



**Dr.WEB®**

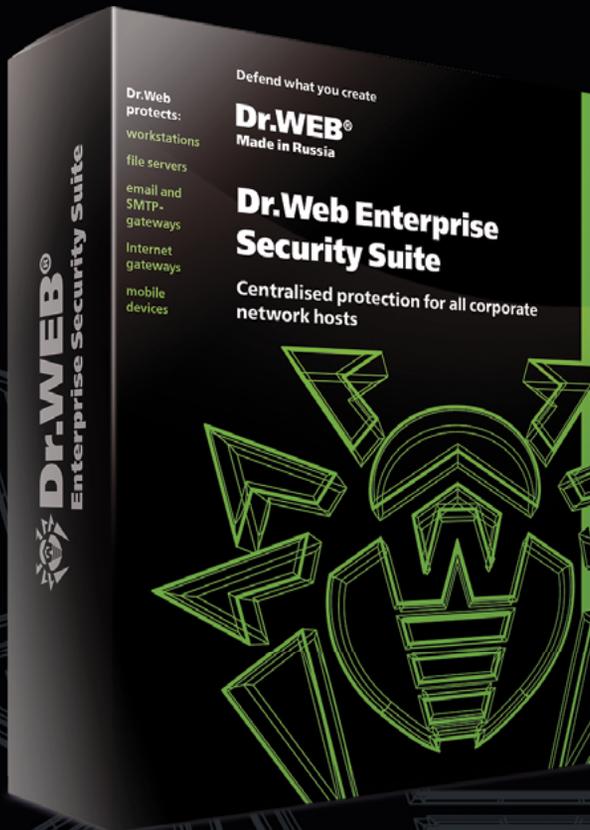
Made in Russia

DEFEND WHAT YOU CREATE

# Dr.Web Desktop Security Suite

für Linux

[www.drweb-av.de](http://www.drweb-av.de)



## Angriffe auf Workstations und Geräte unter Linux sind im Trend. Ihre Verletzlichkeit zieht Eindringlinge jeglicher Art an.

Bis zu tausend oder sogar mehr böswillige Apps werden für Linux pro Tag erstellt, einschließlich Mining-Trojaner und Encoder. Wenn Computer und Geräte der Nutzer infiziert sind, verliert das Unternehmen nicht nur Zeit, sondern auch Geld für die Wiederherstellung des Zugangs zu infizierten Computern und sensiblen Dokumenten. Oft sind die Angreifer selbst nicht in der Lage, die verschlüsselten Daten zu dekodieren, kassieren aber gerne das verlangte Lösegeld.

Dank Dr.Web vermeiden Sie Situationen, in denen Handlungen eines Eindringlings zum Verlust von Unternehmensdaten oder zum Diebstahl von Unternehmensressourcen führen können.

### Diese Aufgaben erfüllt Dr.Web für Linux

<ul style="list-style-type: none"> <li>Zuverlässiger Schutz gegen alle Arten von Malware, u.a. Schädlinge, die durch Doctor Web noch nicht analysiert wurden</li> </ul>	<ul style="list-style-type: none"> <li>Schutz gegen Bedrohungen unter Windows, die unter Linux gestartet wurden, u.a. mit Hilfe der Dr.Web Cloud</li> </ul>	<ul style="list-style-type: none"> <li>Vollständige Virenprüfung des Internetverkehrs, u.a. für geschützte Verbindungen</li> </ul>	<ul style="list-style-type: none"> <li>Fernprüfung von Systemen, auf denen die Installation von Virenschutzsoftware nicht möglich ist</li> </ul>	<ul style="list-style-type: none"> <li>Hohe Leistung und Funktionsstabilität</li> </ul>
<ul style="list-style-type: none"> <li>Prüfung von Objekten im Dateisystem nach Zeitplan</li> </ul>	<ul style="list-style-type: none"> <li>Beschränkung des Zugangs zu potenziell gefährlichen Webinhalten über thematische Kategorien sowie Black- und Whitelists</li> </ul>	<ul style="list-style-type: none"> <li>Sende- und Empfangssperre für E-Mails mit böswilligen Objekten oder unerwünschten Links</li> </ul>	<ul style="list-style-type: none"> <li>Schutz für Workstations auch auf Geschäftsreisen und im Urlaub, wenn der Zugriff zum Verwaltungcenter nicht möglich ist</li> </ul>	<ul style="list-style-type: none"> <li>Überwachung von Netzwerkverbindungen</li> </ul>

