CISCO
SECURE

E-book
Cisco – Public

Hoe moderne security teams cyberdreigingen bestrijden

De reikwijdte van security is groter geworden

Vroeger, toen alle apparaten die een bedrijf gebruikte veilig in een bedrijfsnetwerk zaten, hield security in dat de buitengrens van het netwerk versterkt werd met up-to-date firewalls en dat antivirussoftware werd geïmplementeerd tegen malware die het netwerk toch was binnengedrongen.

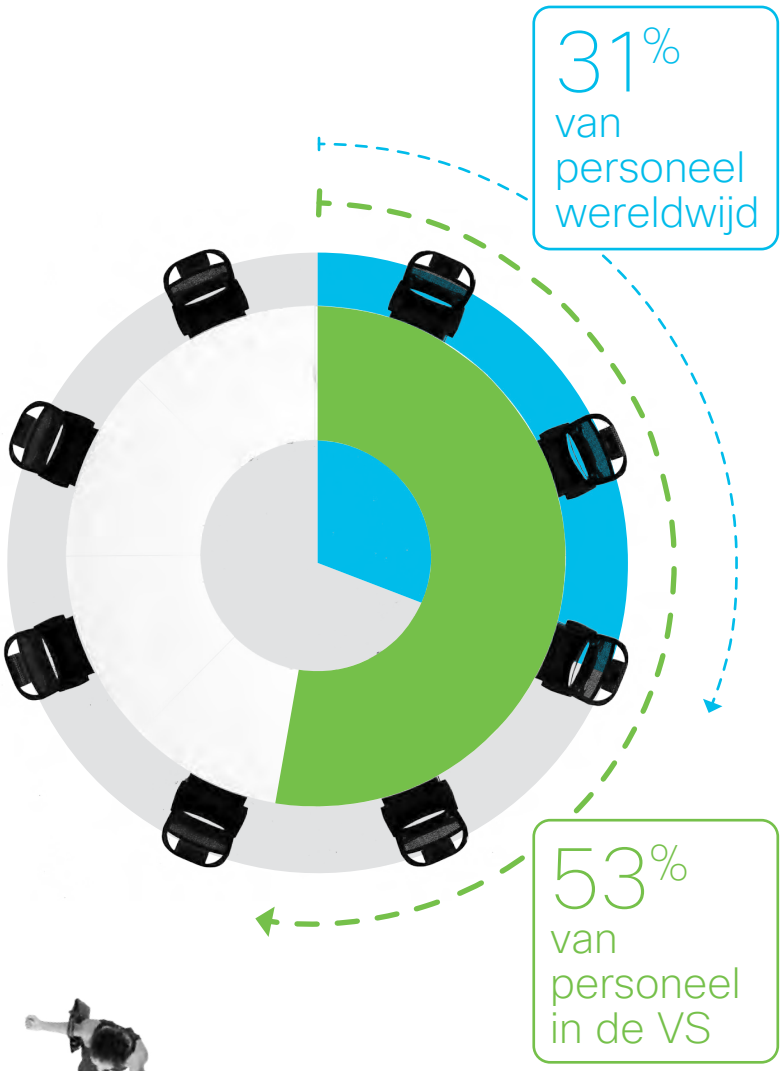
Webproxy's, e-mailgateways en sandboxes boden jarenlang extra ondersteuning voor security. Zolang apparaten in het netwerk bleven, vormden deze services de frontlinie, waar ze reactief aanvallen afweerden en verdreven.

Maar de tijden zijn veranderd.

Gebruikers hebben het gebouw verlaten

Volgens Gartner zal in 2022 53% van personeel in de VS en 31% wereldwijd op afstand werken, een trend die versnelde door de COVID-19-pandemie. Meer gebruikers buiten het netwerk leidde tot toegenomen kwetsbaarheid voor bedreigingen.

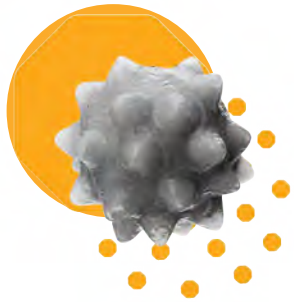
De toegenomen adoptie van hybride werkmodellen betekent dat security teams voortdurend voor de uitdaging staan om gebruikers verbonden en netwerken veilig te houden. Het beveiligen van apparaten is een groeiend probleem voor organisaties die niet meer kunnen rekenen op het verbinden van endpoints met campusnetwerken voor zichtbaarheid en om updates te pushen. Tegelijkertijd maken medewerkers vaker verbinding met bedrijfsmiddelen op persoonlijke, onbeheerde apparaten. Dit leidt tot blinde vlekken voor security teams.



