# Cisco Security Portfolio Overview

**Juni 2019**

- Firewall
- Advanced Malware Protection (AMP)
- Cloud Beveiliging
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- Threat Response
- Beveiligingsbeheer

# Firewall

| Firewall | Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|---|
| | **ASA 5500-X** | • Voor kleine en middelgrote bedrijven, nevenvestigingen<br>• Firewall-doorvoer van 256 tot 1750 Mbps<br>• Bedreigingsinspectie van 125 tot 1250 Mbps<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering | Inbreuken automatisch voorkomen om uw bedrijf actief te houden; Bent u 24/7 beschermd? Cisco Talos analyseert doorlopend bedreigingsinformatie en maakt beveiligingsvoorzieningen aan die door de Cisco Next-Generation Firewall worden gebruikt om inbreuken te voorkomen. We stoppen aanvallen direct, zodat uw bedrijf geen moment hinder ondervindt.<br><br>Zichtbaarheid om bedreigingen snel te detecteren en te stoppen; Beschikt u over een volledig beeld? Kunt u bedreigingen stoppen die u niet kunt zien? Zorg voor diepgaande zichtbaarheid van uw netwerk en beveiliging met behulp van ingebouwde, geavanceerde beveiligingsfuncties zoals NGIPS en geavanceerde malwarebescherming om de meest geavanceerde bedreigingen snel te detecteren en te stoppen.<br><br>Automatiseer processen om tijd te besparen en complexiteit te verlagen; Zorg voor een consistente aanpak van bedreigingen. Laat de Cisco Next-Generation Firewall het werk voor u doen. Door beleid geautomatiseerd toe te passen en af te dwingen bespaart u tijd, die u kunt besteden aan taken met een hoge prioriteit. Cisco firewalls werken samen met de andere geïntegreerde beveiligingstools van Cisco om bedreigingen eerder te detecteren en sneller te stoppen. |
| | **Firepower 2100 series** | • Voor Internet Edge naar datacenter-omgevingen<br>• Firewall-doorvoer van 2,0 tot 8,5 Gbps<br>• Bedreigingsinspectie van 2,0 tot 8,5 Gbps<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering | |
| | **Firepower 4100 series** | • Voor Internet Edge, high-performance omgevingen<br>• Firewall-doorvoer van 12 tot 30 Gbps<br>• Bedreigingsinspectie van 10 tot 24 Gbps<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering | |
| | **Firepower 9000 series** | • Voor Service Provider, datacenter<br>• Firewall-doorvoer tot 225 Gbps<br>• Bedreigingsinspectie tot 9 Gbps<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering, DDoS | |

# Firewall

| Firewall | Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|---|
| | **Cisco adaptive security virtual appliance (ASAv)** | • Geoptimaliseerde cloud- en datacenter-omgevingen<br>• VMware, KVM, Hyper-V hypervisor-ondersteuning<br>• AWS, Azure en Azure Government Cloud<br>• Firewall-doorvoer van 100 Mbps tot 10 Gbps met gebruik van 1 tot 16 GB geheugen<br>• ASA stateful firewall, VPN | Inbreuken automatisch voorkomen om uw bedrijf actief te houden; Bent u 24/7 beschermd? Cisco Talos analyseert doorlopend bedreigingsinformatie en maakt beveiligingsvoorzieningen aan die door de Cisco Next-Generation Firewall worden gebruikt om inbreuken te voorkomen. We stoppen aanvallen direct, zodat uw bedrijf geen moment hinder ondervindt.<br><br>Zichtbaarheid om bedreigingen snel te detecteren en te stoppen; Beschikt u over een volledig beeld? Kunt u bedreigingen stoppen die u niet kunt zien? Zorg voor diepgaande zichtbaarheid van uw netwerk en beveiliging met behulp van ingebouwde, geavanceerde beveiligingsfuncties zoals NGIPS en geavanceerde malwarebescherming om de meest geavanceerde bedreigingen snel te detecteren en te stoppen.<br><br>Automatiseer processen om tijd te besparen en complexiteit te verlagen; Zorg voor een consistente aanpak van bedreigingen. Laat de Cisco Next-Generation Firewall het werk voor u doen. Door beleid geautomatiseerd toe te passen en af te dwingen bespaart u tijd, die u kunt besteden aan taken met een hoge prioriteit. Cisco firewalls werken samen met de andere geïntegreerde beveiligingstools van Cisco om bedreigingen eerder te detecteren en sneller te stoppen. |
| | **Cisco Next-generation firewall virtual (NGFWv)** | • Geoptimaliseerde cloud- en datacenter-omgevingen<br>• VMware, KVM, Hypervisor-ondersteuning<br>• AWS, Azure en Azure Government Cloud<br>• 1,2 Gbps doorvoer firewall + AVC, 1,1 Gbps doorvoer AVC + IPS<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering | |
| | **Meraki MX series** | • Cloud-beheerde UTM voor gedistribueerde omgevingen<br>• Firewall-doorvoer van 250 Mbps tot 6 Gbps<br>• Ingebouwde SD-WAN<br>• Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL-filtering | |

