Computer erfolgreich schützen mit intelligenter Sicherheitssoftware.

Eine Partnerschaft von Perseus und Cylance.

Übersicht

Sie haben Fragen? Wir beraten Sie gerne per Telefon, E-Mail und Chat.

030/959998080 info@perseus.de www.perseus.de

Perseus Technologies GmbH, Hardenbergstr. 32, 10623 Berlin

CylancePROTECT® mit OPTICS

Präzise Übersicht über die von CylancePROTECT erkannten und blockierten Ereignisse

CylancePROTECT mit OPTICS findet den Ursprung von Attacken, damit Ihre Sicherheitsorganisation über die notwendigen Informationen verfügt, und gezielt Maßnahmen ergreifen kann.

Schnellere Reaktion auf Vorfälle

Dank einem genauen Verständnis der Aktivität an den Endpunkten in Ihrer gesamten Umgebung können Sie sofort aktiv auf Vorfälle reagieren.

Verbesserung des Sicherheitsansatzes ohne zusätzliche Ressourcen

Dank der künstlichen Intelligenz und dem maschinellen Lernen sind weniger Verteidigungsmechanismen notwendig, da nur Daten von tatsächlichen Angriffen und verdächtige Dateiaktivitäten untersucht werden.

Präzise Einsicht in bestehende Bedrohungen

Die Landschaft der modernen Cyber-Sicherheit hat sich komplett verändert. Die herkömmlichen Sicherheitskampagnen konzentrieren sich auf Endpunkte und traditionelle Sicherheitswerkzeuge und sind nicht in der Lage, auf fortgeschrittene Bedrohungen zu reagieren und diese zu verhindern. Die Sicherheitsteams brauchen einen umfassenden Schutz zur Verhinderung von Bedrohungen, bevor diese ausgeführt werden, sich ausbreiten und Schäden verursachen.

CylancePROTECT erstickt Malware im Keim und überwacht ihre Aktivität viel besser als traditionelle Endpunktschutz-Lösungen. Jetzt bietet CylancePROTECT mit OPTICS eine Komplettlösung für die Endpunkt-Prävention, mit einem einzigartigen Einblick auf die Aktivität von Bedrohungen an den Endpunkten. Dank CylancePROTECT mit OPTICS können die Sicherheitsbeauftragten schneller und präziser auf Vorfälle reagieren.

CylancePROTECT mit OPTICS nutzt unsere erstklassige Technologie aus künstlicher Intelligenz und maschinellem Lernen, um einen hervorragenden Schutz und Überblick zu gewähren, mit einer klaren Darstellung der erkannten und blockierten Ereignisse. Die Geräteaktivität wird aufgezeichnet, wodurch die Organisationen verdächtige und böswillige Aktivitäten filtern und korrelieren können. So wissen Sie nicht nur, welche Bedrohungen in Ihrer Umgebung bestehen, sondern auch, woher diese kommen, an welchen Stellen sie zuerst erkannt wurden und wie sie dorthin gelangten.

Vorteile von CylancePROTECT mit OPTICS

- Wirksamer Schutz bereits vor der Ausführung reduziert den Bedarf für Incident-Response-Tätigkeiten
- Einblick in den Ursprung von Malware durch CylancePROTECT, mit präziser Ursachenanalyse
- Integration mit CylancePROTECT für einfache Bereitstellung und Verwaltung – ohne zusätzliche Verwaltungskonsolen
- Komplette Übersicht über Angriffe, unabhängig von Infrastrukturen oder Betriebssystemen; erleichtert das Verständnis von logischen Angriffsketten

Die Sicherheitsanalysten können die Aktivitäten auf der gesamten Systemebene einfach anzeigen und damit interagieren, ohne, dass der Prozess durch einzelne Aktivitäten oder Prozessketten verlangsamt wird. Dank CylancePROTECT mit OPTICS können die Analysten erweiterte Bedrohungsdetails heranziehen, um die schnelle Erkennung von Angriffen zu ermöglichen und schnell Maßnahmen zu ergreifen.

Über Cylance

Cylance® ist das erste Unternehmen, welches künstliche Intelligenz, Mathematik und maschinelles Lernen auf die Cybersecurity anwendet und die Art und Weise verbessert, wie Unternehmen, Behörden und Anwender proaktiv die schwierigsten Sicherheitsprobleme der Welt lösen können. Mithilfe eines bahnbrechenden vorhersagenden Analyseprozesses erkennt Cylance schnell und genau, was sicher ist und was als Bedrohung gilt, ohne sich ausschließlich auf eine Blacklist oder Whitelist zu verlassen.

