SECURITYPLATFORM

# Managed security voor je webomgeving


## Met ons advanced securityplatform kun je rekenen op:

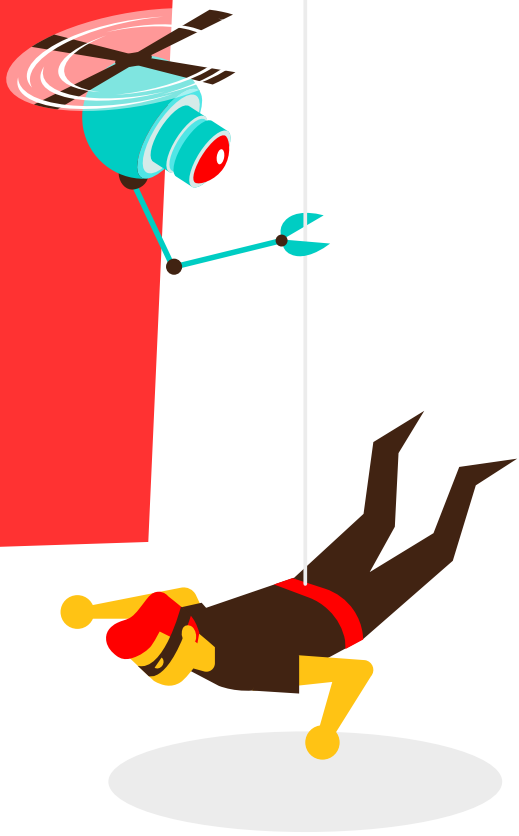
→ Bescherming tegen cross-site scripting (XSS) en SQL-injecties
→ Bescherming tegen Layer 3, 4 en 7 DDoS-aanvallen
→ Real-time inzicht in de type aanvallen (SQL-injecties, XSS) en frequentie
→ Automatische bescherming tegen IP-adressen die op internationale zwarte lijsten staan
→ Een gebruiksvriendelijk controlepaneel waar je eenvoudig IP-adressen blokkeert

**Wil je meer informatie over de security-oplossingen van True?**
**0800 BEL TRUE of ga naar true.nl/security-management**

TRUE

# Kwaadwillenden stoppen niet bij de grens

Wereldwijd nemen digitale aanvallen in rap tempo en op grote schaal toe. DDoS-aanvallen, cryptowormen, SQL-injecties, cross-site scripting, IoT-botnets: iedere organisatie loopt het risico om getroffen te worden. Het gevaar kan uit alle hoeken van de wereld komen: vaak zonder waarschuwing, onder de radar en geautomatiseerd. Als organisatie wil je gevoelige bedrijfsinformatie maximaal beschermen en kwaadwillenden buiten de deur houden.



## Advanced securityplatform: uitgebreide bescherming voor je webomgeving

### Beschermt tegen kwaadwillend verkeer

Bescherm je webomgeving tegen layer 3 traffic floods, layer 4 SYN floods en layer 7 http-aanvallen en beperk het aantal verzoeken dat een persoon mag doen per seconde. Het securityplatform van True signaleert overbelasting en onvoltooide verbindingen (TCP-flooding) en handelen de verzoeken af voordat het uit de hand dreigt te lopen.

### Detecteert verdacht verkeer

Met Intrusion Detection bekijken we het encrypted verkeer en wordt verdacht verkeer tegengehouden. Middels een portal is via een handig overzicht te zien welke kwetsbaarheden er tegen worden gehouden. Tevens zijn IDS-alerts in te stellen zodat je direct actie kunt ondernemen bij mogelijke escalatie.

### Houdt verdachte pakketjes tegen

De ingebouwde Web Application Firewall (WAF) controleert data die naar de website wordt verzonden en houdt verdachte pakketjes tegen. Veel voorkomende hackaanvallen zoals cross-site scripting (XSS), SQL-injecties en andere veel voorkomende hackaanvallen (OWASP top 10) worden door het platform gesignaleerd en tegengehouden voordat ze schade toebrengen.

### Blokkeert malafide IP-adressen

Wereldwijd zijn er talloze botnets beschikbaar. True maakt gebruik van een uitgebreid netwerk van partijen die deze botnets en bijhorende IP-adressen automatisch blokkeren. Wanneer er nieuwe IP-adressen verschijnen in de zwarte lijsten, worden deze automatisch toegevoegd. Gebruikers van foute IP-adressen worden standaard geblokkeerd. Bij twijfel wordt altijd CAPTCHA toegepast.