Aanvallers blijven zich ontwikkelen

Wereldwijd zagen bedrijven een toename in cyber security dreigingen of waarschuwingen tijdens de pandemie. Met gebruikers die op afstand het bedrijfsnetwerk en cloudtoepassingen gebruiken, probeerden kwaadwillenden mogelijke gaten in de security te vinden. Hierdoor zag 61% van organisaties een toename van 25% of meer in cyberdreigingen of waarschuwingen sinds COVID-19 begon.

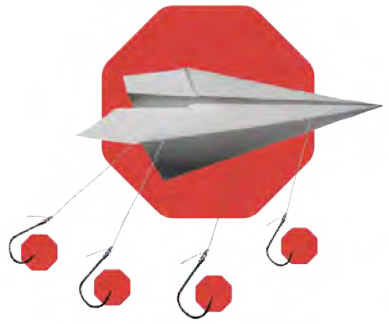
Data over trends in cyber security dreigingen in 2021:



48% van organisaties vond activiteit van malware die informatie steelt

50% van organisaties vond aan ransomware gerelateerde activiteit

69% van organisaties ervoer enige mate van ongevraagde cryptomining



86% van organisaties had één of meer gebruikers die een phishingsite probeerden te bereiken

Aanvallers blijven zich dus ontwikkelen en tegelijkertijd levert de mobiliteit van medewerkers nieuwe uitdagingen op voor security teams.

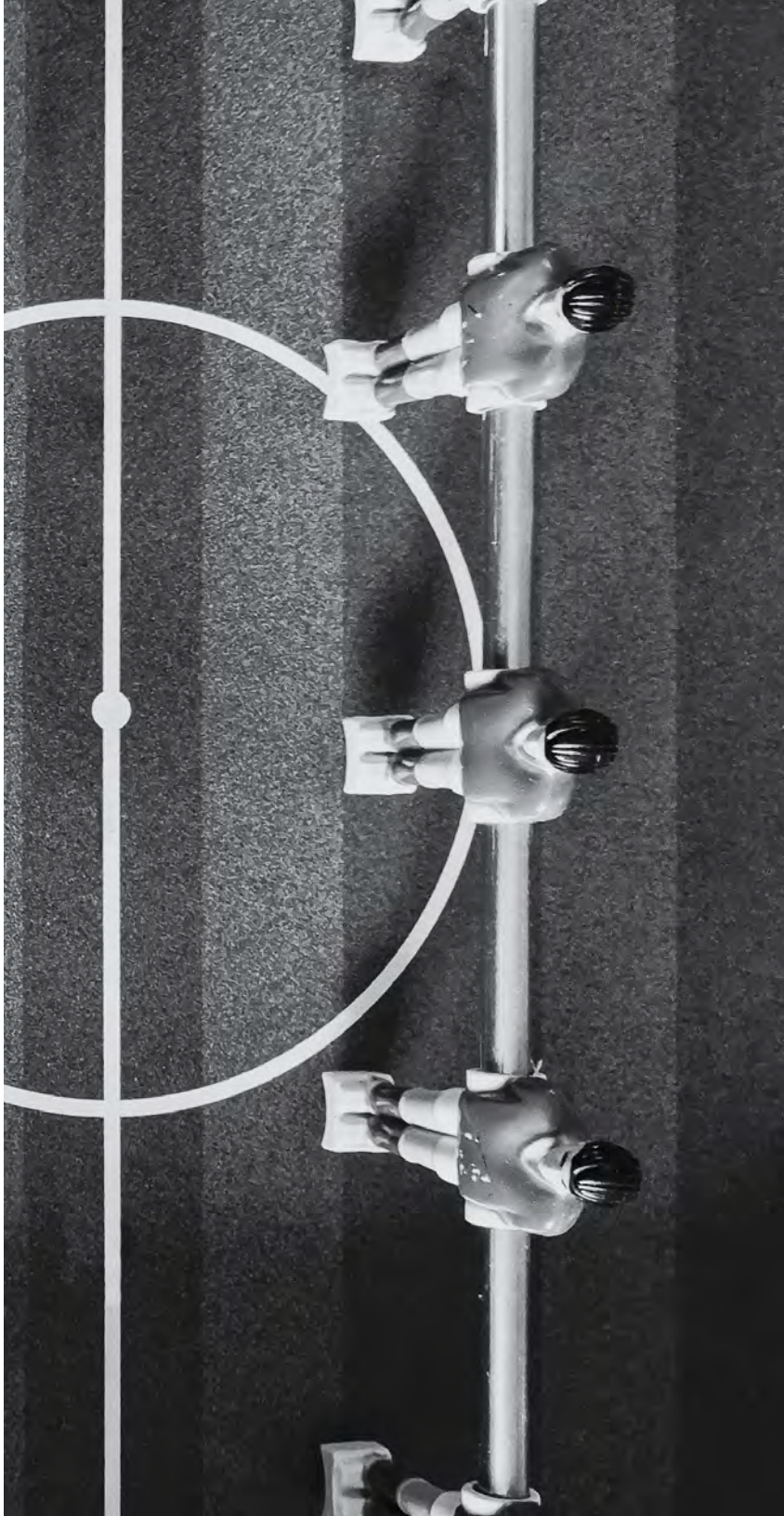
Cryptomining, phishing, ransomware en trojans zijn ongeveer 10x actiever op internet dan alle andere typen bedreigingen

