KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Endpoint-Kontrolle

Leistungsstarke Endpoint-Kontroll-Tools, die nahtlos mit zuverlässigem Malware-Schutz integriert sind, und das branchenweit einzige Whitelisting-Labor schützen Ihr Unternehmen vor der Dynamik der heutigen Bedrohungslage.

SCHUTZ, RICHTLINIENDURCHSETZUNG UND KONTROLLE

Schwachstellen in vertrauenswürdigen Programmen, web-basierte Malware und eine mangelnde Kontrolle über Peripheriegeräte sind nur einige Aspekte einer immer komplexer werdenden Bedrohungslage. Unsere Tools für die Programm-, Web- und Gerätekontrolle geben Ihnen die vollständige Kontrolle über Ihre Endpoints, ohne dabei die Produktivität zu beeinträchtigen.

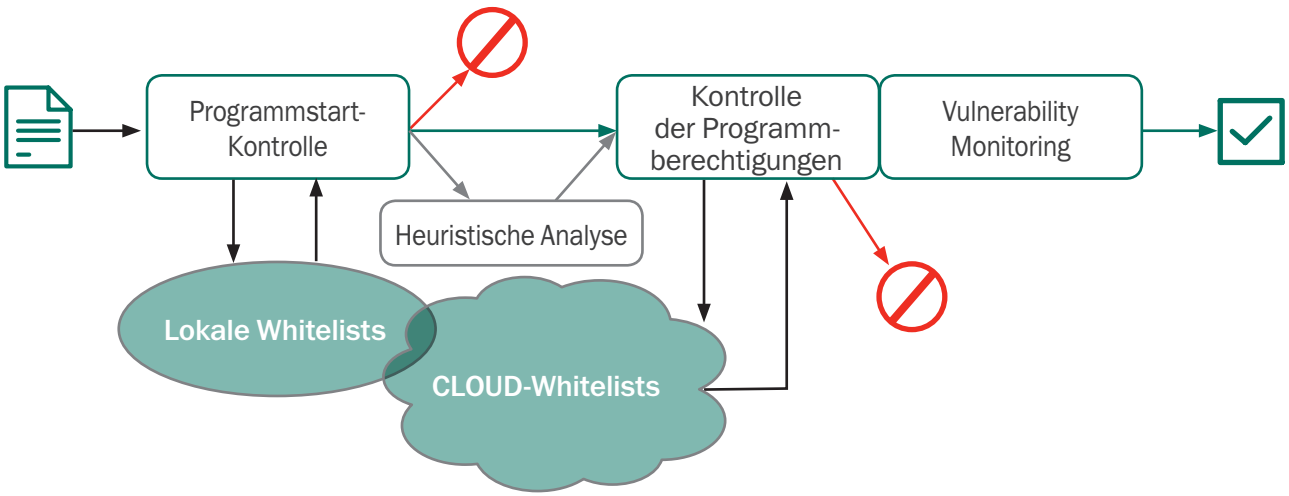
PROGRAMMKONTROLLE UND DYNAMISCHE WHITELISTS

Schützt Systeme vor bekannten und unbekannten Bedrohungen, da Administratoren unabhängig vom Verhalten der Endbenutzer die vollständige Kontrolle über die Anwendungen und Programme haben, die auf den Endpoints ausgeführt werden können. Durch die Überwachung der Programmintegrität können Sie außerdem das Programmverhalten analysieren und die Ausführung unerwarteter Aktionen verhindern, durch die Endpoints oder das gesamte Netzwerk gefährdet werden könnten. Eine vereinfachte, individuell anpassbare und automatische Erstellung und Durchsetzung von Richtlinien hat folgende Vorteile:

- **Kontrolle des Programmstarts**: Zulassen, Blockieren und Prüfen von Programmstarts. Ermöglicht Zugriffsbeschränkungen für nicht unternehmensrelevante Programme.
- **Kontrolle der Programmberechtigungen**: Regulieren und kontrollieren Sie den Zugriff von Programmen auf Systemressourcen und Daten. Klassifizieren Sie Programme als vertrauenswürdig, eingeschränkt vertrauenswürdig oder nicht vertrauenswürdig. Regulieren Sie den Zugriff durch Programme auf verschlüsselte Daten auf Endpoints, z. B. Informationen, die über Webbrowser oder per Skype gepostet werden.
- **Vulnerability Scanning von Programmen**: Proaktive Abwehr von Angriffen auf Schwachstellen in vertrauenswürdigen Programmen.

Die meisten Kontrolllösungen bieten lediglich einfache Funktionen für Blockierung und Zugriff. Die Kontroll-Tools von Kaspersky greifen auf cloudbasierte Datenbanken zu und ermöglichen so Zugriff auf aktuelle Informationen zu Programmen praktisch in Echtzeit.