# Beschermd tegen externe bedreigingen

Maak kennis met het securityplatform van True. Ontworpen door white hat hackers op basis van jarenlange expertise en inzichten uit de hackerscommunity. Regelmatig geüpdatet met nieuwe intelligentie. Zo blijft de webomgeving maximaal beschermd.

| | DDoS-protectie | Advanced securityplatform |
|---|---|---|
| Beschikbaar in multi-datacenter | • | • |
| Layer 3 traffic floods bescherming | • | • |
| Layer 4 SYN floods bescherming | • | • |
| Layer 7 https-aanval bescherming | • | • |
| Layer 8 CAPTCHA vereist instellen | • | • |
| Extra IP-adressen blacklisten in handige portal (ook geolocaties) | • | • |
| IP-adressen van zwarte lijsten automatisch geblokkeerd | 10 uur | • |
| Bescherming tegen XSS, SQL-injecties en OWASP-aanvallen | 10 uur | • |
| Notificaties ontvangen van aanvallen via Intrusion Detection | 10 uur | • |
| Handig overzicht en statistieken van aanvallen | 10 uur | • |

## Next-level support

Bij True gaan we voor de beste support. Neem je ten minste 6 servers af met SLA-niveau Gold? Dan is het securityplatform kosteloos ingbegepen en kun je rekenen op de snelste reactietijden en engineers die 24/7 voor je klaar staan.

## Multi-datacenter

Het securityplatform is volledig multi-datacenter opgezet. Door de redundante uitvoering blijft de beschikbaarheid van het platform maximaal up-and-running. Zo blijft de website, webshop of web-applicatie beschermd.

## Nog meer security

Naast ons securityplatform bieden wij ook diepgaand security-onderzoek aan. Door middel van een security-audit onderzoeken onze security-engineers uitvoerig waar kwets-baarheden in je webapplicatie zitten. Meer informatie: true.nl/securityaudit.

# De hoogste veiligheids- en compliance-standaarden

## Veilig

Dagelijks speurt ons securityteam naar mogelijke gevaren voor de volledige applicatie-infrastructuur. De experts kijken proactief naar hoe de webomgeving beschermd blijft van invloeden van buitenaf.

## Compliant

True is ISO 27001-, ISO 9001- en NEN 7510-gecertificeerd. Dit betekent dat onze informatieprocessen in kaart zijn gebracht en er uitgebreide beveiligingsmaatregelen zijn genomen.

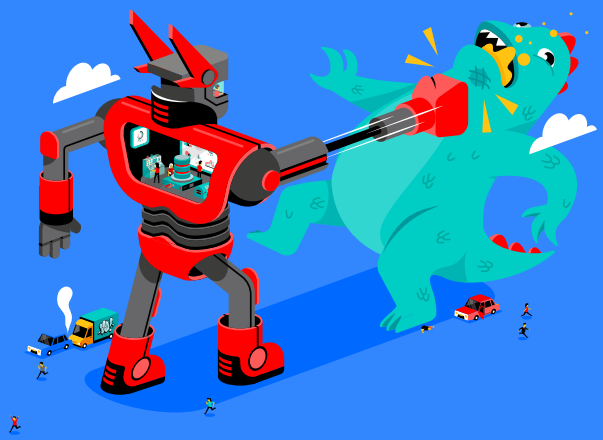
## Schaalbaar

Een webomgeving moet snel in kunnen spelen op veranderingen. Onze servers, database-apps en overige middleware zijn snel up-to-date en klaar om wijzigingen snel door te voeren.

# Saving the world from IT-monsters

Het perfecte samenspel tussen webontwikkelaars, security-, netwerk- en systeemspecialisten is al jaren onze expertise. Ons team bestaat uit experts die de verantwoordelijkheid nemen over de complete webtechnologiestack. Van infrastructuur tot connectiviteit. Van middleware tot data. Voor managed webomgevingen die zijn ingericht om veiligheid, schaalbaarheid en compliance maximaal te borgen. Zo beschermen we de wereld tegen IT-monsters.

**Wil je meer informatie over de security-oplossingen van True? 0800 BEL TRUE of ga naar true.nl/security-management**



**Bezoekadres AMS**
Keienbergweg 100
1101GH Amsterdam

**Bezoekadres MST**
Amerikalaan 1
6199AE Maastricht-Airport

**0800 BEL TRUE**
info@true.nl
www.true.nl