De dark web decoded:

Beveilig je klanten tegen cybersecurity threats

Ontdek in dit whitepaper welke trends er spelen op het dark web én hoe je als MSP je klanten hiervan beschermt.

Powering High Performance MSP's

Avast Business | portland

Eén verkeerde klik...

Je klant opent een e-mail die er precies uitziet als een bericht van één van zijn leveranciers. Of tenminste – bijna dan. Het bericht is namelijk nep: ‘t is een phishing-aanval met AI-ondersteuning, vermomd als belangrijke e-mail van een zakenrelatie. Binnen drie minuten is zijn alle bedrijfsgegevens van je klant gegijzeld.

Een geïsoleerd incident? Dat is het bovenstaande scenario zeker niet. Cyberaanvallen op het mkb zijn namelijk in de afgelopen jaren verdubbeld. Dankzij AI is het makkelijker dan ooit tevoren om een hack of hyper-personalized cyberattack uit te voeren. En... dit betekent dat er werk aan de winkel is voor jou als MSP. Want ook al weet jij precies wat een exploit is, jouw klanten hebben geen idee. En dan kun je nog zo’n mooie firewall installeren – één verkeerde klik op een malifide link en 't was allemaal voor niets.

Vrij spel voor hackers

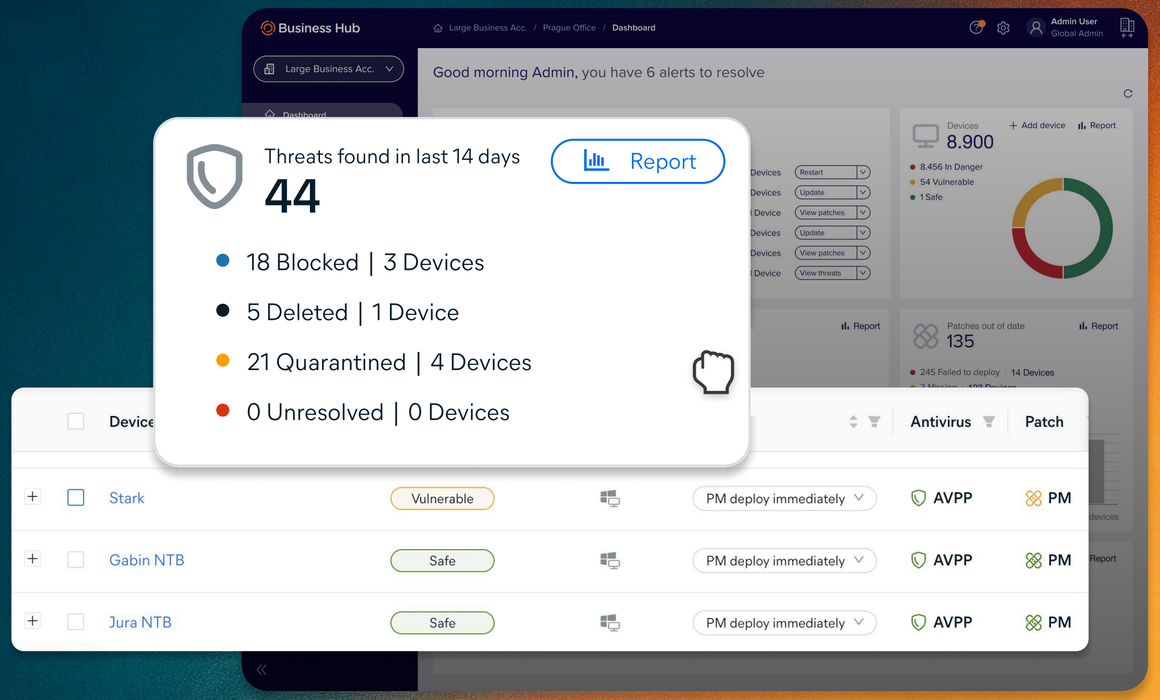
Cybersecurity is een abstract concept voor jouw klanten. Iets wat ze hebben "geregeld" door jou in te huren. Ze klikken op links, downloaden bestanden en loggen in op wifi-netwerken zonder na te denken over de risico's. Ze beschouwen cybersecurity als jouw verantwoordelijkheid – niet als iets waar ze zelf een actieve rol in spelen.

En daar zijn hackers zich maar al te bewust van. Ze weten best dat jouw klanten van cybersecurity geen kaas hebben gegeten en maken daar dan ook gretig misbruik van. Hoe? Door geavanceerde phishing mails te sturen met behulp van AI. Ze ontwikkelen steeds nieuwere malware en vinden steeds vindingrijkere manieren om systemen binnen te dringen. De nieuwste trend? Hyper gepersonaliseerde attacks die ze op grote schaal maken en versturen met behulp van AI. En bij dat alles richten ze zich op de zwakste schakel: jouw klant.

Beveiliging en opvoeding

Natuurlijk zet jij alles op alles om de systemen van je klanten zo goed mogelijk te beveiligen. Maar ook dat wordt steeds lastiger. Want hoe beveilig je je klanten nu écht effectief van een ransomware attack, spyware of AI-aanval? We bundelden de meest risicovolle bedreigingen uit 2024 én de voorspelde risico's van 2025 in dit whitepaper en geven je per stuk tips over effectieve beveiligingstools.

Maar ja, je kunt je klanten nog zo goed beschermen – als zij de achterdeur van ‘t fort openzetten, is het snel gedaan met de pret. Daarom is het minstens nét zo belangrijk om in gesprek te gaan met je klant en hen de risico’s uit te leggen, zodat zij die achterdeur netjes dicht laten zitten.



Inhoudsopgave

Cybercrime als businessmodel

Dat beeld van die eenzame hacker in een grijze hoodie? Die op een stoffig zolderkamertje achter zijn laptop zit te tikken aan zwarte schermen met groene letters? *Sorry to burst your bubble*, maar dat beeld klopt al lang niet meer. Cybercriminaliteit is tegenwoordig een stúk beter georganiseerd dan dat. En het hart van deze praktijken? Dat is het dark web – een verborgen stuk internet waar hackers ongestoord hun gang kunnen gaan en genieten van volledige anonimiteit.

Het dark web

Het dark web is een deel van het internet dat niet toegankelijk is via standaard zoekmachines en browsers. Het maakt deel uit van het 'deep web', het niet-geïndexeerde deel van het internet. Het uitganspunt van dit dark web? Volledige anonimiteit voor alle gebruikers. Daarom is het opgebouwd uit meerdere lagen en kun je alleen toegang krijgen met een tool als Tor: The Onion Router.

