cybereason

ANTIVIRUS DER NÄCHSTEN GENERATION_

Stoppen Sie die Bedrohungen von morgen schon heute

HAUPTVORTEILE

- Eliminieren vonRansomware mit Verhaltens- und Täuschungsmethoden
- Verhindern von dateilosen und speicherinternen Angriffen
- Blockieren von Exploits
- Reduzieren der Risiken von USB-Geräten
- Erweiterung der Firewall-Steuerung auf den Endpunkt
- Konsolidierung von Endpunkt-Agenten zu einem einzigen System
- Reduzieren von Sicherheitslücken, die durch veraltete AV-Systeme entstehen
- Gewinnen Sie volle Angriffstransparenz über alle Endgeräte hinweg

ÜBER CYBEREASON

Die Cybereason Defense Platform kombiniert verwaltete Endpunktprävention, Erkennung und Reaktion in einer schlanken Lösung. Sie bietet mehrschichtige Endpunktprävention mithilfe signaturbasierter und signaturloser Techniken, um bekannte und unbekannte Bedrohungen zu verhindern. Zudem werden Verhaltens- und Täuschungstechniken eingesetzt, um Ransomware- und dateilose Angriffe abzuwehren. Verbinden Sie die beste Cyber-Plattform auf dem Markt mit managed Services durch unser Team von Sicherheitsexperten, um einen umfassenden Schutz zu erhalten.

KLICKEN SIE HIER FÜR EINE DEMOVERSION →

Mit dem raschen Auftreten neuer, ausgefeilter Angriffe sind veraltete AV-Lösungen zum Schutz Ihres Unternehmens nicht länger ausreichend. Die meisten Tools konzentrieren sich auf bereits bekannte Angriffsmuster und nutzen dabei bekannte Anzeichen für Gefährdungen und vorhandene Bedrohungsinformationen. Moderne Bedrohungen verwenden jedoch oft legitime Tools wie PowerShell und .NET, In-Memory-Angriffe und andere fortschrittliche Techniken, die traditionelle Kontrollen ineffektiv machen.

Ihr Unternehmen benötigt eine Sicherheitslösung für Endgeräte, die einen umfassenden, ganzheitlichen Ansatz verfolgt. Cybereason Next-Generation Antivirus bietet Unternehmen umfassenden Schutz vor bekannter Malware, unbekannter binärer Malware, Ransomware, Exploits sowie In-Memory- und dateiloser Malware.

EIN MEHRSCHICHTIGER ANSATZ

Cybereason Next-Generation Antivirus bietet einen umfassenden Security-Stack für die automatische Abwehr. Mit signaturbasierten Techniken können Sie die Ausführung bekannter Malware sofort verhindern. Nutzen Sie maschinelles Lernen und Verhaltensanalysen, um ausgeklügelte Malware zu erkennen und zu verhindern, die typischerweise von veralteten AV-Produkten übersehen wird. Zusätzliche dynamische Präventionsebenen sorgen dafür, dass Sie den sich ständig weiterentwickelnden Bedrohungen immer einen Schritt voraus sind, und ermöglichen Ihnen weiterhin, Angriffe auf beispiellose Art und Weise zu verhindern..

UNMITTELBARE VERTEIDIGUNG GEGEN RANSOMWARE

Cybereason Next-Generation Antivirus stoppt Ransomware durch den Einsatz von Verhaltensanalysen und Täuschungstechniken bereits vor der Verschlüsselung. Analysten können unbekannte, dateifreie und sogar MBR-basierte Ransomware-Stämme erkennen und blockieren. Nutzen Sie unsere Verhaltensprävention in Verbindung mit unseren Täuschungstechniken, um sicherzustellen, dass während eines Angriffs keine legitimen Dateien verschlüsselt werden.

VERHINDERN VON DATEILOSEN ANGRIFFEN

Stoppen Sie dateilose Angriffe, die PowerShell oder .NET-Schwachstellen ausnutzen, indem Sie eine Kombination aus umfassender Sichtbarkeit und Verhaltensanalyse nutzen. Cybereason Next-Generation Antivirus analysiert nicht nur die verschlüsselte oder verschleierte Befehlszeile, sondern verwendet auch Verhaltensanalysen, um alle Aktionen der im PowerShell-Engine ausgeführten Codes zu überprüfen, und bietet im Vergleich zu anderen Lösungen einen besseren Schutz vor dateilosen Bedrohungen.

ENDPUNKTPROTECTION_

01 » NEXTGEN-ANTIVIRUS

02 » ANTI-RANSOMWARE

03 » SCHUTZ VON EXPLOITS

04 » SCHUTZ VOR DATEILOSEN BEDROHUNGEN

UNTERSTÜTZTE VERSIONEN

WINDOWS

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, XP SP3
- Windows Vista Server 2003, Server 2003 R2
- Windows Vista Server 2008, Server 2008 R2

MACOS

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Yosemite (10.10)
- El Capitan (10.11)

LINUX

- CentOS 6 and 7
- Red Hat Enterprise Linux 6 & 7
- Oracle Linux 6 & 7
- Ubuntu 14 LTS & 16 LTS
- Ubuntu 18.04
- SLES 12
- Debian 8 & 9
- Amazon Linux AMI 2017.03

EINE SCHLANKE LÖSUNG

Cybereason Next-Generation Antivirus bietet branchenführende Prävention mit minimalen Auswirkungen auf Geschwindigkeit und Ressourcen – und das ohne die Notwendigkeit, mehrere Lösungen einzusetzen.

Die einzigartige Technologie von Cybereason ermöglicht es der Lösung, kontinuierlich im Benutzerbereich zu arbeiten – so wird die Gefahr von Systemabstürzen vermieden, während Analysten dennoch einen vollständigen, unvergleichlichen Einblick in alle Aktivitäten erhalten. Stellen Sie Cybereason Next-Generation Antivirus in nur 24 Stunden mit minimalen Auswirkungen auf Ihr Unternehmen bereit und beginnen Sie noch am selben Tag, Angriffe zu verhindern.

ZEIT, MÜHE UND GELD SPAREN

Cybereason Next-Generation Antivirus bietet qualitativ hochwertige Warnungen mit geringer Falsch-Positiv-Rate, um die Belastung für Ihr überarbeitetes SOC-Team zu reduzieren. Die Plattform verhindert automatisch Ransomware, Malware und dateifreie Malware, indem sie Signaturen, maschinelles Lernen, Täuschungstechniken, Verhaltenstechniken und tiefe Skriptvisibilität nutzt. Die Plattform verhindert Bedrohungen, bevor der Analyst überhaupt eingreifen muss, sodass sich Ihr SOC auf fortschrittlichere Übergriffe konzentrieren und die Produktivität steigern kann.

STEIGERN SIE IHRESICHERHEIT MIT DER CYBEREASON-PLATTFORM

Cybereason schützt Sie heute und bietet Ihnen gleichzeitig zusätzlichen Kontext und Transparenz, um Ihnen zu helfen, Bedrohungen auch in der Zukunft zu untersuchen. Durch die Kombination von Cybereason Next-Generation Antivirus und Cybereason EDR in einer einzigen Lösung können Sie die gesamte Angriffshistorie für jeden verhinderten Angriff sehen, und zwar mit derselben Konsole und demselben Agenten wie bei Cybereason Next-Generation Antivirus. Verhindern Sie die automatische Ausführung von Malware auf einer kritischen Anlage wie einem Produktionsserver und konzentrieren Sie sich dann sofort darauf, herauszufinden, wie die Malware überhaupt dorthin gelangt ist.