deepinstinct™

RANSOMWARE:

PRÄVENTION IST DIE BESTE MEDIZIN

E-BOOK

EINE WACHSENDE BEDROHUNG

Was ist das derzeit größte Cybersicherheitsrisiko?

Die Bedrohung durch Ransomware ist in aller Munde und ein großes Thema in den Nachrichten. Die jüngsten Vorfälle bei Unternehmen wie Colonial Pipeline und Ireland Health Trust zeigen die schwerwiegenden Auswirkungen von Ransomware-Angriffen auf den Geschäftsbetrieb und auf den wirtschaftlichen Erfolg.

Zwischen 2019 und 2020 – also innerhalb nur eines Jahres – hat die Anzahl der Ransomware-Attacken um 435 % zugenommen*. Aus unserer Sicht gibt es mehrere Gründe für den signifikanten Anstieg dieser Art von Malware. Einer davon ist, dass die Angreifer mittlerweile anders vorgehen: Von 2016 bis 2018 agierten die Cyberkriminellen nach einer auf Masse ausgelegten Strategie. Sie griffen möglichst viele Endkunden nach dem Gießkannenprinzip an. Die Erfolgschancen dieser Methode waren eher gering. Zudem waren viele Opfer, deren Rechner und Daten verschlüsselt wurden, nicht in der Lage oder auch einfach nicht bereit, vier- oder fünfstellige Lösegeldsummen zu zahlen. Für nur wenige war es zwingend notwendig, alle Daten wiederherzustellen – und zahlreiche Opfer hatten ohnehin Backups über ihren Smartphone-Anbieter in der Cloud.

Strategiewechsel

Seit 2019 fokussieren sich die Angreifer vermehrt auf große Organisationen, die eine bedeutende Rolle für die Gesellschaft oder für die Wirtschaft spielen, wie zum Beispiel Krankenhäuser oder andere Institutionen mit zentralen Funktionen. Die Zeit, die diese Unternehmen oder Organisationen benötigen, um den Schaden eines Ransomware-Angriffs zu beheben, wirkt sich nicht nur finanziell aus. Sie gefährdet auch das Leben und das Wohlergehen vieler Menschen. Zu den Sektoren mit besonders hohem Risiko gehören neben dem Gesundheitswesen die verarbeitende Industrie, Regierungen, Energieversorger, Finanzdienstleister, das Bildungswesen und Strafverfolgungsbehörden.

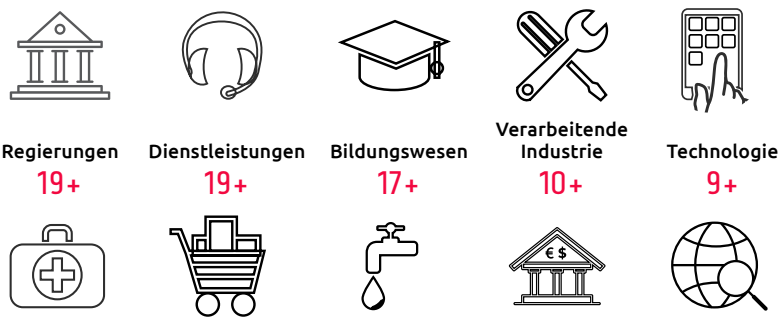
Die Auswirkungen des Colonial Pipeline-Hacks auf Millionen Haushalte und Unternehmen haben deutlich gezeigt, wie Ransomware ganze Infrastrukturen lahmlegen kann. Tragischerweise scheint sich diese Strategie für einige Hackergruppen auszuzahlen, da sie damit immer erfolgreicher sind und hohe Summen erzielen. Lösegelder von mehreren Millionen Dollar sind mittlerweile eher die Regel als die Ausnahme. Viele der besonders gefährdeten Branchen haben entschieden, dass das Lösegeld zu bezahlen das kleinste Übel im Fall eines solchen Angriffs ist.

Ransomware-as-a-Service (RaaS)

Wie Software as a Service (SaaS) ist RaaS ein abonnementbasiertes Modell, mit dem fast jeder ohne hohen Aufwand zum Ransomware-Angreifer werden kann. Dies funktioniert nach einem Franchisemodell, bei dem Cyberkriminelle einen entsprechenden Code schreiben und diesen an die Angreifer verkaufen oder vermieten. Dazu bieten die Franchisegeber technische Anleitungen, wie man einen Ransomware-Angriff am besten durchführt. Ist der Angriff erfolgreich, wird das Lösegeld zwischen dem Franchisegeber und dem Angreifer aufgeteilt. Genauso wie Fast-Food-Ketten mit dem Franchisemodell Reichweiten und Umsätze massiv steigern konnten, hat RaaS zu einem enormen Anstieg von Ransomware-Angriffen geführt.