Het dark web wordt gelukkig niet alleen gebruikt voor criminele activiteiten. Zo gebruiken journalisten het ook om veilig te communiceren onder strenge regimes, of om gevoelige informatie te delen of klokken te luiden. Maar vergis je niet: het merendeel bestaat uit illegale activiteiten en georganiseerde misdaad.

- **Marktplaatsen** waar van alles wordt verhandeld – van gestolen data tot Malware as a Service.
- **Forums** waar duizenden (cyber)criminelen kennis uitwisselen en samenwerken.
- **Hackersmarktplaatsen** waar zero-day exploits en andere hacking tools worden verkocht.
- **Data dumps** waar gestolen data zoals creditcardgegevens, persoonsbewijzen en medische gegevens worden verkocht of vrijgegeven.
- **Ransomware as a Service** (RaaS) waarmee cybercriminelen hun “dienstenpakket” kunnen uitbreiden en ransomware attacks kunnen uitvoeren.

Zit je eenmaal op het darkweb? Dan tref je daar niet (alleen) die stereotype websites waarbij je groene letters ziet op een zwarte achtergrond. Sterker nog: websites op het dark web zijn tegenwoordig amper te onderscheiden van “gewone” websites. Van helpdesks met 24/7 klantenservice tot aan geldterug-garanties en affiliate-programs – het dark web heeft het allemaal. Het enige aspect waaraan je ziet dat je niet op een normale website zit, is die draak van ‘n url.

