio takaavat parhaan mahdollisen tehokkuuden. Säästä omat resurssisi työhön, jolla on merkitystä.

- **Itsenäisesti toimiva suojaus** ympäri vuorokauden poistaa manuaalisen työn ja asiantuntija-avun tarvetta.
- **Taistele ennennäkemättömiä uhkia ja hhyökkäyksiä** vastaan yhdistämällä reaaliaikaisen uhkatiedon, kehittyneet koneoppimisteknologiat ja käyttäytymisanalyysin.
- **Ota ohjelmistojen korjaustiedostot käyttöön heti, kun ne julkaistaan** täysin automatisoidulla ohjelmistotiedostojen hallinnalla.
- **Estä sovellusten ja komentosarjojen suorittaminen** ennaltamääritettyjen sääntöjen tai järjestelmänvalvojasi määritysten perusteella.
- **Suojaa käyttäjiä online-uhilta**, kuten haitallisten sivustojen käytöltä.
- **Tunnista kiristyshaittaohjelmat ja estä tuhot** ja tietojen väärinkäytökset DeepGuard- ja DataGuard-tekniikoilla.
- **Estä hyökkäyksiä pääsemästä järjestelmiisi ja vuotamasta tietojasi** laitteiden kautta.
- **Estä vaarallisia sovelluksia käyttämästä tiedostoja** ja järjestelmäresursseja ilman lupaa.ssion.

52%

yrityksistä on joutunut tietovuodon uhriksi viimeisen kahden vuoden aikana.

42%

tietovuodoista vuonna 2020 johtui siitä, ettei saatavilla ollutta korjaustiedostoa otettu käyttöön.

57%

organisaatioista ei tiedä, mitkä haavoittuvuudet ovat kaikkein riskialtteimpia.

Alustan parhaita ominaisuuksia:

Päätelaitteiden ja pilviympäristöjen suojaus

Haittaohjelmien ja kiristys-haittaohjelmien pysäytys

Haavoittuvuuksien etsiminen ja korjaaminen

Uhkien tunnistus ja metsästys

Tietojenkalastelun ja kehittyneiden uhkien pysäytys Microsoft Office 365:ssä

Tietovuodon kohteeksi joutuneiden yritystilien tunnistus

Nopea reagointi hyökkäyksiin automaatiolla, opastuksella ja ympäri-vuorokautisella tuella

WithSecure™ Elements Endpoint Detection and Response

Päihitä hyökkääjät. Suojaa organisaatiotasi kyberhyökkäyksiltä.

Kukaan ei ole immuuni kyberuhille, eikä nykyisin ole olemassa täydellistä suojausta. Nykypäivän kehittyneet hyökkäykset voivat ohittaa vahvimmatkin ehkäisevät toimet. Ja ne voivat jäädä helposti huomaamatta. Silloin hyökkääjät voivat kaikessa rauhassa aiheuttaa ongelmia ja käyttää tietojasi hyödykseen.

WithSecure™ Elements Endpoint Detection and Response -ratkaisu varustaa sinut toimialan johtavilla tunnistusominaisuuksilla taistossa sekä kohdennettuja että täysin opportunistisia kyberhyökkäyksiä vastaan. Havaitse hyökkäykset ja poikkeamat tarpeeksi ajoissa ja voit vastata niihin tehokkaasti hyödyntämällä automaattisia vastetoimenpiteitä ja asiantuntijoidemme opastuksen avulla.

- **Reaaliaikainen näkyvyys** kaikkeen, mitä päätelaitteissa tapahtuu. Windowsin, macOS:n ja Linuxin kattava telemetria.
- **Uhkien nopea ja tarkka tunnistus** Broad Context Detection -toiminnolla. Havaitset kaiken epäilyttävän toiminnan, myös harmittomalta vaikuttavat toimet.
- **Uhkien tehokas metsästys** tapahtumahaulla ja suodatuksella.
- **Tapahtumaketjujen korrelointi hahmotettavissa** yksinkertaistetuilla visualisoinneilla.
- **Uhkiin voidaan reagoida välittömästi automatisoiduilla reagointitoimilla**, jotka auttavat pitämään organisaatiosi turvassa kellon ympäri.
- **Hyökkäykset kuriin** selkeillä, toimenpidesuosituksilla ja mahdollisuudella siirtää hankalat tapaukset eliittitason uhkien metsästäjillemme ympäri vuorokauden.
- **Yrityksesi pystyy noudattamaan** PCI-, HIPAA- ja GDPR-määräyksiä, joiden mukaan tietovuodoista on ilmoitettava 72 tunnin kuluessa