# Advanced Malware Protection (AMP)

| Malware Protection | Producten | Belangrijkste kenmerken/ Voordelen | Aanvullende informatie |
|---|---|---|---|
| **Geavanceerde malware tegenhouden**<br>**Blinde vlekken verwijderen**<br>**Onderzoeken en oplossen** | **AMP for Endpoints** | Geavanceerde malware tegenhouden | Met behulp van meerdere preventieve engines en cloud-gebaseerde informatie over bedreigingen doet AMP het zware werk voor u. AMP identificeert en stopt bedreigingen automatisch, voordat ze uw eindpunten bereiken. |
| | | Blinde vlekken verwijderen | AMP biedt een totaalbeeld van uw eindpunten, biedt meer inzicht, context en controle over servers en eindpunten die draaien onder Windows, MacOS, Android, iOS of Linux. |
| | | Onderzoeken en oplossen | AMP geeft u de controle terug over uw tijd door de tijd die u besteedt aan het onderzoeken en oplossen van bedreigingen drastisch te verlagen met een volledig overzicht van het bereik en de historie van bedreigingen. Met AMP kunt u de dreigingen voor uw omgeving met een paar klikken wegnemen. |
| | **AMP network** | Doorlopende analyse | Doorlopende analyse zorgt voor monitoring van bestanden nadat deze het netwerk binnenkomen, zodat u kunt zien waar, wanneer en hoe een schadelijk bestand uw netwerk is binnengedrongen om het vervolgens te blokkeren. |
| | | Retrospectieve beveiliging | Doordat AMP doorlopend bestanden en bestandsactiviteiten in het netwerk bewaakt en analyseert, kan AMP een retrospectieve waarschuwing afgeven wanneer een bestand schadelijk gedrag begint te vertonen. |
| | | Minder berichten over gebeurtenissen | Doorlopende updates van bestandsstrategieën op basis van AMPs wereldwijde informatie over bedreigingen helpt bij de detectie van en bescherming tegen malware. Bestands- en applicatiecontrole helpt bij het beperken van het aantal beleidsschendingen door bestanden en gebruikershandelingen. |
| | | Geïntegreerde malware-analyse | Met File capture kunt u bestanden opslaan en ophalen voor verdere analyse. Met het geïntegreerde Threat Grid kunt u onbekende en verdachte bestanden in een zeer veilige sandbox-omgeving onderzoeken, in de cloud of lokaal. |
| | **AMP for Email & Web security** | Bescherm uw e-mail & web | Voeg AMP-functies toe aan apparatuur voor e-mail en web-beveiliging of aan e-mail en web-beveiligingsimplementaties in de cloud. |

- Firewall
- Advanced Malware Protection (AMP)
- **Cloud Beveiliging**
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- Threat Response
- Beveiligingsbeheer