Erfolgreichste Ransomware-Angriffe nach Branchen 2021

Daten von Januar bis April 2021**



*Quelle: 2020 Cyber Threat Landscape Report, Deep Instinct

**Quelle: Blackfog. The State of Ransomware in 2021

FAKT: Ransomware-Angriffe

Die Lösegeldzahlungen haben sich 2021 durchschnittlich um *fast* 50 % erhöht.

Die Auszahlungen betrugen im Durchschnitt 155.000 US-Dollar Ende des Jahres 2020, stiegen aber auf fast 280.000 US-Dollar im Mai 2021.

Quelle: Blackfog. The State of Ransomware in 2021

AKTIVE RANSOMWARE 2021

REvil/Sodin

Diese Ransomware-Gruppe gibt es seit Anfang 2019. Bekannt wurden sie vor allem durch einige erfolgreiche Angriffe auf Managed Service Provider Ende 2019. Die Ransomware, die diese Gruppe nutzt, ist Sodinokibi. Die Attacken laufen standardmäßig so ab, dass die Gruppe Lösegeld fordert, allerdings nicht droht, Kundendaten offenzulegen oder zu verkaufen.

Ryuk/Conti

Diese Gruppe treibt schon seit 2018 ihr Unwesen. Sie ist also keineswegs neu, aber immer noch eine große Bedrohung. Seit März 2021 hat sie nämlich ihr Vorgehen geändert, indem sie ihre Ransomware mit einer wurmähnlichen Fähigkeit ausgestattet hat. Dies ermöglicht die Übertragung von Rechner zu Rechner, sodass die Payload nicht auf jedem einzelnen Server oder PC von außen platziert werden muss.

Egregor

Diese Ransomware folgte der klassischen Funktionsweise, wurde zuletzt aber weniger häufig eingesetzt, da viele Mitglieder der Organisation verhaftet wurden. 2020 war die Ransomware-Gruppe MAZE eine der größten (und erfolgreichsten), die als RaaS-Unternehmen operierte. Im November 2020 wechselten viele MAZE-Mitglieder, die ihre Arbeit fortsetzen wollten, zu Egregor.

Netwalker

Netwalker ist eine sehr innovative Ransomware-Gruppe, die seit Januar 2021 aufgrund von Beschlagnahmungen und Verhaftungen jedoch nur noch wenig auftritt. Zuvor setzte Netwalker vor allem die Trojaner Emotet und Trickbot ein, mit denen sie sich Zugang zu Netzwerken verschaffte und sich in Unternehmen ausbreitete, um sie zu erpressen.

DoppelPaymer

Im Februar 2021 machte ein „Ausfall“ bei Kia Motors of America Schlagzeilen, der sich später als Angriff mit DoppelPaymer-Ransomware entpuppte. Ziel der Attacke war eigentlich Hyundai, aber den Angreifern gelang es, „nur“ Kia zu schädigen. Dem Unternehmen wurde mit der Veröffentlichung massiver Datenmengen und entsprechendem Imageschaden gedroht, wenn es kein Lösegeld zahlen würde.

Darkside

Hierbei handelt es sich um einen Ransomware-as-a-Company/Ransomware-as-a-Service Provider, der von Mitte 2020 bis Mitte 2021 aktiv war. Diese Gruppe machte erstmals im August 2020 auf sich aufmerksam und stellte sich selbst als die „Guten“ dar, die ihre Angriffe nach dem Robin-Hood-Prinzip ausübten: Sie erpressten „gierige Unternehmen“ und spendeten den Erlös aus den Angriffen für wohltätige Zwecke.

Wichtig ist zu erwähnen, dass dieses Ransomware-Unternehmen gemäß seinem Leitbild Angriffe auf Bildungseinrichtungen, gemeinnützige Organisationen, medizinische Einrichtungen und alles, was als „politisch motiviert“ angesehen werden könnte, verbot.

.

