

# Lumension Application Control

## Lückenloser Schutz vor Malware und unerwünschten Anwendungen



Lumension Application Control (LAC), eine Komponente von Lumension Endpoint Security, ermöglicht eine Policy-basierte Kontrolle der Anwendungsnutzung im Hinblick auf den Schutz der Endpunkte vor Malware, Spyware, Zero-Day-Bedrohungen und unerwünschter oder nicht lizenzierter Software. Durch den Rückgriff auf ein Whitelist-Konzept sorgt Lumension Application Control dafür, dass nur autorisierte Anwendungen in Netzwerken sowie auf Servern, Terminal Services-Servern, Thin-Clients, Laptops oder Desktops ausgeführt werden können. Die Ausführung nicht-autorisierter Anwendungen wird kurzerhand verweigert.

Malware wird praktisch eliminiert und Administratoren erhalten uneingeschränkte Kontrolle über unerwünschte und nicht-autorisierte Anwendungen, einschließlich bandbreitenintensiver P2P-Programme.

### **Einfachheit, Schnelligkeit und Flexibilität bei Administration und Management**

Lumension Application Control ermöglicht Administratoren die schnelle Identifizierung von Anwendungen und im Anschluss daran die Zuweisung von Zugriffsrechten für die Anwendungen an Benutzer, Benutzergruppen oder bestimmte Computer.

Die Anwendungspolicies sind mit den in Active Directory™ oder eDirectory™ gespeicherten Benutzer- und Benutzergruppendaten verknüpft und tragen dadurch zu einer wesentlichen Vereinfachung der Verwaltung der Anwendungsressourcen an den Endpunkten bei.

### **Automatisierte Identifizierung**

LAC ist in einem Betriebsmodus ohne Blockierung vorkonfiguriert, um die Identifizierungsphase zu erleichtern. Dadurch werden für die Administratoren alle Anwendungen sichtbar, die an den Endpunkten ausgeführt werden.

### **Detaillierte Audit-Funktionen**

Alle Versuche zur Ausführung von Anwendungen können aufgezeichnet werden. Auch die Aufzeichnung der von den Administratoren durchgeführten Aktionen ist möglich, u. a. der im Rahmen der Anwendungspolicy an den Autorisierungen vorgenommenen Änderungen.

### **Flexible Autorisationsregeln**

Administratoren können vertrauenswürdige Benutzer dazu berechtigen, Autorisierungen für ihre eigenen Anwendungen zu erteilen. Damit ist optimale Flexibilität gegeben. Die Administratoren werden dabei kontinuierlich über jeden Schritt informiert und behalten somit die Kontrolle und die Möglichkeit, lokale Autorisierungen jederzeit zu überschreiben.

### **Application Control Server Edition**

Es steht mit Application Control Server Edition eine Serversicherheitssoftware bereit, die umfassende Unterstützung bei der Umsetzung von Policies zur Anwendungsnutzung bietet im Hinblick auf den standardmäßigen Schutz missionskritischer Server vor nicht autorisierten, illegalen oder unerwünschten Anwendungen und die Verhinderung jeder Unterbrechung des Geschäftsablaufs.

### **Application Control Terminal Services Edition**

Die Umsetzung von Policies zur Anwendungsnutzung im Hinblick auf den standardmäßigen Schutz von Windows- oder Citrix-basierten Terminal-Services-Umgebungen vor nicht autorisierten, illegalen oder unerwünschten Anwendungen wird mit der Terminal Services Edition sicher gestellt.

Zur Verfügung steht ebenfalls Lumension Device Control mit integrierter Konsole. Lumension Device Control ermöglicht eine Policy-basierte Kontrolle der Nutzung mobiler Geräte im Hinblick auf eine Steuerung des ein- und abgehenden Datenflusses an den Endpunkten. Dadurch lässt sich das Risiko eines Datenverlustes um einiges begrenzen.

