
# Blacklist- und Whitelist-basierte Software im Vergleich

**Whitepaper**

Simplifying Computer Management eurosales@faronics.com www.faronics.com
Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL

## Einleitung

Die Risiken, die von Malware in Form von Rootkits, Viren und Trojanern ausgehen, nehmen täglich zu. Gemäß einer aktuellen Studie wachsen die Bedrohungen exponentiell, und im ersten Quartal 2011 wurden täglich im Durchschnitt 73.000 neue Formen von Malware festgestellt. Gegenüber dem Vorjahreszeitraum im Jahr 2010 bedeutet dies für die Malware-Entwicklungsrate eine Zunahme in Höhe von 26 %.

Infolge des explosiven Malwarewachstums verlangen die Unternehmen nach leistungsfähigeren Sicherheitslösungen, die häufig zwei entgegengesetzte Konzepte beinhalten: das Blacklisting und das Whitelisting. Dieses neue Whitepaper erörtert auf Blacklists basierende Software, die eine der gängigsten Lösungen im Kampf gegen die zunehmenden Malwarebedrohungen darstellt. Darüber hinaus befasst es sich auch mit dem relativ neuen und selteneren Konzept, bei dem das Problem mit einer auf Whitelists basierenden Software angegangen wird.

## Warum gibt es Malware?

Seit 1986 der erste Computervirus entdeckt wurde, ist das Malware-Aufkommen förmlich explodiert. Was als Hobby einiger Computerfreaks begann, denen es um die Herausforderung und den Ruhm ging, hat sich zu einem wesentlichen Werkzeug des organisierten Verbrechens entwickelt. Cyberkriminelle sind heutzutage Profis, die es darauf abgesehen haben, durch den Diebstahl und Verkauf von geschützten Daten, Finanzunterlagen, Personalakten, medizinischen Unterlagen, Kundenlisten u. v. m. Geld zu machen.

Die hierzu benötigten Tools sind leicht zugänglich, und Malware-Kits können z. B. aus dem Internet heruntergeladen werden. Heute können sich selbst diejenigen als Hacker betätigen, die nicht über die technischen Kenntnisse verfügen, und in wenigen Minuten Trojaner einrichten und illegale Vorhaben in die Wege leiten. Das Hacken entwickelt sich zu einem Gewerbe, das sich so gut auszahlt, dass die Kriminellen in ihre Angriffe investieren und für Forschung, Programmierer und Tester bezahlen, um der IT-Sicherheit einen Schritt voraus zu sein.

Das Internet ist heutzutage voller Gefahren. 90 % der Sicherheitsvorfälle resultieren daraus, dass das organisierte Verbrechen versucht, an Unternehmensinformationen zu gelangen. An praktisch allen Sicherheitsverletzungen im Jahr 2009 war individualisierte Malware beteiligt, mit der 140 Millionen Datensätze entwendet wurden. Aufgrund der zunehmenden Vorfälle rüsten die Unternehmen ihre IT-Sicherheitsinfrastruktur auf.

## Malware und ihre Folgen

Malware wird heimtückischer, schädlicher und verursacht höhere Kosten als jemals zuvor. Neueren Berichten zufolge nehmen die durch Malware und Sicherheitsverletzungen verursachten Kosten auf alarmierende Art und Weise zu.

## Durch Datenschutzverletzungen verursachte Kosten

Einigen Schätzungen zufolge verursachen Cyberkriminelle in den USA Kosten in Millionenhöhe, während andere von Hunderten von Milliarden sprechen. Eine 2010 vom Ponemon Institute durchgeführte Untersuchung schätzt, dass den einzelnen von Cyberkriminellen geschädigten Unternehmen jährliche Kosten zwischen 1 und 52 Millionen US-Dollar entstehen und der durchschnittliche Schaden 7,2 Millionen US-Dollar beträgt, was gegenüber 2009 einer Zunahme von 7 % entspricht.

## Durch Identitätsdiebstahl verursachte Kosten

Gemäß einer Publikation aus dem Jahr 2011, die von Javelin Strategy and Research veröffentlicht wurde, betragen die jährlichen durch Identitätsdiebstahl verursachten Kosten 37 Milliarden US-Dollar. Hierbei wurden alle Arten von Identitätsdiebstahl berücksichtigt, nicht nur die, die online erfolgen. Ein im Januar 2011

veröffentlichter Artikel gibt an, dass 11,1 Millionen Erwachsene in den USA Opfer eines Identitätsdiebstahls wurden, was gegenüber 2008 einer Zunahme von 12 % entspricht. Die in den USA durch Betrug verursachten Schäden beliefen sich auf 31 Milliarden US-Dollar, während Unternehmen weltweit infolge von Identitätsdiebstählen jährlich 221 Milliarden US-Dollar verlieren.