### Mit Dr.Web für Linux reduzieren Sie die Unternehmenskosten deutlich und erhöhen die Zuverlässigkeit der Geschäftsprozesse.

<p><b>Virenprüfung auf Ferngeräten</b></p> <p>Mit Dr.Web für Linux können Sie nicht nur gewöhnliche Computer, sondern auch IoT-Geräte – Router, TV-Boxen – auf Viren via Fernzugriff prüfen.</p>	<p><b>Hoher Scan-Durchsatz bei der Virenprüfung</b></p> <p>Kompakte Virendatenbanken, die Technologie der Nicht-Signatur-Suche nach unbekanntem Viren Origins Tracing™ und die fortschrittliche heuristische Analyse ermöglichen es Ihnen, jeden bekannten sowie unbekanntem Schädling zum Zeitpunkt des Angriffs zu erkennen.</p>	<p><b>Schutz vor früher unbekanntem böswilligen Apps</b></p> <p>Alle geschützten Dateien und Dokumente werden zum Zeitpunkt des Zugriffs mit Hilfe der neuesten Technologie gescannt, um unbekanntem Malware zu erkennen, sowie solche, die von unbekanntem Packern getarnt werden.</p>
<p><b>Einfache Installation und Anpassung der Programmkonfiguration je nach Anforderungen</b>, leicht kontrollierbare Einrichtung von Dr.Web und flexible Konfiguration über die Administrator-Konsole</p>	<p><b>Einfache Administration</b> über die Weboberfläche und Kommandozeilen-Tools</p>	<p><b>Auswahl verschiedener Scan-Modi</b></p>

## Um zu anderen Betriebssystemen zu wechseln, brauchen Sie Ihre Lizenz nicht zu wechseln bzw. zu erweitern.

### Lizenzierung

Lizenzarten	Optionen
<ul style="list-style-type: none"><li>▪ Nach Anzahl der zu schützenden Workstations</li><li>▪ Nach Anzahl der Clients, die eine Verbindung zum Terminalserver aufbauen</li><li>▪ Nach Anzahl der Clients, die eine Verbindung zum virtuellen Server aufbauen</li><li>▪ Nach Anzahl der Clients der integrierten Systeme</li></ul>	<ul style="list-style-type: none"><li>▪ Rundumschutz</li><li>▪ Rundumschutz + Verwaltungszentrum</li></ul> <p>Das Verwaltungszentrum wird kostenlos lizenziert. <a href="#">Alle Lizenzierungsbedingungen</a></p>
Pre-Sales Support	Technischer Support
<ul style="list-style-type: none"><li>▪ Kostenloses Testen von Dr.Web Produkten — im Netzwerk des Auftraggebers und via Fernzugriff</li><li>▪ Hilfe bei der Produkteinrichtung (via Telefon)</li><li>▪ Präsentation, Webinar, Seminar</li></ul>	<ul style="list-style-type: none"><li>▪ 24h Support via Telefon und über das Online-Formular unter <a href="https://support.drweb-av.de">https://support.drweb-av.de</a></li><li>▪ Support-Kosten für Lizenzen außerhalb der Preisliste sowie unlimitierte Lizenzen werden gesondert vereinbart.</li><li>▪ Kostenloser Support und kostenlose Dekodierung der von Ransomware verschlüsselten Daten für Lizenzen gemäß der geltenden Preisliste</li><li>▪ Kostenpflichtiger VIP-Support</li></ul>