cisco SECURE

Security op de DNS-laag vormt de eerste verdedigingslinie

DNS is een essentiële component van het internet en wordt door elk apparaat in het netwerk gebruikt. Het kan ook een zeer effectieve manier zijn om security af te dwingen. Lang voordat een malwarebestand wordt gedownload en een IP-verbinding via een poort of protocol tot stand wordt gebracht, is er een DNS-aanvraag.

Deze cruciale eerste laag blokkeert schadelijke domeinen nog voordat bedreigingen uw netwerk binnendringen. De implementatie van tools voor security op de DNS-laag is essentieel om aanvallen te stoppen voordat ze de buitengrens passeren.



Simpelere en effectievere cyber security vergroot de business resiliency

Security op de DNS-laag heeft als extra voordeel dat het overal is.

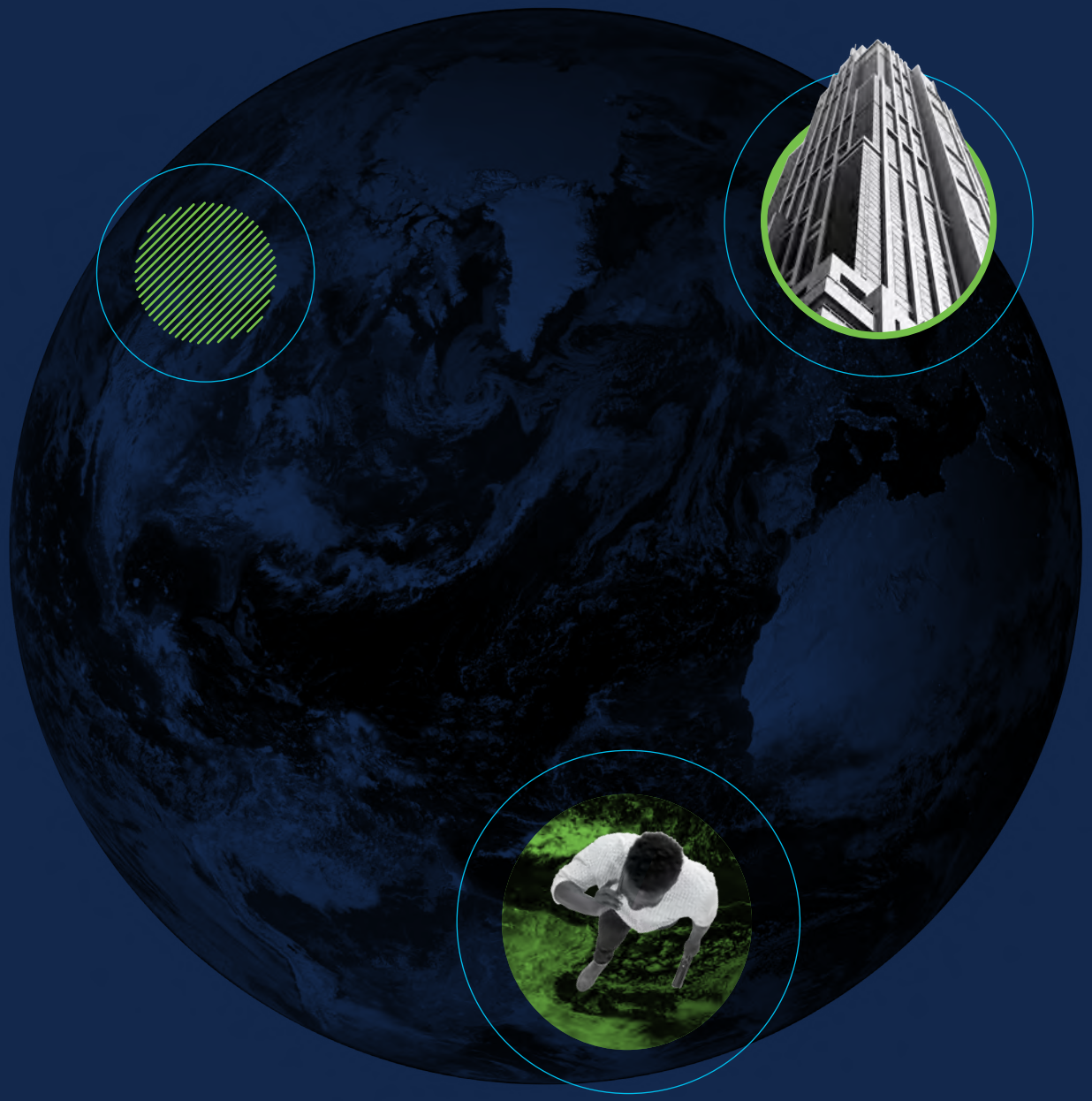
Door alle DNS-aanvragen van de organisatie – of ze nu van het netwerk, endpoints of mobiele apparaten komen – naar dezelfde DNS-provider te verwijzen bieden security teams gebruikers dezelfde bescherming, of ze nu op of buiten het bedrijfsnetwerk werken.