# Cloudbeveiliging

| Cloud Beveiliging | Producten | Belangrijkste kenmerken/ Voordelen | Aanvullende informatie |
|---|---|---|---|
| **Beveiliging voor verbinding met internet**<br>**Beveiliging voor SaaS-applicaties**<br>**Zichtbaarheid van publieke cloudinfrastructuur**<br>**Realtime cloudmonitoring**<br>**Multicloud-netwerkbescherming**<br>**Multicloud-workloadbescherming** | **Cisco Umbrella** | Leren | Verzameling van informatie om huidige en aanstaande dreigingen te ontdekken. |
| | | Zien | Zicht op activiteiten op alle apparaten en poorten, op elke locatie. |
| | | Blokkeren | Vroegtijdige blokkering van phishing, malware en ransomware. |
| | **Email security for Office 365** | Betere bescherming van uw inbox | Uw cloud e-mail heeft een extra beschermingslaag nodig tegen bedreigingen zoals ransomware, inbreuk op zakelijke e-mail, phishing en meer. Cisco biedt u de kennis van een van de grootste bedreigingsdetectieteams ter wereld, in combinatie met de robuuste functies die u nodig hebt om uw gebruikers te beschermen. Microsoft Office 365 en Cisco Email Security zijn samen gewoon beter. |
| | **Cisco Cloudlock** | Gebruikersbeveiliging | Cloudlock maakt gebruik van geavanceerde machine learning-algoritmen om onregelmatigheden te detecteren op basis van meerdere factoren. Cloudlock identificeert ook activiteiten buiten whitelisted landen en detecteert eventueel mogelijke acties, met een verbluffende snelheid en op grote afstand. |
| | | Gegevensbeveiliging | De Cloudlock DTL (Data Loss Prevention) technologie zorgt voor continue bewaking van cloudomgevingen om gevoelige informatie te detecteren en te beveiligen. Het biedt talloze out-of-the-box vormen van beveiligingsbeleid, evenals beleid dat in hoge mate aanpasbaar is. |
| | | App-beveiliging | De Cloudlock Apps Firewall ontdekt en controleert cloud-apps die met uw zakelijke omgeving verbonden zijn. U kunt voor afzonderlijke apps een cloud-gebaseerde Community Trust Rating bekijken. Daarnaast kunt u ze op een lijst van ongewenste apps of een whitelist plaatsen, afhankelijk van het mogelijke risico. |
| | **Cisco Stealthwatch Cloud** | Automatische configuratie en bedreigingsdetectie | Stealthwatch Cloud detecteert automatisch vroege indicatoren van bedreigingen, waaronder verdachte interne activiteiten, malware en aanvallen met meerdere fasen. De software identificeert tevens beleidsschendingen, onjuist geconfigureerde cloudonderdelen, en fouten of misbruik door gebruikers. |

- Firewall
- Advanced Malware Protection (AMP)
- **Cloud Beveiliging**
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- Threat Response
- Beveiligingsbeheer

# Cloudbeveiliging

| Cloud Security | Producten | Belangrijkste kenmerken/ Voordelen | Aanvullende informatie |
|---|---|---|---|
| **Beveiliging voor verbinding met internet**<br>**Beveiliging voor SaaS-applicaties**<br>**Zichtbaarheid van publieke cloudinfrastructuur**<br>**Realtime cloudmonitoring**<br>**Multicloud-netwerkbescherming**<br>**Multicloud-workloadbescherming** | **Cisco Stealthwatch Cloud** | Waardevolle waarschuwingen | Stealthwatch Cloud ontvangt een grote verscheidenheid aan netwerktelemetrie en -logs. Daarbij wordt gebruik gemaakt van modellering om de rol van elke entiteit te bepalen. Wanneer een entiteit afwijkend gedrag vertoont of schadelijke activiteiten uitvoert, wordt er een waarschuwing gegenereerd, zodat u de kwestie snel kunt onderzoeken. Bestaande klanten beoordelen 96 procent van Stealthwatch Cloud-waarschuwingen als nuttig. |
| | | Compliance met regelgeving | U kunt eenvoudig controleren of uw organisatie de van toepassing zijnde regelgeving naleeft, bijvoorbeeld de Payment Card Industry (PCI)-norm, de Health Insurance Portability and Accountability Act (HIPAA) en de Federal Information Security Management Act (FISMA). |
| | | Eenvoudig beheer en makkelijk schaalbaar | Stealthwatch Cloud wordt geleverd als Software as a Service (SaaS), waardoor u de software eenvoudig kunt uitproberen, aanschaffen en gebruiken. U hoeft geen gespecialiseerde hardware aan te schaffen en geen software-agents te implementeren. Ook is er geen speciale expertise vereist. |
| | **AppDynamics** | Visualiseer de prestaties van uw cloudapplicatie in realtime | Ga verder dan basisinformatie over de gezondheid van de infrastructuur en krijg daadwerkelijk inzicht in de prestaties van uw cloudapplicatie tot op het niveau van de zakelijke transactie en de code. |
| | | Monitor de servicelevels van zakelijke transacties | Krijg inzicht in uw cloudapplicaties en hun zakelijke impact met behulp van omvattende monitoring van transactievolume, servicelevel en doorvoer. |
| | | Snel rendement door integratie van AppDynamics met toonaangevende IaaS/ PaaS-cloudplatforms | Optimaliseer de zichtbaarheid en controle over cloudapplicaties ontwikkeld en geïmplementeerd met toonaangevende IaaS/ PaaS-platforms, waaronder Amazon Web Services, Microsoft Azure, Pivotal Cloud Foundry, Redhat OpenShift en Heroku, door diepgaande integratie met IaaS/PaaS-oplossingen. |



