

# AV-Comparatives veröffentlicht die Ergebnisse seines EPR - Endpoint Prevention & Response (EPR) Tests

Das unabhängige ISO-zertifizierte Sicherheitstestlabor AV-Comparatives hat die Ergebnisse seines Endpoint Prevention & Response (EPR) Tests veröffentlicht.

INNSBRUCK, TIROL, ÖSTERREICH, January 20, 2022 /EINPresswire.com/ -- Der EPR-Test von [AV-Comparatives](#) ist die weltweit umfassendste Bewertung dieser Art.

Jedes der 10 getesteten Produkte wurde 50 verschiedenen gezielten Angriffsszenarien unterzogen.

Der höchste Strategic Leader Award wurde an Bitdefender, Palo Alto Networks, Check Point, CrowdStrike, F-Secure, Cisco und ESET verliehen. Symantec von Broadcom wurde mit dem CyberRisk Visionaries Award ausgezeichnet. Zwei weitere Anbieter erhielten den Strong Challengers Award.



DataBreaches können erhebliche finanzielle Auswirkungen haben, wobei die durchschnittlichen Kosten eines Breaches laut IBM derzeit bei 4,24 Millionen Dollar liegen"

*Peter Stelzhammer, co-founder AV-Comparatives*

Der Strategic Leader Award wird an EPR-Produkte verliehen, die eine sehr hohe Investitionsrentabilität und sehr niedrige Gesamtbetriebskosten aufweisen. Diese Produkte zeichnen sich durch herausragende Präventions-, Erkennungs-, Reaktions- und Berichterstattungsfunktionen der Unternehmensklasse aus, kombiniert mit optimalen operativen und analytischen Workflow-Funktionen.

Peter Stelzhammer, co-founder von AV-Comparatives, sagte:

"Herzlichen Glückwunsch an unsere Strategic Leaders. Diese Gewinner zeigen anderen den Weg nach vorne, indem sie sich ehrgeizige Ziele setzen und diese auch erreichen. Sie entwickeln



bahnbrechende Ideen und setzen diese in ihren Produkten um."

"Sicherheitsverletzungen können erhebliche finanzielle Auswirkungen haben, wobei die durchschnittlichen Kosten einer Sicherheitsverletzung laut IBM derzeit bei 4,24 Millionen Dollar liegen."

"Ein wirksames EPR-Produkt, das die negativen Auswirkungen eines Angriffs minimiert, kann eine sehr gute Investition sein. Wenn ein Unternehmen im Falle eines Angriffs 2 Millionen Dollar verlieren kann, ist es finanziell sinnvoll, die Hälfte davon in Sicherheitsmaßnahmen zu investieren."

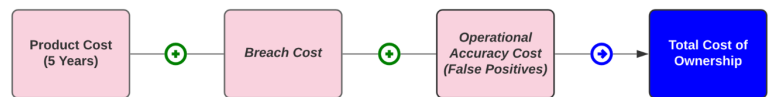
Unternehmen setzen EPR-Produkte ein, um gezielte Angriffe wie Advanced Persistent Threats (ATPs) zu erkennen, zu verhindern, zu analysieren und darauf zu reagieren. Sie sollten in der Lage sein, Malware und Netzwerkangriffe auf einzelne Workstations zu erkennen und zu blockieren sowie mit mehrstufigen Angriffen umzugehen, die darauf abzielen, das gesamte Netzwerk eines Unternehmens zu infiltrieren.

EPR-Systeme sollten nicht nur einzelne Geräte schützen, sondern auch eine detaillierte Analyse des Ursprungs, der Methoden und der Ziele eines Angriffs liefern, damit das Sicherheitspersonal die Art der Bedrohung verstehen, ihre Ausbreitung verhindern, Schäden beheben und Vorkehrungen treffen kann, um ähnliche Angriffe in Zukunft zu verhindern.

Der EPR-Test umfasst eine Vielzahl verschiedener Techniken. Bleiben die Angriffe unentdeckt, durchlaufen sie drei verschiedene Phasen: Endpoint Compromise and Foothold; Internal



AV-Comparatives' Endpoint Prevention and Response (EPR) – ECRQ - Enterprise CyberRisk Quadrant™



AV-Comparatives' Formel zur Ermittlung der Gesamtbetriebskosten für ein Produkt



Logo AV-Comparatives

Propagation and Asset Breach.

Bei den Tests wurde ermittelt, ob das Produkt den Angriff erkannte, automatische Maßnahmen zur Abwehr der Bedrohung ergriff (aktive Reaktion) oder Informationen über den Angriff lieferte, die der Administrator nutzen konnte, um selbst Maßnahmen zu ergreifen (passive Reaktion).

Wenn ein EPR-Produkt einen Angriff in einer Phase nicht blockiert, wird der Angriff in der nächsten Phase fortgesetzt.

Für jedes getestete Produkt wurde ein Zeitfenster von 24 Stunden nach Beginn eines Angriffs festgelegt. Die Tester untersuchten die Fähigkeit der einzelnen Produkte, Abhilfemaßnahmen zu ergreifen, wie z. B. die Isolierung eines Endpoints vom Netzwerk, die Wiederherstellung von einem Systemabbild oder die Bearbeitung der Windows Registry.

AV-Comparatives testete auch die Fähigkeit jedes Produkts, die Art eines Angriffs zu untersuchen, einschließlich eines Zeitplans und einer Aufschlüsselung der Phasen. Schließlich wurde die Fähigkeit jedes Produkts bewertet, Informationen über Indikatoren einer Kompromittierung zu sammeln und in einer leicht zugänglichen Form zu präsentieren.

Wie alle öffentlichen Testberichte von AV-Comparatives ist auch der EPR-Vergleichsbericht 2021 kostenlos erhältlich: [https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR\\_Comparative\\_2021.pdf](https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_Comparative_2021.pdf)

Über AV-Comparatives:

AV-Comparatives ist eine unabhängige Organisation, die systematische Tests anbietet, um die Wirksamkeit von Security-Software-Produkten und mobilen Sicherheitslösungen zu untersuchen. Durch den Einsatz eines der weltweit größten Stichprobenerfassungssysteme hat sie eine reale Umgebung für akkurate Tests geschaffen.

AV-Comparatives bietet Einzelpersonen, Nachrichtenorganisationen und wissenschaftlichen Einrichtungen frei zugängliche Av-Test-Ergebnisse. Die Zertifizierung durch AV-Comparatives ist ein weltweit anerkanntes offizielles Gütesiegel für die Performance von Software.

Peter Stelzhammer

AV-Comparatives

+43 720 115542

media@av-comparatives.org

---

This press release can be viewed online at: <https://www.einpresswire.com/article/561071367>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.