

### Die Zukunft der Applikationskontrolle hat begonnen:

Bereitstellung sicherer Systeme mit automatischer Pflege und Verwaltung der Whitelist in nur 3 Schritten!

#### 1. Clean IT

Bereinigen Sie Ihre Client-Systeme mit herkömmlichen Anti-Malware-Tools oder dem integrierten Lumension AntiVirus.

#### 2. Lock IT

Fixieren Sie Ihre Clients und schützen Sie sie vollständig vor unerwünschten Applikationen und Malware mit nur einem Mausklick!

#### 3. Trust IT

Definieren Sie vertrauenswürdige Veränderungswege zur flexiblen System- und Softwarepflege bei höchstem Automatisierungsgrad.

In der heutigen, extrem dynamischen Bedrohungslandschaft sind Unternehmen zunehmend den hoch komplexen und gezielten Malware-Angriffen finanziell motivierter Cyberkrimineller ausgesetzt. Um diesen neuen Gegebenheiten effektiv Rechnung zu tragen, benötigen Unternehmen eine zentrale Kontrolle über die Konfigurationen an allen Endpunkten, um ihren Sicherheitsstatus ohne Kompromisse bei der Endbenutzerproduktivität verbessern zu können.

### Endpunktsicherheit – Geschäftstreiber und Herausforderungen

In der dezentralisierten, mobilen und stets online aktiven IT-Umgebung von heute erweisen sich die Verwaltung, Sicherheit und Kontrolle der Endpunkte als regelrechte Herausforderung. Zahlreiche Endbenutzer verfügen über lokale Administrationsrechte und laden regelmäßig nicht autorisierte oder unerwünschte Drittherstelleranwendungen herunter. Hinzu kommt die wachsende Bedrohung durch die unaufhörlich steigende Anzahl komplexer und gezielter Malwareprogramme, die speziell zur Umgehung der herkömmlichen Schutzvorrichtungen, wie z. B. AntiVirus-Produkte (AV), konzipiert werden. Kein Wunder also, dass sich IT-Experten heute wesentlich unsicherer fühlen als noch vor einem Jahr.

Der fortwährende, exponentielle Zuwachs an Malware hat angesichts der immer offensichtlicheren Ineffizienz des traditionellen AntiVirus-Schutzes zu einem Anstieg der Kosten für IT-Helpdesks, Remediation-Aktionen und Problembehebungsmaßnahmen geführt: Jedes Unternehmen signalisiert im Durchschnitt über 50 produktivitätshemmende Malware-Vorfälle pro Monat. AV ist zwar nach wie vor integraler Bestandteil einer jeden Strategie zum Endpunktschutz, erweist sich als Standalone-Technologie inzwischen jedoch als ineffektiv und trägt zu einer Erhöhung der Endpunkt-TCO bei:

- AV kann mit den monatlich an die 1,6 Millionen identifizierten neuen Malwareinstanzen einfach nicht mehr Stand halten und bietet keinen effektiven Schutz vor Zero-Day-Bedrohungen und Blended Threats<sup>2</sup>
- AV stellt für die an den Endpunkten installierten und ausgeführten Anwendungen nicht die erforderliche Visibilität bereit und unterstützt in keiner Weise eine zentralisierte Verwaltung der Sicherheitskonfigurationen.
- AV ermöglicht weder die Kontrolle der Aktionen von Benutzern mit lokalen Administrationsrechten noch eine Begrenzung der Einführung unerwünschter Anwendungen.

# Die Zukunft der Applikationsentwicklung hat begonnen

Hier kommen Anwendungskontrolle und Whitelisting ins Spiel – bewährte Konzepte für den Endpunktschutz, die die Spielregeln von Grund auf ändern. Anstatt eine Identifizierung aller im Umlauf befindlichen Malwareprogramme anzustreben – eine angesichts der heutigen Bedrohungslandschaft nicht zu bewerkstelligende Aufgabe –, werden anhand einer Anwendungs-Whitelist alle für den Geschäftsbetrieb erforderlichen Softwareprogramme identifiziert und die Ausführung an den Endpunkten wird auf die Anwendungen begrenzt, die explizit von der IT-Abteilung zugelassen wurden. Die bisherigen Standalone-Technologien zur Anwendungskontrolle und zum Whitelisting stellen jedoch nicht die operationelle Effizienz und Flexibilität bereit, die die IT-Experten zur Verwaltung der Endpunkte in einer dynamischen Endpunktumgebung benötigen. Aus diesem Grund kombiniert Lumension® Intelligent Whitelisting™ die rigorose Sicherheitseffizienz der Anwendungskontrolle und des Whitelistings mit der Flexibilität vertrauensbasierter Richtlinien zum Änderungsmanagement. Dadurch gestalten sich Implementierung und Verwaltung für die IT-Mitarbeiter sowohl in dynamischen als auch in statischen Umgebungen wesentlich einfacher und gleichzeitig werden operationelle Flexibilität und Produktivität gewährleistet.