WARUM RANSOMWARE-ANGRIFFE ERFOLGREICH SIND

Jede Sekunde zählt

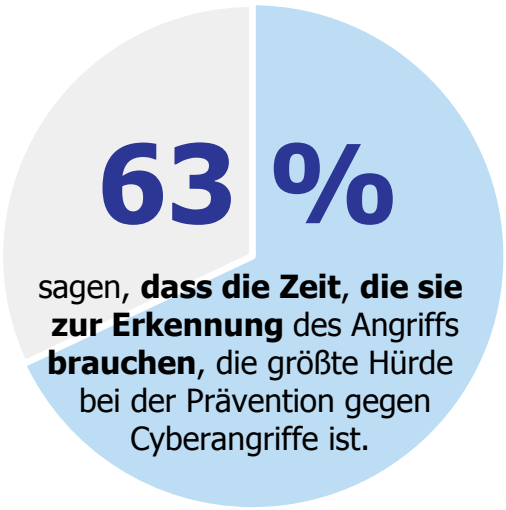
Aktuelle Ansätze zur Bekämpfung von Ransomware konzentrieren sich auf die Erkennung (Detection) und Reaktion (Response). Die meisten Endpoint Detection and Response (EDR)-Lösungen setzen einen Angriff voraus, um ihn als solchen zu erkennen. EDR ist speziell darauf ausgelegt, verdächtige Aktivitäten in Umgebungen zu erkennen, nachdem etwas eingedrungen ist. Klickt ein Benutzer auf eine Datei, die Ransomware enthält, wird diese ausgeführt und das Endgerät kann in weniger als 0,016 Sekunden kompromittiert werden. Eine fortschrittliche EDR-Lösung kann helfen:

- Bedrohungen zu identifizieren
- Bedrohungen zu verfolgen und aufzuzeichnen
- einige Bedrohungen in Quarantäne zu versetzen und einzudämmen
- einige der identifizierten Bedrohungen zu entfernen

Eine EDR-Lösung kommt je nach erkannter Bedrohung ins Spiel und leitet nach der Detektion eine Triage als Reaktion ein. Die Aktionen können Folgendes umfassen:

- Isolierung des kompromittierten Hosts im Netzwerk
- Verfolgung und Aufzeichnung von Endpunktaktivitäten
- Überprüfung des Zeitplans und der Aktivitäten der Ereignisse
- Sammlung und Dokumentation zusätzlicher Bedrohungsindikatoren
- Mögliche Quarantäne und Beseitigung der Bedrohung

Die größte Herausforderung für Unternehmen in diesem Szenario ist die Verweildauer der Ransomware – die Zeit zwischen der Kompromittierung des Endpunkts und der Erkennung und Reaktion. Eine lange Verweildauer erhöht das Risiko, dass eine infizierte Datei ausgeführt wird, sich verbreitet, weitere Payloads ablegt und zudem durch Verschleierung verhindert, dass sie aufgespürt und untersucht werden kann.



Quelle: The Third Annual Study on the State of Endpoint Security Risk. Ponemon Institute LLC, 2020.

DIE ZUKUNFT DER RANSOMWARE-PRÄVENTION

Das weltweit einzige End-to-End Deep Learning Cybersecurity Framework

Deep Learning gibt es schon seit einiger Zeit und es hat in sehr hochentwickelten Branchen zahlreiche Innovationen ermöglicht – vom autonomen Fahren über bessere Empfehlungen auf Streaming-Diensten bis hin zu Spracherkennung etc.