Dank der Verknüpfung von maschinellem Lernen und künstlicher Intelligenz mit dem einzigartigen Verständnis über die Angriffsstrategien bietet Cylance die richtigen Technologien und Services, um fortschrittliche Bedrohungen vorherzusagen und zu vermeiden.

Eine fokussierte Ansicht zeigt den Infektionsvektor und die relevanten Sicherheitsereignisse automatisch an, damit die Analysten einen kompletten Überblick über Angriffe haben und eine entsprechende Nachforschung zum Zwecke der Abwehr anstellen können.

VON CYLANCEPROTECT MIT OPTICS ERFASSTE DETAILS ÜBER BEDROHUNGEN UND EREIGNISSE:

Ereignistyp	Beschreibung der Ereignisse
CylancePROTECT	▪ Durch die Zurückverfolgung von erkannten oder in Quarantäne gesetzten Ereignissen durch CylancePROTECT kann der Infektionspfad bis zum Einsprung der Malware am Gerät nachverfolgt werden
Datei	▪ Erfassungen von Ereignissen wie Erstellen, Ändern, Löschen und Umbenennen - zusammen mit Metadaten und Dateiattributen ▪ Korrelieren von Datei - und Prozesszusammenhängen ▪ Identifizierung alternativer Datenströme (ADS) ▪ Identifizierung von Daten von Wechseldatenträgern
Prozess	▪ Prozesserstellung und - beendung ▪ Laden von Modulen ▪ Injektion von Malware ▪ Korrelieren von Prozessen mit Besitzern und Image ▪ Korrelieren von Prozessen mit der gesamten Aktivität, inkl. Dateien, Registrierungsschlüsseln, Netzwerkverbindungen etc.
Netzwerk	▪ IP - Adresse ▪ Layer 4 - Protokoll
Registry	▪ Erfassen, Erstellen, Ändern und Löschen von Ereignissen für Registrierungsschlüssel und - werte ▪ Identifizierung von über 120 “Persistenzpunkten”, die von der Malware verwendet werden, um nach einem Neustart des Systems auf diesem zu verbleiben ▪ Korrelieren von Registrierungsschlüsseln/Werten mit dem Prozess, durch den sie erstellt wurden ▪ Korrelieren von persistenten Registrierungsschlüssel/-werten mit der Datei durch einen speziellen Parser
Benutzer	▪ Erfassung aller Benutzer, die sich an einem Gerät angemeldet haben ▪ Zuordnung von Benutzern zu den Aktionen, die sie durchführen, inkl. Erstellung, Änderung und Löschen ▪ Korrelieren von Benutzern mit böswilligen Aktivitäten
Wechseldatenträger	▪ Erfassung von Ereignissen in Verbindung mit dem Anschluss von Wechseldatenträgern, inkl. kopierten (auch ausführbaren) Dateien ▪ Erfassung von Gerätedetails ▪ Identifizierung von Prozessen, die Änderungen an Dateien vornehmen oder Dateien von Wechseldatenträgern kopieren ▪ Identifizierung, ob die von CylancePROTECT erkannte Malware von Wechseldatenträgern stammt

CYLANCE™

20161130

CylancePROTECT®

„Der grundlegende Fehler in der Cyber-Infrastruktur von heute besteht darin, dass die Erkennung von Angriffen höhere Priorität hat als die Prävention. Von Menschen erstellte Signaturen, die in erster Linie auf zuvor entdeckten Samples basieren, lösen nicht das eigentliche Problem: Zero-Day-Malware kann unbehelligt und ungehindert weiter laufen."

— **Stuart McClure**,
Cylance® Gründer und CEO

Zukunftssichere Endpunkt-Sicherheit

CylancePROTECT definiert neu, was Antivirus (AV) für Ihr Unternehmen tun kann und tun sollte. Durch den Einsatz von künstlicher Intelligenz erkennt CylancePROTECT Malware UND verhindert in Echtzeit die Ausführung an Ihren Endpunkten.

Durch die Nutzung eines mathematischen Ansatzes zur Identifizierung von Malware, der anstelle von reaktiven Signaturen die zum Patent angemeldeten Techniken des maschinellen Lernens nutzt, stoppt CylancePROTECT zuverlässig neue Malware, Viren und Bot-Aktivitäten und macht das Erstellen hunderter neuer Malware-Varianten durch die Angreifer zu einem nutzlosen Unterfangen.

Cylance® hat die akurateste, effizienteste und effektivste Lösung zur Verhinderung der Ausführung von Advanced Persistent Threats und Malware auf den Endpunkten für Ihr Unternehmen entwickelt.

