

**Persbericht**

**Sophos lanceert XGS-serie firewallapparatuur**

**met Transport Layer Security**

*Recent onderzoek ervaart toename van het aantal cybercriminelen dat TLS gebruikt om aanvallen uit te voeren*

OXFORD, 21 april 2021 – **Sophos lanceert vandaag zijn nieuwe XGS-serie firewallapparatuur met ongekende prestaties en geavanceerde bescherming tegen cyberaanvallen. De nieuwe apparaten zijn voorzien van Transport Layer Security met ondersteuning voor TLS 1.3, en technologie die tot vijf keer sneller is dan andere modellen in de markt op dit moment.**

"Sophos Firewall XGS Series is de belangrijkste hardware-upgrade die we ooit hebben uitgebracht en biedt enorme kansen binnen EMEA" zegt Kevin Isaac, Senior Vice President bij Sophos. “Het afgelopen jaar heeft de digitale transformatie een enorme vlucht genomen. Nieuwe en in rap tempo opgeschaalde digitale bedrijfsprocessen mede door de noodzaak om medewerkers op afstand te ondersteunen hebben nieuwe risico's met zich meegenomen maar ook kansen gecreëerd. Organisaties hebben behoefte aan krachtige next-gen bescherming die hen en hun dagelijkse activiteiten kan beschermen tegen dreigingen zoals ransomware en andere malware."

"Sophos’ Firewall XGS Series vertegenwoordigt de belangrijkste hardware-upgrade die we ooit hebben uitgebracht en biedt ongeëvenaarde opsporing, bescherming en snelheid", vult Dan Schiappa aan, Chief Product Officer bij Sophos. "Securityteams kunnen het zich niet langer veroorloven om versleuteld verkeer over het hoofd te zien uit angst iets kapot te maken of de prestaties te schaden. We hebben de Sophos Firewall-hardware volledig opnieuw ontworpen om het moderne versleutelde internet aan te kunnen. Securityteams hebben nu de mogelijkheid om eenvoudig versleuteld verkeer te inspecteren en hun licht te laten schijnen op wat ooit een zwart gat was. Dit kan nu vol vertrouwen zonder op prestaties in te leveren. "

**TLS om opsporing te voorkomen**

Sophos heeft ook het nieuwe onderzoek "[Nearly Half of Malware Now Use TLS to Conceal Communications](https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications)" gepubliceerd. Hierin wordt vastgesteld dat cybercriminelen bij hun aanvallen Transport Layer Security gebruiken. Deze steeds populairder wordende tactiek wordt door tegenstanders gebruikt om de inhoud van kwaadaardige communicatie te versleutelen en te verdoezelen om opsporing tijdens het uitvoeren van aanvallen te voorkomen.

45% van de malware die tussen januari en maart 2021 door Sophos werd gedetecteerd, gebruikte TLS om kwaadaardige communicatie te verbergen, een stijging c.q. bijna verdubbeling ten opzichte van de 23% die Sophos begin 2020 meldde. Sophos heeft het afgelopen jaar ook een toename gezien in het gebruik van TLS om ransomware-aanvallen uit te voeren – met name bij handmatig ingezette ransomware. Het merendeel van het kwaadaardige TLS-verkeer dat Sophos heeft gedetecteerd, bestaat uit initiële malware zoals loaders, droppers en document-gebaseerde installatieprogramma's zoals BazarLoader, GoDrop en ZLoader.

"TLS heeft de privacy van communicatie via internet ongetwijfeld ten goede veranderd. Ondanks al het goede is het voor aanvallers veel gemakkelijker geworden om kwaadaardige modules te downloaden en te installeren en gestolen gegevens te exfiltreren – dit alles recht onder de neus van IT-beveiligingsteams en de meeste beveiligingstechnologieën”, vervolgt Schiappa. “Aanvallers maken gebruik van TLS-beveiligde web- en cloudservices voor het afleveren van malware. Deze initiële malware is ‘de voorhoede’ voor grotere aanvallen zoals ransomware. "

**Versnellen van bescherming tegen bedreigingen**

Aangedreven door Sophos Firewall's Xstream-architectuur, biedt XGS Series-apparatuur de beste zero-day-bescherming tegen bedreigingen, waarbij de meest geavanceerde bekende en potentiële bedreigingen worden geïdentificeerd en gestopt, inclusief ransomware. Bescherming wordt gevoed door krachtige *threat information*, alleen beschikbaar via SophosLabs Intelix en gebaseerd op petabytes aan SophosLabs-dreigingsdata. Verdachte bestanden worden veilig geëlimineerd in SophosLabs Intelix’ virtuele omgevingen en worden onderworpen aan een diepgaande statische analyse voor extra detectiebereik en dataverzameling.

