Dr.WEB®
seit 1992

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks*

* Neutralisiert aktive Bedrohungen und neue Angriffe

Doctor Web, 2020

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

Signaturfreier Antivirus der neuen Generation zum besseren PC-Schutz in Kombination mit Ihrem üblichen Virenschutzprogramm

Störungen von Geschäftsprozessen, unbefugter Zugriff auf Geräte, Ausnutzen von Sicherheitslücken, Passwort-Ermittlung, Phishing-Angriffe und andere rechtswidrige Handlungen, die unter anderem in virenbedingten Vorfällen durch Malware ausgeübt werden, können einem Unternehmen großen Schaden zufügen.

Leider sollte man sich heutzutage aus verschiedenen Gründen nicht mehr nur auf den Virenschutz eines einzigen Anbieters verlassen.

Bevor technisch komplizierte und besonders gefährliche Viren freigesetzt werden, werden sie von den Virenschreibern mit allen bekannten Antivirenprogrammen sorgfältig auf Erkennbarkeit geprüft.

Wenn man sich also nur auf Virendatenbanken verlässt – so vollständig sie auch sein mögen – werden einem die Cyber-Kriminellen immer einen Schritt voraus sein: Der bösartige Code mag bereits in die Virendatenbank des Virenschutzanbieters eingetragen, aber noch nicht in der Virendatenbank auf dem Gerät des Nutzers vorhanden sein.

Die Gefahr, mit einem neuen UNBEKANNTEN Virus infiziert zu werden, besteht IMMER.

Eine der Möglichkeiten, die Wahrscheinlichkeit einer Infektion zu verringern, ist, mehrere Antivirenlösungen einzusetzen. Eine der Vorschriften des Russischen Föderalen Dienst für technische und Exportkontrolle* lautet:

„4) auf verschiedenen Ebenen eines Informationssystems sollte der Virenschutz durch Einsatz von Antivirenprogrammen mehrerer Hersteller gewährleistet werden".

Wann ist es sinnvoll, zwei Virenschutzprogramme zu verwenden?

- Wenn Ihr üblicher Antivirus Bedrohungen übersieht.
- Wenn Ihr üblicher Antivirus nicht oft aktualisiert werden kann.
- Wenn Ihr PC längere Zeit ohne Internetverbindung arbeiten muss.
- Wenn Ihr PC in einem isolierten Netzwerk arbeitet, in dem nur selten Updates bereitgestellt werden können.

Ein signaturfreier Antivirus ist immer sinnvoll: Sie können nie genau wissen, ob Ihr Antivirus eine Malware bereits übersehen hat oder nicht.

Zum besseren Schutz des lokalen Netzwerks sowie einzelner Computer vor den neuesten und besonders gefährlichen bösartigen Bedrohungen – u. a. vor Verschlüsselungstrojanern – empfehlen wir, neben einem

herkömmlichen signaturbasierten Virenschutzprogramm (nicht Dr.Web) den signaturfreien Antivirus **Dr.Web KATANA** einzusetzen.

Keine Virenschutzsoftware kann zum Zeitpunkt des Eindringens 100 % der bösartigen Programme erkennen. Leider können besonders gefährliche Schadprogramme wie Ransomware herkömmliche Schutzmechanismen umgehen.

Auch wenn Ihr Antivirus Testsieger zahlreicher Vergleichstests ist, sollte berücksichtigt werden, dass Analysten und Testentwickler zum Zeitpunkt des Tests bereits mit den verwendeten Schadprogrammen vertraut sind. Erfolgreiche Testergebnisse zeugen also nicht von der Fähigkeit des Virenscanners, aktive Bedrohungen zu neutralisieren, die zum Zeitpunkt des Angriffs unbekannt sind.

Warum waren so viele Unternehmen von WannaCry betroffen, obwohl sie Virenschutzprogramme verwendeten, die bei verschiedenen Testwettbewerben gut abgeschnitten hatten? In ihren Virenschutzprogrammen fehlten die Signaturen des neuen Trojaners und ihre verhaltensbasierten Analyse-Tools scheiterten.

Die Kunden von Dr.Web waren von WannaCry nicht betroffen.