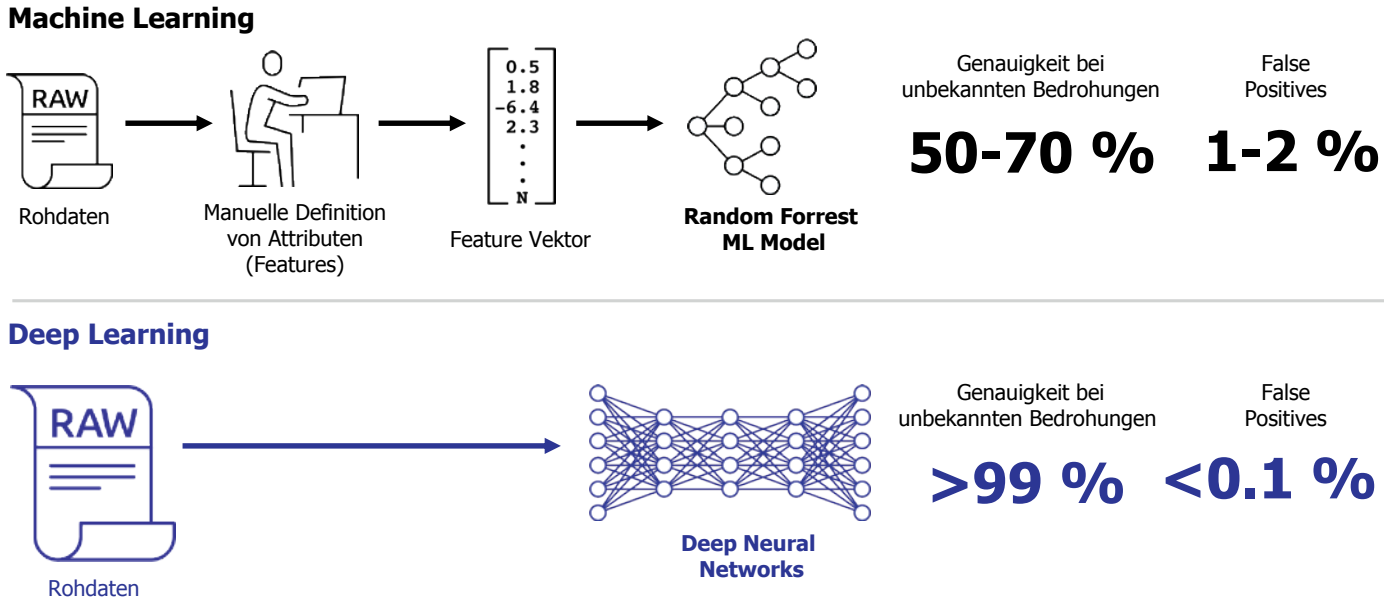
Die Hürde, sich mit Deep Learning zu beschäftigen, ist seit jeher hoch. Man braucht erstklassige Data Scientists, enorm leistungsfähige Rechner mit GPUs (Graphics Processing Units) und man muss mit riesigen Mengen an Rohdaten arbeiten können. Deep Instinct hat sich der Herausforderung gestellt, Deep Learning zur Verbesserung der Erkennung von und der Prävention gegen Cyberbedrohungen zu nutzen. Daher entwickeln wir die einzige dedizierte End-to-End Deep Learning Cybersecurity-Lösung der Welt kontinuierlich weiter. Unser Ziel ist es, Unternehmen mithilfe der besten Vorhersage- und Präventionslösung zu unterstützen, die es gibt.

Die Grenzen von Machine Learning (ML)

Wie können wir also Vorhersagen mit solcher Wirkungskraft und Geschwindigkeit treffen? Deep Learning verfügt über umfangreiche neuronale Netze mit einzigartigen Fähigkeiten, um Aufgaben zu lösen, bei denen Machine Learning (ML)-Modelle an ihre Grenzen stoßen. ML erfordert einen menschlichen Experten, der Attribute (Features) zur Durchführung der Klassifizierung definiert und entwickelt. Diese Attribute (Features) können allerdings von Cyberkriminellen reverse engineered und ausgetrickst werden, wie Forscher in einem Blogartikel für das Produkt Cylance beschrieben haben.

Bei mehreren Gelegenheiten hat unser „Brain" signifikante Ransomware-Familien wie Ryuk erkannt, obwohl es seit zwölf oder 18 Monaten nicht mehr aktualisiert worden war. Wir können Bedrohungen vorhersagen, die noch nicht sichtbar sind.

Oder einfach gesagt: Deep Learning ist weitaus genauer als auf ML basierende Ansätze. Das Beste daran ist vermutlich, dass keine Features entwickelt werden müssen. Dadurch ist es für Cyberkriminelle viel schwieriger, Malware so zu programmieren oder zu verbessern, dass sie unsere Arbeitsweise verstehen und unsere Erkennung und Reaktion aushebeln könnte.



Quelle: The Challenges of Leveraging Threat Intelligence to Stop Data Breaches, Front. Comput. Sci., 28. August 2020

PRÄVENTION VOR DER AUSFÜHRUNG

Ein wichtiges Alleinstellungsmerkmal, das unseren Kunden direkt ins Auge fällt, ist unsere Fähigkeit, Angriffe vor der Ausführung zu verhindern. Statt im Nachhinein Schadensbegrenzung betreiben zu müssen, liegt unser Fokus darauf, zu verhindern, dass eine Bedrohung überhaupt Schaden anrichten kann.

