Häufig Gestellte Fragen

Cylance®

Was ist Cylance?

Cylance ist ein Cybersecurity-Unternehmen mit Hauptsitz in Irvine, Kalifornien. Die Mission von Cylance ist es, uns alle zu schützen. Cylance nutzt die künstliche Intelligenz, die Mathematik und maschinelles Lernen, um sicherzustellen, dass durch Cyber-Bedrohungen kein Schaden entsteht.

Kurzpräsentation von Cylance

Cylance revolutioniert die Cybersicherheit mit Produkten und Dienstleistungen, welche die Ausführung von komplexen, persistenten Bedrohungen und Malware an den Endpunkten proaktiv verhindern. Dies ermöglicht ein Sicherheitsniveau, das weit über die Effizienz traditioneller Branchenlösungen hinausgeht, die heute bei Unternehmen, Behörden und Institutionen weltweit im Einsatz sind.

Wann und wo wurde Cylance gegründet?

Cylance wurde im Juni 2012 in Irvine, Kalifornien gegründet.

Wer sind die Gründer von Cylance?

Stuart McClure, früherer weltweiter CTO von McAfee/Intel Security und Ryan Permeh, früherer wissenschaftlicher Leiter von McAfee/Intel Security.

Ist Cylance ein privates oder öffentliches Unternehmen?

Cylance ist ein mit Risikokapital gegründetes Privatunternehmen. Bis heute hat Cylance 177 Millionen USD an Fonds eingeholt, durch vier Finanzierungsrunden, angeführt von Blackstone, Khosla Ventures, Fairhaven Capital, Dell Ventures, DFJ, KKR, Capital One Ventures, Ten Eleven Ventures und vielen anderen Firmen.

Welches ist das wichtigste Produkt von Cylance?

CylancePROTECT®, ein Endpunktschutzprodukt der nächsten Generation, ersetzt ältere Antivirus-und Anti-Malware-Produkte.

Wer sind die Kunden von Cylance?

Cylance hat über 1,000 Unternehmenskunden, u. a. zahlreiche Unternehmen der Fortune 100. Unsere Technologie schützt derzeit über sechs Millionen Endpunkte.

In welchen Branchen ist Cylance tätig?

Die Produkte und Services von Cylance sind für alle Branchen geeignet, die beabsichtigen, das Risiko zu reduzieren und ihre Endpunkte zu schützen. Cylance wird in über 18 verschiedenen Industriesektoren verwendet; vor allem in den Sektoren Öl, Gas, Energie, kritische Infrastrukturen, Finanzwesen, Gesundheitswesen, Einzelhandel, Transport, industrielle Produktion und Abwehr.

Wo ist Cylance tätig?

Cylance ist derzeit im Vereinigten Königreich, Deutschland, Österreich, der Schweiz, Schweden, Norwegen, Australien und Japan tätig. Weitere Länder kommen ständig hinzu.

CylancePROTECT

Was ist CylancePROTECT?

CylancePROTECT ist ein fortgeschrittenes Schutzprodukt gegen Cyber-Bedrohungen, das an jedem Endpunkt einer Organisation (Desktop-PCs, Laptops, mobile Geräte, Server oder virtuelle Maschinen) eingesetzt werden kann. Es wendet künstliche Intelligenz und maschinelles Lernen an, um Malware- und Cyber-Attacken sofort zu identifizieren und zu verhindern, dass diese auf der Hostmaschine ausgeführt werden.

Wie funktioniert CylancePROTECT?

CylancePROTECT ist ein kleiner, leichtgewichtiger Agent, der an jedem Endpunkt in einer Organisation bereitgestellt wird, um Cyber-Attacken auf Betriebssystem bzw. Speicher zu verhindern. Noch bevor ausführbarer Code auf der Hostmaschine ausgeführt werden, verwendet CylancePROTECT statische Analysen und prognostische Modellierung, um festzustellen, ob diese schädliche Elemente enthalten. Wenn eine Bedrohung erkannt wird, wird die lokale Host-Richtlinie angewendet, um das Objekt in die Quarantäne zu verschieben bzw. Warnungen und Benachrichtigen anzuzeigen.