Unsere Programmkontroll-Technologien nutzen Cloud-basierte Whitelisting-Datenbanken zur Analyse und Überwachung von Programmen in allen Phasen: Download, Installation, Ausführung.



Dynamisches Whitelisting, das über eine lückenlose „Default Deny"-Richtlinie aktiviert werden kann, blockiert die Ausführung von Programmen auf jeder der Workstations, wenn keine explizite Erlaubnis durch einen Administrator vorliegt. Kaspersky Lab ist der einzige IT-Sicherheitsanbieter mit einem eigenen Whitelisting-Labor, das eine laufend aktualisierte Datenbank mit mehr als 500 Millionen Programmen pflegt.

Unsere **Default Deny-Richtlinie kann in einer Testumgebung angewendet werden**, sodass der zuständige Administrator die Legitimität eines Programms überprüfen kann, bevor es blockiert wird. Außerdem lassen sich Programmkategorien auf Basis von digitalen Signaturen erstellen. Auf diese Weise wird der Benutzer daran gehindert, legitime Software zu nutzen, die von Malware modifiziert wurde oder aus einer verdächtigen Quelle stammt.

WEB-KONTROLLEN

Überwachen, filtern und kontrollieren Sie die Webseiten, auf die Endbenutzer am Arbeitsplatz Zugriff haben. Hierdurch sorgen Sie für Schutz vor web-basierter Malware und vor Angriffen.

Unsere Web-Kontrollen basieren auf einem laufend aktualisierten Verzeichnis von Webseiten, das in verschiedene Kategorien unterteilt ist (z. B. Erotik, Gaming, Soziale Netzwerke, Glücksspiel). Dank einfach anzulegender Richtlinien können Administratoren den Zugriff von Endbenutzern auf einzelne Webseiten bzw. Webseiten-Kategorien untersagen, einschränken und überwachen und darüber hinaus eigene Listen erstellen. Schädliche Webseiten werden automatisch gesperrt.

Durch Einschränkung ihrer Nutzung tragen Unsere Web-Kontrollen tragen dazu bei, die Weitergabe von vertraulichen Daten über Soziale Netzwerke und Instant-Messaging-Dienste zu verhindern. Flexible Richtlinien geben Administratoren die Möglichkeit, das Surfen im Internet auf bestimmte Tageszeiten zu beschränken. Die Integration mit Active Directory hat den Vorteil, dass sich die Richtlinien schnell und einfach im gesamten Unternehmen anwenden lassen.

Für noch mehr Sicherheit sorgt die Tatsache, dass die Web-Kontrollen direkt auf dem Endpoint aktiviert werden, d. h die Richtlinien werden umgesetzt, selbst wenn der Benutzer nicht im Netzwerk angemeldet ist.

GERÄTEKONTROLLEN

Das Deaktivieren eines USB-Ports behebt nicht immer die Probleme mit Wechseldatenträgern. Wenn Sie z. B. einen USB-Port deaktivieren, verhindern Sie gleichzeitig den sicheren Zugang per VPN-Token über diesen Port.

Die Gerätekontrollen von Kaspersky Lab bieten eine noch feiner abgestufte Kontrolle auf Ebene von Bus, Typ oder Gerät und erhalten so bei optimaler Sicherheit die Produktivität des Endbenutzers. Die Kontrollen lassen sich sogar auf einzelne Seriennummern von Geräten anwenden.

- Legen Sie Berechtigungen für Anschluss/Lesen/Schreiben für einzelne Geräte fest, und erstellen Sie Zeitpläne.
- Erstellen Sie Gerätekontrollregeln auf Grundlage von Masken, damit Geräte nicht mehr angeschlossen werden müssen, um sie in die Whitelist aufzunehmen. Nehmen Sie mehrere Geräte gleichzeitig in die Whitelist auf.
- Kontrollieren Sie den Datenaustausch per Wechseldatenträger innerhalb und außerhalb des Unternehmens, um das Risiko von Datenverlust und Datendiebstahl zu reduzieren.
- Integrieren Sie die Kontroll-Tools mit unseren Verschlüsselungstechnologien, um Verschlüsselungsrichtlinien auf bestimmten Gerätetypen durchzusetzen.

EINFACHE VERWALTUNG

Alle Kontroll-Tools von Kaspersky Lab lassen sich in Active Directory integrieren. Entsprechend einfach und schnell können globale Richtlinien konfiguriert und umgesetzt werden. Alle Endpoint-Kontrollen werden über dieselbe Konsole und Benutzeroberfläche verwaltet.

Hinweise zum Kauf

Endpoint-Kontroll-Tools von Kaspersky Lab sind nicht separat erhältlich. Sie sind in den Stufen „Select", „Advanced" und „Total" von Kaspersky Endpoint Security for Business aktiviert.

KASPERSKY lab