KOCHCONSULTANCY
Security- & Privacy Awareness

proofpoint®

Proofpoint Essentials

Wat is Proofpoint Essentials?
Belangrijkste functies
Waarom kiezen voor Proofpoint Essentials?
Proofpoint Essentials Security Awareness
Prijzen

Final – 22 mrt 2022

Wat is Proofpoint Essentials?

Het bedrijf Proofpoint is een bekende leverancier van security oplossingen voor zowel grote bedrijven als bedrijven in het MKB segment. Het bedrijf is gespecialiseerd in de bescherming van gebruikers tegen de cyberdreigingen via e-mail. Het e-mail systeem van iedere organisatie is de bron van diverse cyberdreigingen en speelt daardoor een belangrijke rol bij de verspreiding van virussen, malware, ransomware en het uitvoeren van digitale fraude.

Speciaal voor het MKB (tot 1.000 gebruikers) biedt het product "Proofpoint Essentials" effectieve bescherming tegen dergelijke cyber-dreigingen. Het product biedt dezelfde bescherming als de Proofpoint producten die bij grote (enterprise) organisaties worden ingezet, gebruik makend van dezelfde geavanceerde Proofpoint technologie en kennis over cyberdreigingen. Deze kennis wordt door Proofpoint verzameld door middel van security analyses die dagelijks worden uitgevoerd op honderden miljoenen e-mails, attachments, URL's, etc. van hun wereldwijde klanten.

Het belangrijkste onderdeel van Proofpoint Essentials is de "Secure e-mail Gateway". Het beschermt de gebruikers tegen e-mail aanvallen en het verlies van gevoelige / vertrouwelijke informatie via e-mail. Tevens biedt Proofpoint Essentials met een "mailbox voor noodgevallen" continuïteit voor het geval dat het e-mail systeem van de gebruiker zou uitvallen.
Het product werkt zowel voor gebruikers met een eigen e-mail infrastructuur als voor gebruikers van e-mail systemen in de cloud zoals office365 of Gmail.

Samenvattend:
Proofpoint Essentials houdt dreigementen aan de rand van uw e-mail systeem tegen en voorkomt daarmee dat virussen, malware, ransomware, spam, etc. binnen de organisatie worden afgeleverd.

Proofpoint Essentials
Belangrijkste functies

Security
Proofpoint beschermt tegen gerichte aanvallen, ransomware, besmette e-mail attachments, besmette websites, BEC (Business E-mail Compromise) en ongewenste e-mail (spam).

- Spam Filtering
  Met de Proofpoint MLX machine-learning technologie wordt iedere e-mail geanalyseerd op honderden attributen zoals headers, structuur, inhoud, e-mail zender reputatie, images, etc. Hiermee wordt de gebruiker beschermd tegen spam e-mails, malware, andere besmette e-mail, en besmette attachments.

- Anti-Virus
  De geavanceerde anti-virus engine van Proofpoint is effectief en snel. Bekende virussen worden tegengehouden en door middel van “Heuristic scanning” wordt bescherming geboden tegen verdachte patronen van nog niet eerder ontdekte virussen.

- TAP: Proofpoint Targeted Attack Protection (URL- en Attachment bescherming)
  Proofpoint Targeted Attack Protection ontdekt besmette URL’s (internet-links) en besmette attachments voordat gebruikers erop kunnen klikken en geïnfecteerd raken.

- Content Filtering
  Met de Proofpoint Essentials intelligent e-mail content filter krijgt u de mogelijkheid om op een efficiënte manier e-mail communicatie policies door te voeren.

- Zero-Hour Outbreak
  Hiermee worden gebruikers beschermd tegen nieuwe, niet eerder geziene e-mail dreigingen zo gauw als ze ontstaan, nog voor de updates van Anti-Virus producten.

- Policy-gedreven Data Loss Prevention (DLP)
  Door middel van DLP bibliotheken en “Smart Identifiers” kunnen eenvoudig en snel e-mail policies ingesteld worden. Hiermee wordt voorkomen dat gevoelige / vertrouwelijke gegevens zoals intellectuele eigendommen, medische informatie, persoonsgegevens, financiële informatie, etc. buiten de geldende policies de organisatie uitlekken.

- (Automatische en handmatige) e-mail Encryptie
  Er kunnen filters worden gedefinieerd waardoor uitgaande e-mails automatisch worden versleuteld als ze vertrouwelijke / gevoelige informatie bevatten. Gebruikers kunnen ook handmatig hun uitgaande e-mails beveiligd versturen door middel van een “tag” of een “send securely” knop in outlook.

- Social media Bescherming
  Proofpoint Essentials levert bescherming van maximaal 3 Social Media accounts. Deze Social Media accounts worden continue gecontroleerd op ongebruikelijke postings en profiel veranderingen. Hiermee worden uw klanten en volgers beschermd tegen besmette of ongewenste content op de Social media accounts.