Aangezien de security op de DNS-laag aanvallen tegenhoudt voordat ze de buitengrens van het netwerk bereiken, zijn er daarnaast minder security waarschuwingen van een firewall of andere elementen van de security stack.

> “DNS biedt leiders in security en risicobeheer uitstekende kansen om bedreigingen te anticiperen, te voorkomen, te detecteren en erop te reageren.”
>
> Craig Lawson, John Watts, Gartner 2021

Bescherm gebruikers altijd en overal

Security teams moeten beleid kunnen afdwingen en moeten gebruikers overal waar ze werken en op elk apparaat kunnen beschermen.



Hoewel veel organisaties een VPN gebruiken, zetten gebruikers het VPN vaak niet aan, vanwege prestatieproblemen of omdat ze het niet nodig hebben on hun werk te doen, en worden ze daardoor niet beschermd. Security teams hebben een simpelere manier nodig om overal security af te dwingen.

Bescherming op de DNS-laag geeft security teams een cloud security oplossing met flexibele security op en buiten het netwerk, consistent beleid voor externe locaties en overal betere prestaties. Dit is essentieel, zowel voor teams die hun security moeten opschalen in hybride omgevingen als voor security professionals die worstelen met afzonderlijke security oplossingen of waarschuwingen van meerdere platforms.

Door COVID is het arbeidsmodel veranderd:

88%
van organisaties wil hun uitgaven aan cyber security in 2021 verhogen

& 41%
hiervan geeft cloud security prioriteit

Rapport The State of Security 2021

Bescherm gebruikers met Cisco Umbrella

Zo'n 35 datacenters van Cisco Umbrella verwerken dagelijks > 620 miljard internetaanvragen uit meer dan 190 landen. Deze realtime DNS-data wordt aangevuld met data uit private feeds en enkele openbare feeds.

Cisco Umbrella blokkeert dagelijks meer dan 170 miljoen schadelijke DNS-query's en ontdekt jaarlijks meer dan 200 nieuwe kwetsbaarheden. Deze schadelijke knooppunten zijn kansen om infrastructuur voor bedreigingen te identificeren en te neutraliseren voordat deze kan worden gebruikt voor nieuwe aanvallen.

