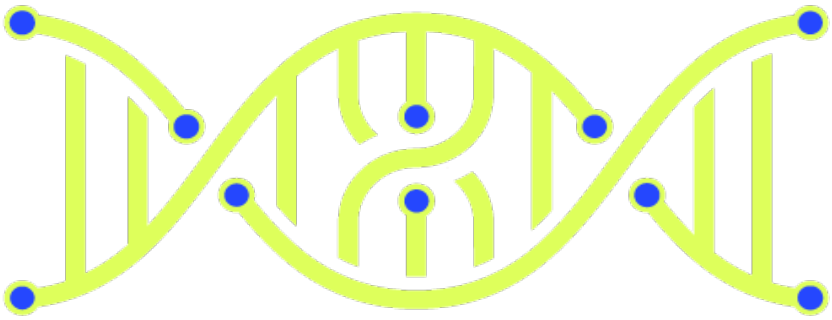


Endpoints mit Intelligenz schützen

Perfekte, schnelle Abwehr unbekannter Bedrohungen mit Deep Learning

Deep Instinct for Endpoints: Die Highlights

- Wehrt Cyberangriffe aller Art direkt auf dem Endpoint in unter 20 Millisekunden ab
- Stoppt auch mehrstufige, komplexe Ransomware-Attacken
- Erkennt 99 Prozent aller unbekannten Malware
- Schützt auch vor PowerShell-, Code-Injection-, Zero-Day- und Fileless-Attacken
- Maximal 0,1 Prozent falsch positive Resultate
- Basiert auf speziell für Cybersecurity zugeschnittener Deep-Learning-Technologie
- Protection-Funktion benötigt keine permanente Internetverbindung

Bisherige Endpoint-Schutzlösungen – von klassischen Antiviruslösungen bis zu EDR-/XDR-Plattformen – setzen bei der Abwehr unbekannter Angriffe primär auf ein reaktives Verhalten. Dadurch wird in Kauf genommen, dass Angriffe im Unternehmensnetzwerk ausgeführt werden und es zu einem Schaden kommen kann. Dies zu ändern und eine präventionsbasierte Bedrohungsabwehr zu ermöglichen, haben die KI- und Cybersecurity-Experten Guy Caspi, Nadav Maman und Dr. Eli David im Jahr 2015 auf ihre Fahne geschrieben und mit der Entwicklung des ersten und bisher einzigen speziell auf Cybersecurity zugeschnittenen Deep-Learning-Frameworks begonnen: der «Deep Instinct Prevention Platform». Daraus hervorgegangen sind einerseits die Firma Deep Instinct mit Hauptsitz in Tel Aviv und andererseits die Lösung «Deep Instinct for Endpoints» – ein Endpunktschutz, der auch unbekannten Schadcode wie Ransomware und andere Malware innert weniger als 20 Millisekunden stoppt. Das ist 750-mal schneller, als die schnellste bekannte Ransomware ihre schädlichen Verschlüsselungsaktivitäten entfalten kann. Das riesige neurale Netzwerk von Deep Instinct lernt im Labor aus Hunderten Millionen guten und bösartigen Dateien sowie Scripts, versteht dadurch die «DNA» von Bedrohungen und passt den Algorithmus für deren Erkennung selbstständig an. Das daraus im Labor entstandene Deep Instinct Brain ist Bestandteil des schlanken Agenten, der auf den Endpunkten zum Einsatz kommt und für die Prävention von Bedrohungen aller Art praktisch in Echtzeit sorgt.

Deep Instinct for Endpoints unterbindet Cyberattacken zuverlässig

Deep Instinct stellt bei der Abwehr von Cyberattacken statt der Reaktion «after the fact» die Prävention in den Vordergrund: Ein schlanker Agent mit dem speziell trainierten Deep Instinct Brain wehrt fortschrittlichste Angriffe inklusive unbekannter Ransomware ab, bevor diese ausgeführt werden und somit Schaden anrichten können.

Prävention durch Deep Learning

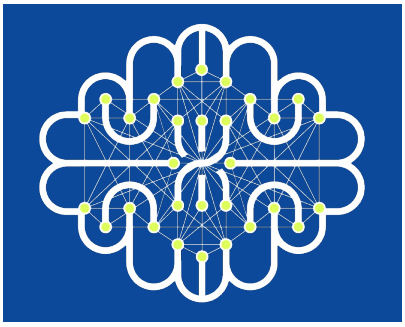
Deep Instinct for Endpoints setzt ganz auf eine eigens entwickelte agentenbasierte Technologie auf der Basis von Deep Learning, einer fortgeschrittenen Form von Machine Learning. Das neurale Netzwerk von Deep Instinct gewinnt aus einer riesigen Menge von Bedrohungsinformationen aus der ganzen Welt, darunter schädliche und unschädliche Dateien sowie Scripts, Erkenntnisse und erstellt daraus gewissermassen den genetischen Fingerabdruck von Cyber-Bedrohungen. Auf dieser Basis entsteht das Deep Instinct Brain. Dieses ist im schlanken Agenten enthalten, der auf den Endpunkten installiert wird und nur wenig Systemressourcen beansprucht. Im Gegensatz zu signaturbasierten Endpunktschutzlösungen benötigt der Agent von Deep Instinct nur ein- bis zweimal pro Jahr ein Update.

Perfekte Ransomware-Abwehr

Ransomware benötigt bis zu 15 Sekunden, bis die böswillige Verschlüsselung der Daten beginnt, während Deep Instinct für die Erkennung und Abwehr nicht einmal 20 Millisekunden braucht. Deep Instinct verspricht zudem eine Erkennungsrate von 99 Prozent unbekannter Malware und garantiert, dass mit weniger als 0,1 Prozent falsch positiven Warnungen zu rechnen ist – eine massgebliche Entlastung für das Security-Team, das sich nur noch um wirklich gravierende Vorfälle kümmern muss.

Schutz vor allen Bedrohungstypen

Das Deep Instinct Brain analysiert und verhindert die Ausführung von Dateien und Scripts, bevor bekannte und unbekannte Malware, Zero-Day-Exploits und Ransomware überhaupt loslegen können. Dabei überprüft die Lösung eine Vielzahl von Dateitypen wie Portable Executables, PDF, Office, Fonts, TIFF, JAR und Makros. Gegen weitere Angriffsarten wie dateilose und mehrstufige Attacken, Remote Code Injection, Spyware oder Credential Theft/Dumping kommen zusätzliche, mehrschichtige Schutzmechanismen wie verhaltensbasierte Analyse oder MITRE ATT&CK Mapping zum Einsatz. Ein spezielles Modul kümmert sich um die Abwehr von Angriffen via Windows PowerShell.



Für die Voraussage und Prävention von Angriffen benötigt der Agent keinerlei Zugriff auf eine Zentraleinheit oder auf die Cloud – ein weiterer für die ausserordentlich hohe Geschwindigkeit ausschlaggebender Faktor.

Flexibel einsetzbar

Deep Instinct for Endpoints ist für Windows, macOS und Linux sowie Chrome OS und Android erhältlich und arbeitet mit SIEM- und SOAR-Plattformen zusammen. Die Lösung lässt sich zudem ergänzend zu EDR-/XDR-Lösungen und zum Microsoft-365-Dienst Defender ATP einsetzen, um die Abwehr am Endpoint gegen unbekannte Malware und Ransomware deutlich zu erhöhen und die Anzahl der falsch positiven Meldungen stark zu reduzieren.

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