



Webroot webbfilter

Surffilter för företag

Hur skyddar du dina användare när de surfar på Internet?

Många är medvetna om riserkerna med att klicka på fel länk eller ladda ner ett program från fel domän, men alla är inte det. Har ni otur så räcker det med ett felklick eller en nedladdning för t.ex. få in ett kryptovirus som krypterar samtliga filer i er gemsama filyta. Är du medveten om vilka sidor dina anställda surfar på? Kanske är det dags att införa filtrering med varningar om att användaren är på väg att besöka en olämplig webbplats? Nu finns verktygen för att skydda dina användare mot cyberattacker, få insyn i webbanvändningen och tillämpa användningsprinciper för att minska säkerhetsrisken och surfa säkrare.

Vad är DNS-skydd?

Innan vi talar om DNS-säkerhet ska vi kort förklara vad DNS är. Domännamnssystemet (DNS) fungerar som en telefonbok för Internet. När en användare skriver in en webbadress i en webbläsare skickas den till DNS-servrarna som översätter den till de unika IP-adresserna (Internet Protocol), som låter webbläsaren öppna den önskade platsen. DNS-protokollet är tyvärr inte utformat med säkerhet i åtanke, och är sårbart för cyberattacker, så som cacheförgiftning, DDoS, DNS-kapning, botnets, man-in-the-middle osv.



IT-Tjänster

Vi är specialister inom IT och tillgodoser era behov och gör er vardag enklare. PrimeQ levererar IT-drift-, support-, moln- och konsulttjänster. Vi vet hur viktigt det är att IT-lösningarna fungerar för att verksamheten ska flyta på och vi lägger stor vikt vid personlig service och tar fram system som är noggrant anpassade utefter era behov.

Vill du veta mer om våra IT-tjänster eller PrimeQ?

Vänligen kontakta:
sales@primeq.se

Webroot Webbfilter



Genom att omdirigera användarnas webbftrafik via en molnbaserad DNS-säkerhetslösning kan ditt företag finjustera och sätta egna regler för era användares webbåtkomst, säkerställa regelefterlevnad och stoppa 88 procent av hoten – innan de någonsin kommer in i nätverk eller klientdatorer. Webroot® DNS-skydd kan stoppa 88% av hoten innan de når ert nätverk.

Varför företag behöver DNS-skydd

Okontrollerad Internetåtkomst är en högriskaktivitet för alla företag, oavsett storlek. Inför dagens sofistikerade attacker är endast antivirusprogram inte längre tillräckligt för att vara skyddad från modern IT-brottslighet. En nyligen publicerad rapport från EfficientIP visar att 77 procent av företag runt om i världen drabbades av minst en DNS-cyberattack under 2018. Vad som är ännu mer oroande – företagen drabbades av i genomsnitt så många som sju attacker under hela året.

DNS-skydd för servrar, slutpunkter och andra nätverksanslutna enheter kan göra hela skillnaden för ett företags framgång (och överlevnad).

Varför Webroot webbfilter är annorlunda

Den helt molnbaserade, säkra och skalbara tjänsten tar bara några minuter att konfigurera.

- Skydda din DNS-anslutning, nätverk och användare från cyberattacker.
- Få detaljerade rapporter på begäran
- Få detaljerade rapporter om alla hot som verksamheten skulle ha varit mottagliga för utan DNS-skydd, och få därigenom full insyn i risk och användning.
- Aktivera riktlinjer efter grupp, enhet eller IP



Webroot Webbfilter

- Kontrollera Internetanvändningen för dina användare med hjälp av förkonfigurerade och anpassade riktlinjer efter grupp, enhet eller nätverk.
- Blockera hot på domännivå
- Över 80 URL-kategorier ger dig detaljerad, principbaserad kontroll för att automatiskt blockera farliga och tvivelaktiga webbplatser (till exempel skadlig kod och pornografiska sidor) eller oönskade webbplatser (till exempel strömmande media).
- Tillämpa ledande webbklassificering
- Minska kostnaderna i samband med infektioner

DNS-skydd stoppar upp till 88 procent av webbaserad skadlig kod på domänlagret, så att den aldrig når ditt nätverk. Det sparar tid och pengar, samtidigt som skyddet minimerar ineffektiv webb användning.

Byggt för framtidens Internet

DNS-agenten byggdes med framtiden i åtanke och stödjer IPv6, nästa generations Internet protokoll. Detta innebär att du kan skydda dina användare med DNS-säkerhet på moderna nätverk, som offentliga hotspots, även i framtiden. Eftersom implementationen av IPv6 fortsätter att stiga, blir det allt viktigare att ditt nätverksskydd kan hantera den här typen av trafik.

DNS-skyddet körs nu på Google Cloud-plattformen

Webroot® DNS Protection har nyligen flyttat till Google Cloud Platform (GCP) för ökad säkerhet, prestanda och tillförlitlighet. Det körs nu på Google Cloud med hög redundans, låg latens nätverk i 16 regioner över hela världen för att maximera prestanda. DNS-skyddet har också nytta av Googles inbyggda DoS-prevention och -begränsning, vilket gör att vi kan stoppa attackerande trafik innan den träffar klienten.