### **Einführung**

Gewährleistet 100%igen Schutz vor allen bekannten und unbekanntem Bedrohungen

Bietet effizienten Schutz vor Zero-Day-Bedrohungen und gezielten Angriffen

Kontrolliert die Nutzung unerwünschter Anwendungen und verhindert dadurch eine Überbeanspruchung der Netzwerkbandbreite

Optimiert die Vorteile neuer Technologien und minimiert das Risiko eines Netzwerkausfalls

### **Schutz vor Malware, Spyware und Zero-Day-Bedrohungen**

Die Sicherheitslandschaft ist im Wandel: An Stelle der breit angelegten, spektakulären Malware-Einbrüche kommt es immer häufiger zu gezielten Bedrohungen. Herkömmliche Lösungen können nicht mit einem ausreichenden Schutz vor dieser Art von Angriffen aufwarten. Das belegt allein die Tatsache, dass im Jahr 2005 von den 99 Prozent aller Unternehmen, die über eine Antivirus-Lösung verfügen, 62 Prozent eine Infizierung zu verzeichnen hatten<sup>1</sup>. Endpunkte sind die anfälligsten Eintrittspunkte für Malware. Und die Bedrohung greift weiter um sich ein führender Antivirus-Anbieter rechnet mit einer Verdoppelung der registrierten Bedrohungen auf 400.000 bis zum Jahr 2008.

Immer mehr Endbenutzer installieren Programme, die in keinerlei Bezug zu ihrer Arbeit stehen, gleichzeitig nimmt die Anzahl der Bedrohungen zu. In diesem Kontext müssen 85 Prozent der Unternehmensrechner jährlich neu konfiguriert werden<sup>1</sup>. Der durchschnittliche Betriebsausfall bei einer Virusattacke beträgt 23 Arbeitstage, wobei für eine vollständige Systemwiederherstellung 31 Arbeitstage erforderlich sind<sup>2</sup>.

#### Quellen:

<sup>1</sup> Studie der Yankee Group aus dem Jahr 2005 zu den "Leaders" (Vorreiter) und "Laggards" (Trödler) im Bereich Sicherheit

<sup>2</sup> Studie des Ponemon Institute aus dem Jahr 2005 zur Benachrichtigung bei Datensicherheitseinbrüchen

