cybereason

CYBEREASON MOBILE_

Sichern Sie auch den letzten anvisierten Endpunkt: Mobile Geräte

HAUPTVORTEILE

» Unvergleichliche Übersichtlichkeit aller Angriffsvektoren

» Erkennung, Untersuchung, Nachforschung und Beseitigung von Angriffen auf herkömmlichen und mobilen Endgeräten

» Von Experten verwaltete Managed Detection and Response (MDR) von Cybereason

» Native Interoperabilität mit UEM-Technologiepartnern

SYSTEMANFORDERUNGEN

ANDROID-VERSIONEN

5 6 7 9 10

IOS-VERSIONEN

9 10 11 12 13

CYBEREASON.COM/DEMO →

Da sie die Produktivität am Arbeitsplatz verbessern, hat der Einsatz von mobilen Geräten in Unternehmen den Einsatz von Desktops und Laptops bereits weltweit überholt. Unternehmen unterliegen derzeit einem digitalen Wandel: Mobile Geräte werden zur bevorzugten Plattform für viele Geschäftsszenarien, und Unternehmen implementieren Bring-Your-Own-Device (BYOD)-Strategien. Angesichts der unzähligen bekannten Malware-Bedrohungen für eine steigende Anzahl an Geräten und Betriebssystemen und der Verbreitung von Cloud- und Mobile-First-Applikationen sind die Unternehmen mit komplexen und zunehmenden Risiken konfrontiert.

NICHT "NUR" EINE MOBILE HERAUSFORDERUNG

Cyberkriminelle sehen mobile Geräte zunehmend als lukratives Ziel, da immer mehr Menschen Smartphones, Tablets, POS-Systeme und andere BYOD-Geräte sowohl privat als auch für ihre Arbeit nutzen.
Verstärkt werden diese Trends durch die rasante Entwicklung der Mobilfunknetze mit der Einführung von 5G und durch die reduzierte Nutzung traditioneller Endpunkte wie Desktop-Computern. Heutzutage können Mitarbeiter von jedem Gerät aus rund um die Uhr arbeiten und greifen dabei auf Unternehmensdaten über Cloud Services zu, bei denen mitunter herkömmliche Sicherheitsfunktionen nicht greifen.

GRENZENLOSE SICHERHEIT FÜR MOBILE MITARBEITER

Der sofortige Zugriff auf geschäftskritische Anwendungen unabhängig von Gerät, Standort oder Uhrzeit ist eine Grundvoraussetzung für ein modernes Unternehmen. Die weit verbreitete Nutzung von betrieblichen und privaten Geräten mit unterschiedlicher Hardware, auf denen verschiedene Betriebssysteme, Versionen und Anwendungen laufen, stellt für Anbieter von Cybersicherheit eine enorme Herausforderung dar.

UEM - EIN TRÜGERISCHES - GEFÜHL DER (CYBER-)SICHERHEIT.

Unified Endpoint Management (UEM/MDM)-Lösungen stehen seit Jahren zur Verfügung. Diese stellen jedoch keine Antwort auf die heutigen Bedenken in Sachen Cybersicherheit dar. Sie bieten zwar einen guten Ansatz, sind aber nicht für die vollständige Abwehr von raffinierten Angreifern ausgelegt. UEM/MDM sind Instrumente für das Gerätemanagement und die Durchsetzung von Richtlinien. Sie sind jedoch nicht in der Lage, den Anforderungen von Unternehmen und den Risiken der mobilen Cybersicherheit gerecht zu werden.

SEPARATE WARNBEREICHE FÜR MOBILE UND HERKÖMMLICHE GERÄTE.

Die Überwindung der Schranken zwischen der Cybersicherheit von mobilen und der Sicherheit von herkömmlichen Endgeräten stellt einen entscheidenden Aspekt für die Schaffung eines nahtlosen Sicherheits-Ökosystems dar. Die Trennung zwischen bestehenden mobilen Sicherheitsprodukten und derer herkömmlicher Endpunkte schafft Lücken in der Unternehmenssicherheit, die von Hackern ausgenutzt werden können.

CYBEREASON MOBILE

Die weltweit führende Plattform Cybereason für den Endpunkt-Schutz unterstützt Sicherheitsteams bei der Prävention, der Erkennung, der Ermittlung, der Nachforschung von und der Reaktion auf hoch entwickelte Angriffe. Die Plattform korreliert die Daten herkömmlicher und Endpunkte der nächsten Generation in einer einzigen Konsole und bietet somit einen effizienteren und vollständigeren Incident Response Prozess, abgerundet durch das Cybereason-Team an erfahrenen Analysten.