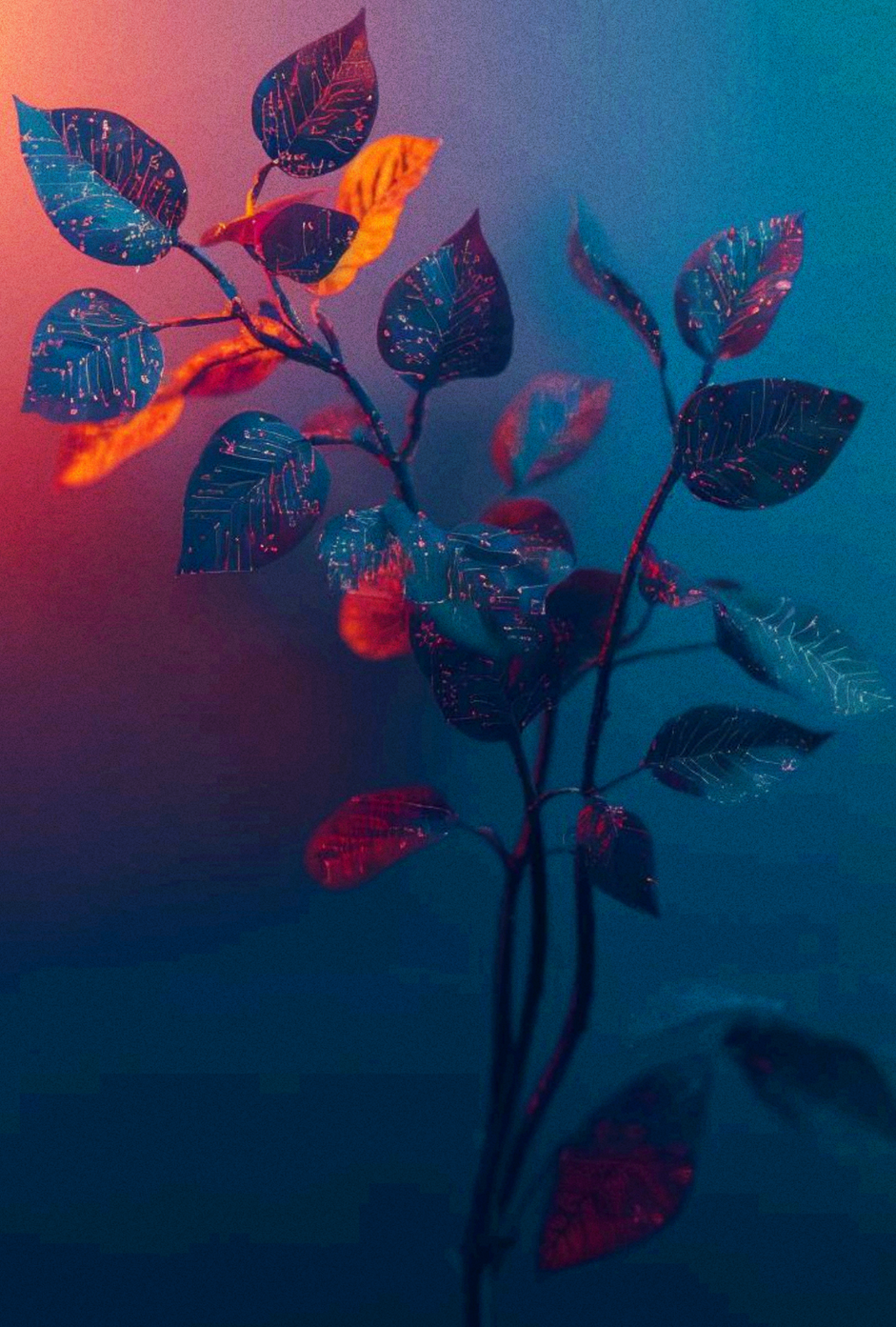
Jouw rol

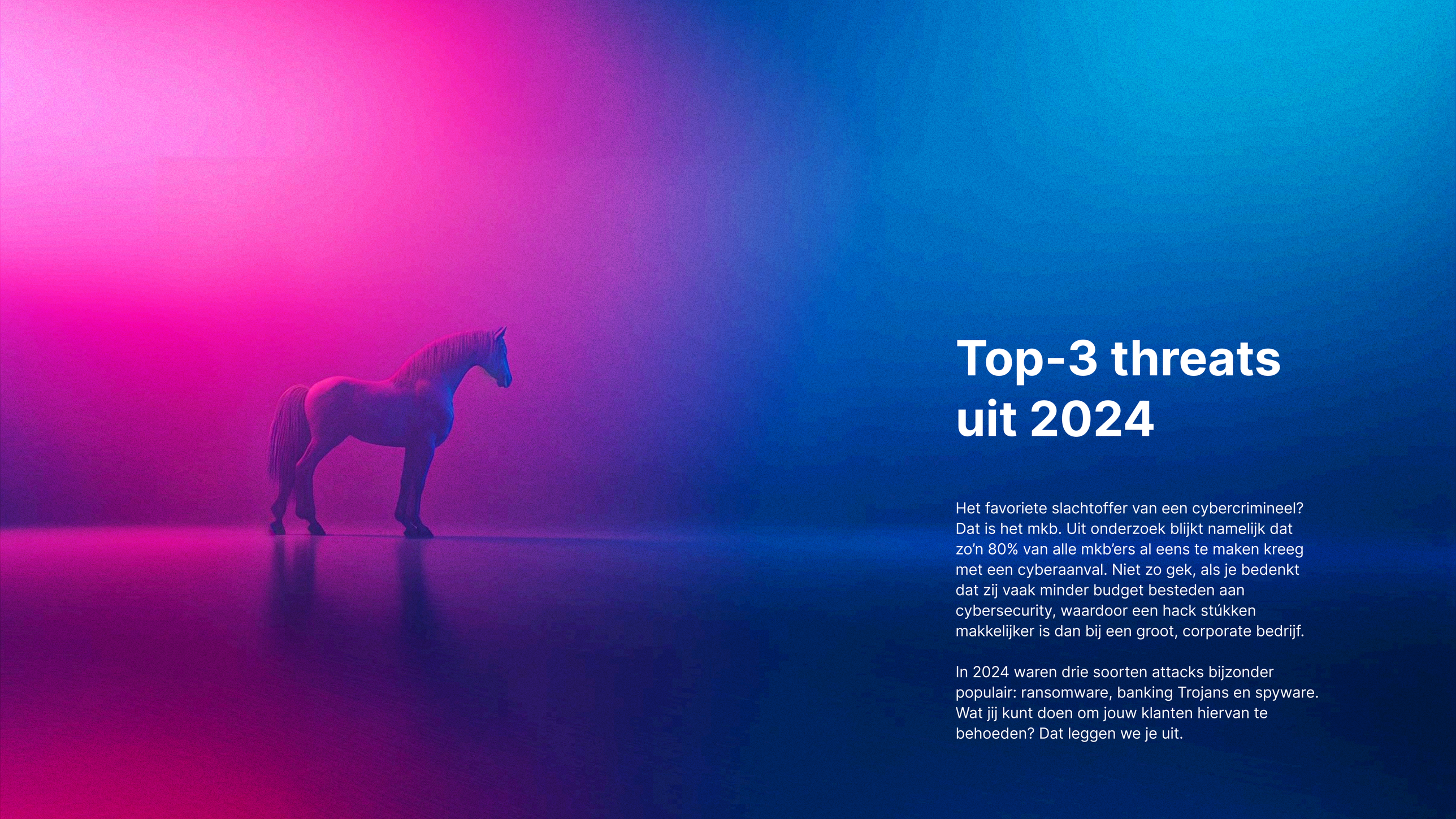
Op het dark web kopen cybercriminelen tools of zelfs diensten waarmee ze data van bedrijven en particulieren stelen. Komt een hacker eenmaal binnen op de netwerken van jouw klanten? Dan zitten ze daar vaak enkele weken of zelfs maanden voordat ze een aanval uitvoeren. In die tijd brengen ze alles in kaart, identificeren ze waardevolle data en bereiden ze de aanval voor. Vervolgens “gijzelen” ze data of sluizen ze ongemerkt waardevolle informatie weg – wat daarna op het dark web voor veel geld wordt verkocht.

En je klant merkt er niks van – tot ze een e-mail krijgen met de vraag om het losgeld te betalen. In bitcoins, welteverstaan. En dan… bellen ze jou. In hun ogen was het namelijk jóúw taak om deze hele sh*tshow te voorkomen. En dus is het ook jouw taak om het op te lossen.

Onze tip?

Zet in op de beveiliging én begeleiding van je klanten, zodat je de risico’s minimaliseert. Hoe je dat doet, lees je in de volgende hoofdstukken.





Top-3 threats uit 2024

Het favoriete slachtoffer van een cybercrimineel? Dat is het mkb. Uit onderzoek blijkt namelijk dat zo'n 80% van alle mkb'ers al eens te maken kreeg met een cyberaanval. Niet zo gek, als je bedenkt dat zij vaak minder budget besteden aan cybersecurity, waardoor een hack stúkken makkelijker is dan bij een groot, corporate bedrijf.

In 2024 waren drie soorten attacks bijzonder populair: ransomware, banking Trojans en spyware. Wat jij kunt doen om jouw klanten hiervan te behoeden? Dat leggen we je uit.

Threat 01

Ransomware

Ransomware is malware die bestanden versleutelt en losgeld eist om de bestanden te ontsleutelen en verwijderen. Wil een klant hun data terug, omdat het bedrijf niet kan functioneren zonder toegang tot financiële records en productieprocessen en willen ze ook de data van het dark web verwijderen? Dan moeten ze dus dubbel dokken. De malware dringt meestal binnen op netwerken en systemen via een phishing e-mail met een bijlage, link of kwetsbare RDO-verbinding.

De gevolgen

Binnen één dag kan een mkb-bedrijf volledig komen stil te liggen na een ransomware attack. De herstelkosten? Die lopen al snel in de miljoenen. Zelfs voor een klein tot middelgroot bedrijf. Niet fijn – vooral niet, wanneer ze jou daarvan de schuld geven. Ze verwachten van jou dat je hun systemen zo snel mogelijk herstelt. En al die extra manuren die je daaraan kwijt bent? Die zijn – volgens je klant – gewoon voor je eigen rekening.

Tools & Features

Minimaliseer de kans op een ransomware attack met deze securitytools:

- **Behavior Shield**
  Herkent en blokkeert verdacht “gedrag” op de servers van je klanten, zoals het massaal versleutelen van bestanden.
- **Ransomware Shield**
  Voorkomt ongeautoriseerde wijzigingen aan kritieke mappen en bestanden.
- **Cloud Backup**
  Zorgt voor automatische, veilige opslag in de cloud. Zo wordt losgeld betalen overbodig.
- **Decryption Tools**
  Herstelt door bekende ransomware versleutelde bestanden zonder losgeld te betalen.

