cybereason | PRODUKTÜBERSICHT

CYBEREASON PREVENTION

Mit mehrschichtiger Prävention über Legacy-Antivirenprodukte hinausgehen

HAUPTVORTEILE:

- Reduzierung des Risikos unbekannter Bedrohungen mit Echtzeit-Verhaltensprävention
- Eliminierung von Ransomware-Bedrohungen mit Verhaltens- und Täuschungstechniken
- Unterbindung von dateilosen- und in-memory Angriffen mit tiefer Skript-Sichtbarkeit
- Konsolidierung mehrerer Agenten zu einem einzigen, kompakten Agenten
- Müheloser Einsatz, in nur 24 Stunden
- Verkürzung langwieriger Untersuchungen mit korrelierten Bedrohungsinformationen über eine intuitive Benutzeroberfläche
- Nutzung von Endpunktkontrollen zur Erfüllung von Zugangs- und Konformitätssicherheitsanforderungen
- Behebung von Bedrohungen in großem Umfang durch einen einzigen Mausklick

Wie Verteidiger über Bedrohungen hinausdenken und diese überwinden

Neue und ausgeklügelte Malware wird jeden Tag aufgespürt. Sie stellt eine große Gefahr für Sicherheits- und IT-Teams dar. Sowohl bei Legacy- als auch bei Nextgen-Lösungen leiden Sicherheitsteams oft unter zu komplexen Arbeitsabläufen, Lücken bei der Erkennung und ressourcenintensiven Agenten. Diese Faktoren tragen insgesamt zu einer mangelhaften Aufstellung in Bezug auf die gesamte Abwehr, einer großen Anstrengung und dem Bedarf an noch mehr zu unterstützenden Tools und Ressourcen bei.

Cybereason Prevention kombiniert signaturbasierte, verhaltensbasierte und maschinelle Lernverfahren, um Bedrohungen in Echtzeit zu beenden - einschließlich bekannter, nie zuvor aufgetretener und dateiloser Bedrohungen. Teams können sich innerhalb weniger Stunden mit einem einzigen, kompakten Agenten auf alle Betriebssysteme und Endpunkttypen konzentrieren. Hiervon ausgehend ist die Analyse einfach, da der gesamte Kontext den Analysten direkt über eine einzige Benutzeroberfläche innerhalb der Plattform zur Verfügung steht, so dass ein zeitintensiver Wechsel zwischen den Anwendungen entfällt und mehr Zeit für die Untersuchung von Bedrohungen aufgewendet werden kann.

Alle Bedrohungen in Echtzeit stoppen

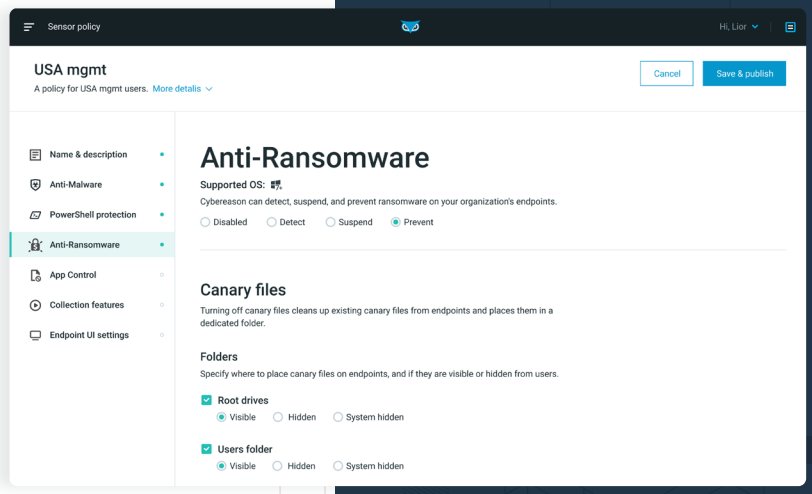
Cybereason Prevention verwendet einen vielschichtigen Ansatz mit intelligenzbasierter Bewertung zur Blockierung bekannter Bedrohungen und Algorithmen maschineller Lernverfahren, die Verhaltens- und statische Attribute analysieren, um dateifreie Angriffe, neue Malware-Varianten und andere neuartige Bedrohungen sofort zu blockieren und langwierige Untersuchungen zu vermeiden. Die Algorithmen der maschinellen Lernverfahren analysieren sowohl verhaltensbasierte als auch statische Attribute von Prozessen und Dateien und unterbinden so die Ausführung dateiloser Angriffe, neuer Malware-Varianten und anderer neuer Bedrohungen, die noch nie zuvor aufgetreten sind. Die verhaltensbasierte Prävention unbekannter Bedrohungen sorgt für eine lückenlose Verteidigung.