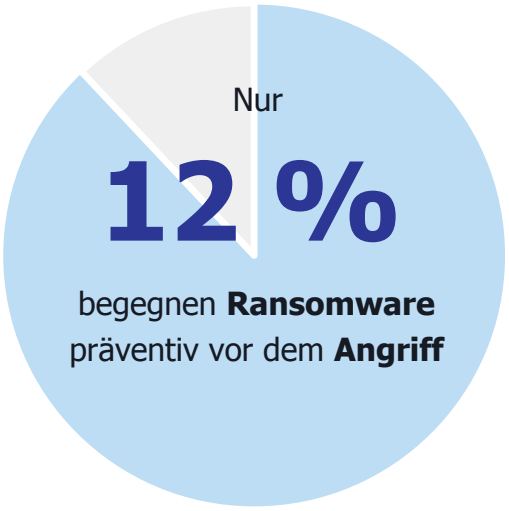
Zehnmal schnellere Entscheidungen als in Echtzeit

Deep Instinct scannt, prognostiziert und verhindert selbst vollkommen neue Malware oder Dateien wie Ransomware und stoppt sie, bevor sie ausgeführt werden. Das heißt, dass Ransomware gar nicht erst in Netzwerke eindringen kann. Unternehmen müssen sich daher keine Sorgen machen, dass ihre Dateien verschlüsselt oder Daten entwendet werden.

Deep Instinct führt diese Scans in weniger als 20 Millisekunden durch. Entscheidungen vor der Ausführung der Malware können dadurch zehnmal schneller getroffen werden. Die meisten Lösungen, die es derzeit gibt, konzentrieren sich hingegen darauf, Ransomware nach erfolgter Ausführung zu erkennen. Die Wahrscheinlichkeit, dass die Cyberkriminellen mit ihrem Angriff erfolgreich sind, ist also höher.

Keine Cloud-Verzögerungen

Der Weg in die Cloud und zurück braucht bei einer Entscheidung Zeit – Zeit, die im Ernstfall darüber entscheidet, ob der Ransomware-Angriff abgewehrt werden kann oder nicht. Deep Instinct kann zwischen gefährlich und harmlos unterscheiden, ohne dass die Daten erst in die Cloud gesendet werden müssen.



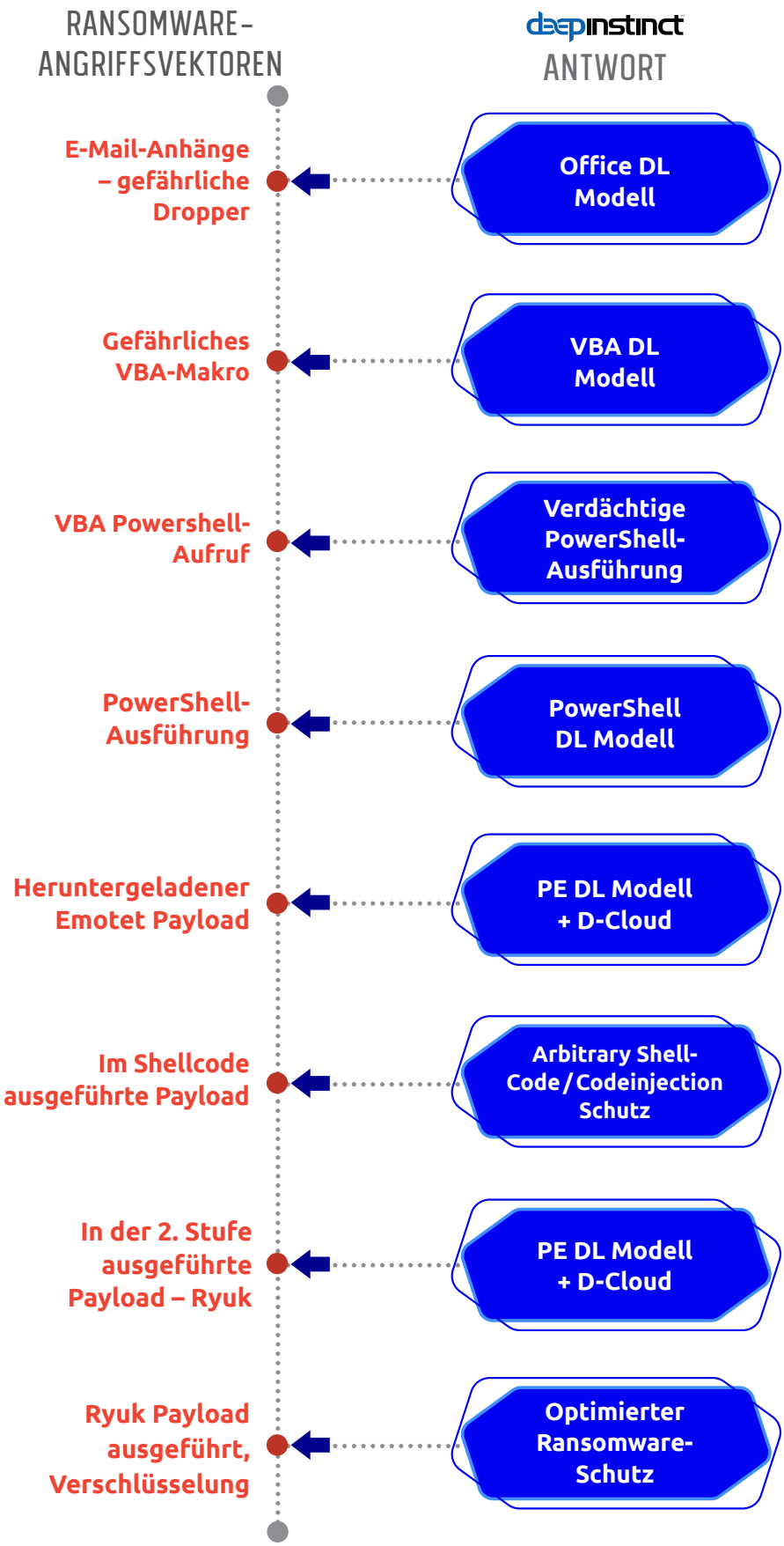
Quelle: The Third Annual Study on the State of Endpoint Security Risk. Ponemon Institute LLC, 2020..

