Whitepaper

Webbeveiliging: beveilig uw gegevens in de cloud

Overzicht

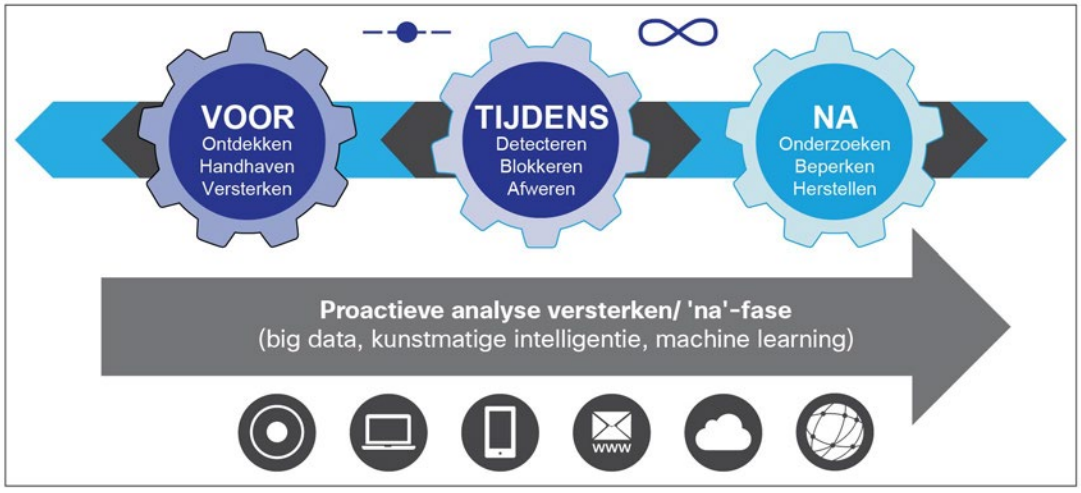
Beveiligingsteams kunnen niet overal zijn, maar het huidige landschap eist dat organisaties hun gegevens overal verdedigen waar een bedreiging kan opduiken. 'Overal' omvat netwerken, mobiele apparaten, virtuele omgevingen en de cloud of het datacenter.

De bedreigingen van vandaag zijn bedoeld om door iedere verdediging heen te dringen. Tegenstanders zijn actief aan het werk om erachter te komen welke soorten beveiliging worden gebruikt. En ze beginnen minder zichtbare, minder detecteerbare gedragspatronen te vertonen. Volgens het **Cisco-beveiligingsrapport 2014** hebben de meeste van deze personen maar één echte missie: het stelen van waardevolle gegevens.[1]

Intussen is door de opkomst van de gedistribueerde onderneming en door het ontstaan van nieuwe bedrijfsmodellen zoals cloudcomputing, mobiliteit en BYOD-omgevingen (Bring-Your-Own-Device) de traditionele beveiligingszone aangetast en het aanvalsoppervlak uitgebreid. Beveiligingsteams kunnen het maar moeizaam bijbenen. Ze weten niet welke bedreigingen ze moeten prioriteren en ze missen veel bedreigingen die ze gewoon niet kunnen zien.

Het is makkelijk te begrijpen waarom preventieve point in time-beveiligingsoplossingen geen voldoende bescherming kunnen bieden aan moderne bedrijven. Natuurlijk is geen enkele detectiemethode perfect, en er zullen altijd bedreigingen blijven die geavanceerd en slinks genoeg zijn om alle verdedigingslagen te passeren. Wat hebben we nodig? Een doorlopende en retrospectieve beveiliging die is ontworpen om het hele aanvalsspectrum te dekken: vóór, tijdens en na een aanval.

Afbeelding 1. Het aanvalsspectrum



[1] Cisco-beveiligingsrapport 2014: http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

Cisco Cloud Web Security Essentials

Cisco® Cloud Web Security (CWS) helpt organisaties bij het handhaven van een doorlopende beveiliging op het uitgebreide netwerk. De oplossing biedt een toonaangevende beveiliging en controle voor gedistribueerde ondernemingen, en het breedste scala aan implementatieopties dat momenteel beschikbaar is. Het Cloud Web Security-platform is een cloudversie van Cisco Web Security dat de webbeveiliging uitbreidt naar mobiele apparaten en gedistribueerde omgevingen. Het beschermt gebruikers via Cisco's informatie over bedreigingen wereldwijd, geavanceerde verdedigingsmogelijkheden en bescherming van mobiele gebruikers.

