WEBROOT
Smarter Cybersecurity™

BrightCloud® Bedreigingsintelligenceservices

Bescherm uw klanten met bewezen, hypermoderne bedreigingsintelligence

Omdat de omvang, snelheid en geraffineerdheid van cyberaanvallen steeds verder toeneemt, is er een oplossing nodig die verder gaat dan traditionele beveiligingsmethoden. Moderne cybercriminelen sturen dynamische, onopvallende bedreigingen de wereld in die zijn ontworpen en die er specifiek op zijn gericht om door de beveiliging heen te komen via meerdere toegangspunten van een netwerk. Beveiligingsleveranciers en andere leveranciers kunnen het zich niet permitteren om het vertrouwen van hun klanten op het spel te zetten of de potentiële waarde van hun eigen producten en services te zien dalen als gevolg van een achterhaalde benadering van beveiliging. Bedrijven hebben hypermoderne oplossingen nodig die net zo dynamisch zijn als de aanvallen waartegen het bedrijf moet worden beschermd, die de huidige toename van de bedreigingen altijd een stap voorblijven en die bescherming bieden tegen nieuwe soorten bedreigingen die slechts enkele uren of minuten aanwezig zijn.

BrightCloud® bedreigingsintelligenceservices bieden voorspellende bedreigingsintelligence over URL's, IP-adressen, bestanden en mobiele apps, die eenvoudig kan worden geïntegreerd om klanten te beschermen tegen aanvallen die eerder zelfs nog onbekend waren. Deze services maken gebruik van het Webroot Threat Intelligence Platform, een geavanceerd, op de cloud gebaseerd beveiligingsplatform, dat met een contextuele analyse-engine wordt versterkt om gegevens met elkaar in verband te brengen, voor een diepgaand inzicht in het landschap van online bedreigingen. Dit geavanceerde, zelflerende platform scant het internet doorlopend en integreert invoeren van miljoenen sensoren, zodat de services van BrightCloud snel en nauwkeurig bedreigingen kunnen opsporen die eerder nog onbekend waren.

Een hypermoderne benadering voor beveiliging bij bedrijven

Er is een driedimensionale aanpak nodig om bedreigingsintelligence te kunnen leveren met:

- brede services die bescherming bieden tegen alle belangrijke bedreigingsvectoren;
- big-data-architectuur voor inhoud, omvang, diepte en snelheid;
- grotere nauwkeurigheid en voorspellende risicobeoordeling door gegevens die afkomstig zijn van eindpunten van echte computers en die eerder niet met elkaar te vergelijken waren, met elkaar in verband te brengen.

Contextuele kennis van bedreigingen via URL's, IP-adressen, bestanden en mobiele apps

1. BrightCloud®-services bieden dekkingsbreedte

De bedreigingsintelligenceservices van BrightCloud bieden beveiligingsleveranciers en anderen collectieve kennis van bedreigingen die altijd actueel, uiterst nauwkeurig, contextueel en bruikbaar is. Webroot doet dit door robuuste beveiliging aan te bieden voor online en mobiele bedreigingen, en bedreigingen uit bestanden. Deze services worden allemaal ondersteund door het Webroot® Threat Intelligence Platform. Voor meer informatie over al deze services gaat u naar www.webroot.com/brightcloud.

Cybercriminelen sturen dynamische, onopvallende bedreigingen de wereld in die zijn ontworpen en die er specifiek op zijn gericht om door de beveiliging heen te komen via meerdere toegangspunten van een netwerk.

De services Webclassificatie en Webreputatie

Webclassificatie biedt contentservices voor meer dan 27 miljard URL's. Dat is meer dan welke service dan ook die vandaag de dag beschikbaar is. Bescherm uw klanten en help ze productief te blijven door schadelijke en ongewenste webcontent te blokkeren op basis van 82 verschillende categorieën.

Webreputatie levert een reputatiescore die een voorspelling doet van het beveiligingsrisico van het bezoeken van een website. Deze score is vergelijkbaar met een kredietwaardigheidsscore die een indicatie geeft van het risico van leningen of investeringen. Bied uw klanten toonaangevende bescherming tegen schadelijke sites door gebruik te maken van risicoscores die onafhankelijk van de contentcategorie worden vastgesteld. Hierdoor kunt u de beveiligingsinstellingen nauwkeurig afstemmen op de unieke behoeften van het bedrijf.