HOME

- Firewall
- Advanced Malware Protection (AMP)
- **Cloud Beveiliging**
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- Threat Response
- Beveiligingsbeheer

# Cloudbeveiliging

| Cloud Security | Producten | Belangrijkste kenmerken/ Voordelen | Aanvullende informatie |
|---|---|---|---|
| **Security for connecting to the Internet**<br>**Security for SaaS applications**<br>**Public cloud infrastructure visibility**<br>**Real-time cloud monitoring**<br>**Multicloud network protection**<br>**Multicloud workload protection** | **NGFW Cloud-oplossingen Cisco Adaptive Security Virtual Appliance (ASAv) & Cisco Next Generation Firewall Virtual (NGFWv)** | Zichtbaarheid | Krijg volledig inzicht in gebruikers, apparatuur, netwerken, applicaties, workloads en processen – want u kunt niet beschermen wat u niet kunt zien. |
| | | Segmentering | Verklein het aanvalsoppervlak door gedetailleerde toegangscontrole aan de netwerkrand en voorkom dat indringers zich tussen het datacenter en de cloud kunnen bewegen. |
| | | Bescherming tegen bedreigingen | Voorkom gegevensdiefstal en verstoring van operationele processen door implementatie van multilayered bedreigingssensoren, die een inbreuk snel detecteren, blokkeren en erop reageren. |
| | **Cisco Tetration** | Een geautomatiseerd whitelist-beleid | Met behulp van realtime telemetrische gegevens van applicatiecomponenten en gedragsanalyselogaritmen wordt een geautomatiseerd whitelist-beleid voor segmentering opgesteld. Monitor gedragsveranderingen om het beleid actueel te houden. |
| | | Maak gebruik van een zero-trust model | Dwing een consistent whitelist-beleid af voor datacenters op locatie en voor publieke clouds, om zero trust mogelijk te maken door middel van applicatiesegmentering. Doorlopende monitoring op schendingen van de compliance, en deze binnen een paar minuten identificeren in uw Productenienetwerk. |
| | | Afwijkingen in het procesgedrag identificeren | Een baseline bepalen voor het gedrag van processen die op de servers draaien. Identificatie van gedragsafwijkingen die duiden op het uitvoeren van malware. De nieuwste gebeurtenissen detecteren, zoals Spectre en Meltdown. |
| | | Kwetsbaarheden in de software detecteren | Een accurate inventaris opstellen van alle softwarepakketten en -versies die op servers zijn geïnstalleerd. Detecteren of er pakketten zijn met bekende CVEs (Common Vulnerabilities and Exposures), en specifieke remedies definiëren. |
| | | Beheer de toegang van gebruikers tot applicaties | Beheer de toegang van gebruikers tot applicaties |
| | | Beschikken over een beveiligingsdashboard | Een samengestelde beveiligingsscore voor workloads op basis van uiteenlopende parameters, waaronder naleving van het beleid, geïdentificeerde kwetsbaarheden en consistent procesgedrag. Snelle identificatie van workloads met afwijkend gedrag en een compliancescore voor applicaties. |



HOME

# E-mailbeveiliging

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Email security** | Bescherm gebruikers tegen e-mailbedreigingen | Ontdek hoe onze multilayer beveiligingsaanpak aanvallers uit de inboxen van uw gebruikers weert. |
| | Verbeter de e-mailbeveiliging van Office 365 | Zorg voor een robuuste verdedigingslaag tegen ransomware, inbreuk op zakelijke e-mail, phishing en meer. Ontdek waarom Cisco Email Security en Office 365 samen beter zijn. |
| | Ga verder dan point-in-time detectie | Zorg voor bescherming tegen risicovolle bestanden zodra ze schadelijk gedrag vertonen, met Cisco Advanced Malware Protection for Email. |
| | Zorg voor uitmuntende bedreigingsinformatie | Alleen Cisco biedt de uitmuntende bedreigingsbescherming van Talos, een van de grootste bedreigingsinformatieteams ter wereld. Elke drie tot vijf minuten komen automatisch nieuwe updates beschikbaar. |
| | Blokkeer geavanceerde phishing-pogingen | Bescherm gebruikers tegen frauduleuze afzenders met realtime informatie over bedreigingen. |
| | Controleer de betrouwbaarheid voordat e-mailtoegang wordt toegestaan | Controleer de identiteit van gebruikers met de eenvoudigste multifactor-authenticatie ter wereld als bescherming tegen phishing. |

