**Sophos lanceert nieuwe versie van Endpoint Detection and Response (EDR)**

*Deze nieuwe versie is ontworpen voor beveiligingsanalisten en IT-beheerders en bevat mogelijkheden voor het live ontdekken en reageren*

**OXFORD, U.K.**– 9 juni 2020 –  **Sophos heeft vandaag een bijgewerkte versie van zijn Endpoint Detection and Response (EDR) onthuld, de eerste oplossing die is ontworpen voor zowel veiligheidsanalisten als IT-beheerders. De nieuwste versie is vanaf heden beschikbaar in Sophos Intercept X Advanced en Intercept X Advanced for Server met EDR. Aanzienlijke verbeteringen en nieuwe mogelijkheden maken het voor beveiligingsanalisten sneller en gemakkelijker dan ooit tevoren om ontwijkende bedreigingen te identificeren en te neutraliseren, en voor IT-beheerders om proactief veilige IT-activiteiten te onderhouden om het risico te verminderen.**

Zoals Sophos onlangs blootlegde in het State of Ransomware 2020-onderzoek, kon in België slechts 23% van de organisaties die door een ransomware-incident waren getroffen de inbraak detecteren en stoppen voordat het hun bestanden kon versleutelen. De nieuwe EDR-mogelijkheden van Sophos helpen beveiligings- en IT-teams om bedreigingen en inbreuken op te sporen die normaal gesproken maanden in beslag zouden nemen. Sophos EDR lost dit probleem op en verkort drastisch de tijd die nodig is om tekenen van een inbreuk te detecteren.

“Cybercriminelen verhogen de inzet en doen er alles aan om te profiteren van uitgebreide aanvalsoppervlakken, aangezien organisaties steeds meer naar de cloud verhuizen en externe arbeidskrachten mogelijk maken. Servers en andere eindpunten zijn maar al te onvoldoende beschermd, waardoor kwetsbare toegangspunten ontstaan ​​die voor aanvallers klaar zijn om te misbruiken,” aldus Dan Schiappa, Sophos’ Chief Product Officer. “Sophos EDR helpt bij het identificeren van deze aanvallen, het voorkomen van inbreuken en schijnt zijn licht op anders donkere gebieden. Live-zoekmogelijkheden die alleen beschikbaar zijn met Sophos EDR in Intercept X stellen organisaties in staat om te zoeken naar eerdere indicatoren van compromissen en de huidige systeemstatus te bepalen. Dit intelligentieniveau is van cruciaal belang voor het begrijpen van het veranderende gedrag van aanvallers en het verminderen van de verblijfstijd van aanvallers.”

Sophos EDR biedt nu een krachtige zichtbaarheid over het hele landscape van een organisatie, waardoor beveiligings- en IT-professionals snel vragen over kritieke bedreigingen en IT-beveiligingsactiviteiten kunnen beantwoorden en gemakkelijk kunnen reageren. Nieuwe functies zijn onder meer:

* **Live Discover:** In tegenstelling tot andere EDR-tools die slechts één tot twee weken gegevens opslaan, biedt Sophos EDR een dataretentie van 90 dagen met het standaardaanbod. Met kant-en-klare SQL-queries kunnen beheerders de jacht op bedreigingen en IT-vragen beantwoorden, en kan worden geselecteerd uit een bibliotheek met vooraf geschreven opties en volledig aangepast door gebruikers. Deze flexibele query-engine biedt toegang tot enkele van de meest gedetailleerde opnamen van eindpuntactiviteiten die verder worden verbeterd met Sophos' deep learning-technologie
* **Live Response**: Op afstand reageren en toegang krijgen tot eindpunten en servers via een opdrachtregelinterface om verder onderzoek uit te voeren en problemen op te lossen; eenvoudig apparaten opnieuw opstarten, software installeren en verwijderen, actieve processen beëindigen, scripts uitvoeren, configuratiebestanden bewerken, forensische tools uitvoeren, machines isoleren en meer

Sophos EDR wordt mogelijk gemaakt door het diepgaande neurale netwerk van Sophos, dat is getraind op honderden miljoenen monsters om te zoeken naar dreigingsindicatoren. Beveiligingsanalisten en IT-beheerders krijgen ook on-demand toegang tot door SophosLabs beheerde informatie over bedreigingen, die dagelijks meer dan 400.000 malwaremonsters opspoort, deconstrueert en analyseert.

Sophos EDR is nu beschikbaar in Sophos Intercept X Advanced met EDR en Intercept X Advanced voor Server met EDR zonder extra kosten, en ondersteunt Windows, MacOS en Linux. De nieuwe Live Discover- en Live Response-functies kunnen eenvoudig worden beheerd in het dreigingsanalysecentrum op het cloudgebaseerde Sophos Central-platform voor realtime informatie-uitwisseling met Sophos' hele portfolio van cyberbeveiligingsoplossingen van de volgende generatie via zijn unieke Synchronized Security-aanpak. Gecombineerd met Sophos Managed Threat Response (MTR), een volledig beheerde service voor het opsporen, detecteren en beantwoorden van bedreigingen, kunnen organisaties hun mogelijkheden vergroten met menselijke analyse voor een verder ontwikkelde benadering van proactieve beveiliging.

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