

Computer bescherming

Managed Antivirus met Web Protectie

Je kunt jouw aanbod nu uitbreiden en de bestaande eindpunt- en netwerkveiligheidsservice van jouw klanten aanvullen met een extra beveiligingslaag. Web Protection is onze eenvoudig beheerbare functie voor internetbeveiliging. Hiermee kun je webbeleidsregels van klanten bijhouden, controleren en afdwingen via één geïntegreerd scherm: het MAX RemoteManagement Dashboard.

Robuust, flexibel, eenvoudig te beheren

Combineer Web Protection met Managed Antivirus, MailProtection, patchbeheer en back-ups om klanten op ieder vlak te beveiligen. Daarmee bied je hen uitgebreide internetbeveiliging, filteren op webinhoud en bandbreedtecontrole. Zo kun je in samenwerking met jouw klanten:

- Hun bedrijf en eindgebruikers beveiligen tegen websites met malware, phishing, proxy's, spyware, adware, botnets en spam
- Voor uiteenlopende websitecategorieën browseregels op basis van tijd en beleidsregels voor het filteren op webinhoud toepassen, en het gebruik van sites die niets met werk te maken hebben beperken, zoals sociale netwerken, veilingen, games en meer
- Werknemers productief houden met logische beleidsregels omtrent internetgebruik op de werkplek
- Het bandbreedtegebruik in de gaten houden en waarschuwingen geven wanneer een apparaat de limiet overschrijdt. Hierdoor kunnen ongewenste kosten worden voorkomen en kan een vertraagd netwerk snel worden hersteld
- Zorgen dat het bedrijf niet wettelijk aansprakelijk kan worden gehouden en het risico op beveiligingsschending verlagen via proactieve besturingsfuncties voor internettoegang

[web-protection-1.png](#)

Computer bescherming

[web-protection-2.png](#)

Zo werkt het

Web Protection is gebaseerd op een beleidsgerichte aanpak. Ieder apparaat dat je inschakelt voor Web Protection wijst dus naar een centraal beleid. Je kunt het beleid bewerken en instellingen voor de apparaten met dat specifieke beleid aanpassen. Zo kun je Web Protection schalen op basis van een reeks apparaten en hoef je niet ieder apparaat in het volledige systeem afzonderlijk in te stellen.

Een groot aantal uitstekende beleidsopties

- Blokkeer onveilige sites zodat gebruikers ze niet kunnen bezoeken
- Pas filteren op webinhoud toe om beleidsregels voor internettoegang op de werkplek toe te passen
- Stel witte lijsten en zwarte lijsten op om categoriegebaseerde filters te overschrijven
- Pas optioneel een planning toe zodat werknemers sites die niets met werk te maken hebben, buiten werktijd of in de lunchpauze kunnen openen

Pagina 2 / 4

Computer bescherming

- Pas een controle op 'webbandbreedte' toe en ontvang een waarschuwing wanneer er te veel bandbreedte wordt gebruikt op een netwerk
- Filter internetactiviteit per dag, categorie en URL om trends, pieken en onregelmatigheden te tonen en URL-gegevens weer te geven of te verbergen, afhankelijk van de vereisten voor gegevensprivacy

... compleet met gedetailleerde rapportagestools waarmee je internetactiviteit kunt analyseren en de effectiviteit van internetbeveiliging kunt aantonen.

[web-protection-3.png](#)

[web-protection-4.png](#)

Computer bescherming

Breid jouw portfolio uit en bied een nog robuustere beveiliging

Met MAX Web Protection kun je alles doen wat nodig is om jouw beveiligingsvoorzieningen zo uitgebreid mogelijk te maken. De oplossing wordt ondersteund door patchbeheer, MailProtection, Managed Antivirus, MDM en Managed Online Backup, waardoor je de beveiligingszorgen van jouw klanten weg kunt nemen.

Unieke FAQ ID: #1439

Auteur: n/a

Laatst bijgewerkt: 2016-06-16 10:20