DriveLock Application Control: Effektiver Schutz vor Schadsoftware

Im Zuge der Digitalisierung kommt den Themen Datenschutz und -sicherheit in Unternehmen eine immer größere Bedeutung zu. Die Anforderungen an heutige IT-Security-Lösungen steigen. Wir haben uns den Schutz Ihrer Daten, Geräte und Systeme zum Ziel gesetzt.

Die Anzahl der Cyberangriffe nimmt kontinuierlich zu. Angreifer gehen immer gezielter und trickreicher vor. Allein 2019 gab es über 1 Mrd. verschiedener Malware- und Ransomware-Varianten, mit verheerenden Folgen. Bei herkömmlichen Angriffsarten wird primär externe Malware auf dem Zielsystem installiert oder ausgeführt. Darüber hinaus missbrauchen Angreifer bei dateiloser Malware Administrations- & System-Tools, die bereits auf dem Zielsystem vorhanden sind.

Application Whitelisting – der effektivste Schutz gegen jegliche Art von Schadsoftware. Wie arbeitet die **DriveLock** Lösung?

Eine Antivirus-Software erkennt nur bekannte Schadsoftware. Aber Malware tarnt sich oder ist zum Zeitpunkt eines Angriffs einer Antivirus-Lösung noch nicht bekannt.

Intelligente Applikationskontrolle ermöglicht Administratoren, die Ausführung jeder beliebigen Anwendung zu kontrollieren. Verschiedene Regeln oder Strategien legen fest, welche Anwendungen ausgeführt und welche gesperrt werden.

Die Flexibilität, Blacklist- & Whitelist-Regeln zu kombinieren, macht die Applikationskontrolle sowohl einfach in der Anwendung als auch leistungsstark in der Absicherung. Mit DriveLock holen Sie das Beste aus beiden Regeln heraus.

Beim Application Whitelisting erstellen Sie eine Liste von vertrauenswürdigen Entitäten (Anwendungen, Softwarebibliotheken, Skripte), die auf ein System oder Netzwerk zugreifen dürfen und blockieren alles andere. Die Konfiguration wird zentral verwaltet und kann gezielt Endgeräten, Gruppen oder Personengruppen zugewiesen werden.

Vorteile Applikationskontrolle

- SCHUTZ VOR MALWARE & RANSOMWARE
- MINIMALER ADMINISTRATIVER AUFWAND
- AUTOMATISCHES LERNEN DER WHITELISTS
- SELF-SERVICE FÜR ENDBENUTZER
- EINHALTUNG GESETZLICHER VORSCHRIFTEN
- SICHERER SCHUTZ FÜR ÄLTERE SYSTEME
- ZENTRALE VERWALTUNG

Cyberbedrohungen - Status

- DIGITALISIERUNG LÄSST UNTERNEHMENSGRENZEN VERSCHWINDEN
- MEHR ALS 50% ALLER UNTERNEHMEN SIND ZIEL EINES ANGRIFFS
- Ø FOLGEKOSTEN EINER ATTACKE: 3,9 MIO. €
- ZU WENIG FACHPERSONAL
- INSIDER-AKTIONEN ODER EXTERNE ANGRIFFE

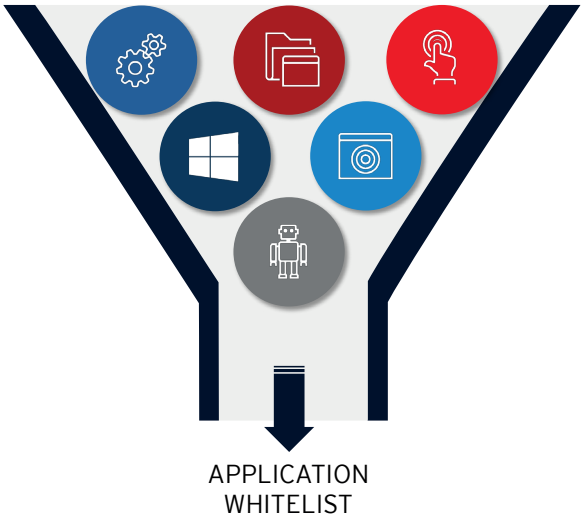
DriveLock

Pflege und Wartung der Whitelist

Predictive Whitelisting
Logarithmus-basierte, automatische Freigabe auf Basis der Herstellerzertifikate