Cloud Web Security bevat intuïtieve tools om inkomend en uitgaand webbeleid te maken, handhaven en bewaken, waardoor bedrijven volledige controle hebben over de manier waarop eindgebruikers op internet surfen. Kortom, Cloud Web Security biedt een beveiligde zone in de cloud. Hiermee kan beleid op een gedetailleerde, contextgevoelige manier worden beheerd en gehandhaafd. En Cloud Web Security doet nog meer:

- Bedreigingen worden in real-time dynamisch geblokkeerd
- Netwerk en gebruikers worden beschermd tegen ongewenste webinhoud
- Netwerkresources worden geoptimaliseerd door vermindering van overbelaste bandbreedten
- Maakt rapportage en bewaking van online activiteiten mogelijk
- De organisatie wordt beschermd tegen gegevenslekken

Cloud Web Security kan worden geïntegreerd met Cisco-firewalls, vestigingsrouters en clientsoftware om overal bescherming te bieden waar gebruikers aan het werk zijn. Al het verkeer (vanuit het hoofdkantoor of vanuit nevenvestigingen, of van mobiele of externe gebruikers) wordt gerouteerd via een wereldwijd netwerk van datacenters. Cloud Web Security elimineert backhaul, versnelt de implementatie van webbeveiliging en helpt de waarde van bestaande Cisco-investeringen vergroten.

Met de recente acquisities van de beveiligingsbedrijven Sourcefire en Cognitive Security kan Cisco nu een verbeterde versie van Cloud Web Security bieden om geavanceerde malwarebedreigingen te blokkeren, vooral in de 'na'-fase van het aanvalsspectrum, en om real-time bedreigingsdetectie in de 'tijdens'-fase te verbeteren. Cisco biedt deze oplossing in een optioneel Premium-abonnement dat hieronder wordt beschreven.

Cloud Web Security Premium

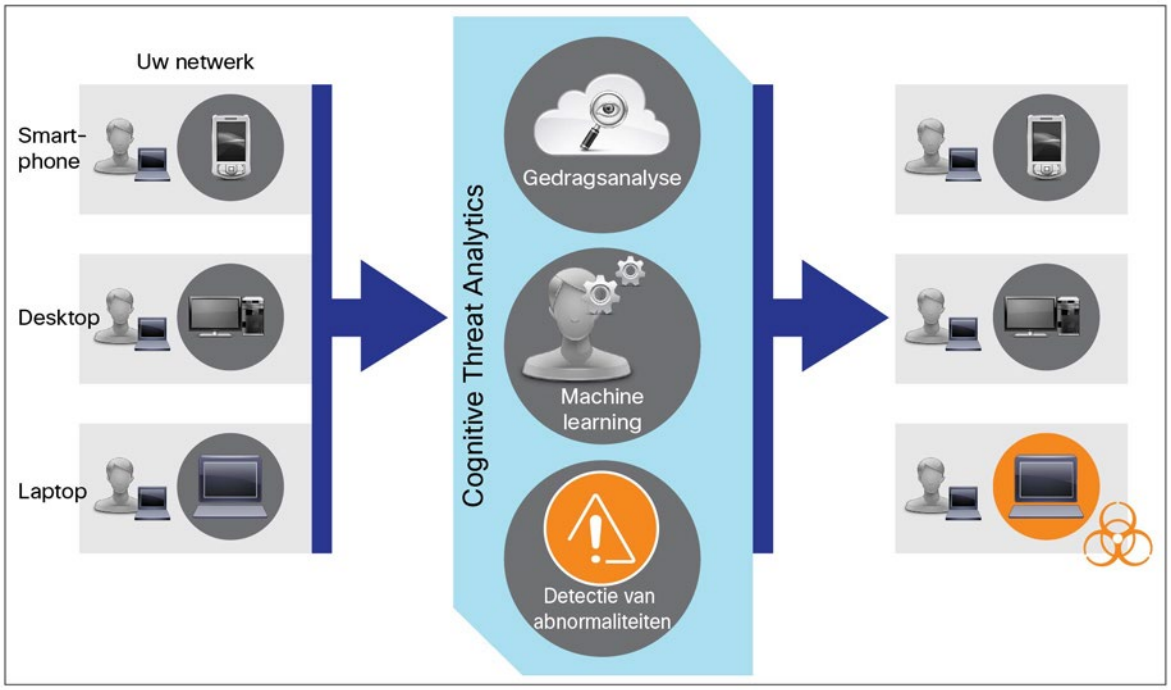
The Premium bundle of Cloud Web Security heeft alle functies van de Essentials-bundel, maar het bevat ook twee innovatieve malwaredetectiesystemen: Cognitive Threat Analytics (CTA) en Advanced Malware Protection (AMP). Met deze systemen wordt het zoeken naar zeer risicovolle bedreigingen in het webverkeer van een organisatie geautomatiseerd. Cloud Web Security Premium biedt extra point in time-bescherming, retrospectieve beveiliging en doorlopende analyse om organisaties te helpen bij het vinden en afhandelen van de belangrijkste bedreigingen. Het systeem verkort ook de tijd tot de detectie van bedreigingen die al actief zijn in hun netwerken.