Dr.Web KATANA-Technologien können zusätzlichen Schutz vor den neuesten Bedrohungen bieten, die Ihrem signaturbasierten Antivirus unbekannt sind: Verdächtige Programme werden analysiert und auf Merkmale bösartigen Verhaltens geprüft. Das Produkt schützt so vor Bedrohungen, die mit herkömmlichen Erkennungsverfahren (Signaturen) nicht erkannt werden.

Alle Trojaner

verwenden ähnliche Algorithmen, nutzen die gleichen Schwachstellen aus, um in Betriebssysteme einzudringen, und verfügen über die gleichen schädlichen Funktionen.	**machen den gleichen Fehler:** sie machen den ersten Zug und greifen das System an.

Sobald der Trojaner aktiv wird, kann Dr.Web KATANA ihn erkennen und neutralisieren.

Der signaturfreie Antivirus Dr.Web KATANA erfüllt dieselben Aufgaben wie herkömmliche Virenscanner:

- er erkennt bösartige Prozesse,
- neutralisiert Malware Angriffe,
- verhindert Versuche der Malware, in das System einzudringen, – aber auf eine elegantere Art.

Dr.Web KATANA erkennt bösartige Aktivitäten, sobald ein Trojaner aktiv wird.

- Viele Trojaner verwenden ähnliche Algorithmen. Sie nutzen die gleichen Schwachstellen aus, um in Betriebssysteme einzudringen und verfügen über die gleichen schädlichen Funktionen.
- Alle Trojaner machen den gleichen Fehler: sie machen den ersten Zug, indem sie das System angreifen.
- Sobald ein Trojaner aktiv wird, kann Dr.Web KATANA den „Feind" erkennen und neutralisieren.
- Dr.Web KATANA analysiert das Verhalten von Bedrohungen in Echtzeit und verhindert sofort die Ausführung von bösartigen Skripten und Prozessen, die Ihr Antivirus nicht erkennen konnte.
- Keine Signaturen sind erforderlich. Dies macht Dr.Web KATANA zu einer extrem leichten Waffe.

Herkömmliche verhaltensbasierte Analyse-Tools beruhen auf den in der Datenbank festgelegten Verhaltensmustern bekannter Schadprogramme.

Auch Cyber-Kriminellen sind diese Muster bekannt!

Sie können Exploits einsetzen und Sicherheitslücken ausnutzen, um diesen Schutz zu umgehen.

Sofortige Erkennung durch Dr.Web KATANA	**Sekundenschnelle Analyse**	**Kein Zugriff auf „schwere" Virendatenbanken erforderlich**

Dr.Web KATANA überwacht

- Prozesse legitimer Anwendungen
- Kritische Systembereiche und -dienste (Bootsektoren, Registry-Schlüssel), einschließlich solcher, die für virtuelle Gerätetreiber verantwortlich sind
- Ausführungsregeln für Programme
- Deaktivierung des abgesicherten Modus
- Einsatz neuer Systemroutinen durch Eindringlinge
- Installation neuer oder unbekannter Treiber
- Kommunikation zwischen den Spyware-Komponenten und dem Verwaltungsserver
- Geplante Backups
- Alle gängigen Webbrowser (Internet Explorer, Mozilla Firefox, Google Chrome, Vivaldi Browser)
- MS Office-Anwendungen (Word/Excel/InfoPath/Lync/Access/Outlook/Visio/WordPad), Windows Media Player
- Systemanwendungen
- Java- Anwendungen (Java 1.8/6/7), Flash- und PDF- Anwendungen (Acrobat Reader).

Features von Dr.Web KATANA

- Schützt kritische Systembereiche vor Änderungen durch Schadprogramme.
- Erkennt bösartige, verdächtige oder unzuverlässige Skripte/Prozesse und verhindert ihre Ausführung.
- Erkennt unerwünschte Dateiänderungen und überwacht alle Prozesse im System, um für Schadprogramme typisches Verhalten (z. B. Aktivitäten der Ransomware) zu erkennen und zu verhindern, dass bösartige Objekte in andere Programme eindringen.
- Erkennt und neutralisiert die neuesten Bedrohungen: Ransomware (Verschlüsselungstrojaner), Injektoren, ferngesteuerte bösartige Objekte (die zur Erstellung von Botnetzen oder zur Spionage verbreitet werden) sowie Virenpacker.
- Schützt vor Exploits – bösartigen Objekten, die Softwarefehler ausnutzen, um in das Betriebssystem einzudringen. Effektiv auch gegen sogenannte „Zero-Day-Bedrohungen", die bisher nur den Virenschreibern bekannt sind, die sie erstellt haben.
- Überwacht die gängigen Browser und ihre Plugins, schützt vor Browser-Blockern.
- Verhindert das Ändern von Bootsektoren durch Schadprogramme (z. B. Trojaner), damit diese nicht auf Ihrem PC ausgeführt werden können.
- Blockiert Änderungen an der Windows-Registrierung, um sicherzustellen, dass der abgesicherte Modus nicht deaktiviert wird.
- Verhindert Änderungen der grundlegenden Systemabläufe durch bösartige Programme. Schützt eine Reihe von Parametern in der Windows-Registry vor Änderungen, wodurch beispielsweise verhindert wird, dass Viren die Anzeige des Desktops ändern oder die Präsenz eines Trojaners im System mit einem Rootkit verbergen.
- Verhindert das Ändern von Startberechtigungen für Programme durch Malware.