Außerdem werden die Kunden durch die CylancePROTECT-Skriptkontrolle darüber informiert, wenn ein Skript ausgeführt werden soll; so können die einzelnen Skripts unmittelbar zugelassen oder verweigert werden. Nach der Bereitstellung auf den Servern verhindert CylancePROTECT Memory Protection eine Ausnutzung der meisten üblichen Sicherheitsrisiken, z. B. bei Pufferüberlauf. CylancePROTECT mit der Optics-Komponente bietet einen kompletten Überblick über versuchte Angriffe, u. a. Details zur vorhandenen Malware, deren Quelle und Urheber, etc.

Inwiefern unterscheidet sich der Ansatz von CYLANCE bezüglich des Endpunktschutzes von dem Rest der Cybersecurity-Industrie?

Der Ansatz von Cylance kommt ohne Signaturen bzw. heuristische Analysen aus. All unsere Erkennungsfunktionen sind prädiktiv und präventiv. Ältere Endpunktschutz-Lösungen und Antivirus-Anbieter verlassen sich auf veraltete Methoden zur Erkennung von Schadsoftware mittels Signaturen, Verhaltensanalyse, Sandboxing,

Mikro-Virtualisierung und der Abfrage von Online-Virusdatenbanken. All diese Strategien sind angesichts aktueller Cyber-Bedrohungen nicht mehr wirksam.

Wie beweist Cylance seine besondere Effizienz auf dem Markt?

Cylance demonstriert regelmässig in realistischen Szenarios seinen Umgang und seine Effizienz mit aktuellen Cyber-Bedrohungen. Bei diesen Tests wird die Funkion von CylancePROTECT live mit klassischen Sicherheitsanbietern verglichen; dabei werden Zero Day-Schadsoftware sowie die aktuellsten Bedrohungen verwendet, von denen manche erst innerhalb von 24 Stunden vor der Demo zum ersten Mal aufgetreten sind. Wir nennen diese Demonstration die "Unbelievable-Tour", da viele unserer Kunden angesichts der Effizienz von CylancePROTECT höchst überrascht sind.

Kann CylancePROTECT bestehende Antivirus- und Endpunktschutz-Lösungen ersetzen?

Ja. CylancePROTECT ist konform mit PCI-DSS Abschnitt 5.0 sowie HIPAA, ein Mitglied der Microsoft Virus Initiative und von Microsoft als Antivirusprodukt anerkannt. CylancePROTECT kann eine bestehende, veraltete AV-Lösung vollständig ersetzen oder zusätzlich zu vorhandenen Lösungen in einer Arbeitsumgebung eingesetzt werden. Beeinträchtigt die Verwendung von CylancePROTECT die Leistungsfähigkeit einer Maschine? Nur minimal. CylancePROTECT scannt einen Computer nicht kontinuierlich, wie z. B. traditionelle AV-Lösungen. Tests zeigen, dass CylancePROTECT weniger als 1% eines typischen Desktop-CPUs und weniger als 60 MB Arbeitsspeicher verbraucht.

Mit welchen Betriebssystemen ist CylancePROTECT kompatibel?

- Windows XP SP3
- Windows Vista
- Windows 7 (32-bit oder 64-bit)
- Windows 8 and 8.1 (32-bit oder 64-bit)
- Windows 10 (32-bit oder 64-bit)
- Windows Server 2008
- Windows Server 2012
- Mac OS X 10.9
- Mac OS X 10.10
- Mac OS X 10.11 —Agent 1310 oder höher

Ist für CylancePROTECT eine ständige Internetverbindung erforderlich?

Nein. CylancePROTECT wurde speziell für sensible, Umgebungen konzipiert. Der CylancePROTECT-Agent wird einzig und allein am Host-Endpunkt ausgeführt, weshalb keine externe Internetverbindung vonnöten ist, um Schadsoftware abzuwehren.

Wie wird CylancePROTECT verwaltet und bereitgestellt?

CylancePROTECT bietet eine benutzerfreundliche Webkonsole für die Bearbeitung von Warnungen, das Zonen-und Richtlinien-Management sowie die Berichterstattung. Die Endpunkt-Agenten nehmen mit der Konsole nur für gelegentliche Updates und Richtlinien-Abfrage Kontakt auf. Der CylancePROTECT-Agent benötigt keine Internetverbindung, um den Endpunkt selbst zu schützen. CylancePROTECT kann leicht in die führenden SIEM-Lösungen integriert werden, indem die REST API verwendet wird, u. a. mit Splunk. CylancePROTECT wird als Standard-MSI geliefert und kann wie alle anderen Arten von Software innerhalb eines Unternehmens bereitgestellt werden.

Künstliche Intelligenz und Maschinelles Lernen bei Cylance

Warum verwendet Cylance künstliche Intelligenz (AI) und maschinelles Lernen?

Die künstliche Intelligenz und das maschinelle Lernen ermöglichen es uns, mathematisch korrekte Beziehungen zwischen den einzelnen Funktionen herzustellen und scheinbar disparate Komponenten zu korrelieren, was weit über die menschlichen Fähigkeiten hinaus geht. Die beiden Disziplinen sind nachweisbar wesentlich leistungsfähiger, effizienter und präziser als nur vom Menschen abhängige oder halbautomatische Ansätze der Cybersecurity. Dieser Ansatz erlaubt es Cylance, in kurzer Zeit höchst präzise Prognosemodelle aufzubauen, die es unseren Endpunkt-Agenten ermöglichen, autonome, intelligente Entscheidungen in Bezug auf Programmcode zu treffen, bevor diese ausgeführt werden.

Wie präzise ist dieser Ansatz?

Extrem präzise. Computer sind für höchst komplexe Datenverarbeitung in Echtzeit konzipiert. Die Anwendung von maschinellem Lernen in den Produkten von Cylance beseitigt alle Bedenken bezüglich falscher (positiver und negativer) Alarme. Bei Live-Demos weist CylancePROTECT eine Präzision von 99 % und eine Fehlalarm-Rate von nur 0,0002 % auf.

Sind Fehlalarme ein Problem?

Bei allen Arten der Erkennung von Schadsoftware sind Fehlalarme ein Problem-auch, wenn diese ausschließlich von menschliche Akteuren durchgeführt wird. Unsere Lösung ist speziell dahingehend optimiert, dass so wenig Fehlalarme wie möglich auftreten. Unsere Raten sind deutlich niedriger als bei traditionellen AV-Anbietern. Außerdem ist ein falscher Alarm verglichen mit einem erfolgreichen Angriff durch Schadsoftware als unkrisitsch zu betrachten.

Ist die künstliche Intelligenz in der Cyber-Sicherheit effizient?

Ja. Die künstliche Intelligenz ist ein breites Forschungsfeld, mit einer Vielzahl an theoretischen und praktischen Anwendungsbereichen. Die wichtigsten Überlegungen für den Versuch, künstliche Intelligenz und maschinelles Lernen zu verwenden, um komplexe Probleme zu lösen, sind die Skala der stützenden Infrastruktur, das Talent und die Kreativität des wissenschaftlichen Datenanalyse-Teams, die Fähigkeit, neue, exotische Funktionen zu programmieren, um eine selbst lernende Umgebung zu erzeugen, sowie der Mut, mit neuen, beeindruckenden Techniken zu experimentieren.