Im Mittelpunkt der Fähigkeit zur Identifizierung von Malware steht die revolutionäre maschinelle Lern-und Forschungsplattform von Cylance, die die Leistungsfähigkeit der Mathematik und der künstlichen Intelligenz nutzt. Die Cylance Engine analysiert und klassifiziert Hunderttausende von Eigenschaften pro Datei, so dass sie in ihre kleinsten Bestandteil aufgelöst werden, um dann in Echtzeit zu erkennen, ob ein Objekt „guter" oder „schlechter" Natur ist.

Wie es funktioniert

Die Architektur von CylancePROTECT besteht aus einem kompakten Agenten, der in bestehende Software-Management-Systeme oder die Cylance-eigene Cloud-Konsole integriert wird. Der Endpunkt erkennt und verhindert Malware durch die Verwendung von auf dem Host angewendeten mathematischen Modellen, unabhängig von einer Cloud oder Signaturen. Dieser Agent ist in der Lage, Malware sowohl in offenen als auch in isolierten Netzwerken zu erkennen und unter Quarantäne zu stellen, ohne die Notwendigkeit ständiger kontinuierlicher Signatur-Aktualisierungen.

Eine effektive Verteidigung erfordert die Anwendung der besten Sichheitsfunktionen an den am meisten gefährdeten Stellen - den Endpunkten. Der mathematische Ansatz von Cylance stoppt die Ausführung von Schadcode, ohne zuvor jegliche Kenntnis zu der Malware oder ihrer besonderen Angriffstaktik oder Ausnutzung einer Schwachstelle zu haben. Keine anderes Anti-Malware-Produkt ist vergleichbar in der Präzision, der einfachen Verwaltung und der Wirksamkeit von CylancePROTECT.

Kompatibel mit Microsoft Windows® und Mac OS® X

CylancePROTECT ist kompatibel mit allen aktuellen Versionen von Microsoft Windows und Mac OS. Die Meldungen erfolgen in der Cloud-basierten Konsole oder Ihren vorhandenen Management-Systemen. Europäische Kunden nutzen exklusiv die in Frankfurt am Main gehostete europäische Cloud-Management Console.

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 fortgeschrittene Bedrohungen wirken.

Microsoft Windows (32 bits und 64 bits)	**Mac OS**
Windows XP SP3 Windows Vista Windows 7 (32-Bit oder 64-Bit) Windows 8 und 8.1 (32-Bit oder 64-Bit) Windows 10 (32-Bit oder 64-Bit) Windows Server 2008 / 2008 R2 Windows Server 2012 / 2012 R2	Mac OS X 10.9 (Mavericks)* Mac OS X 10.10 (Yosemite)* Mac OS X 10.11 (El Capitan)* *Ergänzt Apples integriertes XProtect
2GB Speicher	2GB Speicher
300MB verfügbarer Festplattenspeicher	300MB verfügbarer Festplattenspeicher
Benötigt: .NET Framework 3.5 SP1 Webbrowser Internetverbindung zur Registrierung des Produkts Lokale Administratorenrechte zur Installation der Software	Benötigt: Webbrowser Internetverbindung zur Registrierung des Produkts Lokale Administratorenrechte zur Installation der Software

Cylance Consulting

Cylance Consulting ergänzt CylancePROTECT bei der Verbesserung Ihrer IT-Sicherheit, um Ihr Unternehmen effektiv zu schützen und die Angriffsfläche zu reduzieren. Schwachstellenanalyse und Penetrationstests schaffen eine Basis für die Bewertung Ihrer Sicherheitslage. Eine Bedrohungseinschätzung bestimmt das „Wer“, „Was“, „Wann“ und „Wie“ eines erfolgreichen Angriffs und stellt bewährte Verfahren zur Behebung bereit. Unsere Incidence-Response-Lösungen und maßgeschneiderten Dienstleistungen beheben Probleme schneller und diskreter als die klassischen Ansätze. Alert-Management und die Verwaltung von Whitelists helfen dem IT-Team, ein höheres Maß an Sicherheit zu erreichen, OHNE den Aufwand einer kontinuierlichen Verwaltung, den negativen Auswirkungen auf die Produktivität der Benutzer und ohne die Fehler, die immer dann gemacht werden, wenn Entscheidungen über die Sicherheit von Applikationen zu schnell getroffen werden.