- Verhindert das Herunterladen neuer oder unbekannter Treiber ohne Zustimmung des Nutzers.
- Verhindert Dateneinträge in die Registry durch Schadprogramme und bestimmte Anwendungen (z. B. Anti-Antivirenprogramme) und somit deren automatischen Start.
- Verhindert das Ändern der Registry-Zweige, die Informationen über virtuelle Gerätetreiber enthalten, um sicherzustellen, dass keine neuen virtuellen Geräte erstellt werden.
- Verhindert die Kommunikation zwischen Spyware-Komponenten und den Servern, von denen sie gesteuert werden.
- Verhindert, dass Malware Systemabläufe (z. B. geplante Backups) stört.

Wie funktioniert Dr.Web KATANA?

- Falls Dr.Web den Versuch erkennt, Sicherheitslücken auszunutzen, wird das Schließen des Programms erzwungen. Die Dateien der Anwendung werden weder geändert noch in Quarantäne verschoben.
- Nutzer erhalten Benachrichtigung über die Verhinderung eines bösartigen Prozesses. Eine Reaktion ihrerseits ist nicht erforderlich.
- Im Dr.Web-Ereignisprotokoll wird ein Eintrag über Verhinderung des Angriffs angelegt.
- Die Cloud wird ebenfalls sofort über den Vorfall informiert. Bei Bedarf werden die Experten von Doctor Web umgehend darauf reagieren (z. B. durch Verbesserung des Überwachungsalgorithmus).

Wie trägt Dr.Web Cloud zum Schutz bei?

Dr.Web Cloud enthält:

- Daten über die Funktionsweise von Schadprogrammen
- Informationen über zu 100% virenfreie Dateien
- Informationen über kompromittierte digitale Signaturen bekannter Softwareentwickler
- Informationen über digitale Signaturen von Adware/Riskware
- Schutzalgorithmen von Anwendungen.

Im Cloud-System werden Betriebsinformationen von Dr.Web KATANA, einschließlich Daten über die neuesten erkannten Bedrohungen, gesammelt. Dies ermöglicht es, umgehend auf im System festgestellte Schwachstellen zu reagieren und die lokal auf dem Computer gespeicherten Regeln zu aktualisieren.

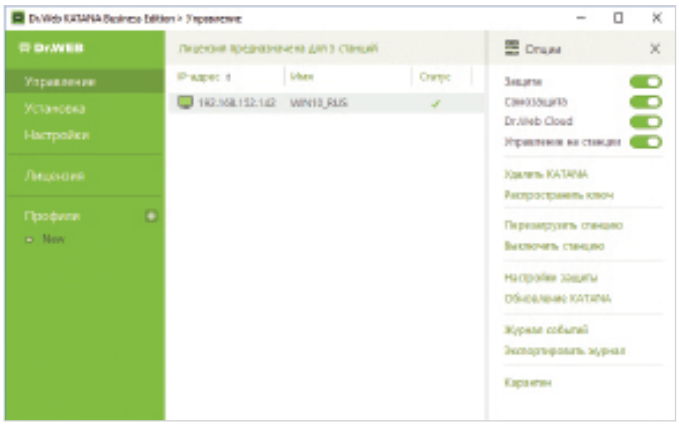
Es werden keine Benutzerdateien von einem geschützten System auf die Server von Doctor Web übertragen!