Beveiligingsteams kunnen nu een doorlopende webbeveiliging bieden die systemen over het hele aanvalsspectrum beschermt. Hier volgt nadere informatie over deze twee malwaredetectiesystemen.

Cognitive Threat Analytics

Cognitive Threat Analytics, of CTA, ontwikkeld door Cognitive Security, is een near-real-time analysesysteem voor netwerkgedrag. Het maakt gebruik van machine learning en geavanceerde statistieken om ongewone activiteiten in een netwerk te signaleren: de symptomen van een infectie. De oplossing is niet afhankelijk van regelsets, waardoor geen menselijke interventie nodig is om de technologie af te stellen. Zodra CTA is ingeschakeld, begint het systeem direct naar bedreigingen te zoeken. Gegevens worden in de cloud gecorreleerd om de snelheid, flexibiliteit en diepte van het CTA-detectievermogen van afwijkingen te versterken.

Afbeelding 2. Overzicht van CTA



CTA leert van wat het tegenkomt. Het past zich in de loop van de tijd aan en identificeert nieuwe command and control-kanalen die niet eerder door de beveiligingsindustrie zijn ontdekt. Het systeem beoordeelt het gedrag van entiteiten (zoals individuele gebruikers) in het netwerk en gebruikt gedragsmodellering om te voorspellen hoe deze entiteiten zich zouden moeten gedragen. CTA gebruikt langetermijnmodellering van netwerkgedrag om kennelijk ongerelateerde activiteiten te correleren. Vervolgens worden deze gecorreleerde gegevens vergeleken met het gedrag van individuele gebruikers in het specifieke klantnetwerk, zodat bedreigingen sneller kunnen worden gedetecteerd.

Het maakt niet uit om welke gedetecteerde bedreiging het gaat. Als er een significante of aanhoudende discrepantie in verwacht gedrag bestaat, zal CTA dat aangeven. De acties van CTA lijken op die van een beveiligingsteam dat een winkeldief probeert op te merken voordat deze de kans heeft gehad om iets te stelen: doet deze persoon iets dat afwijkt van wat andere winkelende personen doen? Draagt hij een grote tas in plaats van een winkelwagen te duwen? Probeert hij de achteruitgang te nemen in plaats van de voordeur? Ook als het verdachte gedrag in orde blijkt te zijn, is het toch de moeite van een onderzoek waard.

CTA ontdekt afwijkingen en stuurt beveiligingsanalisten naar potentiële problemen. Dat vermindert hun werklast en helpt bij de prioritering van bedreigingen. Het is ook een aanvulling op bestaande beveiligingstechnologie van Cisco. De bestaande oplossingen worden nauwkeuriger en zijn beter in staat om onbekend of ongewoon gedrag in het netwerk te detecteren. De beveiligingsmogelijkheden van Cisco worden daarmee uitgebreid tot in de 'na'-fase van het aanvalsspectrum. En het belangrijkste is: CTA biedt een beveiliging die zich ontwikkelt in overeenstemming met het steeds veranderende landschap van bedreigingen.