Continuïteit

Proofpoint Essentials beschermt bedrijven tegen de gevolgen van het uitvallen van het e-mail systeem. Het is mogelijk om e-mails te blijven ontvangen en versturen in het geval van een calamiteit of als de verbinding met de-email server uitvalt.

- Email Spooling
  Op het moment dat de e-mail server “down” gaat of als er bijvoorbeeld een probleem is met de netwerkconnectie, zal Proofpoint Essentials automatisch (gedurende 30 dagen) alle inkomende e-mails opslaan op een backup server.

- Inbox voor noodgevallen (Emergency Inbox)
  Met behulp van de 30-dagen “Inbox voor noodgevallen” kunnen de gebruikers e-mails en attachments blijven sturen, ontvangen, en beantwoorden. Wanneer de connectie met de mailserver weer is hersteld zal Proofpoint Essentials de e-mails in de “inbox voor noodgevallen” weer terugzetten naar de oorspronkelijke mailserver.

E-mail Archief

Proofpoint Essentials biedt (in de professional licentie) een 10-jarig archief voor e-mails voor compliance- of juridische doeleinden.

Management

Proofpoint Essentials biedt meerdere mogelijkheden voor het beheer van de verschillende soorten gebruikers, zowel op user-level als op company-level.

Waarom kiezen voor Proofpoint Essentials?

Hieronder een overzicht over waarom gebruikers kiezen voor Proofpoint Essentials.

Meerlaagse e-mailbeveiliging

Door zijn meerlaagse e-mail beveiliging biedt Proofpoint Essentials een sterk beveiligingsniveau. Proofpoint Essentials is speciaal gericht op MKB bedrijven en biedt dezelfde bescherming die grote “enterprise” bedrijven krijgen.
Proofpoint is een van de grootste leveranciers op de markt voor e-mailbeveiliging. Voor het beschermen van de gebruikers wordt de kennis gebruikt over cyber-dreigingen en -aanvallen die gedurende de afgelopen jaren continu (elke nanoseconde) is bijgewerkt op het Proofpoint Nexus Threat Intelligence platform.

De e-mail gateway maakt gebruik van Proofpoints eigen antivirus-, antispam- en phishing-detectie-engines, die een sterke bescherming bieden tegen e-mailbedreigingen. Al uw e-mails worden in realtime gescand door Proofpoint Essentials voordat ze worden afgeleverd. Hierbij worden e-mail bedreigingen gedetecteerd en eruit gefilterd of in quarantaine gezet.

Met de rapportage krijgen de beheerders inzicht in de details van de bedreigingen (bijv. waar de bedreigingen vandaan komen en of er specifieke targets zijn binnen de organisatie) en de juiste maatregelen nemen om risico’s te verlagen.

Geavanceerde bescherming tegen bedreigingen

De URL- en bijlage-sandboxing van Proofpoint biedt bescherming tegen geavanceerde aanvallen zoals phishing en spear-phishing.
Met behulp van geavanceerde antivirus en sandboxing controleert Proofpoint automatisch de URL-links en bijlagen in realtime om te voorkomen dat gebruikers kwaadaardige e-mail bijlagen openen of phishing-websites bezoeken die proberen gebruikers te misleiden om malware te installeren of accountgegevens op te geven.

Preventie van gegevensverlies en inhoudsfiltering

Essentials biedt de mogelijkheid van een content-beleid voor uitgaande e-mail om verlies van vertrouwelijke/gevoelige gegevens te helpen voorkomen. Met behulp van filters kunnen beheerders ervoor zorgen dat gebruikers geen privé-informatie of gevoelige documenten via e-mail verzenden, vooral niet buiten de organisaties.
Dit is belangrijk voor bedrijven in verband met de compliance aan wet/regelgeving of specifieke certificeringen. Zeker in het kader van dataregelgeving zoals de AVG. Met Proofpoint kunt u automatisch uitgaande gevoelige informatie identificeren en beheren.

Bedrijfscontinuïteit

In het geval van een calamiteit of incident waarbij uw netwerk of de verbinding met de e-mail server uitvalt kunt met de “Inbox voor noodgevallen” van Proofpoint Essentials gedurende 30 dagen gewoon e-mails blijven ontvangen en verzenden.

Beheer van eindgebruikers

Proofpoint kan worden geconfigureerd om eindgebruikers toegang te geven tot hun eigen quarantaine, e-mailarchief en hun lijsten met toestaan/weigeren te beheren. Dit bespaart IT-afdelingen veel tijd.
Eindgebruikers kunnen de e-mails die in quarantaine zijn gezet eventueel zelf terughalen. Gebruikers kunnen ook afzenders blokkeren, wat helpt om spam-mail te verminderen.