Threat 02

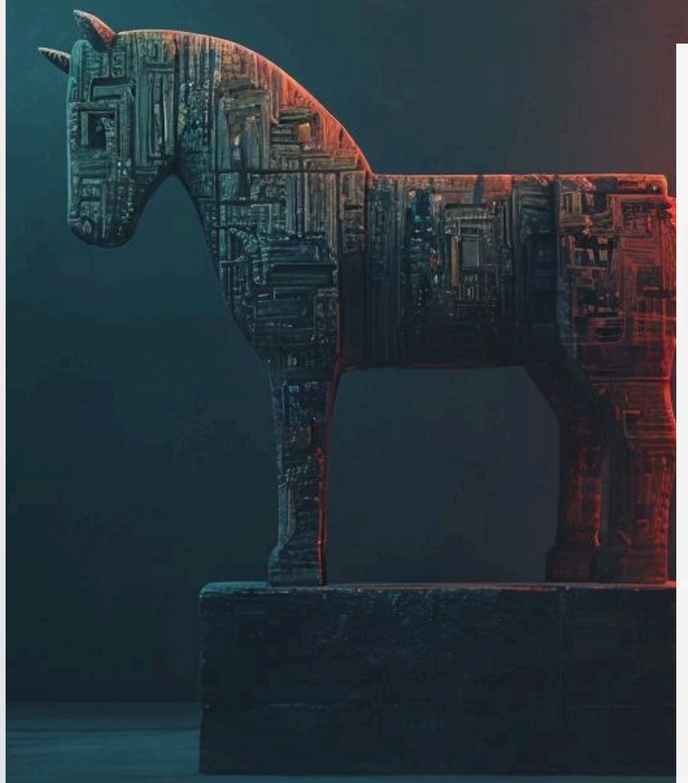
Banking trojans

Terwijl je klant denkt veilig zijn bankzaken te regelen, kijkt een cybercrimineel in Rusland live mee over zijn schouder. Banking trojans zijn digitale Trojaanse paarden die financiële gegevens stelen zonder enig spoor achter te laten. Vermomd als een legitiem softwareproduct of een app in de appstore, registreren ze in het geheim wachtwoorden, financiële gegevens en scherminhoud. En dat is nog lang niet alles – de *best in class*-trojans zijn namelijk zelfs in staat om:

- Authenticatie via tweefactor-authenticatie te omzeilen
- Legitieme banktransacties te wijzigen
- Automatisch geld over te maken naar rekeningen van criminelen

De gevolgen

Het grootste probleem met trojans? Het is bijna onmogelijk om ze te spotten en dus gaan je klanten gewoon hun gang, zonder ook maar enig vermoeden dat al hun activiteiten worden geregistreerd. Tot dat er opeens geld verdwijnt van hun rekening en op dat moment ben je eigenlijk al te laat. Het geld terugboeken is in veel gevallen niet mogelijk. Als ze die klap al overleven, weet je één ding zeker: jij bent de eerste leverancier die ze laten vallen. Tenzij je nu de juiste bescherming implementeert.



Tools & Features

Hoe je voorkomt dat zo'n banking trojan het netwerk van jouw klanten binnendringt? Daarvoor zet je deze tools in:

Behavior Shield
Identificeert verdachte activiteiten zoals het vastleggen van toetsaanslagen of manipuleren van webformulieren.

Web Shield
Blokkeert toegang tot bekende malafide websites die trojans verspreiden.

Browser Extension
Beveiligt online betalingen en waarschuwt voor onveilige websites tijdens bankieren.

Secure Browser
Beschermt tegen *man in the middle*-aanvallen tijdens financiële transacties.

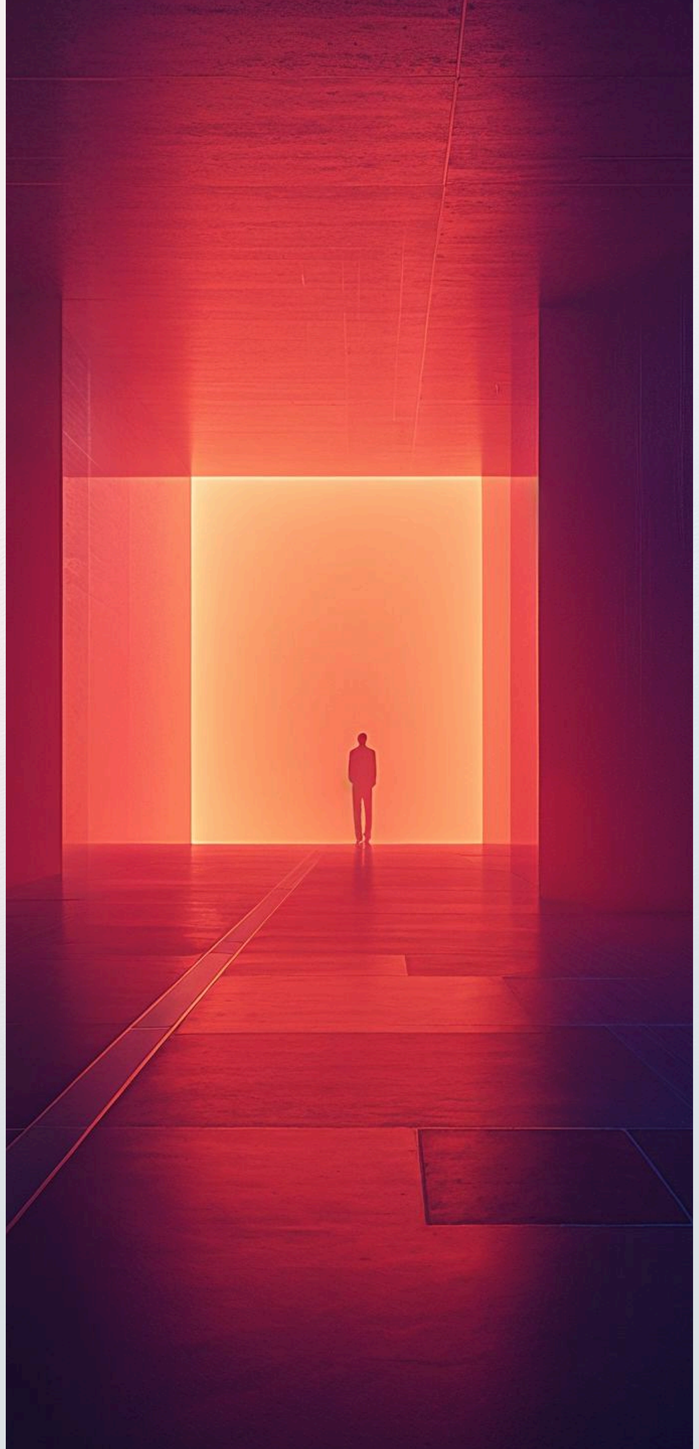
Threat 03

Spyware

Stel je voor: een digitale spion die elk gesprek, elke klik en elke toetsaanslag van een device registreert – 24 uur per dag, wekenlang. Dat is spyware. Zonder enige waarschuwing maakt het schermopnames, registreert het toetsaanslagen, leest het wachtwoorden en slaat het de complete browse-geschiedenis op – zonder dat de gebruiker er ook maar iets van merkt. Hoe deze spion binnendringt? Via gratis software en downloads.

De gevolgen

Zit er spyware op een netwerk? Dan is het gedaan met privacy. Gemiddeld zit zo'n malware 60 dagen op een systeem, voordat het ontdekt wordt. En dat betekent dat bedrijfsgeheimen van je klanten open en bloot op tafel komen te liggen. Intellectuele eigendommen worden gestolen, AVG-compliance komt in 't geding en staat er écht gevoelige informatie op een server? Dan loopt je klant de kans op afpersing of chantage. Zie dat maar eens op te lossen.