WithSecure™ Elements for Collaboration Protection

Kattava lisäsuojaus tunnistaa ja pysäyttää kehittyneet uhat ja tietojenkalasteluviestit.

Tämä on datan kulta-aikaa. Yrityssähköposteissa on valtavasti arkaluonteisia ja luottamuksellisia tietoja. Pilvitallennustilat, kuten Microsoft SharePoint, ovat yritysten immateriaalioikeuksien aarreaittoja. Yritysten sähköpostitilit on usein linkitetty useisiin liiketoiminnan kannalta kriittisiin sovelluksiin. Hyökkääjien käsiin päätyvät käyttäjien käyttäjätiedot avaavat hyökkääjille väylän yritysten kriittisiin järjestelmiin ja tietoihin.

Microsoft Office 365 on maailman suosituin sähköpostipalvelu. Sen suosio saa hyökkääjät suunnittelemaan menetelmänsä nimenomaan Microsoftin vakioturvatoimien ohittamiseksi. Microsoftin sähköpostille tarjoama perustason tietoturva ei ole riittävä kehittyneitä hyökkäyksiä tai hienostuneita tietojenkalasteluyrityksiä vastaan.

WithSecure™ Elements for CollaborationProtection vahvistaa Microsoftin omia tietoturvaominaisuuksia suojaamaan yritystäsi entistä hienostuneemmilta tietojenkalasteluhyökkäyksiltä ja haitalliselta sisällöltä, jotka kohdistuvat sähköpostiin, kalentereihin, tehtäviin ja SharePointiin. Kehittyneet tunnistusominaisuudet sisältävät esimerkiksi sähköpostien poikkeavuuksien ja sähköpostitilien vaarantumisen havaitsemisen. Täysin pilvessä toimiva ratkaisu on suunniteltu Microsoft Office 365:tä varten. Se laajentaa päätelaitteille tarkoitettuja Elements-tietoturvaratkaisuja saumattomasti.

- **Varmista liiketoiminnan jatkuvuus kustannustehokkaasti** monikerroksisella lähestymistavalla.
- **Jatkuvaa suojausta** loppukäyttäjän laitteesta riippumatta, ilman keskeytyksiä käyttäjille.
- **Yksinkertaiset työnkulu**t yhdistetyllä tietoturvan hallinnalla pilvessä olevissa päätelaitteissa.
- **Vaivaton käyttöönotto** muutamassa minuutissa saumattomalla pilvestä pilveen -integroinnilla. Ei middleware-ohjelmistoja eikä laajamittaisia määritystöitä.
- **Estä haitallinen sisältö**, kuten haittaohjelmat, kiristyshaittaohjelmat ja tietojenkalasteluyritykset.
- **Tunnista kaikkein hienostuneimmatkin haittaohjelmat** Outlook- ja Sharepoint-ympäristöissä analysoimalla epäilyttävät tiedostot eristetyssä sandbox-ympäristössä.
- **Huomaat, onko yrityksen tileillä ilmennyt tietovuotoja**, kun saat kattavat tiedot siitä, miten, mitä ja milloin on tapahtunut ja kuinka vakavaa se on.
- **Luota Saapuneet-kansioosi. Tunnista toiminnassa ilmenevät poikkeavuudet**, kuten haitalliset välityssäännöt.
- **Paranna tehokkuutta** automatisoiduilla tarkistuksilla.