## Durch Zero-Day-Attacken verursachte Kosten

Ein weiteres Problem stellen die Zero-Day-Virusattacken dar, gegen die es gegenwärtig keinen garantierten Schutz gibt. Die von Zero-Day-Attacken ausgenutzten Schwachstellen, die eine offene Hintertür zu Betriebssystemen bieten, stellen für Unternehmen eine ernstzunehmende Bedrohung dar. Die neuesten Forschungsergebnisse zeigen, dass mutierende Malware zunimmt und die Angreifer zunehmend

raffinierter vorgehen. Im Durchschnitt sind nur 15 Systeme von einer bestimmten Malwarevariante betroffen, bevor diese sich verändert, um der Erkennung zu entgehen und weiter Schaden anrichten zu können.
Das Gesundheits- und das Bildungswesen sind die beiden Bereiche, die die meisten Datenschutzverletzungen verzeichnen, während im Finanz- und im Regierungssektor die meisten Identitäten gestohlen werden. Die jüngsten Schlagzeilen verdeutlichen, dass keine Branche gegen die Problematik gefeit ist, denn wie sich gezeigt hat, wurden selbst Konzernriesen und führende Sicherheitsunternehmen Opfer von Angriffen.

## Die Lösungen im Überblick

Eine der größten Kategorien, die traditionell gegen Malware eingesetzt wird, ist die Blacklisting-Technologie, zu der althergebrachte Lösungen, wie z. B. Antiviren- und Antispyware-Programme, gehören.

## Traditionelle Blacklisting-Lösungen

Eine Blacklist enthält bestimmte Dinge, wie z. B. Domain-Namen, E-Mail-Adressen oder Viren, die potenziell gefährlich sind oder Schäden verursachen, und deshalb keinen Zugang zur Infrastruktur erhalten, in die sie eindringen möchten. So kann z. B. eine Website in eine Blacklist eingetragen werden, weil bekannt ist, dass sie betrügerischer Art ist, oder weil sie Schwachstellen des Browsers ausnutzt, um Spyware oder ungewünschte Software auf das System zu übertragen.
Darüber hinaus kann das Blacklisting-Konzept auch im Kampf gegen E-Mail-Spam eingesetzt werden. Der Benutzer kann in einem Spamfilter-Programm eine Regel erstellen, die verhindert, dass E-Mails eines bestimmten Ursprungs (bzw. auf die andere festgelegte Kriterien zutreffen) zugestellt werden, obwohl der Spamfilter dies normalerweise zulassen würde.
Typische Beispiele für traditionelle Blacklist-Lösungen sind Antiviren- oder Antispyware-Programme. Blacklist-Software blockiert bekannte Bedrohungen. Antivirensoftwarehersteller pflegen eine Datenbank, die Informationen über bekannte Viren enthält, und stellen diese ihren Kunden zur Verfügung. Sobald ein neuer Virus entdeckt wurde, entwickelt das Unternehmen ein spezielles Gegenmittel, das den Kunden in Form eines Updates geliefert wird.

**Vorteile von Blacklist-Lösungen:**

- Die Aktualisierung der Virendefinitionen erfolgt automatisch und verursacht keine zeitaufwändigen Wartungsarbeiten
- Malware kann identifiziert und manchmal eliminiert werden
- Updates können spontan über einen Update-Services-Server erfolgen
- Die Lösungen bieten kompletten Schutz vor sämtlichen bekannten Bedrohungen
- Sie sind vielseitig und bekämpfen alle Arten von Malwarebedrohungen

**Nachteile von Blacklist-Lösungen:**

- Sie schützen ausschließlich vor bekannten Bedrohungen, was oftmals bedeutet, dass eine neue Bedrohung nur identifiziert werden konnte, weil ihr jemand zum Opfer gefallen ist.
- Malware infiziert durchschnittlich 15 Systeme, bevor sie mutiert, ihre Signatur ändert und so von Blacklisting-Lösungen nicht mehr erkannt werden kann.
- Antivirenlösungen stoppen im Durchschnitt nur etwa 19 % der Bedrohungen.
- Voraussetzung dieser Lösungen ist es, dass Viren oder Spyware identifiziert und zur Blacklist hinzugefügt wird, weshalb Workstations und Netzwerke anfällig für Zero-Day-Attacken sind.
- Der Anwender überlässt im Grunde die Kontrolle seiner Netzwerke einem Drittanbieter und muss seine Viren- und Spywaredefinitionen kontinuierlich aktualisieren, was sowohl für die Hardware als auch die Netzwerkbandbreite eine Belastung darstellt.
- Diese Art von Lösung ist von Natur aus sehr ressourcenintensiv und wirkt sich negativ auf die Leistungsfähigkeit der Computer aus.