## Effektiver und operationeller Endpunktschutz für dynamische Umgebungen

Lumension® Intelligent Whitelisting™ ist Bestandteil der Lumension® Endpoint Management and Security Suite und nicht zuletzt die branchenweit erste intelligente Endpunktsicherheitslösung, durch die Unternehmen neben der AV-üblichen Effizienz von der erweiterten sicherheitsspezifischen und operationellen Effizienz der Whitelist-basierten Anwendungskontrolle und des Patch Management profitieren. Durch den kombinierten Einsatz von Lumension® AntiVirus, Lumension® Application Control und Lumension® Patch and Remediation in einem voll integrierten und einheitlichen Workflow stattet Lumension IT-Experten mit allen Funktionen aus, die für einen umfassenden Endpunktschutz ohne Beeinträchtigung der Unternehmensproduktivität erforderlich sind.

### Besondere Vorteile von Lumension® Intelligent Whitelisting™:

- **Erhöhung der Endpunktsicherheit** und Verhinderung von Zero-Day- und gezielten Attacken durch eine Defense-in-Depth-Strategie, bei der ausschließlich vertrauenswürdige und bekannte Anwendungen an den Endpunkten ausgeführt werden können.
- **Umfassende Kontrolle über die Endpunkte** durch Einschränkung des Risikos in Verbindung mit lokalen Administrationsrechten. Endbenutzer mit lokalem Administrationsstatus bringen ein hohes anwendungs-, schwachstellen- und konfigurationsbedingtes Risiko für das Unternehmen mit sich und schaffen Sicherheitslücken, die von Zero-Day und anderer Malware missbraucht werden können.
- **Bereitstellung einer flexiblen, effektiven und benutzerfreundlichen Anwendungskontrolle/Whitelisting-Methode.** Im Gegensatz zu herkömmlichen Standalone-Produkten zur Anwendungskontrolle stellt die integrierte intelligente Whitelisting-Lösung von Lumension ein großes Maß an Flexibilität bereit und ermöglicht IT-Mitarbeitern die effektive Verwaltung vertrauensbasierter Änderungen in einer dynamischen Endpunktumgebung.
- **Steigerung der Betriebsproduktivität** durch die Vermeidung von Malware- und Softwarekonflikten, die außerplanmäßige Ausfallzeiten verursachen. Dadurch werden IT-Ressourcen für strategische Initiativen frei gesetzt und die Auszeit der Endbenutzer aufgrund von Malware-Infizierungen wird auf ein Minimum begrenzt – u. a. durch die konsequente Anwendung detaillierter Richtlinien zur Anwendungsnutzung für alle Rollen und Benutzer.
- **Reduzierung der endpunktspezifischen TCO** durch die Minimierung der IT-Helpdesk-Bearspruchung und des Arbeitsaufwands bei Malwarevorfällen und Softwarekonflikten sowie durch die Reduzierung der Komplexität bei der Verwaltung unterschiedlicher und separater Punktprodukte.

## Funktionsweise

Lumension® Intelligent Whitelisting™ bietet eine flexible Kontrolle über die Anwendungsnutzung an den Endpunkten. Dazu werden nicht einfach bestimmte Änderungen blockiert, sondern konkrete Regeln für die Einführung von Änderungen aufgestellt. Daraus ergibt sich ein operationelles Modell für eine effektive Verwaltung der Endpunktsicherheit. In diesem Sinne stellt Lumension einen einfach zu handhabenden und dabei effizienten einheitlichen Lösungsworkflow bereit:

**1. Bereinigung:** Analyse der Endpunktumgebung mit Lumension® AntiVirus oder einem anderen Anti-Malware-Produkt zur automatischen Identifizierung und Entfernung aller bekannten Malwareprogramme.

**2. Identifizierung:** Bereitstellung einer beispiellosen Visibilität für alle an den Endpunkten ausgeführten Anwendungen. Alle bekannten und unbekanntes Endpunktanwendungen werden erfasst, sodass Sie in kürzester Zeit das damit verbundene Risikopotenzial bestimmen können.