IP-reputatieservice

Deze service biedt een dynamische lijst met 8 tot 12 miljoen schadelijke IP-adressen die op elk moment kan worden toegepast om te voorkomen dat schadelijk verkeer een netwerk binnendringt. Klanten kunnen ook toegang krijgen tot aanvullende intelligence en gebruikmaken van voorspellende risicoscores om de netwerkinstellingen aan te passen op basis van de behoeften en risicotolerantie.

Realtime anti-phishingservice

Deze service, die speciaal is ontwikkeld voor het onderscheppen van geavanceerde phishingaanvallen die een organisatie kunnen blootstellen aan lekken en gegevensverlies, kan bescherming bieden wanneer dat nodig is, doordat deze een realtime scan uitvoert voordat iemand een site bezoekt.

Streaming Malware Detection

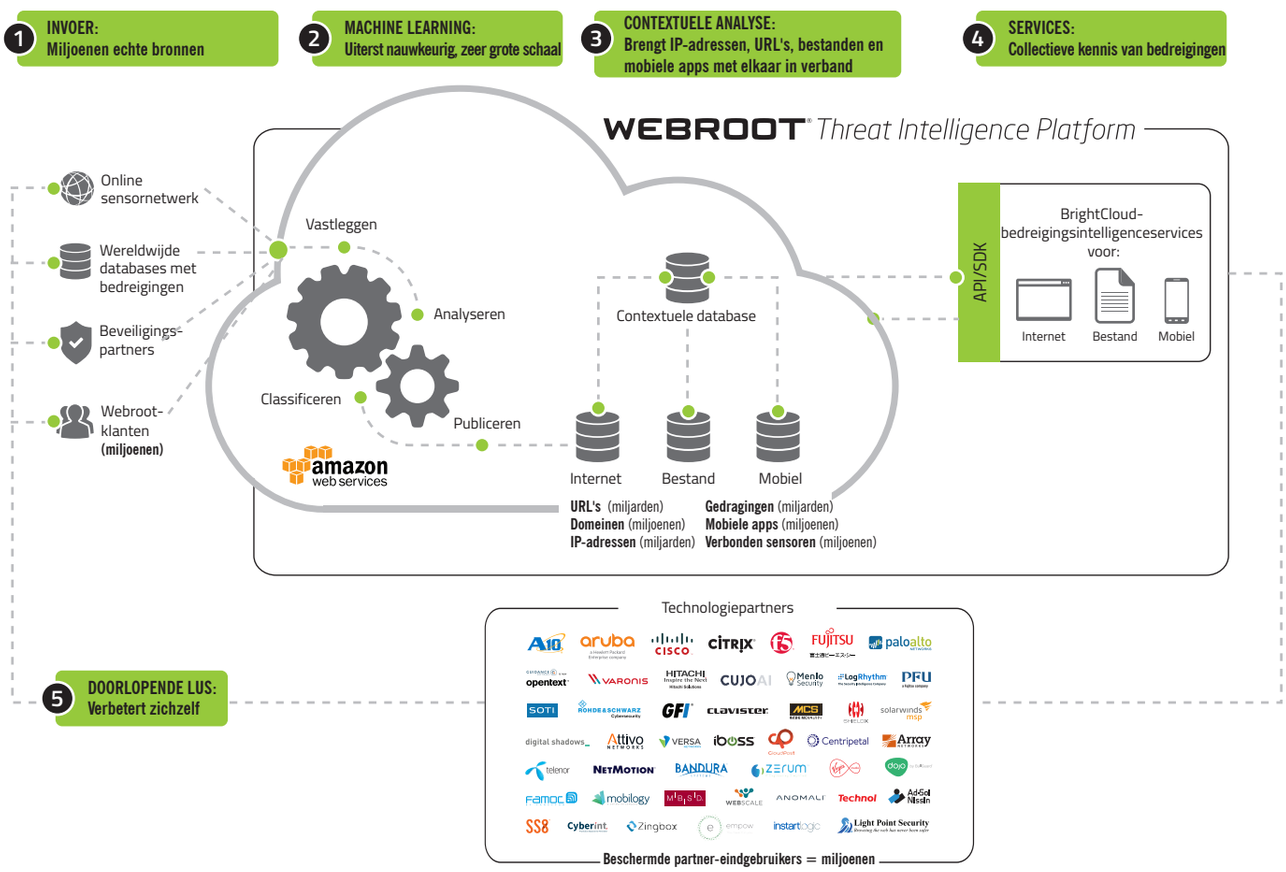
Deze innovatieve technologie, die is ontwikkeld om polymorfe malware te bestrijden, geeft bestanden een risicoscore terwijl die door de buitengrenzen van het netwerk heen komen, wat gebruikers in staat stelt om snel te beslissen of bestanden moeten worden toegelaten of geblokkeerd, of dat ze moeten worden onderzocht.