Cisco Umbrella heeft een malwaredetectiepercentage van meer dan 70% (ver boven die van vergelijkbare oplossingen) en biedt de drie elementen die onmisbaar zijn voor moderne organisaties en security teams: wereldwijde zichtbaarheid, voorspellende intelligentie en bescherming op de DNS-laag.

84% van gebruikers van Cisco Umbrella halveerde het aantal malware-infecties

cisco SECURE

Doe uw voordeel met informatie van experts

Bij Cisco menen we dat u cyberaanvallen beter kunt voorspellen en voorkomen dan erop reageren en herstellen na de aanval. Hiervoor hebben security teams tools nodig met internetbrede zichtbaarheid buiten bedrijfsnetwerken, tot waar aanvallers infrastructuur opzetten voor huidige en toekomstige aanvallen.

Ze hebben ook betrouwbare, up-to-date informatie nodig om het toenemende aantal geraffineerde bedreigingen te bestrijden. De meeste huidige threat intelligence is statisch, verouderd of onvolledig en is niet echt bruikbaar in het gevecht tegen zich voortdurend ontwikkelende aanvallers.

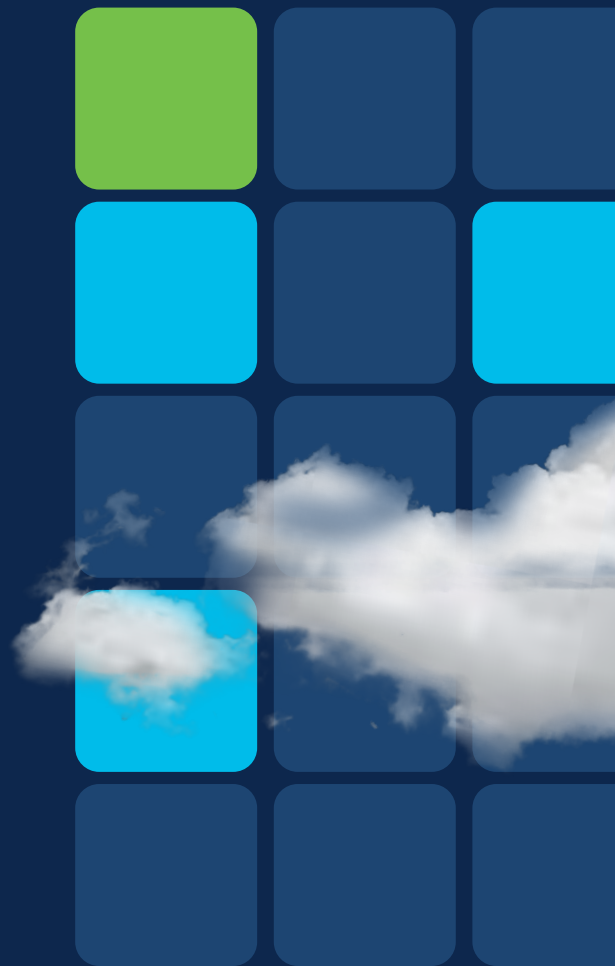
Stelt u zich nu een team voor met honderden security onderzoekers. Met Cisco Talos threat intelligence zet Umbrella statistische en machine learning-modellen in om nieuwe aanvallen op het internet te ontdekken. Daarnaast bieden de console en API van Umbrella Investigate realtime context over malware, phishing, botnets en andere bedreigingen. Dit versnelt het onderzoek van en de respons op incidenten.

Cisco Umbrella is de oplossing voor moderne security uitdagingen

Als vertrouwde partner van meer dan 24.000 bedrijven biedt Cisco Umbrella de snelste, effectiefste manier om uw security stack te verbeteren. Binnen minuten heeft u een nieuwe beschermingslaag tegen beveiligingslekken, met internetbrede zichtbaarheid op en buiten uw netwerk, ongeacht uw bedrijfsomvang.

Umbrella:

- Biedt cloudgebaseerde security op de DNS-laag, waarmee security teams elk apparaat in uw netwerk kunnen beschermen.
- Kan initiële infecties voorkomen, command and control-callbacks beperken en data-exfiltratie van al besmette apparaten tegenhouden.
- Heeft geen hardware om te installeren of software om te beheren.
- Legt alle internetactiviteit vast en biedt API-gebaseerde integraties met uw huidige security stack voor bescherming overal.



Probeer het 14 dagen uit.

Start een gratis trial