# Endpoint

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco AMP for Endpoints** | Geavanceerde malware tegenhouden | Met behulp van meerdere preventieve engines en cloud-gebaseerde informatie over bedreigingen doet AMP het zware werk voor u. AMP identificeert en stopt bedreigingen automatisch, voordat ze uw eindpunten bereiken. |
| | Blinde vlekken verwijderen | AMP biedt een totaalbeeld van uw eindpunten, biedt meer inzicht, context en controle over servers en eindpunten die draaien onder Windows, MacOS, Android, iOS of Linux. |
| | Onderzoeken en oplossen | AMP geeft u de controle terug over uw tijd door de tijd die u besteedt aan het onderzoeken en oplossen van bedreigingen drastisch te verlagen met een volledig overzicht van het bereik en de historie van bedreigingen. Met AMP kunt u de dreigingen voor uw omgeving met een paar klikken wegnemen. |
| **Cisco AnyConnect VPN** | Veel meer dan VPN | Maak het voor uw medewerkers mogelijk om overal en op elk moment te werken – op laptops van het bedrijf of op hun eigen mobiele apparaten. AnyConnect vereenvoudigt beveiligde eindpunttoegang en biedt de beveiliging die vereist is om uw organisatie veilig en beschermd te houden. |
| **Cisco Security Connector** | Diepgaande zichtbaarheid | Bedrijven hoeven zich geen zorgen meer te maken over gebrek aan zichtbaarheid van het netwerk. Met de mogelijkheid van Security Connector om alle door iOS-apparaten en -applicaties gegenereerde netwerkverkeer te verzamelen, kunnen beveiligingsteams effectief, snel en nauwkeurig de omvang van incidenten bepalen. |
| | Overal beschermd | Een typefout in een URL is zo gemaakt, of iemand kan per ongeluk een phishing-link in een bericht aanklikken, en als gevolg kunnen schadelijke sites worden geopend. Security Connector voorkomt connecties op DNS- en IP-adresniveau, zelfs via mobiele netwerken en publieke Wi-Fi. |
| | Eenvoudige implementatie en eenvoudig beheer | Cisco Security Connector is een cloud-beheerde oplossing. Bedrijven kunnen deze oplossing eenvoudig implementeren via een enterprise mobility management-oplossing, zoals Cisco Meraki Systems Manager, IBM MaaS360, InventIT MobiConnect, Jamf Pro, MobileIron of VMware Workspace ONE powered by AirWatch. |
| **Cisco Umbrella** | Leren | Verzameling van informatie om huidige en aanstaande dreigingen te ontdekken. |
| | Zien | Zicht op activiteiten op alle apparaten en poorten, op elke locatie. |
| | Blokkeren | Vroegtijdige blokkering van phishing, malware en ransomware. |

HOME

# Adaptieve Multi-Factor Authenticatie

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco DUO** | Two Factor Authentication (2FA) | De identiteit van alle gebruikers identificeren met de eenvoudige 2FA-goedkeuring van DUO. |
| | Zichtbaarheid van apparaten | Krijg inzicht in alle beheerde en onbeheerde apparaten om ervoor te zorgen dat ze aan uw beveiligingsnormen voldoen, voordat u de apparaten toegang verleent. |
| | Adaptieve authenticatie | Dwing beleid voor toegangsbeveiliging af op basis van het risico op het niveau van de gebruiker, het apparaat en de applicatie |
| | Secure single sign-on (SSO) | Stroomlijn de inlogworkflow door gebruik van één dashboard voor toegang tot alle applicaties |
| | Bescherm elke applicatie, ongeacht waar deze zich bevindt | Beveiliging van de toegang tot alle applicaties op locatie en in de cloud met ingebouwde integraties. |
| | Veilige toegang op afstand | Bied clientless toegang op afstand voor multicloud-omgevingen en medewerkers op afstand. |