Fakt:

Ein Ransomware-Angriff kostet insgesamt durchschnittlich 440.750 US-Dollar, doch **nur 10 % dieser Kosten wurden bisher in die Prävention dieser Art von Angriffen investiert.**

Quelle: 2020 Cyber Threat Landscape Report, Deep Instinct

MEHRSCHICHTIGER PRÄVENTIONSANSATZ



Deep Instinct arbeitet mit einem mehrschichtigen Sicherheitsansatz, der Unternehmen viele Möglichkeiten zur Verhinderung eines Ransomware-Angriffs bietet.

Herzstück des Produkts ist die Deep Static Analysis oder das „D-Brain". Das D-Brain nutzt Deep Learning, was eine weitaus höhere Genauigkeit bietet als Signaturlösungen-, heuristische oder klassische ML-Lösungen. Die Deep Static Analysis gliedert sich in mehrere Schichten oder Modelle auf.

Zu diesen Schichten gehören das PE DL-Modell, das Office DL-, das VBA DL- und das PowerShell DL-Modell. Sie alle spielen eine wichtige Rolle beim Schutz eines Systems, auf dem die Deep Instinct-Plattform läuft. Das Office-Modell sucht zum Beispiel nach vernetzten und eingebetteten Office-Objekten: OLE, Office Open XML: OOXML, eingebettete Makros (in OLE- und OOXML-Dateien), eingebettete DDE-Objekte oder PDF-Dateien.

Zu den Komponenten der Deep Instinct-Verhaltensanalyse gehört der Schutz vor intelligentem Ransomware-Verhalten, In-Memory-Protection, Remote Code Injection, Schutz vor willkürlichem Shell-Code, Ausführung bekannter Payloads und verdächtige PowerShell-Ausführungen.

Zudem ermöglichen die D-Cloud-Dienste von Deep Instinct eine sofortige Suche nach der erkannten gefährlichen Datei und kategorisieren die Art der Bedrohung mithilfe eines sekundären DL-Modells.

BESTEHENDE SICHERHEITSLÖSUNGEN VERSTÄRKEN UND OPTIMIEREN

Wenn wir uns die derzeitige Cybersecurity-Landschaft ansehen, sind viele der aufgeführten Technologien bereits vorhanden. Deep Instinct ergänzt sie – zum Beispiel optimieren wir EDR mit aussagekräftigen Informationen, schützen Offline-Ressourcen wirksamer und beseitigen Schwachstellen im Zusammenhang mit der Cloud. Unsere tiefgehende Klassifizierung gibt den Mitarbeitenden in Security Operations Centern (SOC) detaillierte Einblicke in die Materie, mit der sie es zu tun haben.