## Joe, der VIP-Manager mit der Gästeliste, und die Blacklist-Technologie

Joe arbeitet als VIP-Manager der Hi-Tek-Bar. Jede Nacht, wenn die Bar öffnet, steht Joe an der Tür und ist dafür verantwortlich, wer rein darf und wer nicht. Um ihm diese Arbeit zu erleichtern, gibt ihm sein Chef eine Liste derjenigen, die Hausverbot haben. Wenn diese Personen dann an der Tür erscheinen und hoffen, eingelassen zu werden, geht Joe seine Liste durch, findet den entsprechenden Eintrag und weist sie ab.

Wenn sich allerdings jemand eine Glatze rasiert und einen Schnurrbart wachsen lässt, kann es sein, dass Joe ihn beim nächsten Mal nicht erkennt. In diesem Fall würde Joe ihn höchstwahrscheinlich rein lassen, und derjenige könnte in der Bar tun und lassen, was er will. Abgesehen davon bedeutet die Tatsache, dass jemand noch nicht auf der Liste der Personen mit Hausverbot steht, noch lange nicht, dass er oder sie für die Bar keine Bedrohung darstellt. Es bedeutet lediglich, dass diese Person in der Bar noch nicht durch unerwünschtes Verhalten aufgefallen ist. Joe hat also keine Möglichkeit festzustellen, wer eventuell gefährlich sein könnte.

## Moderne Blacklist-Lösungen

Blacklist-Lösungen beschränken sich heute nicht mehr nur darauf, bekannte Bedrohungen abzuwehren, sondern setzen auch heuristische Methoden ein. Als Heuristik bezeichnet man die Lösung eines Problems mithilfe von erfahrungsbasiertem Wissen. Im Bereich der Antivirensoftware bezeichnet man damit manchmal die Fähigkeit, Dateien zu überprüfen und herauszufiltern, die wahrscheinlich einen Computervirus oder Malware enthalten.

Software, die heuristische Methoden anwendet, sucht nach bekannten Quellen, häufig verwendeten Textbausteinen und Übertragungs- oder Inhaltsmustern, die in der Vergangenheit im Zusammenhang mit Viren enthaltenden Dateien aufgefallen sind. Der Begriff Heuristik wurde von Antivirenforschern geprägt, um ein Antivirenprogramm zu beschreiben, das Viren aufspürt, indem es – anstatt einfach nur nach Signaturen zu suchen – die Programmstruktur, das Verhalten und andere Eigenschaften analysiert.

**Vorteile von Heuristik-Lösungen:**

- Sie benötigen keine Aktualisierungen der Virendefinitionen
- Sie können ggf. Zero-Day-Attacken abwehren
- Sie bieten eine zusätzliche Schutzebene, da sie sich nicht ausschließlich auf Definitionsdateien verlassen; manchmal spüren sie Bedrohungen auf, die nicht in einer Blacklist enthalten sind

**Nachteile von Heuristik-Lösungen:**

- Sie treffen Annahmen über das zu lösende Problem und können suboptimale Ergebnisse liefern
- Es kann vorkommen, dass die Muster auch auf virenfreie Dateien zutreffen und die Lösungen entsprechend falsch-positive Ergebnisse liefern, die die Auslieferung zulässiger Dateien oder E-Mails verzögern.
- Die Technologie ist noch relativ jung, und die Entwicklung und Verbesserung benötigt noch Zeit.

## Joe, der VIP-Manager mit der Gästeliste, und Heuristik-Lösungen

In der Hi-Tek-Bar hat sich Joes Chef dazu entschieden, einen anderen Ansatz auszuprobieren. Anstatt eine Liste mit bestimmten Namen und Fotos von Personen zu erstellen, die die Bar nicht betreten dürfen, wird nun eine eher allgemeine Reihe von Regeln verwendet, um festzustellen, wer rein darf und wer nicht. Bei der Erstellung dieses Regelwerks wurde berücksichtigt, welche Art von Personen in der Vergangenheit Ärger gemacht hat. So hat man Joe beispielsweise aufgetragen, alle mit kahlrasierten Köpfen und Oberlippenbärten abzuweisen, weil es früher mit Leuten, die so aussahen, Probleme gab.