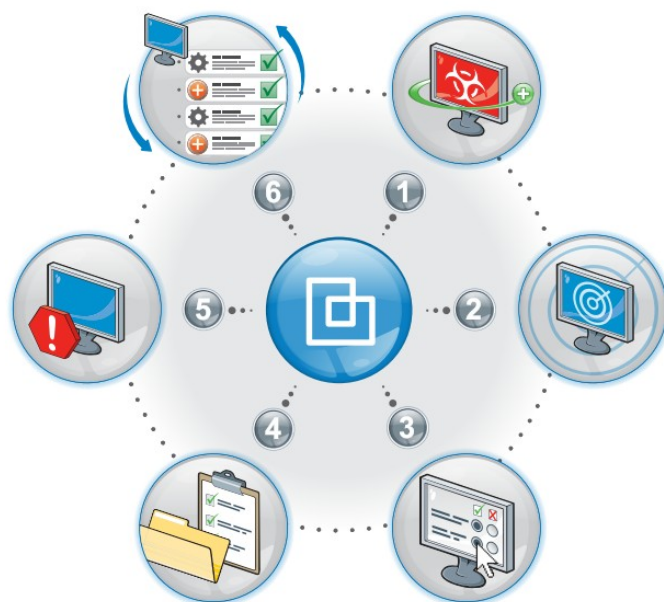
**3. Definition:** Erstellung von Momentaufnahmen der Endpunkte zur Definition von Basis-Richtlinien für das Anwendungs-Whitelisting. Software-Updates von vertrauenswürdigen Softwareherausgebern, Pfaden und Benutzern werden automatisch genehmigt, die Verwaltung der Whitelist wird durch den Einsatz der flexiblen und regelbasierten Trust Engine von Lumension um einiges vereinfacht. Die Richtlinien zum Anwendungs-Whitelisting werden an den identifizierten Endpunkten dann ohne Unterbrechung des Geschäftsbetriebs aktualisiert und implementiert.

**4. Überwachung:** Kontinuierliche Überwachung der Whitelist-Richtlinien außerhalb des Umsetzungsprozesses und Protokollierung aller Ausführungsversuche. Beurteilung der potenziellen Wirkung der Whitelist-Richtlinien und Anpassung der Trust Engine-Regeln im Hinblick auf ein optimales Gleichgewicht zwischen effektivem Endpunktschutz und Endbenutzerproduktivität.

**5. Umsetzung:** Standardmäßige Blockierung der Ausführung unbekannter und nicht autorisierter Anwendungen und automatische Verhinderung von Zero-Day-Angriffen noch vor der Implementierung der neuesten AntiVirus-Definitionen oder Schwachstellen-Patches. Umfassende Reduzierung des IT-Risikos durch die Ausdehnung der Whitelist-Richtlinien auf Endbenutzer mit lokalen Administrationsrechten.

**6. Verwaltung:** Vereinfachung der Whitelist-

Betriebsprobleme durch die nahtlose Integration mit Lumension® Patch and Remediation bzw. mit Patching- und Software-Verteilungs-Tools von Drittherstellern. Bei der Implementierung der neuesten Software-Updates und Schwachstellen-Patches führt Lumension® Intelligent Whitelisting™ automatisch eine entsprechende Aktualisierung



# Zentrale Features

## Anwendungskontrolle / Whitelisting

Identifiziert automatisch alle vertrauenswürdigen Softwareprogramme, die an den Endpunkten ausgeführt werden dürfen und verhindert die Ausführung aller anderen Anwendungen – ob bösartig, unerwünscht oder einfach nicht vertrauenswürdig. Unterstützt alle exe-Typen, einschließlich der Standarddateien .EXE, .DLL, .COM usw. Trägt zu einer grundlegender Verbesserung der Produktivität der IT-Mitarbeiter und Endbenutzer bei.

## Trust Engine

Automatisiert die Whitelist-Aktualisierung auf der Grundlage vertrauensbasierter Richtlinien. Dadurch werden Flexibilität für die Whitelist und Anpassungsfähigkeit des Geschäftsbetriebs garantiert und das ohne einen arbeitsintensiven, manuellen Prozess. Die Trust Engine trägt zu einer grundlegenden Vereinfachung der Whitelist-Verwaltung in dynamischen Umgebungen bei. Sie umfasst folgende Komponenten:

- **Trusted Publisher:** Der „Vertrauenswürdige Herausgeber“ ermöglicht Änderungen an der Whitelist während des Betriebs, sofern die Änderungen von einem gültigen und signierten Zertifikat des Anwendungsanbieters begleitet werden. Derartige Änderungen werden automatisch genehmigt und erfordern keinen Eingriff seitens des Administrators.
- **Trusted Updater:** Der „Vertrauenswürdige Updater“ lässt eine automatische Aktualisierung der Whitelist zu, sofern die Änderungen von speziell autorisierten Programmen vorgenommen werden.
- **Trusted Path:** Der „Vertrauenswürdige Pfad“ lässt eine automatische Aktualisierung der Whitelist zu, wenn die Änderungen in der Bibliothek der bekannten, harmlosen Anwendungen vorgenommen werden.
- **Local Authorization:** Durch die „Lokale Autorisierung“ können Endbenutzer auf verantwortliche und kontrollierte Weise Ad-hoc-Änderungen durchführen, da alle benutzerspezifischen Änderungen mitverfolgt werden und die Administratoren die Möglichkeit erhalten, die Änderungen nach Bedarf wieder rückgängig zu machen. (Verfügbar im 3. Quartal 2011)