Proofpoint Essentials Security Awareness

Phishing simulaties en security awareness training

Proofpoint Essentials Security Awareness biedt de mogelijkheid om phishing simulaties uit te voeren en security awareness training te verzorgen aan medewerk(st)ers. Hiermee worden de medewerk(st)ers geleerd op de juiste manier om te gaan met cyber-dreigingen en op de juiste manier te reageren als er sprake is van een dreiging.

Met de ThreatSim phishing simulaties van Proofpoint kunt u de gevoeligheid van de organisatie peilen voor phishing aanvallen. Er zijn duizenden phishing templates beschikbaar in diverse categorieën. Deze phishing templates zijn verkregen vanuit het Proofpoint Nexus Threat Intelligence Platform. Met behulp van deze templates kunnen de volgende dreigingen worden gesimuleerd:

- Kwaadaardige attachments (E-mail bijlagen)
- Ingevoegde URL-links in een E-mail waarop de slachtoffers moeten klikken
- Verzoeken om persoonlijke en/of vertrouwelijke informatie in te voeren

Gebruikers die in een phishing simulatie trappen kunnen automatisch uitgenodigd worden voor het volgen van interactieve training (E-learning modules). Hierbij worden de gebruikers geleerd over de gevaren van phishing en hoe ze in de toekomst dergelijke phishing e-mails kunnen herkennen.

E-Learning bibliotheek

De bibliotheek van security-onderwerpen die worden behandeld tijdens de interactieve- en spel-gebaseerde trainingen wordt constant bijgehouden en up-to-date gemaakt. De lesstof behandelt een breed scala aan security risico's en is beschikbaar in meer dan 40 talen.
Alle modules zijn "on demand" beschikbaar, wat betekent dat de medewerk(st)ers de modules kunnen bekijken op een moment dat het hen het beste uitkomt. De modules zijn ook geschikt om te bekijken vanaf een mobiel apparaat. De schermindeling wordt dan automatisch aangepast. De modules duren tussen de 5 en 15 minuten. Dit is een kleine investering in tijd voor dit belangrijke onderwerp.

Awareness vergroting is een continu proces

Een éénmalige activiteit is niet voldoende om de awareness van medewerk(st)ers te vergroten en ze te overtuigen van het nut en de noodzaak van veilig gedrag. Er zal dan snel worden "terug gevallen" naar het oude, onveilige gedrag.
Awareness vergroting vraagt om een continu proces van meten en leren en rapporteren. Proofpoint Essentials geeft u de mogelijkheid van een continu meet- en leerproces. Het geeft de kwetsbare plekken in de organisatie aan en levert gerichte training op die plekken waar het nodig is.

Proofpoint Essentials prijzen

Hieronder een overzicht van de prijzen van Proofpoint Essentials, de Security Awareness training en de speciale “Threat Protection” bundel. Met deze bundel wordt het extra aantrekkelijk om beide onderdelen aan te schaffen.

Product	Prijs
Proofpoint Essentials (E-mail security + databescherming)	
• Proofpoint Essentials (Advanced)	€ 3.25
Proofpoint Essentials Security Awareness Training	
• PE-SAT	€ 1,35
Bundel “Proofpoint Threat Protection”	
• Incl. Proofpoint Essentials Advanced	
• Incl. PE-SAT	
• Bundelprijs	€ 4,10

Genoemde prijzen zijn per gebruiker per maand
Alle genoemde prijzen zijn excl. BTW.

Voorbeeld:
Voor een bedrijf met 50 medewerk(st)ers is de benodigde investering per jaar:

Losse onderdelen:
Proofpoint Essentials (advanced): 50 x € 3,25 x 12 = € 1.950
Proofpoint Essentials PE-SAT (Security Awareness): 50 x € 1,35 x 12 = € 810

Bundel:
Proofpoint Threat Protection Bundel: 50 x € 4,10 x 12 = € 2.460

Overige voorbeelden (kosten per jaar):

	20 gebruikers	50 gebruikers	100 gebruikers	250 gebruikers
Losse onderdelen				
Proofpoint Essentials	€ 780	€ 1.950	€ 3.900	€ 9.750
Security Awareness	€ 324	€ 810	€ 1.620	€ 4.050
Bundel:				
Proofpoint Threat Protection	€ 984	€ 2.460	€ 4.920	€ 12.300

Prijzen zijn per jaar. Let op: de bundelprijs is gunstiger dan twee losse onderdelen.

Meer informatie?
Wilt u meer informatie over de voordelen van Proofpoint Essentials?
Wilt u een toelichting op de informatie in dit document
Wilt u een demonstratie van Proofpoint Essentials (online of bij u aan huis)
Wilt u een offerte aanvragen voor het afsluiten van een Proofpoint Essentials licentie?

Neem dan gerust contact op via onderstaande contactegevens

Contact informatie

Koch Consultancy BV
Beetzlaan 5
3762 CA Soest

Tel: 06-53233269

Website: www.kochconsultancy.nl
E-mail: info@kochconsultancy.nl

KOCHCONSULTANCY
Security- & Privacy Awareness