**VDB Computers B.V.**
Vlakdissel 9
1648 HJ De Goorn
info@vdbcomputers.nl
0229-544704

# CyberSecure Enhanced by Proofpoint, 1 year

Artikelnummer: UI-CyberSecure-1Y-D

## €118,00

Incl. 21% BTW

**UniFi CyberSecure is een premium beveiligingsdienst die de ingebouwde bescherming van UniFi Network verbetert op twee kritieke gebieden:**

**Intrusio…**

UniFi CyberSecure is een premium beveiligingsdienst die de ingebouwde bescherming van UniFi Network verbetert op twee kritieke gebieden:

Intrusion Detection and Prevention (IDS/IPS), aangedreven door Proofpoint.

Verbeterde contentfiltering, aangedreven door Cloudflare.

UniFi beschikt over een uitgebreide suite van cybersecuritytools die zijn gebouwd rond zero-trust networking (ZTNA), waardoor je volledige controle krijgt over de beveiliging van je netwerk. Met UniFi kun je gevoelige systemen isoleren, het aanvalsoppervlak minimaliseren, bedreigingen in realtime monitoren en gedetailleerde, beleidsgestuurde toegangscontrole afdwingen op elke laag van je netwerk.

Compatibiliteit:

UDM-Pro-Max, UDM-Pro, UDM-SE, UCG-Fiber, UCG-Max, UCG-Ultra, UCG-Industrial, UDR7, UX7, UXG-Fiber, UXG-Max, UXG-Pro, UDW, UDR, UDM

Belangrijkste cybersecurityfuncties

Ontdek de krachtige functies van UniFi CyberSecure, elk gericht op het beschermen van je netwerk:

Netwerk- en clientisolatie: Voorkom laterale beweging door VLAN’s, draadloze netwerken en individuele clients te isoleren—zodat apparaten alleen communiceren waar dit expliciet is toegestaan.

Organisaties & IdP-integratie: Centraliseer beheer en stroomlijn gebruikersbeheer met naadloze onboarding en offboarding, en veilige authenticatie via identity providers zoals Google Workspace en Microsoft Entra ID, inclusief ondersteuning voor MFA.

Intrusion Detection and Prevention (IDS/IPS): Monitor en analyseer netwerkverkeer in realtime om verdachte activiteiten te detecteren en te

blokkeren, zodat ongeautoriseerde toegang, exploits en andere bedreigingen worden voorkomen.

Content- en domeinfiltering: Blokkeer expliciete, kwaadaardige of ongewenste domeinen binnen je netwerken met vooraf ingestelde filters en aangepaste regels.

CyberSecure verbeterd door Proofpoint en Cloudflare: Maak gebruik van realtime threat intelligence en domeinfilterdiensten om een extra beveiligingslaag voor je netwerk te bieden.

Applicatiefiltering: Blokkeer of sta snel specifieke applicaties of volledige categorieën van applicaties toe.

SSL-inspectie: Ontsleutel en inspecteer verkeer om verborgen bedreigingen te detecteren en een completer beveiligingsniveau te verkrijgen.

Veilige VPN en SD-WAN: Zorg voor veilige connectiviteit tussen locaties en externe gebruikers met intelligente routering en versleuteling, geoptimaliseerd voor prestaties en betrouwbaarheid.

Verkeerslogs: Bekijk gedetailleerde flowlogs van alle netwerkactiviteiten om gebruikspatronen te analyseren, beveiligingsgebeurtenissen te monitoren en problemen op te lossen.

Systeemactiviteitslogs: Houd administratieve acties, systeemgebeurtenissen en configuratiewijzigingen binnen je UniFi-omgeving bij voor audit- en compliance-inzichten.

Honeypot: Implementeer lokservices in je netwerk om kwaadaardige scans of inbraakpogingen te detecteren en te registreren voordat echte systemen worden gecompromitteerd.

Verbeterde Intrusion Detection en Prevention

Het IDS/IPS-systeem van UniFi Network scant verkeer op bekende dreigingspatronen — zogenaamde signatures — zoals IP-adressen, poorten of protocolafwijkingen.

CyberSecure breidt dit systeem uit met:

Een signaturebibliotheek uitgebreid tot meer dan 95.000 definities.

Wekelijkse updates met 30–50+ nieuwe signatures, afkomstig van Proofpoint en het Microsoft Active Protections Program (MAPP).

Minder false positives dankzij zorgvuldig samengestelde signature-sets.

Ondersteuning voor meer dan 50 dreigingscategorieën, waardoor gerichtere beleidscontrole mogelijk is.

Verbeterde Contentfiltering

CyberSecure verbetert de standaard contentfilter van UniFi door Cloudflare-gestuurde filtering te activeren met meer dan 100 gedetailleerde categorieën, waardoor je nauwkeurige controle krijgt over wat gebruikers en apparaten kunnen openen. Hierdoor kun je op maat gemaakte filterbeleid opstellen op basis van compliance-eisen, gebruikersgroepen of VLAN’s. Dit is vooral waardevol voor professionele omgevingen die meer nodig hebben dan eenvoudige, standaard filtering.

Dit is ideaal voor netwerken die het volgende vereisen:

Fijnmazige controle over webtoegang

Naleving van organisatorisch of regulatoir beleid (bijv. CIPA)

Schaalbare contentfiltering voorbij netwerkbrede standaardinstellingen