Tools & Features

En dus is het beter om spyware te voorkomen. Hoe je dat doet? Door deze slimme tools voor je te laten werken:

- **Behavior Shield**
  Detecteert verdachte activiteiten zoals ongebruikelijke toegang tot camera of microfoon.
- **File Shield**
  Scant bestanden in realtime voordat ze worden geopend, stopt spyware vóór installatie.
- **VPN**
  Versleutelt internetverkeer, voorkomt afluisteren van gegevens, zelfs op openbare WiFi.
- **AntiTrack**
  Voorkomt digitale vingerafdrukken en blokkeert trackers die gebruikersgedrag volgen.

Top-3 expected threats in 2025

Ook dit jaar zitten hackers en cybercriminelen niet stil. En hoewel 2025 natuurlijk nog maar net onderweg is, zien we nu al drie trends ontstaan in het online criminele circuit: APTs en ransomware, AI-gedreven scams, fraude en AI-aanvallen. We leggen je uit wat deze attacks inhouden én hoe je je klanten ervoor behoedt.

Threat 01

APTs & Ransomware

Advanced Persistent Threats (APTs) zijn langdurige, gerichte cyberaanvallen waarbij een aanvaller langere tijd onopgemerkt toegang heeft tot een netwerk. Bij zo'n aanval komt de hacker binnen via zorgvuldig voorbereide spearphishing-campagnes, aanvallen op de toeleveringsketen of nog onbekende kwetsbaarheden (zero-days).

Is de hacker eenmaal binnen? Dan nestelt hij zich als een digitale parasiet in het netwerk en blijft daar maanden zitten. Al die tijd verkent hij het netwerk, zodat 'ie alles weet over de infrastructuur, beveiliging en meer. Hij zoekt zwakke plekken in het netwerk en lanceert vervolgens een gerichte ransomware attack op die plekken, volledig afgestemd op de structuur van het netwerk van je klant.

De gevolgen

Doordat een hacker tijdens een APT lange tijd toegang heeft tot de systemen en netwerken van je klant, weet 'ie precies hoe zij er financieel voorstaan. En... dat gebruikt de hacker maar al te graag in zijn voordeel. Losgeldbedragen voor de gegijzelde data worden bepaald op basis van de financiële gegevens van het bedrijf en liggen over het algemeen een stuk hoger dan bij "traditionele" ransomware-aanvallen.

Maar daar houdt het nog niet op. Je klant komt namelijk bij jou verhaal halen: hoe heeft dit kunnen gebeuren? Waarom is er niks gedetecteerd en hoe konden de hackers zo goed profiteren van zwakheden in het netwerk? Aan jou de taak om forensisch onderzoek te doen naar de aanval en het herstelproces in werking te zetten.

Tools & Features

Onze tip? Zet in op preventie, zodat je dat gesprek niet hoeft te voeren met je klant. Schakel de volgende tools in om het netwerk van je klant nóg beter te beveiligen en de kans op een APT-aanval te verkleinen.

Behavior Shield
Detecteert abnormale activiteiten die wijzen op een APT, zoals ongebruikelijke systeemtoegang of verdachte dataverplaatsingen.

File Shield
Scant alle bestanden om malware te identificeren voordat deze kan worden uitgevoerd.

Firewall
Beperkt ongeautoriseerd netwerkverkeer en voorkomt laterale beweging binnen het netwerk.

Remote Access Shield
Beschermt tegen misbruik van remote desktop verbindingen, een favoriete toegangspoort voor APT-groepen.

Cloud Backup
Zorgt voor veilige backups die kunnen worden hersteld na een aanval, zelfs als ransomware lokale backups heeft versleuteld.

Network Inspector
Identificeert kwetsbaarheden in het netwerk die door APTs kunnen worden uitgebuit en stelt je in staat deze proactief te patchen.

Threat 02

Scams & fraude

Die scam-mailtjes van je achterneef uit Soedan? Die krijgen je klanten al lang niet meer. Nee, tegenwoordig zijn hackers een stúk verder dan dat en sturen zij steeds vaker hyper-gepersonaliseerde AI-attacks. Ze zetten AI in om gegevens uit eerdere data lekken te combineren en zo een compleet persoonlijk profiel te bouwen om medewerkers van bedrijven mee op te lichten.

Medewerkers krijgen e-mails of telefoontjes van 'hun directeur' die met exact dezelfde stem, accent en stopwoordjes als hun echte baas, maar in werkelijkheid is ‘t een AI voice clone of deep fake. De berichten staan vol van de persoonlijke details. En... hoe geavanceerder AI wordt, hoe moeilijker je deze scams onderscheidt van ‘t echte werk.

De gevolgen

Een simpele phishing-training is écht niet meer genoeg om deze scams-mails te kunnen onderscheiden van een echte. Dus hoe bescherm je dan je klanten en voorkom je dat ze tonnen schade oplopen? Je kunt simpelweg niet blijven doen wat je altijd deed – dan krijg je namelijk niet de resultaten die je altijd kreeg. En dus is ‘t tijd om jouw securitystrategie een flinke boost te geven.

Tools & Features

Vertrouwen herstellen na zo'n succesvolle AI-scam? Dat is een vak apart. Zet daarom in op preventie met behulp van deze tools:

Web Shield
Blokkeert toegang tot bekend malafide websites en detecteert phishing-pagina's die traditionele filters omzeilen.

Mail Shield
Analyseert inkomende e-mails op verdachte inhoud, ongebruikelijke afzenderpatronen en andere tekenen van AI-gegenereerde phishing.

Advanced Anti-Fraud Detection
Maakt gebruik van machine learning om verdachte patronen te identificeren in communicatie en transacties.