Jedoch zur Überraschung des Eigentümers der Hi-Tek-Bar ist dessen Sohn gerade nach einem Jahr als Rucksacktourist in Asien mit einem kahlrasierten Kopf und einem Oberlippenbart zurückgekehrt. Joe schaut ihn an und lässt ihn nicht rein, weil sein Aussehen genau dem Profil eines Störenfrieds entspricht, und zwar obwohl der Sohn des Eigentümers ein absolut friedliebender, vertrauenswürdiger Stammkunde ist.

## Ein unterschiedlicher Ansatz: Die Whitelist-Lösung

Die Whitelisting-Technologie ist das Gegenteil der Blacklisting-Technologie und somit eine Liste von Dingen, wie z. B. Domain-Namen, E-Mail-Adressen oder ausführbaren Dateien, denen der Zugang zum System gestattet ist. Eine Whitelist mit Domain-Namen ist z. B. eine Liste der URLs, die unabhängig von den Regeln eines E-Mail-Spam-Programms angezeigt werden dürfen.

Das bekannteste Beispiel einer Whitelist ist eine von den Benutzern erstellte Liste von autorisierten E-Mail-Adressen, von denen – unabhängig von den Regeln eines Antispamprogramms – Nachrichten erhalten werden dürfen.

Einer der wichtigsten Bereiche des Whitelistings ist das Anwendungs-Whitelisting. Hierbei dürfen auf einem Rechner nur zuvor festgelegte Programme ausgeführt werden, und für jegliche andere Programme, die nicht im Voraus genehmigt wurden, wird die Ausführung unterbunden.

**Vorteile des Anwendungs-Whitelistings:**

- Schützt vor Malware, Zero-Day-Attacken und gezielten Angriffen, da keine nichtautorisierten ausführbaren Dateien ausgeführt werden können
- Verbessert die Mitarbeiterproduktivität und die Leistungsfähigkeit der Workstations, da keine unerwünschten Anwendungen, wie z. B. Chatprogramme, P2P-Anwendungen, Spyware oder Trojaner installiert oder ausgeführt werden können
- Eliminiert das Risiko kostspieliger Überprüfungen und Strafen für Lizenzverstöße, da keine illegale oder nichtlizenzierte Software installiert werden kann
- Ermöglicht dem Unternehmen Einsparungen, indem es die Ausfallzeiten verringert, die Lebensdauer der PCs verlängert und die Anzahl an Support-Anfragen senkt und so Möglichkeiten für Kostenübertragungen schafft, die das Unternehmen in die Lage versetzen, mit weniger mehr zu erreichen

**Nachteile von Whitelist-Lösungen:**

- Das Erstellen einer Whitelist kann, solange keine moderne Anwendungs-Whitelisting-Lösung verwendet wird, sehr zeitaufwändig sein
- Updates können in Ermangelung fortschrittlicher Kontrolloptionen eine Herausforderung darstellen, da sich durch die Aktualisierung die Identität der zugelassenen Anwendung derart ändern kann, dass sie nicht

mehr dem entspricht, was in der vorliegenden Whitelist eingetragen wurde, und das Programm folglich nicht mehr gestartet werden darf

## Joe, der VIP-Manager mit der Gästeliste, und die Whitelist-Technologie

Joe arbeitet noch immer als VIP-Manager in der Hi-Tek-Bar. Mittlerweile probiert er mithilfe eines neuen dritten Konzepts, unerwünschte Gäste fern zu halten. Dieses Mal hat er von seinem Chef eine Liste derjenigen bekommen, die er in die Bar hineinlassen darf. Wer nicht rein darf, spielt jetzt keine Rolle mehr.
Joe achtet nicht mehr darauf, wer evtl. basierend auf allgemeinen Regeln aussieht wie ein Störenfried. Er lässt ganz einfach nur diejenigen in die Bar, die auf der genehmigten Liste stehen. Fehler sind so ausgeschlossen, und er kann ganz beruhigt sein. Er ist nun viel glücklicher.