Tiefgreifende Einblicke in dateilose Angriffe

Moderne Bedrohungen erfordern tiefgreifende Einblicke seitens der Sicherheitsprodukte. Um Sicherheitsteams in die Lage zu versetzen, den wachsenden Risiken dateiloser Angriffe entgegenzuwirken, setzt Cybereason Prevention denselben Agenten ein, der in seinem Produkt Endpoint Detection and Response zum Einsatz kommt, um eine beispiellose Wirksamkeit bei bösartigen Prozessen und Skripten zu erreichen. Die Cybereason Defense Platform ist als erste auf dem Markt in der Lage, böswillige .Net-Ausführungen zu blockieren, und bietet eine qualitativ hochwertige Erkennung von PowerShell-Skripts, .Net-Missbrauch, Makro-Skripts und anderen anspruchsvollen Bedrohungen, um den Ermittlungsaufwand und die Reaktionszeit für Sicherheitsteams mit eingeschränkten Ressourcen zu reduzieren.

Ransomware aufhalten, bevor Schaden entsteht

Immer mehr Unternehmen sehen sich mit einer Reihe von Ransomware-Angriffen konfrontiert. Diese Entwicklung stellt ein erhebliches Risiko dar. Cybereason entwickelte eine einzigartige Kombination von Täuschungs- und Verhaltenstechniken, um Ransomware aufzuhalten, bevor Schaden angerichtet wird. Cybereason Prevention ist in der Lage, unbekannte, dateilose und selbst MBR-basierte Ransomware automatisch zu erkennen und zu blockieren. Dies versetzt Teams in die Lage, die automatische Verhaltensprävention in Verbindung mit Täuschungstechniken einzusetzen, um sicherzustellen, dass legitime Dateien während eines Angriffs nicht verschlüsselt werden.



Reduzieren der Ermittlungszeit durch eine intuitive Benutzeroberfläche

Prävention ist notwendig, aber sie ist oft nur der erste Schritt bei einem Angriff. Die eigentliche Herausforderung besteht darin, die tatsächliche Ursache eines Angriffs zu verstehen und zu bekämpfen. Mit Cybereason Prevention können Sicherheitsteams über eine einzige Schnittstelle Warnmeldungen für alle betroffenen Geräte einsehen und diese nach Priorität ordnen, untersuchen und wiederherstellen. Analysten werden ausgehend von allen Warnmeldungen mit wenigen Mausklicks weitere Einsichten erhalten und können so den zu behandelnden Kontext einfach erfassen, so dass sie komplexe Arbeitsabläufe zwischen verschiedenen Produkten überflüssig machen.

Einleitung von Abhilfemaßnahmen auf allen Geräten durch einfachen Mausklick

Dank einer Vielzahl von Abhilfemöglichkeiten ermöglicht Cybereason Prevention Analysten das schnelle Eingreifen bei Erkennung und Blockierung einer Bedrohung. Ist mehr als ein Endpunkt betroffen, können Analysten alle befallenen Geräte schnell und einfach mit einem einzelnen Mausklick wiederherstellen.

Ein einziger, kompakter Agent, der alle Funktionen vereint

Cybereason Prevention bietet eine mehrschichtige Prävention, bei der NGAV- und Endpunktkontrollen mit minimalen Auswirkungen auf Geschwindigkeit und Ressourcen kombiniert werden, ohne dass mehrere Agenten eingesetzt werden müssen. Die Cybereason Defense Platform kombiniert Endpoint Prevention (EPP) mit unserer branchenführenden Endpoint Detection und Response (EDR)-Lösung und proaktiver Bedrohungssuche für umfassende Sicherheit durch einen einzigen, kompakten Agenten und eine intuitive Benutzeroberfläche.

Über Cybereason:

Cybereason ist der Branchenführer unter den modernen Abwehrprogrammen für Cyber-Sicherheit mit zukunftsorientiertem Schutz vor Angriffen. Es erstreckt sich vom Endpunkt über das gesamte Unternehmen und darüber hinaus. Die Cybereason Defense Platform kombiniert die branchenweit besten Erkennungs- und Abwehrmaßnahmen (EDR und XDR), Virenschutz der nächsten Generation (NGAV) und proaktive Bedrohungssuche, um eine kontextbezogene Analyse jedes Elements einer bösartigen Operation (Malop) zu liefern. Infolgedessen können Verteidiger Cyberangriffe von Endpunkten aus und überall beenden.

CYBEREASON.COM/DEMO

Weitere Informationen unter cybereason.com →

cybereason