Threat 03

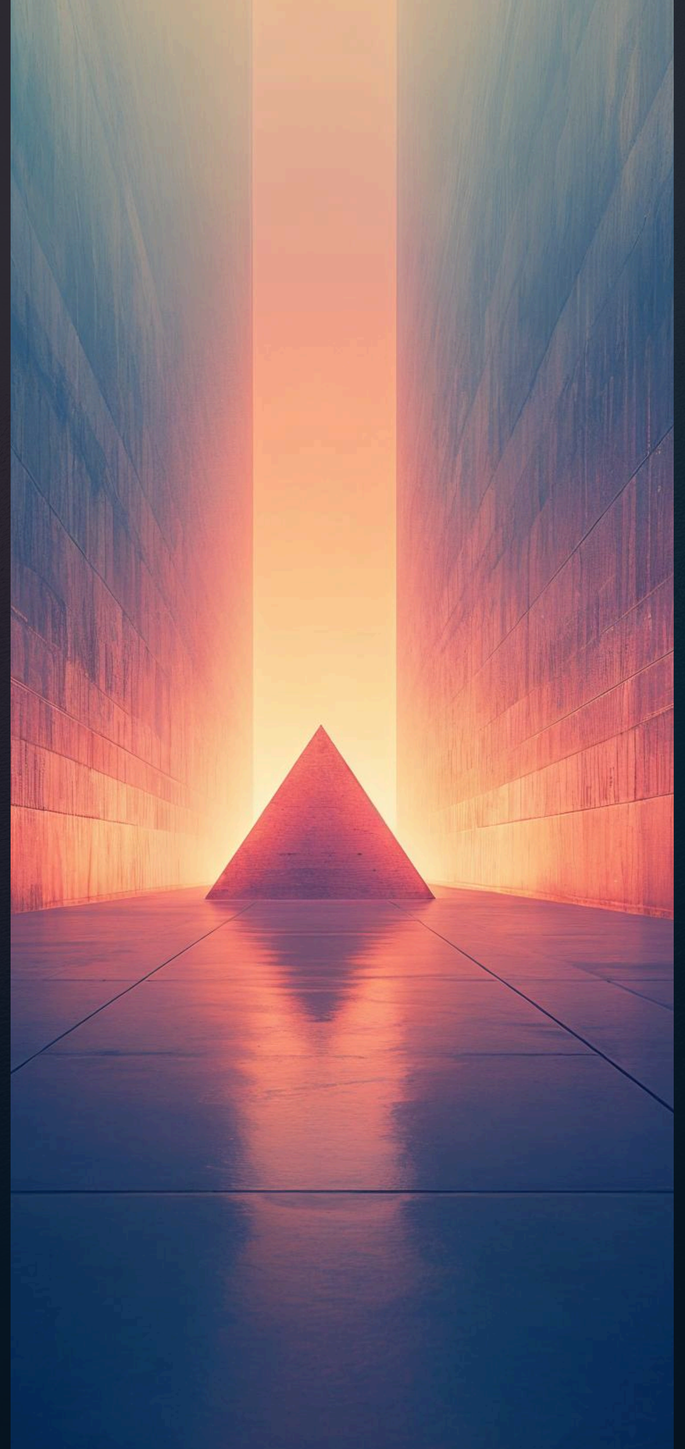
AI-Orchestrated Attacks

Cybercriminelen zetten AI dus in om persoonlijke profielen te maken van targets én op basis hiervan mensen in de val te lokken. Maar... da's lang niet het enige doel waarvoor AI wordt ingezet. Met behulp van AI kunnen hackers namelijk razendsnel kwetsbaarheden in netwerken detecteren én kunnen ze hun aanvallen automatiseren en versnellen.

Hoe zo'n aanval wordt ingezet? Met behulp van geautomatiseerde scanners die 24/7 zoeken naar de zwakste plek in het netwerk van je klant. Of de malware komt binnen via een zero-day: een onbekend beveiligingslek.

De gevolgen

Het gevolg? Een cyber attack die slimmer en sneller is en daardoor moeilijker te detecteren. Oftewel: een tsunami van 'n hack die een heel bedrijf overrompelt voor je d'r erg in hebt. Handmatig zo'n aanval stoppen? Dat is onmogelijk. En dus zul jij óók moeten investeren in AI-gestuurde oplossingen, maar dan voor de beveiliging van netwerken. Hiermee monitor je sneller het systeem en automatiseer je je respons, waardoor je responstijd aanzienlijk lager wordt.



Tools & Features

De enige manier om je hiertegen te weren? Door vuur met vuur te bestrijden. Bijvoorbeeld door deze slimme features in te zetten:

- **AI Response Engine**
  Gebruikt geavanceerde machine learning om aanvallen in realtime te detecteren en automatisch te reageren.
- **Predictive Threat Analysis**
  Voorspelt potentiële aanvalsvectoren voordat ze worden gebruikt, gebaseerd op globale dreigingsintelligentie.
- **Automated Patch Management**
  Identificeert en sluit beveiligingslekken voordat ze kunnen worden uitgebuit door AI-gestuurde aanvallen.
- **Anomaly Detection**
  Herkent afwijkend gedrag dat mogelijk wijst op een AI-gestuurde aanval, zelfs wanneer deze menselijk gedrag probeert na te bootsen.

Bescherm je klanten tegen alle risico’s

Even in ‘t kort: welke features en tools heb je nu écht nodig om jouw klanten van al deze cyber threats te beschermen?

	Core Values				Ransomware Defense			Online Beveiliging				Netwerk & Infra				AI-Defense			
	Behavior Shield	File Shield	Web Shield	Mail Shield	Ransomware Shield	Cloud Backup	Decryption Tools	Browser Extension	Secure Browser	VPN	AntiTrack	Firewall	Remote Access Shield	Network Inspector	Automated Patch Management	Advanced Anti-Fraud	AI Response Engine	Predictive Analysis	Anomaly Detection
Ransomware	✓	✓			✓	✓	✓					✓	✓		✓				
Banking Trojans	✓		✓	✓				✓	✓			✓				✓			
Spyware	✓	✓								✓	✓								✓
APTs & Ransomware	✓	✓	✓	✓	✓	✓	✓					✓	✓	✓	✓		✓	✓	✓
Scams & Fraud			✓	✓				✓	✓	✓	✓					✓	✓	✓	✓
AI-orchestrated attacks	✓	✓	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓	✓	

Features

Behavior Shield

Why? Dit is jouw beste wapen tegen AI-gestuurde aanvallen die traditionele detectie omzeilen.

How? Analyseert applicatiegedrag in realtime op verdachte patronen.

Gain? Vangt zero-day malware die andere beveiligingslagen mist.

Web Shield

Why? In 2025 zien we veel meer hypergepersonaliseerde scams die Microsoft Defender simpelweg mist.

How? Controleert alle data die via browsers wordt geladen.

Gain? Blokkeert phishing-sites en malware-downloads automatisch.

Ransomware Shield

Why? Eén succesvolle ransomware-aanval kost je klant gemiddeld een paar ton. En... Defender kan dit vaak niet stoppen.

How? Beschermt specifiek tegen ongeautoriseerde bestandsversleuteling.

Gain? Een gerichte verdedigingslinie tegen je duurste beveiligingsdreiging.

File Shield

Why? Eén geïnfecteerd bestand kan binnen enkele seconden je hele klantennetwerk compromitteren.

How? Realtime scanning van bestanden vóór ze worden geopend.

Gain? Stopt malware direct voordat het kan worden uitgevoerd.