Bestandsreputatieservice

Een realtime service die continu wordt bijgewerkt en die bekende schadelijke bestanden en bestanden op de witte lijst opspoort. Deze service biedt dynamische informatie over de reputatie van bestanden, waardoor beveiligingsbronnen zich op de meest urgente bedreigingen kunnen richten.

Mobiele beveiligings-SDK

Deze SDK, die eenvoudig in een mobiele applicatie kan worden ingebouwd, biedt toonaangevende bescherming tegen mobiele bedreigingen met behulp van antivirus- en antimalwaretools, ondervraging van apparaten en applicaties, veilig browsen op het web en webclassificatie, samen met risicoscores voor apparaten.



Webroot® Threat Intelligence Platform

2. Slimmere cloudarchitectuur voor inhoud, omvang, nauwkeurigheid en snelheid
De meeste moderne malware wordt met een bepaald doel gemaakt en zodra de missie is volbracht, is de dreiging weg. Traditionele, reactieve beveiliging op basis van lijsten, die werkt door bekende bedreigingen op te merken, is ineffectief bij de bestrijding van geraffineerde aanvallen. Daarom maken de services van BrightCloud gebruik van een proactieve benadering.

Via het Webroot Threat Intelligence Platform worden gegevens van miljoenen sensoren wereldwijd en van eindpunten op echte computers ingevoerd in de cloud, waar ze worden geanalyseerd en met andere gegevenspunten worden gecombineerd, zodat er een uitgebreid beeld ontstaat van het landschap van online bedreigingen. Die informatie wordt dan in realtime beschikbaar voor de rest van het netwerk, zoals voor partners van Webroot, die er toegang toe hebben via de bedreigingsintelligenceservices van BrightCloud. Het Webroot Threat Intelligence Platform beschikt over een onbeperkte omvang, razendsnelle gegevensverwerking en een wereldwijd verspreide databasecluster voor topprestaties en een hoge veerkracht.

3. Gegevenscorrelatie voor contextuele, voorspellende bedreigingsintelligence
De bedreigingsintelligenceservices van BrightCloud maken gebruik van een krachtige contextuele analyse-engine die ongelijksoortige gegevens uit Webroot Threat Intelligence Platform-toevoer haalt en die gegevens met elkaar verbindt, zodat er een diepgaand inzicht ontstaat in het landschap van onderling verbonden URL's, IP-adressen, bestanden en mobiele apps. Door de relaties tussen deze verschillende gegevenspunten in kaart te brengen, kan Webroot zijn partners uiterst nauwkeurige en bruikbare informatie verstrekken, die altijd actueel is. Hierdoor kan Webroot, aan de hand van de connecties van een internetobject met andere URL's, IP-adressen, bestanden en mobiele apps, nauwkeurig voorspellen hoe groot de kans is dat dit object in de toekomst schadelijk wordt. Zo kan een ogenschijnlijk betrouwbaar IP-adres, dat door andere services als veilig wordt bestempeld, connecties te hebben met andere URL's, IP-adressen, bestanden of mobiele apps die in het verleden wel degelijk gevaarlijk zijn gebleken. Onze geavanceerde analyse biedt een voorspellende reputatiescore, die gebruikers in staat stelt om zich proactief te beschermen door middel van beleidsregels die ze zelf hebben gedefinieerd op basis van hun risicotolerantie. Alle bedreigingsintelligenceservices van BrightCloud kunnen deze correlatie-engine gebruiken om gebruikers proactief te beschermen tegen bedreigingen die niet door traditionele technologieën kunnen worden opgespoord.