# Zichtbaarheid en Segmentering van het netwerk

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Stealthwatch** | Breid de netwerkzichtbaarheid uit | Detecteer voor de hele digitale business aanvallen die langs de beveiliging glippen. Detecteer schadelijke patronen in versleuteld verkeer. Voor onze Encrypted Traffic Analytics-technologie en multilayer machine learning is geen decodering nodig. |
| | Versnel de respons en het forensisch onderzoek bij incidenten | Detecteer snel zero-day malware, interne bedreigingen zoals command-and-control communicaties en data-exfiltratie, geavanceerde persistente bedreigingen en andere geavanceerde aanvallen. Sla telemetrische gegevens voor lange perioden op. Maak gebruik van geavanceerde analyse voor beter onderzoek. |
| | Vereenvoudiging van netwerksegmentering | Effectieve segmentering van het netwerk. Gebruik de Stealthwatch-integratie met Cisco Identity Services Engine (ISE) om beleid te definiëren en af te dwingen. En voorkom dat niet-geautoriseerde gebruikers en apparaten toegang krijgen tot beperkt toegankelijke delen van het netwerk. |
| | Beveilig uw datacenter | Breid de zichtbaarheid en controle uit naar uw datacenter en monitor zowel het noord-zuid- als het oost-westverkeer. Voeg op rollen gebaseerde monitoring en betere netwerksegmentering toe door gebruik van Stealthwatch met Cisco ISE en Cisco TrustSec. |
| | Breid de zichtbaarheid uit naar de publieke cloud | U kunt nu zichtbaarheid en detectie van bedreigingen in de publieke cloud realiseren zonder gebruik van software-agents. Cisco Stealthwatch Cloud is een gebruiksvriendelijke SaaS-oplossing voor de beveiliging van workloads in Amazon Web Services (AWS), Google Cloud Platform en Microsoft Azure. |
| **Cisco Identity Services Engine** | Bied uw interne klanten de toegang die ze willen en nodig hebben | Zorg voor alomtegenwoordige toegang. Automatiseer integratie van apparatuur. Verminder het spanningsveld tussen IT en gebruikers. |
| | Zorg voor volledige eindpuntzichtbaarheid | Krijg de beschikking over de volledige contextuele identiteit en de profielen van alle gebruikers, apparaten en applicaties in uw IT- en OT-netwerken. |
| | Optimaliseer de beveiliging en beperk schendingen | Beveilig uw netwerk. Verklein het aanvalsoppervlak. Harmoniseer en automatiseer de beveiliging tegen bedreigingen. |
| | Stroomlijn uw netwerkbeheer | Automatiseer complexe wijzigingen op een intuïtieve manier. Zorg voor inbedding van compliance-normen. Integreer ongelijksoortige oplossingen |

# Zichtbaarheid en Segmentering van het netwerk

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Trustsec** | Verlaging van het risico | Segmenteer apparaten zonder het netwerk opnieuw te ontwerpen. Beheer eenvoudig de toegang tot enterpriseresources. Beperk laterale bewegingen van bedreigingen met micro-segmentering. |
| | Pas beleid toe op het hele netwerk | Snel schalen en beleid consistent afdwingen in het hele netwerk. Het beveiligingsbeheer voor alle domeinen stroomlijnen. Gebruik Cisco ISE om TrustSec-beveiligingsgroeptags te beheren en informatie te delen met andere groep-gebaseerde beleidsschema's. |
| | Lagere operationele kosten | De bevindingen van een analyse uitgevoerd door Forrester Consulting van klanten die TrustSec software-gedefinieerde segmentering in productienetwerken gebruiken: TrustSec verlaagt de operationele kosten met 80 procent en zorgt ervoor dat beleidswijzigingen 98 procent sneller kunnen worden doorgevoerd. |
| | Stroomlijnen van compliance | Beheer de toegang tot gereguleerde applicaties met eenvoudig, op groepen gebaseerd beleid. Beperk de scope van compliance voor regelgeving zoals PCI, HIPAA en DFARS. |