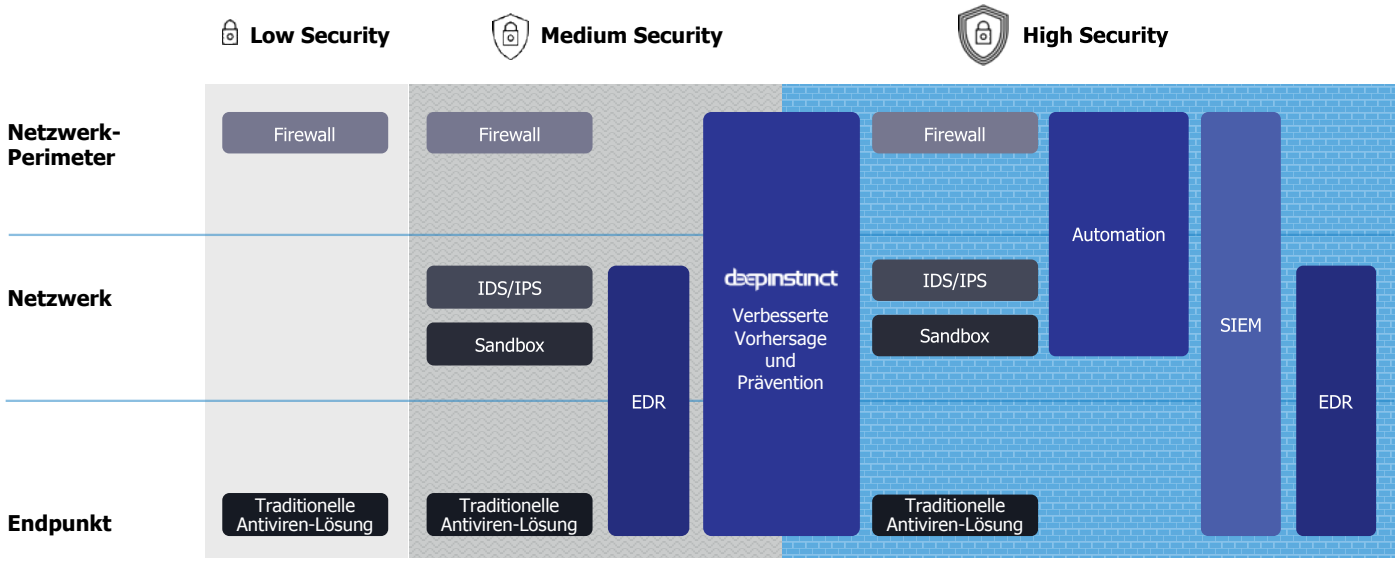
Entscheidend ist jedoch der Paradigmenwechsel im Umgang mit Cyberbedrohungen, den wir mit vorantreiben: Weg von der rein reaktiven Beseitigung, hin zu Vorhersagen und zur Prävention - und das auf einem Niveau, das es bis jetzt nicht gab. Dabei spielen EDR-Technologien nach wie vor eine wichtige Rolle, etwa bei der Untersuchung von Sicherheitsvorfällen.

Täglich werden Tausende neue, hochgradig spezialisierte Angriffsmethoden entwickelt und eingesetzt. Unternehmen benötigen heute einen mehrschichtigen Ansatz integrierter Lösungen, die im Zusammenspiel für den Schutz des Unternehmens sorgen.

Cyberkriminelle wissen, wo sie in den Infrastrukturen, Netzwerken und Sicherheitslösungen von Organisationen nach Schwachstellen und Lücken suchen müssen. Durch die weltweite Vernetzung von Technologien bieten Unternehmensnetzwerke viele Angriffsflächen und Einfallstore – und traditionelle Antiviren-Software umgehen Angreifer meist spielend. Sie zielen auf Schwachstellen und verwenden dabei hochentwickelte Tools wie:

- Speicherbasierte Angriffe
- PowerShell-Skriptsprache über Remote-Anmeldungen
- Makrobasierte Angriffe
- Und viele andere

Unternehmen müssen ihre grundlegenden „Cyberhygiene"-Maßnahmen überprüfen und neu bewerten, um ihre Sicherheit zu verbessern. Zu dieser Neubewertung gehört die Untersuchung jeder einzelnen Sicherheitslösung und ihrer Rolle im Gesamtkonzept. EDR kann eine Fülle wertvoller Einblicke liefern, aber parallel ist ein Höchstmaß an Prävention erforderlich.



PROBLEMLOSE IMPLEMENTIERUNG UND SOFORTIGE WIRKUNG

Schneller und einfacher Start

Einige unserer Kunden erzählen uns als erstes, dass sie bereits mehrere Lösungen im Einsatz haben und fragen, wie Deep Instinct ihren bestehenden Security-Stack ergänzen, die Wirksamkeit verbessern, False Positives reduzieren und mehr Bedrohungen stoppen kann.

