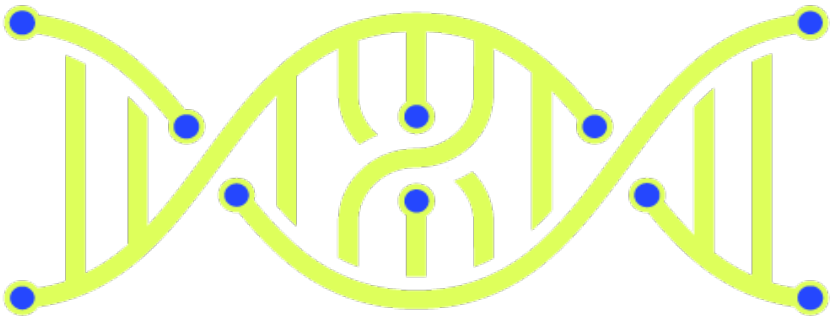


Protéger les endpoints avec intelligence

Une défense parfaite et rapide des menaces inconnues avec deep learning

Deep Instinct for Endpoints: les points forts

- Repousse les cyberattaques en moins de 20 millisecondes
- Bloque également les attaques de ransomware complexes à plusieurs niveaux
- Détecte 99 % des logiciels malveillants inconnus
- Maximum 0,1 % de faux positifs
- Basé sur une technologie de deep learning spécialement conçue pour la cybersécurité
- La fonction de protection ne nécessite pas de connexion Internet permanente

Jusqu'à présent, les solutions de protection endpoint – de l'antivirus classique à la plateforme EDR/XDR – misaient principalement sur un comportement réactif pour se défendre contre les attaques inconnues. Le risque que des attaques soient lancées sur le réseau de l'entreprise et qu'elles causent des dommages est ainsi encouru. Pour changer cela et permettre une défense contre les menaces basée sur la prévention, les experts en IA et en cybersécurité Guy Caspi, Nadav Maman et le Dr Eli David se sont attelés à la tâche en 2015 et ont commencé à développer le premier et jusqu'à présent le seul cadre d'apprentissage en profondeur spécialement adapté à la cyber sécurité: la «plateforme de prévention Deep Instinct». De cette plateforme sont nées d'une part la société Deep Instinct, dont le siège est à Tel Aviv, et d'autre part la solution «Deep Instinct for Endpoints» – une protection des points de terminaison qui stoppe également les codes malveillants inconnus tels que les ransomwares et autres malwares en moins de 20 millisecondes. Soit une vitesse 750 fois plus rapide que la capacité de cryptage du ransomware connu le plus rapide. L'immense réseau neural de Deep Instinct apprend en laboratoire à partir de centaines de millions de fichiers et de scripts bons et malveillants, arrive à comprendre l'«ADN» des menaces et adapte de manière autonome l'algorithme de leur détection. Le cerveau Deep Instinct ainsi créé en laboratoire fait partie intégrante de l'agent léger qui est déployé sur les endpoints et assure la prévention de toutes sortes de menaces pratiquement en temps réel.

Deep Instinct for Endpoints bloque les cyberattaques de manière fiable

Deep Instinct met l'accent sur la prévention plutôt que sur la réaction «after the fact» dans la défense contre les cyberattaques: un agent léger doté du cerveau spécialement entraîné de Deep Instinct repousse les attaques les plus avancées, y compris les ransomwares inconnus, avant qu'elles ne soient lancées et ne puissent donc causer des dégâts.

Prévention grâce au deep learning

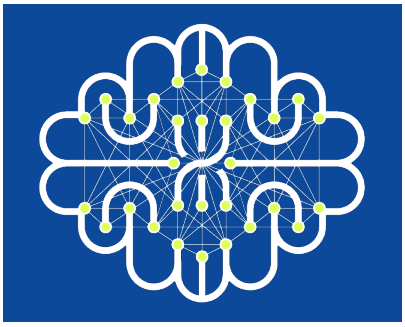
Deep Instinct for Endpoints s'appuie entièrement sur sa propre technologie basée sur des agents et le deep learning, une forme avancée d'apprentissage automatique. Le réseau neural de Deep Instinct tire des enseignements d'une énorme quantité d'informations sur les menaces provenant du monde entier, y compris des fichiers et des scripts malveillants et inoffensifs, et en tire en quelque sorte l'empreinte génétique des cybermenaces. C'est sur cette base que le cerveau Deep Instinct est créé. Celui-ci est contenu dans l'agent léger qui est installé sur les terminaux et n'utilise que peu de ressources système. Contrairement aux solutions de protection des endpoints basées sur des signatures, l'agent de Deep Instinct ne nécessite qu'une à deux mises à jour par an.

Défense parfaite contre les ransomwares

Les ransomwares mettent jusqu'à 15 secondes pour commencer à crypter les données, alors que Deep Instinct n'a besoin que de 20 millisecondes pour les détecter et les bloquer. Deep Instinct promet en outre un taux de détection de 99 % des logiciels malveillants inconnus et garantit moins de 0,1 % de faux positifs, ce qui réduit considérablement la charge de travail de l'équipe de sécurité, en lui permettant de ne s'occuper que des incidents vraiment graves.

Protection contre tous les types de menaces

Le cerveau Deep Instinct analyse et empêche l'exécution de fichiers et de scripts avant même que les logiciels malveillants connus et inconnus, les exploits zero-day et les ransomwares ne puissent se déclencher. La solution vérifie un grand nombre de types de fichiers tels que les exécutables portables, PDF, Office, les polices, TIFF, JAR et les macros. Contre d'autres types d'attaques – telles que les attaques sans fichier et à plusieurs niveaux, l'injection de code à distance, les logiciels espions ou le vol d'identifiant/dumping – des mécanismes de protection supplémentaires à plusieurs niveaux sont utilisés, comme l'analyse comportementale ou le mappage MITRE ATT&CK. Un module spécial s'occupe de la défense contre les attaques via Windows PowerShell.



Pour la prévision et la prévention des attaques, l'agent n'a pas besoin d'accéder à une unité centrale ou au cloud – un autre facteur déterminant pour la vitesse exceptionnellement élevée.

Utilisation flexible

Deep Instinct for Endpoints est disponible pour Windows, macOS et Linux, ainsi que pour Chrome OS et Android, et fonctionne avec les plateformes SIEM et SOAR. La solution peut également être utilisée en complément des solutions EDR/XDR et du service Defender ATP de Microsoft 365, afin d'augmenter considérablement la défense au niveau des postes de travail contre les logiciels malveillants et les ransomwares inconnus et de réduire fortement le nombre de faux positifs.

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Téléphone +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Téléphone +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Téléphone +49 731 85074823 / info@boll-europe.com / www.boll-europe.com