# Volgende Generatie Inbraakpreventiesystemen

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Firepower 2100 Series** | Ontworpen voor verkoopafdelingen en nevenvestigingen<br>Bedreigingsinspectie van 2,0 tot 8,5 Gbps<br>Omvat AVC, met AMP- en URL-opties<br>Fail-to-wire interfaces beschikbaar | Zichtbaarheid met Firepower Management Center. U ziet meer contextuele gegevens uit uw netwerk en u kunt uw beveiliging finetunen. Bekijk applicaties, tekenen van inbreuk op informatie, host-profielen, bestandstrajecten, sandboxing, informatie over kwetsbaarheid, en zichtbaarheid van het OS op apparaatniveau. Gebruik deze gegevensinvoer om de beveiliging te optimaliseren met beleidsaanbevelingen of Snort-aanpassingen.<br><br>Effectiviteit. NGIPS ontvangt elke twee uur nieuwe beleidsregels en handtekeningen. Uw beveiliging is dus altijd up-to-date. Cisco Talos maakt gebruik van het grootste bedreigingsdetectienetwerk ter wereld om te zorgen voor effectieve beveiliging met elk Cisco-beveiligingsproduct. De toonaangevende beveiligingsinformatie werkt als een waarschuwingssysteem dat doorlopend wordt bijgewerkt met nieuwe bedreigingen.<br><br>Operationele kosten. Gebruik NGIPS-automatisering om de operationele efficiency te verhogen en te zorgen voor minder overhead door gebeurtenissen waarop actie kan worden genomen te scheiden van ruis. Prioriteer bedreigingen voor uw medewerkers en verbeter uw beveiliging met beleidsaanbevelingen die gebaseerd zijn op de kwetsbaarheden van het netwerk. Blijf op de hoogte van welke regels geactiveerd of gedeactiveerd moeten worden en filter gebeurtenissen die relevant zijn voor de apparatuur in uw netwerk.<br><br>Flexibiliteit. Cisco Firepower NGIPS-opties voor flexibele implementatie voldoen aan de behoeften van de onderneming. De software kan worden geïmplementeerd aan de netwerkrand, bij de datacenterdistributie/core of achter de firewall, om missie-kritische assets, gasttoegang en WAN-verbindingen te beschermen. NGIPS kan worden geïmplementeerd voor inline inspectie of passieve detectie.<br><br>Integratie. Firepower NGIPS kan op uw netwerk worden aangesloten zonder grote hardwareveranderingen en zonder veel implementatietijd te vragen. Gebruik en beheer meerdere beveiligingsapplicaties vanuit één scherm met Firepower Management Center. Navigeer naadloos tussen NGIPS, NGFW en AMP om uw beveiliging te optimaliseren en gegevens van derden te benutten met Cisco Threat Intelligence Director. |
| **Firepower 4100 Series** | Ontworpen voor Internet-edge, high-performance omgevingen<br>Bedreigingsinspectie van 10 tot 20 Gbps<br>Omvat AVC, met AMP- en URL-opties<br>Fail-to-wire interfaces beschikbaar | |
| **Firepower 9000 Series** | Ontworpen voor serviceprovider- en datacenterimplementaties<br>Bedreigingsinspectie tot 90 Gbps<br>Omvat AVC, met AMP- en URL-opties<br>Fail-to-wire interfaces beschikbaar | |
| **NGIPSv for VMware** | Kleine nevenvestigingen en locaties op afstand<br>Bedreigingsinspectie tot 800 Mbps<br>Oost-west datacenter/PCI-kritische servers<br>Volledige NGIPS-functionaliteit met opties | |
| **Firepower Threat Defense for ISR** | Ontworpen voor nevenvestigingen en locaties op afstand<br>Bedreigingsinspectie tot 800 Mbps<br>Geïmplementeerd op ISR G2 en 4000 Series routers<br>Verhoogde beveiliging, lagere WAN-kosten | |

- Firewall
- Advanced Malware Protection (AMP)
- Cloud Beveiliging
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- **Threat Response**
- Beveiligingsbeheer

# Threat Respons

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Threat Response** | Gecombineerde bedreigingsinformatie | Cisco Threat Response integreert informatie van Cisco Talos en bronnen van derden om automatisch Indicators of Compromise (IOC's) te onderzoeken en bedreigingen snel te identificeren. |
| | Geautomatiseerde verrijking | Cisco Threat Response voegt automatisch context van geïntegreerde Cisco Security-producten toe, zodat u onmiddellijk weet welk systeem wordt aangevallen, en hoe. |
| | Intuïtieve, interactieve visualisaties | Cisco Threat Response laat de resultaten zien in intuïtieve, configureerbare grafieken, voor beter inzicht in de situatie en snelle conclusies. |
| | Incidenten traceren | Cisco Threat Response biedt de mogelijkheid om belangrijke onderzoeksinformatie te verzamelen en op te slaan, en om de voortgang en bevindingen te beheren en documenteren. |
| | Naadloos inzoomen | Cisco Threat Response maakt het eenvoudig om diepgaander onderzoek uit te voeren naar geïntegreerde Cisco Security-producten. Wilt u weten waar dat schadelijke bestand precies is gebleven? Met één klik bent u in Cisco AMP for Endpoints, met alle informatie over het traject van het bestand. |
| | Direct verhelpen | Met Cisco Threat Response kunt u direct vanuit de interface corrigerende acties ondernemen. Blokkeer verdachte bestanden, domeinen en meer – zonder dat u eerst in een ander product hoeft in te loggen. |