Voordelen van de BrightCloud-bedreigingsintelligenceservices

» **Geen bedreiging ontkomt aan de bedreigingsintelligence van Webroot**
Webroot evalueert gedragsgegevens en contextuele gegevens voor het categoriseren van en het toekennen van een score aan het risico van bedreigingen die nog niet eerder zijn voorgekomen. Via de BrightCloud-bedreigingsintelligenceservices krijgen partners de inzichten die ze nodig hebben om voor het beveiligen van de netwerken en eindpunten van klanten, en kunnen ze effectieve beleidsregels maken voor het beheren van risicotolerantie en behoeften op het gebied van toegankelijkheid.

» **Wij vinden aanvallen voordat die uw klanten hebben gevonden**
Met miljoenen sensoren die doorlopend gegevens vastleggen, kan het Webroot Threat Intelligence Platform in realtime schadelijke aanvallen analyseren en identificeren. Met de services van BrightCloud hebben onze partners toegang tot deze collectieve kennis van bedreigingen, zodat ze de netwerken en eindpunten van hun klanten kunnen beschermen voordat ze geïnfecteerd raken.

» **Perfecte kennis = superieure bescherming**
De bedreigingsintelligenceservices van BrightCloud maken gebruik van contextuele informatie en gedragsanalyse om zo zelfs de nieuwste malware te snel af te zijn, waardoor de nieuwste generatie bedreigingen al achterhaald is zodra een cyberaanval opduikt in een netwerk of op een apparaat dat is verbonden met het Webroot Threat Intelligence Platform.

» **Beveiliging uit alle bronnen, op alle apparaten**
De zakelijke beveiligingsomgeving wordt bedreigd, zowel van binnenuit als van buitenaf. Door cybercriminelen en Bring Your Own Device (BYOD) wordt het voor beveiligingsbeheerders lastiger om hun netwerken te beschermen. Met hypermoderne oplossingen voor eindpunten, mobiele apparaten en netwerken leveren de bedreigingsintelligenceservices van BrightCloud realtime bedreigingsintelligence om apparaten in alle soorten omgevingen te beschermen.

Flexibele integratieopties

De bedreigingsintelligenceservices van BrightCloud kunnen via de Webroot® software-ontwikkelingskit (software development kit, SDK) en een eenvoudig te gebruiken REST API worden geïntegreerd met bestaande beveiligingsoplossingen. Een service kan, afhankelijk van het type service, op drie manieren worden geïntegreerd (gehost, lokale database of hybride), waardoor partners het type integratie en implementatie kunnen kiezen dat het beste aansluit bij hun behoeften. Op het gegevensoverzicht van iedere service vindt u meer informatie over de integratieopties.

Meer informatie

Voorzie uw beveiligingsoplossingen van de snelheid en nauwkeurigheid die nodig zijn om uw klanten te beschermen tegen een nieuw, geraffineerd soort online bedreigingen. Met de bedreigingsintelligenceservices van BrightCloud kunt u zelfs de nieuwste malware te snel af zijn, waardoor de nieuwste generatie bedreigingen meteen al achterhaald is; kunt u uw klanten in realtime beschermen tegen schadelijke actoren; en kunt u de buitengrenzen van bedrijfsnetwerken, die zich steeds verder uitbreiden, beveiligen met beveiligingsoplossingen voor het web, voor bestanden en voor mobiele apparaten.

Ga naar www.webroot.com/brightcloud voor meer informatie.

Over Webroot

Webroot was het eerste bedrijf dat gebruikmaakte van de cloud en kunstmatige intelligentie om bedrijven en particulieren te beschermen tegen cyberdreigingen. We bieden de beste beveiligingsoplossing voor aanbieders van beheerde diensten en kleine ondernemingen, die op Webroot vertrouwen voor eindpuntbescherming, netwerkbescherming en training over beveiligingsrisico's. De Webroot BrightCloud®-bedreigingsintelligenceservices worden onder andere gebruikt door marktleiders als Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks en A10 Networks. Webroot zet de mogelijkheden van machine learning in om miljoenen bedrijven en particulieren te beschermen, waar ter wereld ze ook verbonden zijn. Webroot heeft een hoofdkantoor in Colorado en is actief in Noord-Amerika, Europa en Azië. Ontdek Smarter Cybersecurity® oplossingen op webroot.com.

Wereldwijd hoofdkantoor
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ierland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australië
+61 (0) 2 8071 1900