

# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

## ANTI-MALWARE

### Zuverlässige Sicherheit

IT-Sicherheitssoftware ist nur so effektiv wie die ihr zugrunde liegende Sicherheits-Engine. Patch Management, MDM, Verschlüsselung, Gerätekontrolle, Phishing-Schutz – all diese Technologien sorgen für wichtige zusätzliche Schutzschichten. Unternehmen sollten beim Schutz vor bekannten, unbekanntem und hoch entwickelten Bedrohungen keine Kompromisse eingehen.

Unsere Sicherheits-Engine wird kontinuierlich durch unser neuestes und dynamisches Sicherheitswissen aktualisiert und somit verbessert. Unser permanenter Fokus auf alle Sicherheitsthemen, zusammen mit unserer globalen Erfahrung, macht es möglich unseren Kunden beständig ein starker Partner zu sein.

Eine Vielzahl unabhängiger Tests beweisen, dass die Anti-Malware Engine, innerhalb des Security-Marktes eine herausragende Stellung einnimmt. Diese Engine ist integrativer Bestandteil der Kaspersky Endpoint Security for Business Plattform.

- Erkennung von bekannten, unbekanntem und hoch entwickelten Bedrohungen
- Verhaltensanalyse & Heuristik
- Kaspersky Security Network: Cloud-basierter Schutz
- Active Disinfection
- Schutz vor Verschlüsselung und Ransomware
- Automatischer Exploit-Schutz
- HIPS & Persönliche Firewall
- Network Attack Blocker
- Einfache und übersichtliche Verwaltungskonsole

### WICHTIGSTE VORTEILE

#### GESTAFFELTER SICHERHEITSANSATZ

Da unsere Technologien intern bei Kaspersky Lab entwickelt werden, greifen die einzelnen leistungsstarken und aufeinander abgestimmten Schutzschichten nahtlos ineinander, sodass die Leistung Ihrer Systeme nur minimal beeinträchtigt wird.

Jede dieser Schutzschichten geht die Cyberbedrohungen aus einer anderen Perspektive an. Dadurch ist es unseren IT-Experten möglich eng miteinander verzahnte Sicherheitstechnologien zu implementieren. Auf diese Weise entsteht ein Schutz, der sowohl in die Breite als auch in die Tiefe geht.

#### WELTWEIT FÜHRENDES SICHERHEITSWISSEN – IHRE GEWÄHRLEISTUNG FÜR FORTLAUFENDEN SCHUTZ

Das globale Sicherheitswissen von Kaspersky Lab ist weltweit anerkannt und findet seine Anwendung in unseren Sicherheitslösungen, die darauf angelegt wurden, sich einer ständig veränderten IT-Landschaft anzupassen.

### PROFESSIONELLER SCHUTZ, MEHRFACH BEWIESEN – DIE FAKTEN

2014 haben die Endpoint-Lösungen von Kaspersky Lab an **93 unabhängigen Tests und Bewertungen teilgenommen**. Unsere Produkte landeten **66 Mal unter den ersten Drei**, ein **TOP3-Ergebnis von 71 %**, und schnitten **51 Mal als Sieger** ab, also bei weitaus mehr als der Hälfte der Tests.

## FUNKTIONEN

### HEURISTISCHE SICHERHEITSVERFAHREN SORGEN FÜR EINE GERINGERE BELASTUNG IHRER SYSTEME

Musterbasierte Malware-Identifizierungsverfahren garantieren höhere Erkennungsraten, ermöglichen kleinere Update-Dateien und sorgen für mehr Sicherheit.

### VERHALTENSANALYSE

Anti-Malware von Kaspersky Lab arbeitet bei der Aktivitätsanalyse von Software mit zwei besonderen Komponenten:

- **Emulator** – Reproduziert und überprüft die beabsichtigten Aktivitäten eines Programms.
- **Aktivitätsmonitor** – Überwacht die Aktivitäten von bereits ausgeführten Programmen und erkennt und analysiert Verhaltensmuster, die charakteristisch für Malware sind.

### CLOUDBASIERTE MALWARE-ERKENNUNG DURCH DAS KASPERSKY SECURITY NETWORK (KSN)

Über 60 Millionen freiwillige Nutzer von Kaspersky-Software ermöglichen einen konstanten Strom von aktuellen Daten zu versuchten Malware-Angriffen und verdächtigem Verhalten. Diese Informationen ermöglichen Kaspersky Lab die umgehende Beurteilung verdächtiger Dateien. Auf diese Weise profitieren alle unsere Kunden von Echtzeitschutz und einer geringeren Anzahl von Fehlalarmen.

### AUTOMATISCHER EXPLOIT-SCHUTZ

Der automatische Exploit-Schutz bietet insbesondere Schutz vor Malware, die Schwachstellen in weit verbreiteten Programmen ausnutzt, indem typische oder verdächtige Verhaltensmuster analysiert werden. Einmal erkannt, erstickt die Technologie Exploits dann im Keim und hindert bereits heruntergeladenen Schadcode an der Ausführung.

#### Hinweise zum Kauf

Malware-Schutz von Kaspersky Lab ist nicht separat erhältlich. Er ist in allen Stufen von Kaspersky Endpoint Security for Business und in Kaspersky Small Office Security enthalten.

### SCHUTZ VOR UNERWÜNSCHTER DURCH RANSOMWARE

Wenn verdächtige Prozesse versuchen, auf wichtige Dateien zuzugreifen, bewahrt der Aktivitätsmonitor Kopien dieser Dateien im temporären Speicher auf. Sollte eine Ransomware den Versuch unternehmen, die Originale zu verschlüsseln, lassen sich die unverschlüsselten Kopien wiederherstellen.

### ACTIVE DISINFECTION

Diese Technologie nutzt unterschiedliche Verfahren, um erkannte Infektionen zu „heilen“, z. B. durch die Verhinderung der Datei- und Prozessausführung inklusive Autostart, das Zerstören von Malware und das Zurücksetzen von gespeicherten Dateien in ihren Originalzustand.

### SYSTEM ZUR ANGRIFFSÜBERWACHUNG AUF HOST-BASIS (HOST-BASED INTRUSION PREVENTION SYSTEM, HIPS) UND PERSÖNLICHE FIREWALL

Einige Programmaktivitäten sind ausreichend risikobehaftet, um eine Einschränkung ratsam erscheinen zu lassen, auch wenn sie sich möglicherweise nicht als schädlich erweisen. Das System zur Angriffsüberwachung auf Host-Basis (Host-based Intrusion Prevention System, HIPS) von Kaspersky Lab schränkt Aktivitäten innerhalb eines Systems ein. Grundlage hierfür ist die dem jeweiligen Programm zugeordnete Vertrauensstufe. Unterstützt wird dieser Vorgang durch eine persönliche Firewall, welche die Netzwerkaktivität von Programmen einschränkt.

### NETWORK ATTACK BLOCKER

Erkennt und überwacht verdächtige Aktivitäten in Ihrem Netzwerk und ermöglicht es Ihnen, die Reaktion Ihres Systems auf verdächtiges Verhalten festzulegen.

### REGELMÄSSIGE UPDATES

Updates zum Schutz vor neuen Bedrohungen durch Malware werden durch den wohl schnellsten Aktualisierungsmechanismus der gesamten Branche in Ihre Sicherheitsdatenbank eingepflegt. Hinzu kommt die kontinuierliche Aktualisierung von Daten zu neu entdeckter Malware durch das Kaspersky Security Network (KSN).