Über Cylance

Cylance ist das erste Unternehmen, das für die Cyber-Security künstliche Intelligenz, Algorithmik und maschinelles Lernen anwendet und damit die Art und Weise signifikant und nachhaltig verbessert, wie Unternehmen, Behörden und Regierungen sowie Endnutzer proaktiv die schwierigsten Sicherheitsprobleme der Welt lösen. Mit einem bahnbrechenden, prädiktiven Analyseprozess identifiziert Cylance schnell und präzise, welche Dateien sicher sind und welche eine Bedrohung darstellen, und klassifiziert nicht einfach nur in Black-oder Whitelists.

Durch die Kopplung von komplexem maschinellen Lernen und künstlicher Intelligenz mit einem einzigartigen Verständnis für die Denkweise eines Hackers, bietet Cylance die Technologien und Dienstleistungen an, die wirklich prädiktiv und präventiv gegen fortgeschrittenen Bedrohungen wirken. Für weitere Informationen besuchen Sie uns auf cylance.com

Haben andere Cybersecurity-Unternehmen versucht, AI und maschinelles Lernen anzuwenden?

Mehrere andere Cybersecurity-Unternehmen haben versucht, künstliche Intelligenz (AI) und maschinelles Lernen zu nutzen; in vielen Fällen führte dies allerdings zu vielen Fehlalarmen und einer mangelnden Strategie bei der Identifizierung der zu lösenden Problemen. Der Unterschied ist, dass viele andere Unternehmen versucht haben, maschinelles Lernen zu verwenden, um abnormale Verhaltensweisen und Ereignisse nach Angriffen zu isolieren; Cylance dagegen hat ein System aufgebaut, das in der Lage ist, schädliche Dateien zu klassifizieren und zu analysieren, wie diese vorgehen, BEVOR sie ausgeführt werden.

Ist Cylance einfach nur einer von vielen Antivirus-Anbietern?

Der revolutionäre Ansatz von Cylance definiert die Endpunktsicherheit völlig neu und macht diese proaktiv und präventiv, anstatt reaktiv. Die traditionelle Antivirus-Technologie, die auf Signaturen basiert, ist heute vollkommen veraltet. Cylance hat eine Lösung geschaffen, bei der kein Vorwissen über eine schädliche ausführbare Datei notwendig ist, um die böswillige Absicht dieser Datei zu erkennen.

Sonstige Dienstleistungen von Cylance

Bietet Cylance auch Beratungsdienste an?

Eine komplette Suite an Beratungsdiensten, die ein detailliertes Fachwissen und unserem innovativen Ansatz kombiniert, der auf künstlicher Intelligenz und maschinellem Lernen basiert, ergänzt die Produkte von Cylance. Wir bieten im Rahmen unserer Dienstleistungen z. B. Risikoevaluierungen, Penetrationstests, Notfall-Reaktionstests, Ausbildungen und Zusatzpersonal an.

Die ThreatZERO-Services optimieren den Nutzwert der Produkte, beschleunigen die Bereitstellung, behandeln die Risiken mit sofortiger Wirkung, erzeugen Mehrwert und helfen unseren Kunden, den gewünschten Status - ohne aktive Bedrohungen - zu erreichen. Das Beraterteam von Cylance bietet industriespezifische Services wie z. B. den Anwendungs-Penetrationstest für industrielle Steuerungssysteme, bei dem die Sicherheit von ICS und HMI-Schnittstellen-basierten Anwendungen evaluiert wird, und das Med Secure-Evaluierungs-Framework, welches es Organisationen im Sektor des Gesundheitswesens ermöglicht, das Sicherheitsrisiko einzuschätzen, das sich aus ursprünglich nicht verbundenen Ressourcen wie medizinischen Geräten ergibt. Die Gruppe spezialisiert sich auch auf Aktivitäten für den Schutz kritischer Infrastrukturen und wichtiger Ressourcen für Regierungsbehörden und spezifische Sektoren.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

R1_20161130