## Einfache Sperre

Vereinfacht den Whitelisting-Prozess durch die unmittelbare Anwendung der definierten Richtlinien und die Blockierung nicht autorisierter Änderungen. Ausgehend von einer automatisch angefertigten Momentaufnahme aller Endpunkte wird eine Whitelist erstellt und mit der konkreten Anwendung der Whitelisting-Richtlinien begonnen. Dadurch steht sofortiger Schutz vor neuen Zero-Day- und anderen Malware-Angriffen bereit – und der IT-Arbeitsaufwand wird grundlegend reduziert.

## Easy Auditor

Ermöglicht Administratoren die Beobachtung und das Auditing der Whitelisting-Richtlinien, um deren Angemessenheit in Bezug auf die Betriebs- und Sicherheitsanforderungen noch vor der globalen Anwendung in der Praxis sicherzustellen. Es können Basis-Richtlinien auf der Grundlage einer lokalen Momentaufnahme erstellt und dementsprechend geeignete Maßnahmen ergriffen werden, ohne dass auf ein globales „Golden Image“ zurückgegriffen werden muss. Reduziert den IT-Arbeitsaufwand bei der Erstellung und Verwaltung einer Whitelist mit vertrauenswürdigen Anwendungen.

## Einheitlicher Workflow

Gewährleistet einen reibungslosen Prozess für die Analyse der IT-Umgebung, die Entfernung bekannter Bedrohungen, die Sperre der IT-Umgebung, die flexible Verwaltung von Änderungen in der Umgebung und die Beseitigung operationeller Konflikte zwischen IT-Betrieb und IT-Sicherheit. Reduziert den Schulungs- und Implementierungsaufwand und den Zeitraum bis zur Gewährleistung eines effizienten Schutzes.

# Zentrale Features

## Integrierter AntiVirus

Mit dem vollständig integrierten AntiVirus-Produktmodul von Lumension werden alle Endpunkte vor der Sperrung und Aufnahme in die Whitelist von allen bekannten Malwareprogrammen bereinigt. Neben der Basisfunktion zur Identifizierung der Malware-Signaturen stehen fortschrittlichste Funktionen bereit, wie z. B. Sandboxing, Verhaltensanalyse und partieller Mustervergleich. In Verbindung mit dem Anwendungs-Whitelisting ist dadurch zusätzlicher Schutz gegeben. Automatisiert die Entfernung von Malware zur Steigerung der IT- und Endbenutzerproduktivität.

## Integriertes Patch Management

Durch den Einsatz des voll integrierten Patch and Remediation-Moduls von Lumension können gleichzeitig anwendungs- und betriebssystemspezifische Schwachstellenrisiken und Sicherheitskonfigurationen verwaltet werden. Wenn operationelle Änderungen zur Begrenzung des Schwachstellenrisikos vorgenommen werden müssen, z. B. durch die Implementierung neuer Software und die Durchführung von Änderungen an den Systemkonfigurationen, werden die Whitelist-Richtlinien entsprechend aktualisiert, um eine reibungslose Umsetzung ohne Störung der Endbenutzeraktivität oder zusätzliche Belastung der Administratoren sicherzustellen. Verbessert die Endpunktsicherheit, ohne die IT- und Endbenutzerproduktivität zu beeinträchtigen.

## Lumension® Endpoint Management and Security Suite

Fungiert als Plattformarchitektur für Lumension® Intelligent Whitelisting™ mit einem einzigen Agent und einer einzigen Konsole. Durch die hoch skalierbare Architektur lässt sich eine Reduzierung der globalen TCO und eine Verbesserung der Visibilität von IT-Betrieb und IT-Sicherheit erzielen.

## Ihr Partner für IT Security und IT Automation

### Deutschland / Österreich:

IBV Informatik GmbH  
Junkersstrasse 5  
DE-82178 Puchheim

Tel: +49 89/800 70 98 290  
Fax: +49 89/800 70 98 299

### Schweiz:

IBV Informatik AG  
Schönenwerdstrasse 7  
CH - 8902 Urdorf

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

