# Next-Generation ANTIVIRUS

CylancePROTECT®

CylancePROTECT ist ein Antivirus Produkt der nächsten Generation (NGAV), das neu definiert, was Antivirus (AV) zum Schutze Ihres Unternehmens tun kann und tun sollte. Durch den Einsatz von künstlicher Intelligenz erkennt CylancePROTECT Malware UND verhindert in Echtzeit die Ausführung an Ihren Endpunkten.

Die Cyber-Security Industrie ist von Veränderungen geprägt. Dennoch sind die Grundlagen für die Erkennung von Malware seit mehr als drei Jahrzehnten die gleichen. Und trotz der ständigen Innovationen von Angreifern konzentrieren sich Antivirus-Hersteller weiterhin auf veraltete Technologien, die Signaturanalysen verwenden und Verhaltensanalysen NACH erfolgten Angriffen durchführen, um Computer zu schützen. Es ist Zeit für einen neuen Ansatz.

Algorithmik und maschinelles Lernen bringen durch neue Ansätze eine neue Balance, um vor der Ausführung eine Datei effektiv zu identifizieren, zu diagnostizieren, zu kategorisieren und zu kontrollieren. Cylance führt diese Revolution mit prädiktiven und präventiven Produkten wie CylancePROTECT an, die Next Generation AV definieren.

## Definition von NGAV

Das veraltete Konzept der Blacklisten setzt bei der Erkennung von Angriffen fast ausschließlich auf Signaturen und simple Verhaltensinformationen. Das funktionierte eine Weile, da der Reaktionsaufwand und die Kosten für Angreifer und Verteidiger gleich waren. Sobald die Angreifer aber neue Tricks hinzufügten, haben sich die Verteidiger angepasst und weiterentwickelt, wodurch wiederum die Angreifer zu neuen Innovationen gezwungen wurden. Heute nun sind die Angreifer im Vorteil. Die schiere Zahl der Bedrohungen explodiert exponentiell, mit einer großen Anzahl von täglich neuen Bedrohungen. Geräte, die beständig eingeschaltet und verbunden sind, bieten einen fruchtbaren Boden für Angriffe. Verbesserungen in der Sicherheitsarchitektur werden mit schnellen und verbesserten Antworten der Angreifer übertroffen - bis zu dem Punkt, wo Gegner einen bedeutenden Vorteil gewinnen. Aufgrund veralteter Erkennungs- und Incident-Response-Strategien sind die Kosten für die Angreifer heute weit niedriger als für die Verteidiger. Herkömmliche Methoden versagen.

**Wesentliche Elemente von einem Antivirus der nächsten Generation umfassen:**

Automatisierte statische Code-Analyse – Stiller und inaktive Code soll vor der Ausführung auf dem Endpoint quasi auf Ebene der Kern-DNA, also seiner Eigenschaften, analysiert werden. Die Skala reicht hier von grundlegenden Eigenschaften, wie z.B. die PE-Dateigröße oder der verwendete Compiler, bis hin zu so komplexen Eigenschaften wie eine Überprüfung des ersten Sprungs in der binären Logik. Cylance extrahiert Millionen von einzigartigen Eigenschaften von potenziell gefährlichen Dateien und wendet eine maschinelle Analyse an, um ihre Absicht zu bestimmen.

Ausführungskontrolle – Die Erkennung von schlechten, nicht-normalen und guten Dateien sollten an die Fähigkeit gekoppelt sein, das Objekt in Echtzeit zu steuern, anstatt sich auf das Vergleichen von Hash-Werten oder Heuristikfunktion zu stützen. Um zu bestimmen was zu tun ist, bewertet Cylance die Objekte früh im ersten Laufzeitprozess in weniger als 100 Millisekunden. Dadurch kann der Cylance-Agent die Ausführung verhindern, wenn das Objekt als schädlich erkannt wird.

Keine tägliche Aktualisierungen – Eine wesentliche Schwäche von traditionellen Sicherheitslösungen, die auf Black- und White-Listen setzen, ist die Notwendigkeit, große Datenbanken von Hashes (MD5, SHA256 usw.) und anderen Signaturen bekannter Malware oder auch zugelassener Anwendungen zu speichern. CylancePROTECT ist ein technologisch hochentwickelter Agent, der auf dem Host durch die Klassifizierung der Eigenschaften eines Objektes und mittels optimal ausgearbeiteten statistischen Modellen in Echtzeit Entscheidungen trifft. Diese Modelle werden nach mehreren Monaten aktualisiert, behalten ihre Wirksamkeit aber viel länger. Es besteht keine Notwendigkeit, ständig neue Dateisignaturen herunterzuladen und sich dabei zu sorgen, dass ein Scan eine Bedrohung nicht erkennt, nur wel an einem Tag eine Aktualisierung verpasst wurde.

Keine Konnektivitätsanforderungen – Viele traditionelle Sicherheitslösungen verlassen sich für die Ergänzung Ihrer Schutzkapazität stark auf die Cloud. Auch wenn meistens ein Internetzugang zur Verfügung steht, ist es nicht immer möglich oder gewünscht, große Informationsmengen an den Lieferanten zu leiten. CylancePROTECT arbeitet autonom. Die Klassifizierung von Bedrohungen erfolgt

## 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, prädikativen 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 fortgeschrittene Bedrohungen wirken. Für weitere Informationen besuchen Sie uns auf cylance.com

durch einen vollständig isolierbaren Agenten. Eine autonome Entscheidungsfindung ist zwingend notwendig in Situationen, in denen Netzwerke durch ein Air Gap vom Internet abgeschottet sind, wie sie in industriellen Steuerungssystemen verwendet werden. Auch für Netzwerke mit geringer Bandbreite, wie die von Niederlassungen, Remote-Mitarbeitern und Point-Of-Sale-Systemen im Einzelhandel, steht keine Cloud-Anbindung zur Verfügung. Die Erkennungsraten traditioneller Lösungen brechen dann nochmals signifikant ein.

**Unterbrechungsfrei —** Die IT-Sicherheitsarchitektur sollte für Benutzer nicht spürbar und für Administratoren einfach zu implementieren und zu verwalten sein. CylancePROTECT Agent ist kompakt und benötigt im Durchschnitt weniger als 2% CPU-Last. Er ist leicht mit gängigen Software-Management-Tools zu verteilen und bietet ein Browser-basiertes Alarmierungs- und Policy-Management.

**Kontextbezogene Sichtbarkeit —** Die IT-Sicherheitsarchitektur sollte für Benutzer nicht spürbar und für Administratoren einfach zu implementieren und zu verwalten sein. CylancePROTECT Agent

**Unterbrechungsfrei —** Die IT-Sicherheitsarchitektur sollte für Benutzer nicht spürbar und für Administratoren einfach zu implementieren und zu verwalten sein. CylancePROTECT Agent

**Unterbrechungsfrei —** Die IT-Sicherheitsarchitektur sollte für Benutzer nicht spürbar und für Administratoren einfach zu implementieren und zu verwalten sein. CylancePROTECT Agent

+49-89-244455571
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPP0



20161222