**Faronics Anti-Executable**

Faronics Anti-Executable setzt im Kampf gegen Malware auf ein anderes Konzept. Anti-Executable lässt den Administrator auswählen, welche Anwendungen auf einer Workstation ausgeführt werden dürfen. Jegliche nicht durch Anti-Executable autorisierte ausführbare Dateien können weder installiert noch ausgeführt werden. Anti-Executable basiert auf dem Whitelist-Konzept. Anstatt festzulegen, welche ausführbaren Dateien blockiert werden sollen, werden mithilfe der Lösung die ausführbaren Dateien autorisiert, die auf dem System erwünscht sind.
Seit einiger Zeit weiß die IT-Branche um die Leistungsfähigkeit des Anwendungs-Whitelistings. Die Schwierigkeiten bei der Einrichtung der anfänglichen Whitelist sowie die Kosten für die Pflege der Whitelists haben jedoch viele Unternehmen davon abgehalten, diese Sicherheitsstrategie einzuführen. Dank seiner hilfreichen modernen Funktionalitäten profitieren Unternehmen mit Faronics Anti-Executable von den Vorteilen des Anwendungs-Whitelistings, ohne dass dadurch der Arbeitsaufwand für das IT-Team steigt.

Anti-Executable schließt die Sicherheitslücken, die Antivirenlösungen allein nicht bewältigen können. Täglich entstehen zehntausende neue Malwareformen, und Antivirenprogramme können angesichts dieser unglaublichen Flut einfach nicht mithalten. In Anbetracht der von mutierender Malware, gezielten Angriffen und Zero-Day-Attacken ausgehenden Risiken reicht es nicht mehr aus, dass man sich darauf verlässt, dass bekannte Bedrohungen abgefangen werden. Im Durchschnitt dauert es 11,6 Tage, bis ein Antivirenprogramm eine neue Bedrohung erkennt, und das ist einfach viel zu lange, wenn man bedenkt, dass ein Unternehmensnetzwerk während dieser Zeit ernsthaften Risiken ausgesetzt ist.
Anti-Executable schützt vor den beiden wichtigsten Werkzeugen, die Hacker während eines Angriffs einsetzen, um die Kontrolle zu übernehmen. Es schützt vor der Ausführung von nichtautorisierten Keyloggern und Remote-Access-Programmen, mit denen sich Kriminelle Zugang zu Unternehmensnetzwerken verschaffen. Anti-Executable bietet den ultimativen Schutz vor Zero-Day-Attacken, indem es die schädlichen ausführbaren Programme ganz einfach nicht als im Voraus genehmigte Anwendungen anerkennt. Das hat zur Folge, dass durch Malware verursachte Ausfallzeiten erheblich zurückgehen.
Mithilfe seiner modernen Whitelist-Technologie hilft Faronics Anti-Executable den IT-Experten bei der Minimierung der Herausforderungen, die traditionelle Whitelisting-Lösungen mit sich bringen. Hierzu gehört beispielsweise die Möglichkeit der Whitelist-Erstellung während der Bereitstellung, sodass die IT-Mitarbeiter nicht manuell für jeden Rechner eine neue Liste einrichten müssen. Darüber hinaus können Softwareanbieter, wie z. B. Microsoft, als vertrauenswürdig gekennzeichnet werden, was den IT-Fachkräften das Updatemanagement vereinfacht, wodurch wiederum die kontinuierliche Verfügbarkeit der Rechner gewährleistet werden kann.
Whitelist-Lösungen bieten eine unkomplizierte und sichere Möglichkeit zur umfassenden Systemkontrolle. Setzt man das Whitelisting-Konzept zum Wohle der Workstationsicherheit ein, ermöglicht man dem Administrator die volle Kontrolle und kann noch unbesorgter sein.

## Über Faronics

Faronics verfügt über eine etablierte Erfolgsbilanz in der Unterstützung von Unternehmen bei der Verwaltung, Vereinfachung und Sicherung ihrer IT-Infrastrukturen. Dank Faronics ist es möglich, mit weniger Aufwand mehr zu erreichen, indem der Nutzen der bestehenden Technologie maximiert wird. Mit unseren Lösungen profitieren Sie von absolut zuverlässigen Workstations, der vollständigen Systemkontrolle und einer reibungslosen Energieverwaltungslösung für PCs.

Das 1996 gegründete Unternehmen Faronics verfügt über Niederlassungen in den USA, Kanada und Großbritannien sowie ein globales Netzwerk an Vertriebspartnern. Unsere Lösungen werden weltweit in über 150 Ländern und von mehr als 30.000 Kunden eingesetzt.

## Copyright





Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL