Whitepaper

Detailhandelbeveiliging: Klantgegevens beschermen en geld en tijd besparen

Overzicht

IT-omgevingen voor detailhandel hebben te maken met een ongekend niveau van technologische veranderingen. Aan winkels worden meer eisen gesteld en de klanten verwachten zowel goede prestaties als veiligheid wanneer ze de in-storeservices gebruiken. Detailhandelorganisaties hebben ook te maken met georganiseerde en van geld voorziene hackers die misbruik maken van alle zwakke plekken in netwerken en verkooppuntsystemen (POS, Point-Of-Sale). Het ongelukkige resultaat van veel aanvallen is diefstal van creditcard- en andere klantgegevens.

In deze whitepaper vindt u een overzicht van de problemen waar detailhandelnetwerken mee te maken hebben, en een beschrijving van een Cisco®-beveiligingsoplossing die een effectieve, actuele en betrouwbare bescherming biedt: Cisco Cloud Web Security (CWS).

Bedreigingen voor IT-omgevingen in de detailhandel nemen toe

In-storenetwerken ophogen naar de vereiste prestaties en beveiliging is geen kleinigheid. Van eenvoudige controle over in-store-internettoegang tot aan de complexe nalevingsvereisten van de PCI DSS (Payment Card Industry Data Security Standard): detailhandelsorganisaties moeten proactief nadenken over hun controle op netwerkverkeer. Een effectieve beveiliging moet twee dingen doen: netwerkbeheer bieden en zich tegelijk aanpassen aan de toenemende snelheid waarmee in-storenetwerken veranderen. Het allerbelangrijkste is aanpassing aan de toenemende complexiteit van de bedreigingen.

Het aantal grootschalige aanvallen en inbraken in IT-omgevingen in de detailhandel blijft toenemen, ondanks alle inspanningen van experts in de industrie en de beveiliging. Slachtoffers vallen onder zowel Fortune 10-retailers als wereldwijde franchiserestaurants (afbeelding 1). Aanvallers hebben het altijd voorzien op de betalingssystemen. Deze inbraken hebben geleid tot schade aan bedrijfsmerken en klantvertrouwen, en ook tot schadebeperkingen en restituties die kunnen oplopen tot honderden miljoenen dollars.

Afbeelding 1. De grootste gegevensinbraken in de Amerikaanse geschiedenis (op basis van kosten)

Bronnen: Bloomberg, Privacy Rights Clearinghouse, Breach Level Index

Ervaringen met in-store-WiFi voor bezoekers en interactief mobiel winkelen hebben geleid tot steeds meer nieuwe aanbiedingen zoals winkel-apps en in-storenetwerktoegang. Deze in-storeservices bieden een aantoonbare meerwaarde voor klanten, maar ze vergroten ook de complexiteit van winkelnetwerken en leggen meer druk op bestaande IT-resources. De onlineservices zorgen voor een uitbreiding van het aanvalsoppervlak, waardoor bedrijven kwetsbaarder zijn voor degenen die op zoek zijn naar zwakke plekken in netwerken om van te profiteren. Daarom is het voor retailers belangrijk dat ze investeren in de beveiliging van klantgegevens, zowel in winkels als op hoofdkantoren.

Een andere IT-trend waar retailers mee te maken krijgen, is het IoT (Internet of Things). Het IoT is een netwerk van fysieke objecten dat in verbinding staat met internet via ingebedde technologie, en dat interactie heeft met het interne netwerk en de externe omgeving. Een retailer kan bijvoorbeeld relevante realtimegegevens over producten doorgeven aan mobiele apparaten van geïnteresseerde klanten op basis van contextuele klantgegevens die is verzameld aan de hand van promotiemateriaal in de winkel.

Andere IoT-bedrijfstoepassingen zijn het traceren van inkomende voorraad in real time door het gebruik van RF-labels, of het bieden van toegang tot toeleveringsketens aan leveranciers via interne systemen en gegevens om de processen sneller te laten verlopen. De vele apparaten in het IoT verhoogt het aantal kritieke technologieën binnen de winkel zelf. In veel gevallen is in deze apparaten geen beveiliging ingebouwd; die wordt pas naderhand toegevoegd.