Eigenschaften	Funktionen	Vorteile
Whitelist	Benutzern oder Benutzergruppen werden Zugriffsberechtigungen für autorisierte Anwendungen zugewiesen Standardmäßig gilt: Keine Autorisierung, kein Zugriff	Eliminiert unbekanntes bzw. unerwünschte Anwendungen in Ihrem Netzwerk und reduziert das Risiko von Malware und Spyware. Und nicht zuletzt lässt sich dadurch die Stabilität des Netzwerks verbessern
Standard- Dateidefinitionen	Klassifizierte, vorgeladene Whitelist mit allen unterstützten OS-Dateien	Beschleunigt und vereinfacht die Whitelist-Definition
Automatisierte Anwendungsidentifizierung	Prozess der Identifizierung, Kategorisierung und Autorisierung von Anwendungen, bei dem ein Datensatz mit allen EXE-Dateien auf Client-Rechnern, Dateiservern und/oder in lokalen Verzeichnissen erstellt wird	Stellt Optionen für eine flexible und schnelle Erstellung bzw. Aktualisierung von Whitelists bereit
Skript/Makro-Schutz	Kontrolle der Ausführung von VBScript, Microsoft Office VBA und JavaScript über eine zentrale Autorisierung oder eine Eingabeaufforderung für lokale Benutzer	Erweitert die Umsetzung der Anwendungspolicy und bietet größeren Schutz durch die Berücksichtigung von Skripten/Makros
Pfadschutz	Optionale Dateiautorisierung auf der Grundlage von Speicherort- oder Pfadregeln. Erstellung eines vertrauenswürdigen Benutzers ("Trusted Owner"), z. B. den Administrator, für die Durchsetzung der Sicherheit	Bietet die erforderliche Flexibilität für die Unterstützung von EXE-Dateien, für die Hash-Definitionen nicht sinnvoll oder anwendbar sind (d. h. automatisch geänderte EXE-Dateien)
Modus ohne Blockierung	Ausführung und Protokollierung aller Aktivitäten für eine Prüfung durch den Administrator	Ermöglicht die Identifizierung des aktuellen Zustands vor der Definition und Umsetzung einer Policy
Flexible Dateiautorisierung	Mithilfe des Versatile File Processor (FileTool.exe) können sowohl im Online- als auch im Offline-Modus Verzeichnisse und Unterverzeichnisse analysiert und dabei neue Anwendungen und Pakete ausfindig gemacht werden	Stellt eine flexible und schnelle Möglichkeit zur Identifizierung neuer und aktualisierter Anwendungen im Hinblick auf deren Prüfung und letztendlich für die Erstellung von Whitelists dar
Verschachtelte EXE-Dateigruppen	Hierarchische Struktur zur Anordnung von Dateigruppen	Ermöglicht eine schnelle Verwaltung von Dateigruppen sowie eine problemlose Zuweisung von Benutzerberechtigungen
Abgeschwächte Anmeldung	Ausführung von Anmeldeskripts auch ohne Autorisierung und automatische Umschaltung des Systems in den Blockiermodus nach Ablauf eines bestimmten Zeitraums oder nach Abschluss der Skriptausführung	Ermöglicht die Umgehung einer Verwaltung der Anmeldeskripts in Lumension ohne Kompromiss hinsichtlich der Sicherheit des Systems
Lokale Autorisierung	Vertrauenswürdige Benutzer können Anwendungen lokal autorisieren, wobei zur Prüfung durch den Administrator ein entsprechendes Protokoll angelegt wird	Stattet den Benutzer mit Flexibilität aus, ohne die administrative Kontrolle zu vernachlässigen
Verbreitungsprüfung	Deaktiviert verdächtige EXE-Dateien, die auf zu vielen Rechnern in einer bestimmten Zeitspanne lokal autorisiert worden sind	Begrenzt das Risiko einer Verbreitung von bösewärtigen Code im Netzwerk aufgrund lokaler Autorisierung
Extrem skalierbare Architektur	Multi-Tier-Architektur mit Datenbank, einem oder mehreren Anwendungsservern und Clients	Bietet flexible und skalierbare Implementierungsoptionen in weitflächigen und komplexen Netzwerken
Leistungsstarke Protokollanalyse und Berichterstellung	Detaillierte Protokollanalyse mit flexiblen Filter-, Sortier- und Anzeigeeinstellungen und gespeicherten Abfragevorlagen sowie zentrale Berichterstellung	Ermöglicht die Sicherstellung der Policy-Konformität sowie das Drill-Down bei verdächtigem Verhalten im Hinblick auf die Ergreifung rechtlicher oder verwaltungstechnischer Schritte
Offline-Schutz für Computer	Auf jedem Rechner werden lokale Kopien von aktualisierten Hashes und Genehmigungen gespeichert	Gewährleistet einen konstanten Schutz für dezentral oder offline tätige Benutzer
Unterstützung von Active Directory und eDirectory	Die bereits vorhandenen Benutzer- und Benutzergruppendefinitionen in Active Directory und eDirectory werden genutzt	Reduziert den Konfigurations- und Verwaltungsaufwand für Benutzer und Benutzergruppen
Unterstützung für zahlreiche Sprachen	Auf den Lumension-Clientrechnern werden 12 Sprachen unterstützt	Verbessert die Arbeit der Benutzer in internationalen Unternehmen
Benutzerdefinierte Berichte	Benutzerdefinierte Abfragevorlagen können für eine automatische Generierung von Berichten im HTML-, XML- oder CSV-Format erstellt und per E-Mail oder Netzwerk-Dateisharing übermittelt werden	Ermöglicht die Generierung von Daten, die für die Konformitäts-Audits und Management-Berichterstellung in einem Bericht- oder Datenformat im Hinblick auf die problemlose Integration in ein Drittherstellersystem erforderlich sind
Unterstützung für 64-Bit-Plattformen	Nutzen Sie Ihre leistungsstarke 64-Bit-Unternehmensinfrastruktur und bieten Sie ihr ausreichenden Schutz mit Hilfe von Lumension - dazu gehört Agent-Support für 64 Bit Windows Server 2003, Windows und Windows Vista sowie 64-Bit-Support für SQL Server 2005	Verbessert die Arbeit der Benutzer in internationalen Unternehmen

## Ihr Partner für IT Automation und IT Security

**Deutschland/Österreich:**  
**IBV Informatik GmbH**  
**Marie-Curie-Str. 8**  
**D - 79539 Lörrach**

Tel. +49 7621/40 92 0  
 Fax +49 7621/40 92 22

Internet: [www.ibvinfo.com](http://www.ibvinfo.com) +++ E-Mail: [info@ibvinfo.com](mailto:info@ibvinfo.com)

**Schweiz:**  
**IBV Informatik AG**  
**Schönenwerdstrasse 7**  
**CH - 8902 Urdorf**

Tel. +41 44/745 92 92  
 Fax +41 44/ 745 92 93