- Firewall
- Advanced Malware Protection (AMP)
- Cloud Beveiliging
- E-mailbeveiliging
- Endpoint
- Adaptieve Multi-Factor Authenticatie
- Zichtbaarheid en Segmentering van het netwerk
- Volgende Generatie Inbraakpreventie-systemen
- Threat Response
- **Beveiligingsbeheer**

# Beveiligingsbeheer

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Firepower Management Center (FMC)** | Centraal beheer | Het is nu eenvoudiger dan ooit om gebeurtenissen en beleid te beheren voor deze netwerkbeveiligingsoplossingen: Firepower Next-Generation Firewall (NGFW), ASA met FirePOWER Services, Firepower NGIPS, FirePOWER Threat Defense for ISR en Advanced Malware Protection (AMP). |
| | Totale zichtbaarheid voor uw netwerk | Bekijk de gebruikers, hosts, applicaties, bestanden, mobiele apparaten, virtuele omgevingen, bedreigingen en kwetsbaarheden die aanwezig zijn in uw voortdurend veranderende netwerk. Omdat u bedreigingen niet kunt stoppen als u ze niet kunt zien. |
| | Realtime bedreigingsbeheer | Beheer de toegang tot uw netwerk, beheer het gebruik van de applicaties en zorg voor bescherming tegen bekende aanvallen. Gebruik AMP- en sandboxing-technologieën om onbekende aanvallen aan te pakken en besmettingen door malware in het netwerk te traceren. |
| | Automatisering van de beveiliging | Het management center correleert automatisch beveiligingsgebeurtenissen rond kwetsbaarheden in uw omgeving. Het prioriteert aanvallen, zodat uw team eenvoudig kan zien welke gebeurtenissen als eerste moeten worden onderzocht. Bovendien worden er beleidsaanbevelingen gedaan. |
| | Threat Intelligence Director | Threat Intelligence Director werkt met informatie uit verschillende bronnen door gebruik van open standaard interfaces. Vervolgens worden de vereiste acties voor monitoring en containment toegepast. Observaties worden gecorreleerd met bronnen van derden om het totale aantal waarschuwingen dat u moet bekijken, te verlagen. |

# Beveiligingsbeheer

| Producten | Belangrijkste kenmerken/Voordelen | Aanvullende informatie |
|---|---|---|
| **Cisco Defense Orchestrato (CDO)** | Eén beveiligingsbeleid | Stel eenmalig een beleid op en dwing het consistent af op meerdere beveiligingsapparaten in uw uitgebreide netwerk. Vergelijk, filter, bewerk en definieer nieuw beleid vanuit één centrale console. |
| | Problemen met het beveiligingsbeleid oplossen | Analyseer uw bestaande beleid en objecten op beveiligingsapparaten om fouten en inconsistenties te identificeren. Verbeter de beveiliging en de apparatuurprestaties doordat u ze eenvoudig kunt corrigeren. |
| | Snelle implementatie van apparatuur | Implementeer nieuwe apparatuur sneller door standaard beleidssjablonen te maken die zorgen voor consistente en effectieve beveiliging van uw Cisco-omgeving. Naarmate uw bedrijf groeit, nemen nieuwe implementaties automatisch het bijgewerkte beleid over. |
| | Eenvoudige upgrades van firewallsoftware | Versnel de toegang tot beveiligingspatches en nieuwe functies met upgrades van software-images, die met slechts een paar keer klikken worden afgerond. Voer upgrades in realtime uit of plan ze op een bepaald tijdstip in. |
| | Slimmer configuratiebeheer | Elke wijziging die wordt aangebracht, wordt doorlopend gedocumenteerd en kan in het wijzigingslog worden teruggevonden. Op elk moment updates ongedaan maken tot de laatst bekende, goed werkende configuratie. |