> **“Valitsimme SIEM:n sijaan WithSecuren ratkaisut, koska sen koneoppimiseen perustuva toiminnan- tunnistusjärjestelmä vähensi väärien hälytysten määrää merkittävästi. Lisäksi hälytykset esitettiin tavalla, joka helpotti analysointia ja päätöksentekoa huomattavasti."**

Jeovane Monteiro Guimarães, IT Supervisor, Móveis Itatiaia

WithSecure™ Elements Vulnerability Management

Kartoita ja vahvista hyökkäyspinta-alaasi.

Dynaamiset, monimutkaiset IT-yritysympäristöt muodostavat laajoja hyökkäyspinta-aloja. Hyökkääjät etsivät jatkuvasti mahdollisuuksia hyödyntää haavoittuvia järjestelmiä, jotta he saisivat arvokkaita tietoja luvatta käyttöönsä. Uusia tietoturvaan vaikuttavia korjaustiedostoja julkaistaan päivittäin, ja niiden käyttöönotto ajoissa on äärimmäisen tärkeää, jotta tiedot voidaan turvata ja liiketoiminnan jatkuvuus voidaan taata. Kyberturvallisuuden vahvistaminen alkaa resurssien ja kokoonpanojen määrittelystä.

WithSecure™ Elements Vulnerability Management tunnistaa organisaatiosi resurssit ja auttaa korjaamaan haavoittuvaiset kohdat ja kriittisimmät porsaanreiät täsmällisesti. Minimoi hyökkäyspintasi ja riskit. Etsi sisäiset ja ulkoiset heikot kohdat ennen muita.

- **Holistinen näkyvyys** ja tarkka kartoitus kaikista resursseista, järjestelmistä ja sovelluksista sekä varjo-IT:stä.
- **Pienennä hyökkäyspinta-alaa** tunnistamalla haavoittuvaiset hallinnoidut ja hallinnoimattomat järjestelmät, ohjelmistot ja virheelliset konfiguraatiot.
- **Vähennä riskejä** tekemällä ennakoivia ja ehkäiseviä toimia ennen tapausten ilmenemistä.
- **Nopeuta työnkulkuja** automatisoiduilla ajoitetuilla tarkistuksilla. Priorisoi korjaustoimet sisäänrakennetulla riskiarvioinnilla.
- **Laajenna haavoittuvuuksien tarkistus etälaitteisiin** verkkosi ulkopuolella Windows-päätelaitteiden agenttiohjelmalla.
- **Näytä ja perustele, miten arvokasta** liiketoiminnan jatkuvuuden ylläpitäminen on. Laadi vakiomuotoisia ja mukautettuja raportteja tietoturvan tilasta ja riskeistä eri sidosryhmille.
- **Vaatimustenmukaisuus toteutuu** PCI ASV -sertifioidulla haavoittuvuustarkistusratkaisulla ja räätälöidyillä raporteilla.

Tukipalvelut:

Headline	Advanced	Premium
Tuki normaalin työajan puitteissa (englanniksi, suomeksi, ranskaksi, saksaksi, japaniksi ja ruotsiksi)	✓	✓
Teknisen tuen palvelut etusijalta	✓	✓
Online-työkalut ongelmailmoituksiin ja jatkotoimiin	✓	✓
Puhelinpalvelu ja takaisinsoitto	✓	✓
Chat- ja etäpalvelu		✓
Ympärivuorokautinen tuki (englanniksi)		✓
Reagointi kriittisiin tapauksiin tunnin sisällä		✓
Eskalointi johtotasolle		✓
Konsultoinnin päivitys		✓
Neuvoja haittaohjelmien poistoon		✓

Me olemme tukenasi. Lisätukipaketit sisältävät kattavia ja sujuvia palveluja, joilla liiketoimintasi pysyy käynnissä. Advanced- ja Premium-versiot saatavana.

Me tunnemme kyberturvallisuuden

30 vuoden kokemus kyberrikoksista tutkimuspohjaisella lähestymistavalla, jonka toimivuudesta ovat todisteena useat kiittävät arvioinnit ulkopuolisista vertailuista.

withsecure.com/elements
twitter.com/withsecure
linkedin.com/withsecure

Kokeile jo tänään