## Dienste und Services

### Dr.Web vxCube

- Intelligenter und interaktiver Cloud-Dienst zur Analyse von verdächtigen Dateien
- Sofortige Erstellung eines speziellen Dr.Web CureIt!-Pakets basierend auf der durchgeführten Analyse
- Für IT-Sicherheitsspezialisten und Cyber-Kriminalisten

Dr.Web vxCube ist ein unverzichtbares Tool für Situationen, in denen eine bösartige Datei in den geschützten Perimeter eingedrungen ist oder Sie den begründeten Verdacht haben, dass das Netzwerk von einem «Fremden» infiltriert wurde.

Dr.Web vxCube prüft umgehend die Böswilligkeit der Datei und erstellt ein Dienstprogramm, um die Folgen zu beseitigen. Die Prüfung dauert etwa eine Minute! Über die Ergebnisse der Analyse wird ein Bericht erstellt, den Sie in Ihrem Dr.Web vxCube-Konto einsehen oder als Archiv herunterladen können.

Falls eine Bedrohung gefunden wird, erhalten Sie mit Dr.Web vxCube sofort ein Gegenmittel in Form eines speziellen Dr.Web CureIt!-Pakets (sofern in Ihrer Lizenz enthalten), um Ihr System zu behandeln.

**So können Sie eine neue Bedrohung schnell neutralisieren, ohne auf ein Update der installierten Virenschutz-App warten zu müssen.**

Dr.Web CureIt! erfordert keine Installation, auch wenn Sie bereits eine andere Virenschutz-App (nicht Dr.Web) installiert haben.

Testversion anfordern: <https://download.drweb-av.de/vxcube/>

Mehr zu Dr.Web vxCube: <https://www.drweb-av.de/vxcube/>

## Antivirus-Analysen

### Analyse von böswilligen Dateien durch Spezialisten von Doctor Web

Kein automatisierter Dienst kann die Erfahrung und das Wissen eines Virenanalysten ersetzen. Wenn die Beurteilung der analysierten Datei nicht eindeutig ist und Sie Zweifel am Ergebnis haben, empfehlen wir Ihnen die Dienste unserer Virenanalysten, die über langjährige Erfahrungen in der Virenanalyse verfügen.

Zu unseren Dienstleistungen gehört die Analyse von böswilligen Dateien jeglicher Komplexität. Nach Abschluss der Analyse wird ein Bericht erstellt, der folgende Informationen enthält:

- Beschreibung von Funktionsalgorithmen von Malware sowie deren Modulen;
- Kategorisierung von Objekten: eindeutig böswillig, potenziell böswillig (verdächtig) usw.;
- Analyse des Netzwerkprotokolls und Identifizierung von Befehlsservern;
- Einfluss auf das infizierte System und Empfehlungen zur Beseitigung der Infektion.

Für Fragen rund um die Antivirus-Analysen stehen wir Ihnen unter <https://support.drweb-av.de> zur Verfügung.

## Analyse von virenabhängigen Computervorfällen

Wenn das IT-System in Ihrem Unternehmen von Malware betroffen ist und Sie Expertenhilfe benötigen, kontaktieren Sie unser Team von Virenanalysten.

Über die Analyse: <https://antifraud.drweb-av.de/expertise>

Analyse anfordern: <https://support.drweb-av.de/expertise>



© «Doctor Web», 2003–2020

Doctor Web ist ein russischer Entwickler von IT-Sicherheitslösungen unter dem Markennamen Dr.Web. Dr.Web Produkte werden seit 1992 entwickelt.

Doctor Web Deutschland GmbH  
Quettigstr. 12, 76530 Baden-Baden  
Telefon: +49 (0) 170 4884028

[www.drweb-av.de](http://www.drweb-av.de)