AUTONOMER SCHUTZ

Cybereason Mobile bietet einen geräteeigenen, verhaltensbasierten Schutz für die Erkennung einer Vielzahl verdächtiger Aktivitäten: Von böswilliger Nutzung mobiler Apps über ungewöhnliche Nord-Süd Netzwerkverbindungen bis hin zu Schwachstellen im Betriebssystem. Die App schützt die mobilen Geräte sofort und erfordert keine Einlernphase. Diese Vorteile können für jedes Gerät überall und jederzeit ohne Regeln, ohne Signaturen und ohne manuelle Analyse gewährleistet werden.

EIN HACKER- FELDZUG - EIN BÖSWILLIGER ANGRIFF

Anstatt segmentierter, komplexer und uneinheitlicher Warnungen können Sie mit der Cybereason Mobile Malicious Operation (Malop™) jeden geräteübergreifenden Angriff identifizieren, plattformübergreifend nachforschen und schädlichen Kontext über alle Phasen des Angriffs hinweg verfolgen. Malop ist vollständig auf das MITRE ATT&CK for Mobile-Modell abgestimmt, so dass Sicherheitsanalysten Verbindungen herstellen und unterschiedlichste böswillige Aktivitäten über verschiedene Endpunkte kommunizieren können. Schützen Sie sich vor benutzer- oder unternehmensbezogenen Angriffen mit weniger Fehlalarmen und optimierter Vorfallsreaktion.

DO-NO-HARM-ANSATZ

Mit dem nicht-intrusiven und effizienten Ansatz von Cybereason Mobile kann das mobile Gerät ohne Beeinträchtigung seiner Leistung, des Benutzererlebnisses oder der Privatsphäre des Benutzers geschützt werden. Die schlanke Anwendung mit dem Do-No-Harm-Ansatz für die mobile Leistung ist so ausgelegt, dass die Netzwerkbandbreite und Akkulaufzeit auf dem Gerät ohne die Einführung von Latenzen und bei gleichzeitigem Schutz der personenbezogenen Informationen (PII) des Benutzers effizient genutzt werden.

KORRELIEREN, ERKENNEN, BEKÄMPFEN—WIEDERHOLEN

Cybereason Mobile erfasst das gesamte Spektrum mobiler Risiken und Bedrohungen und versetzt Sicherheitsteams damit in die Lage, raffinierten Bedrohungen, die von den herkömmlichen Endpunktkontrollen völlig übersehen wurden, vorzubeugen und diese umgehend abzuwehren. Cybereason Mobile bietet einen umfassenden Kontext für das gesamte Betriebssystem, Speicher, CPU und darüber hinaus. Somit kann ungewöhnliches Verhalten identifiziert und alle betroffenen Endpunkte, Benutzer und die Kommunikation des Angreifers aufgedeckt werden.

DIE VORTEILE VON CYBEREASON

Der Schutz von Endgeräten auf herkömmliche Weise ist schlicht nicht mehr ausreichend. Aus diesem Grunde stärkt das neue Angebot Cybereason Mobile die Cybereason Defense Platform und stellt einen umfassenden Schutz für herkömmliche ebenso wie für mobile Endgeräte bereit. Durch das Cybereason Mobile MDR-Angebot optimiert unser Team die Analyse und beschleunigt das Ergebnis. Cybereason bewältigt die große Masse an Sicherheitsdaten, die in den komplexen IT-Umgebungen der Gegenwart anfallen, ohne aufwändige Installation, Wartung oder Aufsicht durch Analysten.

SCHLÜSSELSTATISTIKEN

„Gartner prognostiziert, dass bis 80 % der Arbeitsaufgaben bis zum Jahre 2020 auf einem mobilen Gerät erledigt werden."

GARTNER, „VORBEREITUNG AUF EIN UNIFIED ENDPOINT MANAGEMENT ALS ERSATZ FÜR MDM UND CMT" JUNI 2018

48 % priorisieren Geschwindigkeit und Gewinn gegenüber mobiler Sicherheit, wobei fast die Hälfte der Befragten angibt, dass sie bei der Sicherheit Abstriche gemacht haben, um weiterarbeiten zu können. 46 % derjenigen, die Sicherheit vernachlässigten, gaben zu, einen Kompromiss eingegangen zu sein.

VERIZON MOBILE SECURITY INDEX (MSI) BERICHT 2019

cybereason