Door de beperkte winstmarges in de detailhandel staan organisaties voor een harde realiteit: ze moeten de steeds verder ontwikkelende bedreigingen aanpakken en tegelijk zorgen voor innovatieve, persoonlijke winkelervaringen voor klanten. Het wordt steeds belangrijker om verkooppuntsystemen bij te werken of om te investeren in beveiligingstechnologieën om de risico's op gegevensverlies te beperken. De detailhandelindustrie ziet niet werkeloos toe bij de groeiende dreigingen. Organisaties hebben zich onlangs verzameld voor de ontwikkeling van het R-CISC-initiatief (Retail Cyber Intelligence Sharing Center).

De zwakke plek in de detailhandel

In 2013 stonden detailhandelorganisaties en restaurants op de tweede plaats in de lijst van vaakst aangevallen instanties, volgens het Verizon Data Breach Investigations-rapport van 2013. Uit een rapport van Retail News Insider in 2014 blijkt dat, zelfs als klanten blijven winkelen bij een retailer die is aangevallen, ze vaker contant geld gaan gebruiken in plaats van creditcards, waardoor ze minder uitgeven.

Volgens een rapport in 2014 van Interactions Consumer Experience Marketing zijn er bewijzen dat aanvallers niet zo creatief zijn als ze het gemunt hebben op detailhandelorganisaties. 'Vergeleken bij andere industrieën gebruiken aanvallers relatief weinig verschillende methoden om gegevens te verkrijgen bij het aanvallen van detailhandelorganisaties', zo bleek. Bij detailhandelaanvallen werd in 97 procent van de gevallen met het betalingssysteem geknoeid.

Detailhandelorganisaties staan voor een grote uitdaging bij het detecteren van beveiligingsinbraken. Meestal verblijft kwaadaardige malware in de IT-omgeving van detailhandels totdat een derde partij (meestal politie of fraude-inspectie) aanwijzingen vindt van ongewone activiteiten. Volgens een driejarig onderzoek door Verizon Enterprise Solutions, geciteerd in een artikel van Bloomberg Businessweek uit 2014, ontdekken bedrijven inbraken maar in 31 procent van de gevallen aan de hand van hun eigen bewaking. Voor retailers is dat 5 procent.

In tabel 1 ziet u vier voorbeelden van de grootste inbraken die in 2014 zijn gemeld, samen met hoeveel tijd de malware zich in de IT-omgeving bevond voordat die werd ontdekt.

Tabel 1. Kenmerken van de grootste netwerkinbraken in 2014

Aanval	Tijdsduur	Aanvalsmethode	PoF (Point of Failure)
Amerikaans drankbedrijf	17 maanden	'Low-and-slow'-malware	Technologie
Amerikaanse en Canadese hobbywinkelketen	8 tot 9 maanden	Aangepaste verkooppuntsystemen	Processen
Amerikaanse en Canadese woonwinkelketen	6 maanden	Aangepaste malware voor het ontwijken van detectie en het aanvallen van registers	Beveiliging geen prioriteit; ongebruikte productkenmerken
Online detailhandeluitwisseling	3 maanden	Gehackte database	Mensen en technologie

Bronnen: Sophos, Bank Information Security, Krebs on Security, Bloomberg News, Private WiFi.com en de Huffington Post

Mogelijkheden en functionele IT-eisen nemen toe

De IT-netwerkomgevingen van detailhandels worden ingewikkelder. En ze worden steeds ingewikkelder te beheren. In de IT-industrie neemt het tekort aan expertise toe, waardoor het nog moeilijker wordt om deze in-store, met internet verbonden omgevingen te hanteren. Om deze schaarste te bestrijden, vooral in de cyberbeveiliging, centraliseren IT-groepen het beheer en de bediening van de IT-omgeving van detailhandels.

Een van de lastigste en meest ingewikkelde gebieden betreft in-storenetwerken die eerst worden gebruikt om verkooppuntaansluitingen te verbinden met back-endservers en het bedrijfs-WAN. Deze in-storenetwerken, die voor weinig verkeer zijn bedoeld, moeten nu allerlei andere toepassingen hanteren zoals marketing, intranet- en internettoegang voor werknemers, IoT-gebruik, alarm- en videobewakingssystemen en Wi-Fi voor bezoekers.

Er komt steeds meer noodzakelijke technologie online voor retailers die voor klanten heel handig zijn, waardoor het 'must-haves' worden die retailers in hun winkels moeten gebruiken. Tegelijk vragen deze oplossingen meer bandbreedte en meer gegevensverwerking. Wat de zaken nog lastiger maakt, is dat de bandbreedte-eisen per faciliteit verschillen en dus moeilijk te voorspellen zijn. Deze eisen zijn niet alleen afhankelijk van de grootte van elke winkel, maar ook van het gebruik van de diverse technologieën.