CYLANCE™

20161205

CylanceOPTICS™

Für CylancePROTECT®-Endpunkte konzipierte Erkennung und Bekämpfung von Bedrohungen auf Endpunkten

Funktionen

- **Ursachenanalyse:** Web-basierte On-Demand-Ursachenanalyse zu den von CylancePROTECT blockierten Angriffen
- **Intelligente Jagd auf Bedrohungen mit InstaQuery:** Sofortige Durchsuchung von Endpunktdaten, um versteckte potenzielle Bedrohungen auf Endpunkten aufzuspüren
- **Dynamische Bedrohungserkennung und Alarmierung:** Sofortige Benachrichtigung, wenn verdächtige Aktivitäten auf einem Endpunkt erkannt werden
- **Automatisierte Reaktion auf Vorfälle:** Individuelle Anpassung automatisierter, mit Regelsätzen verknüpfte Gegenmaßnahmen zur Eliminierung der Verweilzeit zwischen der Erkennung von Bedrohungen und der Reaktion auf Vorfälle
- **Für Skalierbarkeit konzipiert:** Auf Skalierbarkeit ausgerichtete Hochleistungsarchitektur

Die Herausforderung bei der Absicherung von Endpunkten

Mit der Sicherheit von Endpunkten betraute Teams werden mit Daten der im Netzwerk implementierten Sicherheitsprodukte überschwemmt. Da eine Sicherung der Geschäftskontinuität oberste Priorität hat, steht diesen Teams jedoch wenig Zeit für eine proaktive Jagd auf Bedrohungen oder strategische Verbesserungen des Sicherheitsniveaus zur Verfügung. Das Ergebnis: kritische Bedrohungen bleiben unerkannt und gefährden das Unternehmen.

Diese Situation wird durch die Knappheit an qualifizierten Sicherheitsexperten verschärft. Daher müssen sich Unternehmen auf Sicherheitstools verlassen, um die Erkenntnisse zu erhalten, die sie benötigen, um Sicherheitsvorfälle zu identifizieren, zu erkennen und darauf zu reagieren. Leider sind viele dieser Tools nicht geeignet, um auf die heute vorherrschenden Bedrohungen einzugehen.

Ein neuer Ansatz für die Erkennung und Bekämpfung von Bedrohungen auf Endpunkten

CylanceOPTICS, Teil der präventionsorientierten Cylance Security Platform, ist eine auf künstlicher Intelligenz (KI) beruhende Lösung zur Erkennung und Bekämpfung von Bedrohungen auf Endpunkten (Endpoint Detection and Response, EDR). Sie ist darauf ausgelegt, den von CylancePROTECT gebotenen Schutz durch eine Ursachenanalyse, eine skalierbare Jagd auf Bedrohungen und eine automatisierte Erkennung und Bekämpfung von Bedrohungen zu ergänzen, ohne Ihre Kosten oder den Arbeitsaufwand für Ihr Sicherheitsteam zu erhöhen.

Im Gegensatz zu anderen EDR-Produkten, die beträchtliche Investitionen in die Infrastruktur vor Ort erfordern oder ein Unternehmen zwingen, Daten zur Speicherung und Analyse kontinuierlich in eine Cloud-Umgebung zu streamen, läuft CylanceOPTICS auf dem Endpunkt, speichert Daten lokal und macht zusätzliche Hardware sowie die mit dem Streaming von Daten in die Cloud verbunden Kosten und Risiken überflüssig.

Mit CylanceOPTICS können Sicherheitsexperten jeden von CylancePROTECT erkannten und blockierten Angriff gründlich analysieren, um schnell die Grundursache zu ermitteln und das Sicherheitskonzept insgesamt zu verbessern. Darüber hinaus bietet CylanceOPTICS eine optimierte Funktion für eine Jagd auf Bedrohungen, die es für jeden Benutzer leicht macht, sich einen Überblick über die unternehmensweite Situation zu verschaffen.

Sicherheitsfachleute können CylanceOPTICS verwenden, um bei Bedarf unternehmensweit Jagd auf Bedrohungen zu machen und nach Dateien, ausführbaren Programmen und Anzeichen auf eine Kompromittierung zu suchen und schnell zu ermitteln, ob ein Endpunkt gefährdet ist. So können die Angriffs- und Verweilzeit minimiert und die Angriffsfläche verkleinert werden, um noch schneller auf Vorfälle reagieren zu können.

ERFASSTE ENDPUNKTDATEN

Ereignistyp	Beschreibung der Ereignisse
CylancePROTECT	▪ Durch die Zurückverfolgung von erkannten oder in Quarantäne gesetzten Ereignissen durch CylancePROTECT kann der Infektionspfad bis zum Ursprung der Malware am Gerät nachverfolgt werden.
Datei	▪ Erfassungen von Ereignissen wie Erstellen, Ändern, Löschen und Umbenennen - zusammen mit Metadaten und Dateiattributen ▪ Korrelieren von Datei- und Prozesszusammenhängen ▪ Identifizierung alternativer Datenströme (ADS) ▪ Identifizierung von Daten von Wechseldatenträgern
Prozess	▪ Prozesserstellung und -beendung ▪ Laden von Modulen ▪ Injektion von Malware ▪ Korrelieren von Prozessen mit Inhabern und Image ▪ Korrelieren von Prozessen mit der gesamten Aktivität, inkl. Dateien, Registrierungsschlüsseln, Netzwerkverbindungen etc.
Netzwerk	▪ IP-Adresse ▪ Layer 4-Protokoll ▪ Quell- und Zielports
Registry	▪ Erfassen, Erstellen, Ändern und Löschen von Ereignissen für Registrierungsschlüssel und -werte ▪ Identifizierung von 120 „Persistenzpunkten“, die von der Malware verwendet werden, um nach einem Neustart des Systems auf diesem zu verbleiben ▪ Korrelieren von Registrierungsschlüsseln/-werten mit dem Prozess, durch den sie erstellt wurden ▪ Korrelieren von persistenten Registrierungsschlüssel/-werten mit der Datei durch einen speziellen Parser
Benutzer	▪ Erfassung aller Benutzer, die sich an einem Gerät angemeldet haben ▪ Zuordnung von Benutzern zu den Aktionen, die sie durchführen, inkl. Erstellung, Änderung und Löschen ▪ Korrelieren von Benutzern mit böswilligen Aktivitäten
Wechseldaten-träger	▪ Erfassung von Ereignissen in Verbindung mit dem Anschluss von Wechseldatenträgern, inkl. kopierten (auch ausführbaren) Dateien ▪ Erfassung von Gerätedetails ▪ Identifizierung von Prozessen, die Änderungen an Dateien vornehmen oder Dateien von Wechseldatenträgern kopieren ▪ Identifizierung, ob die von CylancePROTECT erkannte Malware von Wechseldatenträgern stammt

Vorteile

Verringerung der Angriffsfläche

Weiterentwicklung des Sicherheitskonzepts eines Unternehmens zur Entschärfung von Angriffsvektoren und Verringerung des Risikos einer Datenschutzverletzung.

Erlangung eines Überblicks über die Situation

Verständnis dafür, wo in Ihrer Umgebung Bedrohungen bestehen, und schnelle Ergreifung von Gegenmaßnahmen.

Verringerung der Belastung von Sicherheitsteams

Automatisierung von Reaktionen zur Identifizierung von Bedrohungen rund um die Uhr, ohne das Sicherheitsteam zu stören.

Integrierte Funktionen zur Erkennung und Bekämpfung von Bedrohungen erkennen automatisch verdächtiges Verhalten sowie weitere Anzeichen auf komplexe Bedrohungen auf Endpunkten und können ohne menschliche Eingriffe gezielte Gegenmaßnahmen einleiten. Dies bedeutet, dass das Unternehmen rund um die Uhr sicher ist, ohne Ihr Sicherheitsteam zu stören.

Eine effektive Erkennung von Bedrohungen beginnt mit erstklassigem Schutz

Eine 100%ige Erkennung und Verhinderung aller Bedrohungen ist zwar nicht möglich, es ist jedoch wichtig, dass Unternehmen ihren Weg hin zu vollkommener Endpunktsicherheit mit einer starken *Präventionsstrategie* beginnen. Indem sie alles vernünftigerweise Mögliche tun, um zu verhindern, dass Bedrohungen ihr Geschäft beeinträchtigen, können sich Unternehmen darauf konzentrieren, stufenweise Technologien und Prozesse einzuführen, die darauf abzielen, die schwer zu verhindernden Bedrohungen für ihr Geschäft zu erkennen und darauf zu reagieren.

Die Kombination aus CylancePROTECT und CylanceOPTICS bietet die Präventions-, Erkennungs- und Reaktionsfunktionen, die für eine vollkommene Endpunktsicherheit benötigt werden. Durch Einsatz dieser leistungsstarken Technologien können Unternehmen ihre vertraulichen Daten schützen, das Risiko einer weitläufigen Kompromittierung reduzieren und ihr Sicherheitsniveau insgesamt verbessern.

CYLANCE™

20171101-2793

perseus.

Schützen Sie jetzt die Computer Ihres Unternehmens.

Eine Partnerschaft von Perseus und Cylance.

Sie haben Fragen?
Wir beraten Sie gerne persönlich.


030/959998080


info@perseus.de


www.perseus.de

Perseus Technologies GmbH, Hardenbergstr. 32, 10623 Berlin