Nieuwe Xstream-flowprocessoren in de apparaten versnellen automatisch vertrouwd netwerkverkeer, zoals software as a service (SaaS), software-defined wide-area networks (SD-WAN), en cloudtoepassingen, waardoor maximale resources worden geboden voor verkeer dat TLS en diepere inspectie vereist. Dit vermindert de latency aanzienlijk en verbetert de algehele prestaties voor belangrijke bedrijfstoepassingen, met name die welke realtime gegevens gebruiken. Bovendien zijn de Xstream-flowprocessoren software-programmeerbaar, waardoor Sophos in de toekomst nog meer verkeer kan offloaden. Samen met meer flexibiliteit om de connectiviteit op de hardware zelf te verbeteren en aan te passen, beschermt dit de hardware-investering van klanten gedurende de volledige levenscyclus, terwijl ook hun bedrijf wordt beschermd.

Sophos biedt een uniek en intuïtieve dashboardzichtbaarheid van TLS-verkeer en inspectieproblemen, en beveiligingsbeheerders kunnen met één klik uitzonderingen toevoegen voor problematische streams. De prestaties zijn ook out-of-the-box geoptimaliseerd met een uitgebreide set regels die worden bijgewerkt en onderhouden door SophosLabs om veilig verkeer van inspectie uit te sluiten.

Sophos Firewall XGS Series-apparatuur en -firmware kunnen eenvoudig worden beheerd op het cloudgebaseerde Sophos Central-platform naast Sophos 'volledige portfolio van de volgende generatie cyberbeveiligingsoplossingen. Oplossingen delen informatie over bedreigingen en reageren automatisch op beveiligingsincidenten via de unieke gesynchroniseerde beveiligingsaanpak van Sophos. Integratie met Sophos Managed Threat Response verhoogt de bescherming verder met menselijke analyse voor 24/7 volledig beheerde opsporing en respons op dreigingen.

**Beschikbaarheid**

Sophos Firewall XGS-serie desktop en de meeste 1U rackmount-apparaten zijn exclusief verkrijgbaar via Sophos' wereldwijde kanaal van meer dan 53.000 partners en MSP's. De modellen zijn geschikt voor kleine, middelgrote en gedistribueerde organisaties als een allesomvattende netwerkbeveiligingsoplossing met een sterke prijs-prestatieverhouding en diverse add-on connectiviteitsopties. Aanvullende modellen die zijn ontworpen voor enterprise edge-omgevingen die een maximale doorvoer vereisen voor complexere netwerkconfiguraties zijn in de komende weken beschikbaar. Vereenvoudigde licentieverlening omvat gebundelde bescherming met verbeterde ondersteuning voor de ultieme bescherming en maximale waarde.

**Over Sophos**

Als een wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties, ongeacht bedrijfsgrootte, in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen van vandaag. Aangedreven door SophosLabs, een wereldwijd team gespecialiseerd in bedreiginginformatie en wetenschappelijke data, beveiligen Sophos’ cloud-native en AI-verbeterde oplossingen endpoints (laptops, servers en mobiele apparaten) en netwerken tegen immer evoluerende cybercriminele tactieken en technieken. Hieronder vallen onder meer geautomatiseerde en actieve, vijandige inbreuken, ransomware, malware, exploits, data-exfiltration, phishing en meer. Het cloudgebaseerde Sophos Central-platform integreert Sophos’ gehele portfolio - van Intercept X-endpointoplossing tot XG Firewall - in een enkel systeem: Synchronized Security.

Sophos-producten zijn exclusief verkrijgbaar via een wereldwijd kanaal van meer dan 53.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën ook beschikbaar aan consumenten via Sophos Home. Het bedrijf is gevestigd in Oxford, Verenigd Koninkrijk. Meer informatie: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816.