Het beveiligingsmodel van de meeste in-storenetwerken is oorspronkelijk gebouwd voor de bescherming van intern netwerkverkeer. Winkels ondersteunen nu communicatie buiten het thuisnetwerk, waaronder verbindingen met bedrijfspartners, leveranciers en internet.

Voor een afdoende beveiliging moeten organisaties nieuwe preventieve en detecterende controlemiddelen implementeren in in-storenetwerken voor een meer geavanceerde segregatie op netwerkniveau van apparaten en gebruikers, geavanceerd netwerkgebruiksbeheer, en een beleid voor acceptabel gebruik. Gegeven de soorten malware en aanvallen in de detailhandel is het duidelijk dat alle apparaten die verbinding hebben met detailhandelnetwerken, in een vijandige omgeving verkeren.

Hoe kan deze bedreigende omgeving worden gedefinieerd? Ten eerste richten aanvallers zich op het pad van de minste weerstand om in een omgeving voet aan de grond te krijgen. Meestal betekent dit dat ze zich richten op verkooppuntterminals. Helaas bevatten de meeste toonaangevende verkooppuntsystemen standaard hardware, besturingssystemen en softwareonderdelen die met simpele aanvallen makkelijk kunnen worden binnengedrongen. Ook als de verkooppuntleveranciers de systemen goed updaten, blijft het bijwerken van honderdduizenden apparaten een dure aangelegenheid die vaak handmatig moet gebeuren.

De traditionele verbindingen van verkooppuntsystemen met het openbare internet vormen een groot risico. Zo'n opzet maakt externe bediening mogelijk wanneer de back-endsystemen van verkooppunten zich in een andere faciliteit bevinden en waar externe ondersteuning kan worden gegeven. Maar operationele groepen moeten kiezen tussen een gestroomlijnd beheer van hun apparaten en het verlagen van de risico's van netwerkaanvallen. Dit is geen eerlijke of noodzakelijke afweging.

Voor traditionele webbeveiligingsgateways moet een gecentraliseerde gateway worden geïnstalleerd in het hoofdkantoor. Elke winkel of nevenvestiging stuurt al zijn verkeer door naar het centrale verzamelpunt voor inspectie voordat het naar internet gaat. Met het toenemende verkeer (inkomend en uitgaand) in winkels verbruikt deze aanpak een groot deel van de beperkte bandbreedte. Ook naleving is een belangrijke overweging, omdat detailhandel-IT onder de PCI DSS valt. Als organisaties willen voldoen aan de voorschriften en door de jaarlijkse controles willen komen, moeten ze proactieve netwerkcontroles implementeren om verbindingen te beveiligen en te zorgen voor doorlopende beveiliging van systemen waarmee kaartgegevens worden verwerkt.

Kortom: in-storenetwerken zijn meestal uitsluitend gebouwd met het doel om verkooppuntsystemen te verbinden met het bedrijfs-WAN. Deze oplossingen werden doorgaans gebruikt binnen de beveiligingsgrens van de organisatie. De recente beveiligingsinbraken in detailhandels met als doel de verkooppuntsystemen laten zien dat deze netwerkarchitectuur niet meer geschikt is voor het bouwen of gebruiken van in-storenetwerken.

Gebruikelijke lekken in IT-omgevingen

Vanwege de tijdskritieke druk op retailers om iets te doen aan beveiligingsproblemen gaan detailhandels er meestal van uit dat een deeloplossing belangrijke materialen zal beschermen. Maar een samenhangend beveiligingsmodel moet meer bieden dan een deeloplossing. Het moet voldoende netwerkbeveiligingscontroles implementeren om tegemoet te komen aan de problemen van vandaag en de eisen van morgen.

Het verschil tussen een deeloplossing en een uitgebreide beveiligingsoplossing is te zien aan de implementatie van directe internetverbinding met de winkels. Als een directe internetverbinding wordt geïmplementeerd, wordt een nieuwe firewall toegevoegd om het winkelnetwerk te beveiligen. De firewall wordt in een van de twee modellen geïmplementeerd.