Mail Shield

Why? Het gros van alle malware-infecties begint met een phishing mail - en jij kunt je klanten niet 24/7 controleren.

How? Scant inkomende en uitgaande e-mails inclusief bijlagen op malware.

Gain? Stopt de meestvoorkomende infiltratiemethode voordat jouw klanten er slachtoffer van worden.

Cloud Backup

Why? Je ultieme nooduitgang als aanvallers toch binnenkomen - zonder losgeld te betalen.

How? Automatische, geëncrypteerde backups naar de cloud.

Gain? Herstel binnen 4 uur na ransomware of dataverlies.

Features

Decryption tools

Why? Zonder decryptie zie je niet wat versleuteld verkeer écht bevat – en daar verbergt 90% van de malware zich tegenwoordig.

How? Onderzoekt versleuteld netwerkverkeer (zoals HTTPS) op verborgen bedreigingen.

Gain? Ontmaskert verborgen malware die anders ongemerkt je netwerk binnenkomt.

Secure browser

Why? Reguliere browsers laten te veel sporen na – en dat is een goudmijn voor cybercriminelen.

How? Biedt een veilige browseromgeving met ingebouwde privacy- en veiligheidsfuncties.

Gain? Voorkomt dat gevoelige gegevens zoals wachtwoorden of bankinfo uitlekken via de browser.

AntiTrack

Why? Elk klikgedrag wordt gevolgd – en verhandeld. Privacy is business.

How? Verbergt digitale vingerafdrukken en voorkomt tracking door websites en adverteerders.

Gain? Houdt gebruikersdata privé en voorkomt profilering door externe partijen.

Browser extention

Why? Gebruikers klikken. Altijd. En 60% van de dreigingen start via een browser.

How? Scant websites op reputatie en blokkeert foute domeinen, advertenties en trackers.

Gain? Een extra beschermingslaag op het gedrag van eindgebruikers, zonder dat jij ernaar hoeft om te kijken.

VPN

Why? Hybride werken is realiteit - voorkom datalekkage wanneer je klanten vanuit cafés en thuis werken.

How? Creëert een 256-bit versleutelde tunnel voor alle internetverbindingen.

Gain? Beschermt gebruikersdata, zelfs op onveilige openbare Wi-Fi-netwerken.

Advanced Firewall

Why? Zelfs als trojans geïnstalleerd raken, zonder servercontact kunnen ze geen data stelen of instructies krijgen.

How? Monitort en blokkeert verdacht netwerkverkeer op basis van gedragspatronen.

Gain? Voorkomt dat malware communiceert met command-and-control servers van cybercriminelen.

Features

Remote Access Shield

Why? Remote werk is de norm - zorg dat deze toegangspoort niet je zwakke plek is.

How? Beschermt RDP-verbindingen tegen brute force aanvallen die elke 39 seconden plaatsvinden.

Gain? Blokkeert gemiddeld 642 aanvalspogingen per endpoint per maand.

Advanced Anti-Fraud

Why? Fraude-e-mails en -websites worden steeds overtuigender en vallen buiten standaard detectie.

How? Herkent frauduleuze inhoud en nepwebsites met behulp van realtime bedreigingsinformatie.

Gain? Voorkomt dat gebruikers slachtoffer worden van social engineering of identiteitsfraude.

Anomaly Detection

Why? Niet alle aanvallen zijn malware. Soms is het een gebruiker die zich opeens ‘anders’ gedraagt.

How? Signaleert afwijkend gedrag van apparaten, gebruikers of netwerken.

Gain? Vroegtijdige opsporing van interne dreigingen of laterale bewegingen van aanvallers.

Network Inspector

Why? Je netwerk is zo sterk als je zwakste apparaat - en IoT-apparaten zijn 43% vaker het doelwit.

How? Identificeert alle apparaten op het netwerk en controleert op 35+ beveiligingsproblemen.

Gain? Ontdekt kwetsbare IoT-apparaten die Defender volledig mist.

AI Reponse Engine

Why? Dreigingen zijn sneller dan ooit. Reactie in minuten is te laat.

How? Detecteert, analyseert en reageert automatisch op bedreigingen op basis van AI-algoritmes.

Gain? Verkort de reactietijd van uren naar seconden – zonder tussenkomst van een mens.

Predictive Threat Analyses

Why? Wachten op een aanval is geen strategie. Proactief zijn wél.

How? Analyseert trends en gedragspatronen om toekomstige aanvallen te voorspellen.

Gain? Voorkomt incidenten door eerder in te grijpen dan de aanval plaatsvindt.

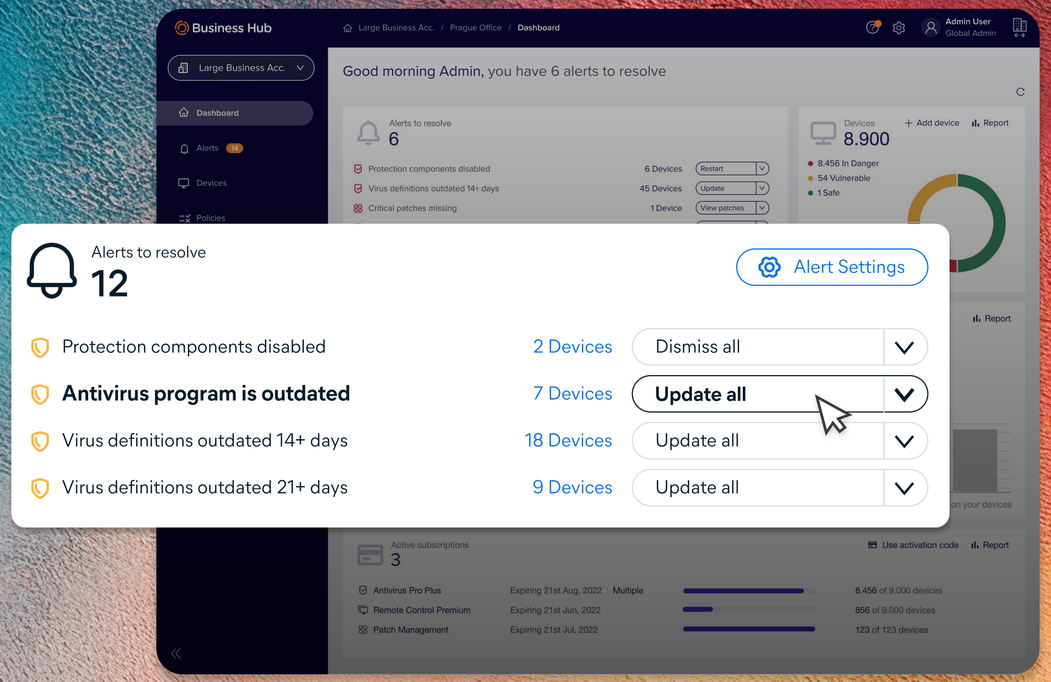
Features

Automated Patch Management

Why? 60% van alle succesvolle aanvallen exploiteren bekende, maar ongepatchte kwetsbaarheden die Windows Defender niet aanpakt

How? Automatiseert updates voor Windows én 350+ third-party apps in één klik.

Gain? Dicht kwetsbaarheden gemiddeld 57% sneller dan handmatige processen.



Avast Business Hub

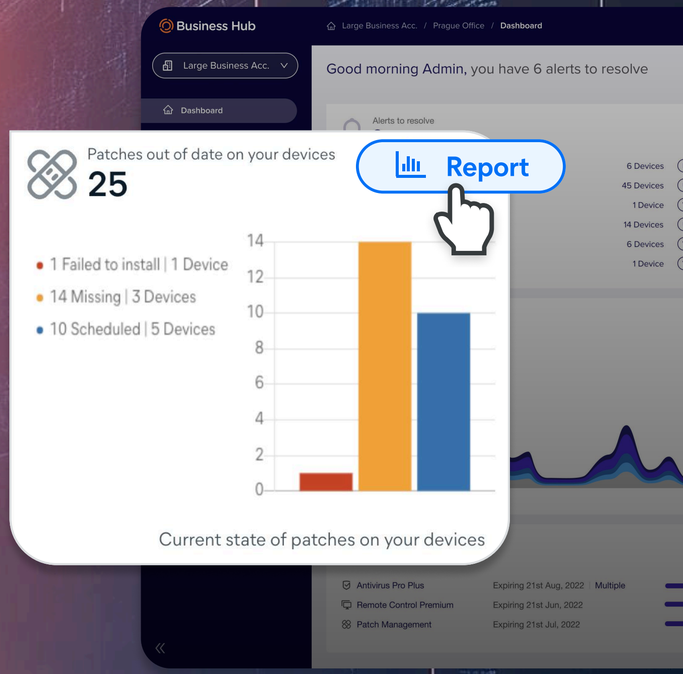
Nu kun je natuurlijk voor al die features een ander abonnement afsluiten, bij een andere vendor. Maar – *less is more*. Vooral wanneer ‘t aankomt op het aantal tools in jouw tech stack. Want eerlijk? Niemand zit te wachten op een berg licenties en beheerwerk.

Consolideren, dus. En laten wij nu net de perfécte tool hebben waarmee je al deze features in één overzichtelijk en gebruiksvriendelijk dashboard beheert. De Avast Business Hub.

Alles in één

Dankzij de Business Hub regel je de cybersecurity van al je klanten eenvoudig via één centraal en gebruiksvriendelijk platform – da's nog eens praktisch. De software vormt de *first line of defense* tegen alle meest voorkomende cyber threats. Daardoor is de software enorm krachtig – zonder de boel onnodig complex te maken. Zo houdt Avast de prijzen laag en zorgen ze voor een makkelijk hanteerbare oplossing.

- Bespaar tot 60% tijd en kosten door afscheid te nemen van losse tools en alles te beheren vanuit één *single pane of glass*.
- Reageer sneller op incidenten met realtime dreigingsdetectie, monitoring en directe waarschuwingen bij beveiligingsincidenten.
- Vereenvoudig je workflow – één platform betekent minder training, makkelijkere rapportages en betere resultaten.
- Of je klanten nu werken met een Windows- of Mac-computers, je beheert ze efficiënt en met multi-tenant support, speciaal ontworpen voor MSP's.
- Houd alle endpoints automatisch up-to-date zonder handmatige interventie dankzij ingebouwde updatefunctionaliteit.



USP’s

Remote Control

Why? Bij security-incidenten telt elke minuut - snelle respons = tevreden klanten.

How? Veilige, versleutelde toegang tot klantapparaten binnen 3 seconden.

Gain? Los problemen direct op zonder kostbare site visits - bespaar tot €125 per incident.

Centraal dashboard

Why? MSPs verliezen gemiddeld 5,4 uur per week met switchen tussen tools - die tijd kun je beter besteden.

How? Één overzichtelijk controlecentrum voor al je beveiligingsdiensten op 1 scherm.

Gain? Direct inzicht in alerts, problemen en dreigingen across alle klanten.

Multi-tenant support

Why? Omdat handmatig tussen accounts schakelen zó 2020 is en je winstmarges onder druk staan.

How? Beheer onbeperkt aantal klanten vanaf één plek met gedifferentieerde toegangsrechten.

Gain? Schaalbaarheid zonder extra kosten - groei je klantenbestand zonder evenredig je werklast te verhogen.

Gedetailleerde rapportages

Why? Klanten vernieuwen 78% vaker hun contract als ze zien welke aanvallen je hebt gestopt.

How? Genereert branded uitgebreide rapporten over dreigingen, updates en beveiligingsstatus.

Gain? Toon je klanten precies wat je voor ze doet - en welke aanvallen je hebt geblokkeerd.

Avast Business

Over Avast

Avast is een gebruiksvriendelijke, all in one-oplossing die perfect is voor MSP'ers met middelkleine klanten. Met Business Hub beheer je de beveiliging van al dien klanten op een gemakkelijke en betaalbare manier.

- **24/5 expert support zonder verborgen kosten**
- **Virusvrij-garantie met geld-terug belofte**
- **Complete ondersteuning bij herstel na een aanval**

Kortom: met Avast krijg je efficiëntie, eenvoud, kwaliteit én een breed scala aan functionaliteiten. En dat allemaal met een mooi prijskaartje eraan. Wat wil je nog meer? Neem contact op om de mogelijkheden van Avast Busines Hub te ontdekken voor jouw MSP-business.

Get in touch

Avast Business | portland

Over Portland

Sinds 1998 zijn wij de IT-dienstverlener van MSP's in de Benelux. Een soort van Master MSP – if you will. Bijzonder werk, want als MSP enabelen én beveiligen we, samen met jou, het mkb en kmo in Nederland en België.

We power High Performance MSP's

Onze missie? Van jouw bedrijf een High Performance MSP maken. Wij scheiden het kaf van het koren wanneer het aankomt op nieuwe tools en programma's, zodat jij dat niet meer hoeft te doen. We bijten ons vast in je bedrijf en stellen voor jou een high performance tech stack samen, waarmee je jouw business – en die van je klanten – een niveau hoger tilt.

- **25 jaar ervaring in het adviseren van MSP's**
- **Portfolio met de beste software op de markt**
- **Eén centraal portaal voor licenties en Cloud-abonnementen**
- **Onafhankelijk, eerlijk en glashelder**