Bestmögliche Vorbeugung	Außergewöhnliche Resistenz	Offline-Modus
▪ Dr.Web KATANA beginnt schon während des Hochfahrens mit dem Schutz des Systems. ▪ Das Schutztool wird aktiv, noch bevor Ihr üblicher signaturbasierter Antivirus geladen wird!	▪ Dr.Web KATANA wird durch das einzigartige Selbstschutzmodul Dr.Web SelfPROtect geschützt. ▪ Falls ein Trojaner Ihren üblichen Antivirus deaktiviert, wird er an dem Dr.Web KATANA-Selbstschutzmodul scheitern. ▪ Dr.Web KATANA wird den Angriff abwehren und den bösartigen Prozess beenden.	▪ Trojaner können sich nicht selbständig verbreiten. ▪ Mitarbeiter verbreiten sie auf USB-Sticks und anderen Wechselmedien. ▪ Ist die Installation eines „schweren“ signaturbasierten Antivirus nicht möglich, kommt der signaturfreie Antivirus Dr.Web KATANA zu Hilfe. Das Produkt hat minimale Systemanforderungen und kann ohne Internetverbindung arbeiten.

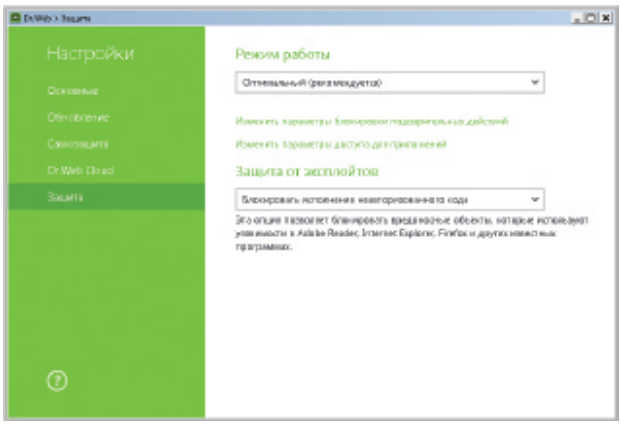
Steuerung

▪ Zentralisierte Installation auf geschützten Netzwerkstationen, Einstellung und Überwachung der Virenvorfälle sowie des Dr.Web KATANA Status auf geschützten Workstations.	▪ Vorinstallierte Schutzszenarien (optimal, mittel, paranoid) – das Produkt ist sofort einsatzbereit.	▪ Möglichkeit, flexible Regeln für vertrauenswürdige Anwendungen zu erstellen und zu verhindern, dass Softwarekonflikte durch die Nutzung von Dr.Web KATANA auftreten.	▪ Möglichkeit, Parameter zur Sicherheitskontrolle für eine bestimmte Anwendung einzustellen, sodass diese nur auf bestimmte Ressourcen zugreifen kann.

Verwaltungscenter



Agent



Kompatibilität

Während der Entwicklungsphase hat Dr.Web KATANA Kompatibilitätstests mit Produkten von TrendMicro, Symantec, Kaspersky, Mcaffee, ESET, etc. erfolgreich bestanden.

Über Doctor Web

Doctor Web Ltd. ist ein führender, weltweit agierender Hersteller von Antivirus- und Antispam-Lösungen. Das Doctor Web Team entwickelt seit 1992 Anti-Malware-Lösungen und beschäftigt weltweit 400 Mitarbeiter, davon 200 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln.

Über 120 Mio. Nutzer vertrauen Dr.Web

Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Baden-Baden vertrieben. Zu den weltweit über 120 Mio. Nutzern von Dr.Web gehören Privatanwender, namhafte und international agierende, börsennotierte Großunternehmen, Banken und öffentliche Einrichtungen. Zahlreiche Zertifikate und Auszeichnungen zeugen von einem hohen Maß an Vertrauen in Dr.Web Antivirensoftware.

Hier finden Sie einige Kunden von Doctor Web: https://customers.drweb.com.

Warum Dr.Web?

Alle Rechte an Dr.Web Technologien gehören Doctor Web Ltd. Das Unternehmen ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Doctor Web Ltd. verfügt über hauseigene innovative Technologien und unterhält ein Virenlabor, einen globalen Virenüberwachungsdienst und Support-Dienst.

Doctor Web Deutschland GmbH
Quettigstraße 12
76530 Baden-Baden
Deutschland
Telefon: +49 (0) 170 4884028
Internet: www.drweb-av.de