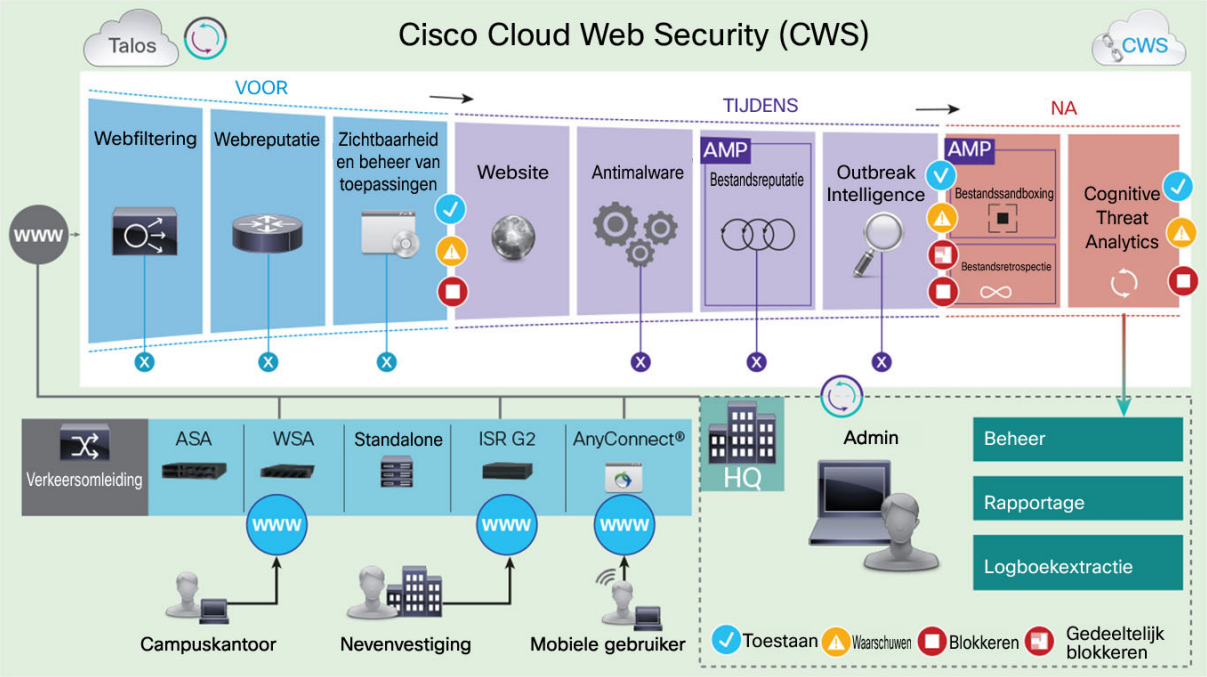
1. Er kunnen regels worden ingesteld in de WAN-router om verkeer naar internet naar de nieuwe firewall te leiden.
2. De in-storenetwerkapparaten kunnen de firewall gebruiken als standaardgateway, waardoor de controle of bewaking van het netwerk wordt verplaatst. Als er een in-store-WiFi-verbinding wordt geïmplementeerd, en als het verkeer niet goed naar een inspectiepunt wordt gerouteerd, kan niet worden gegarandeerd dat er geen bedrijfsgegevens naar het internet lekken. Bovendien is het niet zeker dat het beleid voor acceptabel gebruik altijd wordt gevolgd.

Alles bij elkaar leidt een lappendeken van deelproducten tot een situatie waarin het echte risico voor de organisatie niet gemakkelijk kan worden bewaakt, gezien of beheerd.

De bedreigingen voor retailers zijn al jaren in het nieuws, zoals de grote detailhandelinbraak in 2006 waarbij de gegevens van een miljoen creditcards in gevaar kwamen. Hackers gebruikten de zwakke controlepunten in de winkels om toegang te krijgen tot creditcardgegevens en andere klantgegevens. Als aanvallers eenmaal een zwakke plek hebben gevonden, kunnen ze zich zijwaarts bewegen door bedrijfsnetwerken en toegang krijgen tot steeds meer privégegevens.

Hackers kunnen aanvalstactieken delen en automatiseren; ze richten zich op grote bedrijven via de zwakste schakel in de keten, vaak een detailhandelslocatie met controles die onder de maat zijn.

Afbeelding 2. Hoe Cisco Cloud Web Security werkt



Flexibele bescherming en bewaking

Cisco heeft een serie producten en functies ontwikkeld die geschikt zijn voor de behoeften van beveiliging en netwerken van IT-omgevingen in de detailhandel. Deze oplossingen variëren van draadloze access points, routering en switching tot geavanceerde cloudbeveiligingsservices.

In afbeelding 3 ziet u een overzicht van de opties voor de aanschaf van Cisco CWS.

Afbeelding 3. Cisco CWS-aanschafopties

Web Security Essentials	Web Security Premium	Geavanceerde bedreigingsdetectiebundel	à la carte
	Cognitive Threat Analytics Adv.Malware Protection	Cognitive Threat Analytics Adv.Malware Protection	AMP Logboekextractie
Webfiltering (URL) Malwarescanning AnyConnect Mobility	Webfiltering (URL) Malwarescanning AnyConnect Mobility		

De toonaangevende producten Cisco Web Security Appliance (WSA) Cisco Cloud Web Security (CWS) bieden flexibele implementatiemodellen voor inhoudbeveiliging zowel op locatie als vanuit de cloud. Als u Cisco WSA kiest voor netwerkbeveiliging op het hoofdkantoor en tegelijk Cisco CWS voor nevenvestigingen, voldoet u aan de IT-beveiligingseisen zonder dat u nieuwe hardware hoeft aan te schaffen voor alle nevenvestigingen voor betere beveiliging. Door zijn directe integratie met in-storetechnologieën, waaronder Cisco Adaptive Security Appliance-firewalls (ASA),

Cisco Integrated Services Routers (ISR's) en de Cisco AnyConnect®-client, kunt u met Cisco CWS bestaande investeringen en operationele ondersteuningsprocessen gebruiken voor meer beveiliging en een efficiëntere operationele ondersteuning.

Cisco verplaatst de bescherming van internetverbindingen naar winkelniveau zonder dat er extra hardware nodig is, waarbij backhaulingverkeer alleen nodig is wanneer het beleid daarom vraagt. Verkeer met laag risico gaat direct naar internet, terwijl ander verkeer naar de centrale locatie wordt gestuurd voor verdere inspectie.

Voor bescherming tegen zowel bekende als nieuwe bedreigingen zoekt Cisco CWS naar aanvallen met behulp van diverse technieken, waaronder traditionele malwarehandtekeningen, maar ook bestands- en sitereputatiefilters en outbreakfilters. Daarnaast integreert Cisco CWS met de Cisco Collective Security Intelligence (CSI), de toonaangevende bedreigingsinformatie van Cisco, waaronder de Talos-beveiligingsinformatie en -onderzoeksgroep. Cisco CSI en Talos zorgen ervoor dat klanten profiteren van de tientallen duizenden klanten die gebruikmaken van Cisco-technologie.

Cisco CWS biedt rapportagedetails met traditionele informatiebeveiligingsgegevens, naast een gedetailleerde analyse van bandbreedteverbruik en -gebruik. In omgevingen met een beperkte bandbreedte is deze zichtbaarheid essentieel voor efficiënte prestaties. Een andere geavanceerde rapportagefunctie biedt WiFi-surfgewoonten van bezoekers. Dit betekent zichtbaarheid van en bescherming tegen vergelijkend winkelen en prijscontroles met onlineretailers, en tevens het bekijken van aanstootgevende inhoud. De rapportagefuncties van Cisco CWS zijn dus niet alleen waardevol voor het IT-beveiligingsteam, maar voor de hele detailhandelorganisatie.

En misschien nog belangrijker: als cloudoplossing biedt Cisco CWS (afbeelding 2) eenvoudige schaling en optimalisatie van bandbreedte voor iedere organisatie. Dit betekent een directe, kwantificeerbare kostenbesparing en een drastische verbetering van de effectiviteit van het in-storebedreigingsbeheer van een organisatie. Deze besparingen worden bereikt door alle verwerking van verkeersbeheer en controle te verplaatsen van lokale hardware naar cloudsystemen. Door het gebruik van een SaaS-model (Software-as-a-Service) voor het leveren van beleidsbeslissingen over verkeer zorgt Cisco CWS bovendien voor een aanzienlijke lastverlaging van de in-storenetwerkhardware.

Hoe Cisco CWS een detailhandelorganisatie van dienst kan zijn

Dit levensechte voorbeeld laat zien hoe Cisco CWS een detailhandelorganisatie kan beschermen tegen de bedreigingen van vandaag: een IT-beveiligingsbeheerder heeft opdracht gekregen om een keten met 1500 winkels te beveiligen die bezig is met het uitrollen van in-storetechnologie voor internettoegang voor klanten, samen met een aantal andere services. De beveiligingsbeheerder is op de hoogte van de recente hausse aan geavanceerde malwareaanvallen op in-storesystemen (waaronder verkooppuntapparaten), en wil dat deze aanvallen snel worden gedetecteerd en effectief worden opgelost. Wat de zaken nog lastiger maakt, is dat veel winkels een beperkte bandbreedte hebben, en de oplossing moet de netwerkverbindingen met elke winkel optimaliseren.

De beveiligingsbeheerder implementeert Cisco ISR-edgerouters in elke winkel. Deze apparaten ondersteunen de functies van Cisco Intelligent WAN (IWAN) om de bandbreedte van elke winkel te beschermen en te optimaliseren. IWAN kan de bandbreedte helpen beheren door het gebruik van goedkopere internetverbindingen, in tegenstelling tot duurdere privénetwerkkoppelingen. Het product biedt ook een elegant migratiepad waardoor de organisatie in kalm tempo kan migreren vanuit de privénetwerkkoppelingen. De Cisco Identity Services Engine (ISE) beschermt de in-storesystemen door vast te stellen welke gebruikers en apparaten toegang hebben tot welke delen van winkelnetwerken: daardoor maken mobiele apparaten in elke winkel gebruik van het juiste netwerk.

Voor het beschermen van webverkeer gebruikt de organisatie Cisco CWS Premium voor directe internettoegang, dat kan worden geïmplementeerd via de Cisco ISR-edgerouters zonder dat extra hardware nodig is. Cisco CWS Premium bevat Cisco Advanced Malware Protection (AMP) en Cognitive Threat Analytics (CTA) ter bescherming van alle gebruikers via geavanceerde verdedigingsmogelijkheden. CTA is een near-realtimeanalysesysteem voor netwerkgedrag dat gebruikmaakt van machine learning en geavanceerde statistieken voor de identificatie van ongewone activiteit op een netwerk om mogelijke aanvallen te detecteren. AMP maakt gebruik van een combinatie van bestandsreputatie, bestandssandboxing en retrospectieve bestandsanalyse voor het identificeren en stopzetten van bedreigingen die al in het netwerk aanwezig zijn.

Dankzij deze Cisco-beveiligingsproducten kan deze keten van 1500 winkels nu zijn bandbreedtegebruik, toegangsniveaus voor gebruikers, verdediging en inhoudsbeveiliging beheren. Dit is maar één mogelijke combinatie van Cisco-beveiligingsproducten. In dit geval bereikt de IT-beveiligingsbeheerder de netwerk- en beveiligingsdoelen voor het gedistribueerde detailhandelnetwerk van het bedrijf.

Voordelen van Cisco CWS

Een organisatie die de geïntegreerde Cisco-oplossing gebruikt om zijn netwerken te beschermen, kan een gemeenschappelijk beleid opleggen, geavanceerde aanvallen detecteren en het bandbreedtegebruik op het WAN optimaliseren. Cisco CWS Premium, geïntegreerd met de Cisco ISR-edgerouters, maakt eveneens botnettracering mogelijk. Dit zorgt ervoor dat verkooppuntapparaten niet worden aangevallen en hun gegevens veilig naar het hoofdkantoor kunnen sturen. Daarnaast kan de organisatie meer besparen door de oplossingen te bundelen.

De organisatie hoeft zich geen zorgen te maken over integratie van de individuele elementen van de oplossing, omdat alle functies zijn ontworpen voor samenwerking. Het resultaat is een besparing voor IT-personeel: volgens schattingen van Cisco kan dat oplopen tot 40 procent minder tijd voor ondersteuning van configuratie en implementatie. De organisatie profiteert tevens van een hoog en consistent beveiligingsniveau op het wereldwijde netwerk. Daardoor kan het bedrijf blijven groeien en zich richten op de zaken, in plaats van zich zorgen te maken over aanvallers die willen inbreken bij in-storenetwerken.

Conclusie

Retailers kunnen hun operationele lasten van bewaking, beheer en onderhoud van hun netwerken aanzienlijk verlagen als ze cloudtools zoals Cisco CWS gaan gebruiken. CWS werkt uitstekend samen met Cisco ASA- en Cisco ISR-producten en zorgt voor een intelligente vermindering van het afdwingen van lokaal beveiligingsbeleid, wat weer zorgt voor een verlaging van de bandbreedte-eisen per afzonderlijke winkel. Cisco CWS is erkend als marktleider door Gartner. Het biedt een slimme manier om de effectiefste beveiligingsmogelijkheden toe te voegen aan in-storenetwerken, zonder extra operationele complexiteit.

Meer informatie

Ga voor meer informatie naar http://cisco.com/go/cws.

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 C11-733817-00 02/15