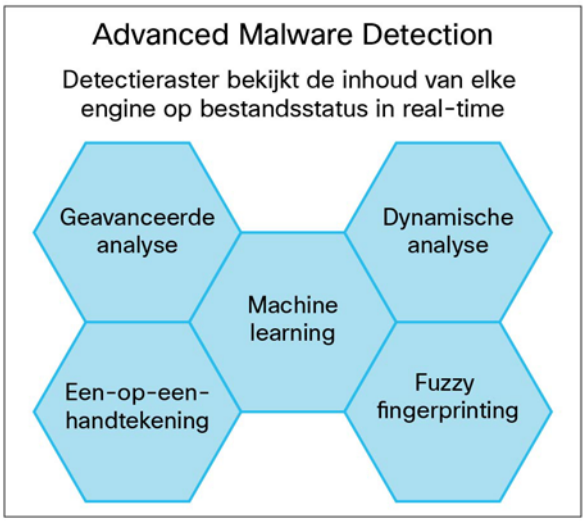
Advanced Malware Protection

Het tweede detectiesysteem in Cloud Web Security Premium is Advanced Malware Protection (AMP) van Sourcefire. AMP is niet afhankelijk van malwarehandtekeningen: het kan weken of maanden duren voordat die zijn gemaakt voor elk nieuw stukje malware. In plaats daarvan wordt gebruikgemaakt van een combinatie van bestandsreputatie, bestandssandboxing en retrospectieve bestandsanalyse om bedreigingen in het hele aanvalsspectrum te vinden en stop te zetten.

Bestandsreputatie

Bij bestandsreputatie kan worden gekeken naar databases van bestanden om te bepalen of een bestand 'schoon' is, of het bekendstaat als malware, of onbekend is. AMP legt een 'vingerafdruk' vast van elk bestand dat de Cloud Web Security-service passeert en doorzoekt het collectieve cloudinformatienetwerk van Cisco en Sourcefire om een reputatieoordeel of een 'score' te krijgen. Aan de hand van deze resultaten kan AMP vervolgens kwaadaardige bestanden automatisch blokkeren en beleidsregels toepassen die door beheerders zijn gedefinieerd. In afbeelding 3 ziet u de verschillende engines in real time aan het werk om geavanceerde malware te detecteren en bestandsreputaties vast te stellen.

Afbeelding 3. Advanced Malware Protection



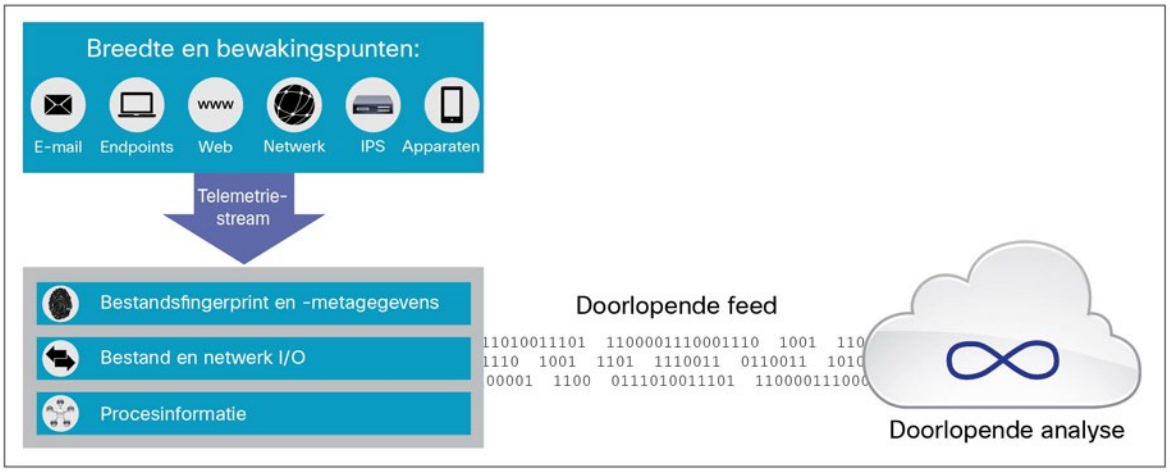
Bestandssandboxing

Bestandssandboxing is een essentiële functie van AMP, en uiteindelijk ook van Cloud Web Security Premium. Met bestandssandboxing analyseert AMP de onbekende bestanden die het netwerk passeren. In een sterk beveiligde sandboxomgeving verzamelt AMP exacte details over het gedrag van een bestand en combineert deze gegevens met een gedetailleerde menselijke en machineanalyse om het bedreigingsniveau van het bestand te bepalen. Deze informatie wordt vervolgens ingevoerd in het collectieve cloudinformatienetwerk van Cisco en Sourcefire en wordt gebruikt voor een dynamische update van de AMP-cloudgegevensset. Met actieve rapportage kunnen beveiligingsteams eenvoudig te lezen rapporten vol gegevens bekijken over de geanalyseerde bestanden.

Bestandsretrospectie

De retrospectieve analysefuncties zijn misschien wel het belangrijkste kenmerk van AMP. Daarmee kunnen organisaties teruggaan in de tijd om vast te stellen wanneer een uitbraak is opgetreden, en daarna de schade taxeren. Bestandsretrospectie biedt een doorlopende analyse van bestanden die de beveiligingsgateway zijn gepasseerd, met real-time-updates van het cloudinformatienetwerk van Cisco en Sourcefire.

Afbeelding 4. Het retrospectieve analyseproces van AMP

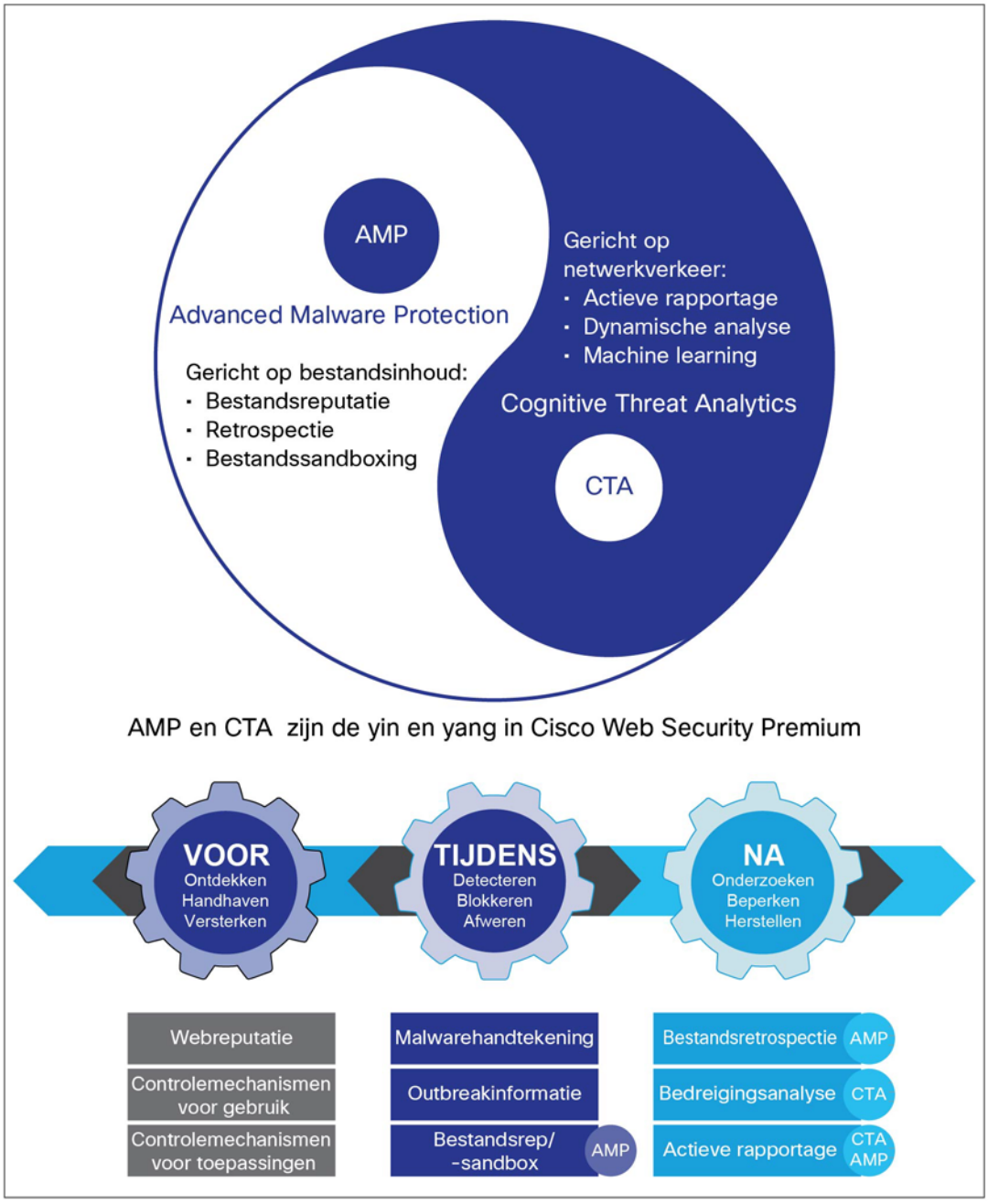


Soms laat een retrospectieve analyse zien dat een bestand dat als 'schoon' werd bestempeld tijdens het passeren van een verdediging aan de rand, in werkelijkheid toch goed vermomde, geavanceerde malware is. AMP zal de beveiligingsbeheerder onmiddellijk waarschuwen en uitzoeken welke netwerkgebruiker was geïnfecteerd en wanneer. Beveiligingsteams kunnen de aanval snel aanpakken voordat deze zich kan verspreiden.

Conclusie

Cloud Web Security Premium met CTA en AMP is afgestemd op de strategie van Cisco om organisaties te helpen bij de aanpak van bekende en nieuwe beveiligingsproblemen. Het systeem helpt de bedreigingen te detecteren, te begrijpen en stop te zetten. De cloud levert doorlopende analyse en beveiligingsinformatie in real-time. Deze worden gedeeld met alle beveiligingsoplossingen om hun effectiviteit te vergroten. De combinatie van deze drie oplossingen helpt organisaties bij het identificeren van nieuwe command and control-kanalen die niet eerder door de industrie zijn gedetecteerd, en bij de aanpak van beveiligingsproblemen in het hele aanvalsspectrum.

Afbeelding 5. Cloud Web Security met AMP en CTA: Beveiliging in het hele aanvalsspectrum



Vóór: ontdekken, handhaven, versterken

Cloud Web Security levert webreputatie, controlemechanismen voor gebruik en toepassingen (ook microtoepassingen), malwarehandtekeningen en uitbraakinformatie om beveiliging te bieden vóór en tijdens een aanval.

Tijdens: detecteren, blokkeren, afweren

AMP verbetert de beveiliging in de 'tijdens'-fase van het aanvalsspectrum met zijn functies voor bestandsreputatie en bestandssandboxing. Het systeem blokkeert automatisch kwaadaardige bestanden en past door beheerders gedefinieerde beleidsregels toe op basis van de reputatie van een bestand. Het analyseert ook onbekende bestanden die het netwerk passeren en werkt de bedreigingsinformatie dienovereenkomstig bij. Deze functies helpen beveiligingsanalisten bij de prioritering van bedreigingen die moeten worden onderzocht.

Na: onderzoeken, beperken, herstellen

Zowel CTA als AMP bieden een doorlopende analyse en herstel in de cruciale 'na'-fase van het aanvalsspectrum. CTA biedt analyse van netwerkgedrag in real-time om afwijkend gedrag in het netwerk te identificeren. Intussen pakt de bestandsretrospectie van AMP het probleem aan van kwaadaardige bestanden die de verdediging aan de rand weten te passeren. De actieve rapportage van AMP maakt de reputatie en het gedrag zichtbaar van bestanden die het netwerk zijn binnengekomen. Beveiligingsteams kunnen aanvallen gemakkelijker opsporen en de omvang vaststellen, en voor een sneller herstel zorgen.

Vervolgens wordt machine learning bij CTA en AMP in de 'na'-fase gebruikt om de near-real-timedetectie te verbeteren die Cloud Web Security Premium tijdens een aanval toepast.

Meer informatie

Ga voor meer informatie over Cisco Cloud Web Security Essentials en Cloud Web Security Premium naar http://www.cisco.com/go/cws.

Ga voor meer informatie over CTA naar http://www.cisco.com/go/cognitive.

Ga voor meer informatie over AMP naar http://www.cisco.com/go/amp.

Hoofdkantoor Amerika
Cisco Systems, Inc.
San Jose, CA

Hoofdkantoor Zuidoost-Azië
Cisco Systems (USA) Pte, Ltd.
Singapore

Hoofdkantoor Europa
Cisco Systems International BV Amsterdam.
Nederland

Cisco beschikt wereldwijd over meer dan 200 kantoren. Adressen, telefoonnummers en faxnummers vindt u op de Cisco-website op **www.cisco.com/go/offices**.

Gedrukt in de VS C11-734836-00 06/15