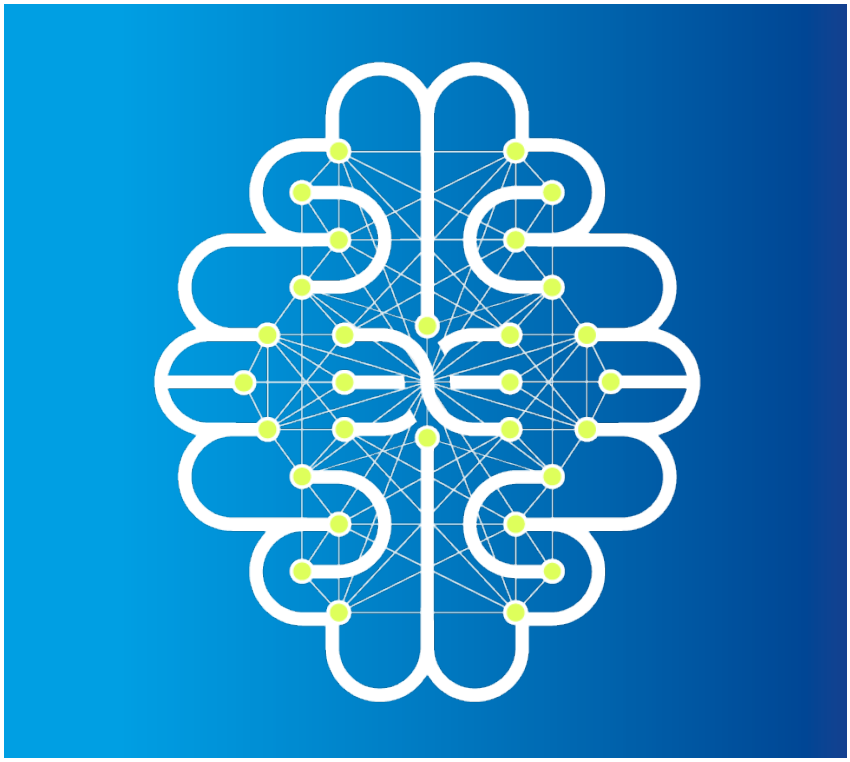
La protection endpoint parfaite: la prévention plutôt que la réaction

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. Deep Instinct emprunte une autre voie et place la prévention au premier plan: un agent léger doté d'un deep learning engine spécialement développé bloque même les attaques les plus avancées avant qu'elles ne puissent causer des dommages.

Les solutions traditionnelles de protection endpoint basées sur des signatures, règles et heuristiques bloquent de manière fiable les codes malveillants connus, mais échouent souvent face aux parasites inconnus, aux attaques zero-day et aux méthodes d'attaque avancées de plus en plus fréquentes. Mais c'est surtout la vitesse effarante à laquelle les attaques de ransomware cryptent les données qui appelle à trouver de nouvelles solutions. Les solutions «extended detection and response» (EDR/XDR) fournissent certes une protection accrue, mais n'offrent pas encore la vitesse nécessaire pour se défendre contre les nouvelles menaces en temps réel. En effet, au cœur de ces solutions se trouve la post-analyse des processus suspects «after the fact», c'est-à-dire lorsque le code malveillant est souvent déjà exécuté. Pour protéger le réseau de l'entreprise et limiter les dégâts, les points finaux infectés sont souvent isolés automatiquement. Par conséquent, quelqu'un doit analyser les dommages potentiels. A cela s'ajoute la restauration correspondante de l'état initial.



Prévention grâce au deep learning

Le spécialiste de la cybersécurité Deep Instinct, dont le siège principal est à New York et le site de développement à Tel Aviv, adopte une approche différente, inédite et prometteuse. «Deep Instinct for Endpoints» mise entièrement sur une technologie allégée, basée sur des agents et sur le deep learning, une forme avancée du machine learning. Le réseau neural de Deep Instinct apprend à partir de centaines de millions de fichiers et de types de fichiers (y compris des fichiers malveillants et non malveillants), comprend l'«ADN» des menaces, adapte automatiquement les algorithmes et empêche les attaques pratiquement en temps réel ou en moins de 20 millisecondes, c'est-à-dire bien avant que le logiciel malveillant ne se propage.

Les ransomwares mettent généralement jusqu'à 15 secondes avant de commencer à crypter les données de manière malveillante, soit bien plus que les 20 millisecondes maximum nécessaires à Deep Instinct pour les détecter et les bloquer. De plus, Deep Instinct promet un taux de détection de 99 % pour les logiciels malveillants inconnus et garantit moins de 0,1 % d'alertes faussement positives. Ce dernier point allège considérablement la charge de travail de

l'équipe de sécurité. Le deep learning n'est pas nouveau en soi – il est utilisé par exemple pour la conduite autonome, la reconnaissance faciale ou en médecine. Contrairement au machine learning classique, le deep learning fonctionne automatiquement et ne nécessite pas l'entraînement de modèles par des acteurs humains. Pour sa solution de protection endpoint, Deep Instinct utilise un cadre d'apprentissage en profondeur spécialement conçu pour la cybersécurité, ce qui lui permet de proposer une solution de bout en bout à partir d'une source unique, sans dépendre de fournisseurs tiers. Il s'agit du premier et du seul framework de deep learning pour la cybersécurité à ce jour.

Intelligence incarnée par l'agent

Dans le cas de «Deep Instinct for Endpoints», l'intelligence artificielle entièrement formée, en quelque sorte le «cerveau» de la solution, se trouve directement dans l'agent sur le terminal, qui ne sollicite pourtant que très peu les ressources du système. L'agent n'a pas besoin d'accéder au cloud pour prédire et prévenir les attaques par des logiciels malveillants connus et inconnus, des exploits du zero-day, des ransomwares et des scripts courants – un autre facteur déterminant pour la vitesse exceptionnellement élevée. La solution prend en charge un grand nombre de types de fichiers, y compris les fichiers PDF, Office, fonts, TIFF, JAR et les macros. Des mécanismes de protection supplémentaires à plusieurs niveaux, comme l'analyse comportementale, sont utilisés contre d'autres types d'attaques, tels que les attaques sans fichier et à plusieurs niveaux, l'injection de code à distance, les logiciels espions ou le vol/dumping de données. Un module spécial s'occupe de la défense contre les attaques via Windows PowerShell.

«Deep Instinct for Endpoints» est disponible pour Windows, MacOS et Linux ainsi que pour Chrome OS et Android. Dans certains scénarios de PME, la solution répond entièrement aux besoins de protection des points finaux. Deep Instinct peut également être utilisé en complément des solutions EDR/XDR et du service Defender ATP de Microsoft 365, afin d'augmenter considérablement la défense au niveau du poste de travail contre les logiciels malveillants inconnus et les ransomwares. Deep Instinct réduit également considérablement le nombre de faux positifs dans les solutions XDR, SIEM et SOAR, ce qui allège considérablement la charge de travail de l'équipe de sécurité du client final ou du partenaire de sécurité.

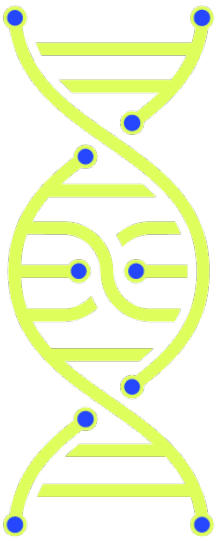
Deep Instinct for Endpoints: les points forts

- 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
- Fonctionne avec des agents légers et adaptés au système sur les endpoints

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15,
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch



deep instinct™

→ **www.boll.ch/de/deepinstinct**