Zentrale Regeln
Vorgabe von zentralen Regel anhand verschiedener Regeltypen

Betriebssystem
Automatische Freigabe von Systemkomponenten und Windowsupdates



Temporäres Entsperren
Manuelle Softwareinstallation mit aktiviertem Lernmodus

Vertrauenswürdige Quellen
Quellen wie "Admin-Shares" oder der Cache des Softwareverteil-agenten

Vertrauenswürdige Prozesse
Automatische Software- und Patchinstallation

Vorteile der DriveLock Application Control durch intelligentes Whitelisting

Der Ansatz mit statischen Blacklists oder Whitelists funktioniert in der sich schnell ändernden Bedrohungslage nur bedingt und erfordert oftmals überproportionalen Pflegeaufwand. „Predictive" Whitelisting reduziert den Aufwand für die Pflege.

Zum Zeitpunkt der DriveLock Installation wird das System „versiegelt". Ab jetzt gibt es nur noch definierte und konfigurierte Wege, wie Änderungen an der Whitelist selbstlernend vorgenommen werden. Das automatisierte Lernen der Whitelist gewährleistet stets den Sicherheitsstandard, da die Implementation und Ausführung von unbekannten Anwendungen verhindert wird.

Sicher und produktiv

Bei unbekannten Anwendungen gestattet DriveLock verschiedene Möglichkeiten, wie Benutzer benachrichtigt werden und steuernd eingreifen können. Je nach Sicherheitseinstellungen werden Benutzer nur informiert oder bestimmen selbst, wie sich das System verhalten soll. Dies gibt IT-Abteilungen die Möglichkeit, Verantwortung an die Endbenutzer abzugeben. Die IT-Verantwortlichen überprüfen anschließend an zentraler Stelle, welche Anwendungen durch Selbstfreigaben installiert und gestartet wurden.

Test im Simulationsmodus

Bevor Sie mit der Sperrung von Programmen beginnen, bietet sich der Simulationsmodus an, um Ihre Regeln vorab zu testen und zu ermitteln, welche Anwendungen gesperrt werden. Während der Simulation erzeugt DriveLock Ihren Regeln entsprechend Ereignismeldungen für gestartete oder blockierte Anwendungen. Die Ausführung selbst wird dabei aber noch nicht verhindert. Dieser Modus ist ideal für eine schrittweise Einführung in Produktionsumgebungen.

Regeltypen

- HERSTELLER-ZERTIFIKATE
- DATEI-EIGENTÜMER
- APPLIKATIONS-HASH WERTE
- VERTRAUENSWÜRDIGE QUELLEN
- REGELN FÜR OS-KOMPONENTEN, UPDATES, .NET FRAMEWORK ETC.
- WHITE- UND BLACKLISTEN JEGLICHER SCRIPTS SOWIE MSI-PAKETE
- GENEHMIGUNG DURCH BENUTZER

DriveLock – Features

- SIMULATIONSMODUS
- AUDIT ONLY ERFASST POTENZIELLE AUSFÜHRUNGEN
- WHITELIST / BLACKLIST / ODER KOMBINATION
- DLL- UND SCRIPT-KONTROLLE
- ANGEPASSTE BENUTZER-BENACHRICHTIGUNGEN
- ZENTRALES DASHBOARD

DriveLock: Experte für IT- und Datensicherheit seit mehr als 20 Jahren

Das deutsche Unternehmen **DriveLock SE** wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für cloud-basierte Endpoint-und Datensicherheit. Die Lösungen umfassen Maßnahmen der Prävention wie auch zur Erkennung und Eindämmung von Angreifern im System.

DriveLock ist Made in Germany mit Entwicklung und technischem Support aus Deutschland.

DriveLock SE • Germany • France • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com