Deep Instinct ist für schnelle und effiziente Implementierung bekannt, bei der die Produktivität nicht beeinträchtigt wird. Die D-Agents lassen sich über unsere REST API und Standardoptionen einfach bereitstellen, konfigurieren und in jede Implementierungssoftware und Asset-Tracking-Lösung integrieren.

Minimaler Eingriff

Bei jeder neuen Technologie kommen Fragen zur Wartung und zur Administration auf die Sicherheitsteams zu. Deep Instinct wird nur ein paar Mal jährlich aktualisiert, bleibt aber trotzdem hocheffektiv, selbst wenn ein Update verzögert durchgeführt wird. Viele andere Legacy-Technologien benötigen im Vergleich dazu wesentlich häufiger Patches. Trotz der enormen Rechenleistung von Deep Instinct ist der „Fußabdruck“ winzig: Die Plattform verbraucht weniger als 1 % der CPU. Dadurch dauert die Installation auf den einzelnen Endgeräten meist weniger als 60 Sekunden.

Viele Sorgen weniger

In Zusammenarbeit mit Munich Re, einem der weltweit größten Rückversicherer, haben wir zwei branchenführende Garantien* entwickelt. Sie sind im Rahmen des Premium-Abonnements erhältlich und bieten zusätzliche Sicherheit in zwei wichtigen Bereichen:

Ransomware-Garantie bis 3 Mio. USD

In dem höchst unwahrscheinlichen Fall eines erfolgreichen Ransomware-Angriffs übernehmen wir die Betriebskosten für Wiederherstellung, Fehlerbehebung etc. Gemäß den Richtlinien des Office of Foreign Assets Control (OFAC), der Kontrollbehörde des US-amerikanischen Finanzministeriums, willigen wir nicht in Lösegeldzahlungen ein. Diese Garantiesumme wird daher nicht für Lösegeldzahlungen oder zur Rückerstattung verwendet, wenn der Kunde sich trotzdem dafür entscheidet.

Die branchenweit einzige Entschädigung bei False Positives

Eine Vielzahl von False Positives wirkt sich negativ auf die Effizienz und Effektivität der SecOps-Teams aus und verursacht unnötigen Verwaltungsaufwand zulasten strategischer Projekte. Mit deutlich weniger False Positives können Sicherheitsteams viel effizienter arbeiten und die Gesamtbetriebskosten (TCO) senken. Unser Commitment liegt bei 0,1 False Positives. Sollten bei einem Kunden mehr False Positives in zwei aufeinanderfolgenden Quartalen auftreten, entschädigen wir ihn dafür. Kein anderer Cybersecurity-Anbieter bietet diese Form der Leistungsverpflichtung.

**Erhältlich beim Kauf oder der Verlängerung eines zweijährigen Premium-Abonnements für 10k+ Endpunkte.*

„Nach dem Proof-of-Value hat der Rollout etwa zwei Wochen gedauert und nur einen IT-Mitarbeiter beschäftigt, der den Prozess überwachte.“

Direktor Informationstechnologie im Bildungsbereich

Quelle: Forrester Research, “The Total Economic Impact Of Deep Instinct Advanced Endpoint Security Solution” The Cost Savings And Business Benefits Enabled By Deep Instinct Advanced Endpoint Security Solution NOVEMBER 2020

Verbessern Sie Ihre aktuelle Ransomware-Abwehr

Egal, welche Security-Lösungen Sie bisher einsetzen (AV, MTD, EDR oder andere) – Deep Instinct macht sie effektiver.

Deep Instinct ist anders.

Predict

Dank unserer einzigartigen deterministischen und prädiktiven Deep-Learning-Algorithmen erkennt und verhindert Deep Instinct verdächtige und tatsächliche Bedrohungen mit unübertroffener Geschwindigkeit und Wirksamkeit, selbst angesichts der sich ständig verändernden Bedrohungslage.

Prevent

Dadurch, dass Deep Instinct Angriffe stoppt, bevor sie ausgeführt werden, und das mehr als zehnmal schneller als in Echtzeit, haben Ransomware-Angriffe weit weniger Chancen auf Erfolg.

Promise

Unser Vertrauen in unsere Lösung und unser Commitment unseren Kunden gegenüber spiegelt sich in unserem Angebot wider:

- Eine Ransomware-Garantie: Bis zu 3 Millionen US-Dollar der im Fall eines erfolgreichen Angriffs entstehenden Kosten werden übernommen.
- Eine Effizienzgarantie: Wir stehen hinter unserer außergewöhnlich niedrigen False-Positive-Rate.