

Warum „kostenlose“ Patch-Management-Tools letztendlich mehr Kosten verursachen können...

Die aktuelle Wirtschaftslage stellt die ungeheure Bedeutung einer detaillierten Analyse sämtlicher Geschäftsausgaben heraus, und das insbesondere im IT-Bereich. Zwar erscheinen punktorientierte Patching-Produkte auf den ersten Blick attraktiver, bei einer tiefer gehenden Prüfung jedoch stößt man schnell auf versteckte Kosten und fehlende Funktionen. Das Ergebnis: Ein fragmentiertes Patch Management und ein schwächerer Sicherheitsstatus – und das bei einer kostenträchtigeren und wesentlich schwerfälligeren Verwaltung für die Unternehmen.

Die Wahl der geeigneten Lösung bedeutet Zeit- und Geldersparnis für Ihr Unternehmen

Die aktuelle Wirtschaftslage stellt die ungeheure Bedeutung einer detaillierten Analyse sämtlicher Geschäftsausgaben heraus, insbesondere im IT-Bereich. Da Unternehmen in diesem Kontext alles daran setzen, ihre Betriebsausgaben so gering wie möglich zu halten, gewinnen „kostenlose“ Technologielösungen zwangsläufig an Attraktivität. Bei der Auswahl einer Lösung für das Patching Ihrer Systeme und Server sollten Sie jedoch unbedingt die TCO (Total Cost of Ownership) sowie den Unterschied zwischen den Hauptfunktionen punktorientierter Patching-Produkte und umfassender Patch-Management-Lösungen berücksichtigen. Zwar erscheinen punktorientierte Patching-Produkte auf den ersten Blick attraktiver, bei einer tiefer gehenden Prüfung jedoch stößt man schnell auf versteckte Kosten und fehlende Funktionen. Diese Lösungen können für Unternehmen im Hinblick auf den kompletten Schutz ihrer IT-Umgebungen letztendlich sogar einen höheren Kostenaufwand verursachen, nämlich aufgrund der mangelnden Skalierbarkeit, des begrenzten Deckungsbereichs und der geringen Flexibilität. Das Ergebnis: Ein fragmentiertes Patch Management und ein schwächerer Sicherheitsstatus – und das bei einer kostenträchtigeren und wesentlich schwerfälligeren Verwaltung für die Unternehmen.

Punktorientiertes Patching – Komplettes Patch Management

Punktorientierte Patching-Produkte ermöglichen die Behebung ganz spezifischer Probleme, ein grundlegendes Handicap dieser „kostenlosen“ Dienstprogramme ist jedoch die fehlende Unterstützung für heterogene Umge-

bungen mit verschiedenen Plattformen und Dritthersteller-Anwendungen. Darüber hinaus ist mit diesen Tools weder eine Konsolidierung noch eine Zentralisierung der Verwaltung von gemischten Systemen und Anwendungen, Patch-Implementierungen und Wartungstools möglich. Auch die Identifizierung nicht verwalteter Blindpunkte wird vernachlässigt. Daraus ergibt sich ein punktorientiertes Produkt mit einem fragmentierten Schwachstellenmanagement-Konzept und einer nur begrenzten Sichtbarkeit des globalen Patching- und Risikostatus. Dadurch dass keinerlei Möglichkeit zur Verwaltung von Dritthersteller-Anwendungen und -Betriebssystemen gegeben ist, sehen sich Unternehmen häufig zum Rückgriff auf mehrere separate Tools sowie zur Mobilisierung umfangreicher Mitarbeiterressourcen gezwungen.

„Patching ist ein wesentlicher Bestandteil unserer Sicherheitsstrategie. Wir benötigen eine detaillierte Kontrolle über das Patching in unserer Umgebung und können uns dabei nicht auf eine globale Windows-Aktualisierung für alle unsere Computer beschränken, denn wir arbeiten mit einer ganzen Reihe eng miteinander verknüpfter Anwendungen. Vor der Implementierung von Patches müssen wir zunächst einen entsprechenden Test durchführen, um sicherzustellen, dass unsere Kernsysteme dadurch keine Beeinträchtigung erfahren. Mit Lumenion ist das möglich, und zwar auf äußerst effiziente Weise.“

Tony Hildesheim, Vice President des Bereichs IT, WSECU

Als eindeutig bessere Wahl erweist sich deshalb eine komplette Patch-Management-Lösung, die wesentlich mehr zu bieten hat als nur die einfache Ausgabe von Patches an Windows-Geräte. Umfassende Patch-Management- und Remediation-Lösungen decken den gesamten Zyklus des Schwachstellenmanagements:

- » Automatische Identifizierung aller nicht verwalteten und gefährlichen Geräte im Netzwerk
- » Lückenloses Scannen des Netzwerks zur Erfassung aller Schwachstellen und Sicherheitslücken
- » Schnelles Patching und Remediation aller IT-Komponenten über eine zentrale Managementkonsole
- » Kontinuierliche Validierung und Wartung zutreffender Patch- und Konfigurationsebenen in den Systemen
- » Robustes Management und Reportin

Eine komplette Patch-Management-Lösung stellt eine einzige Plattform und ein robustes Content-Repository bereit und ermöglicht dadurch die Umsetzung einer holistischen Patch-Management-Strategie. Damit entfällt der Bedarf an zahlreichen punktorientierten Produkten bzw. an einer Erweiterung der Mitarbeiterressourcen für die Erstellung von Skripten für Dritthersteller-Anwendungen auf einer Ad-hoc-Basis. Der Vorteil dieser Lösungen liegt in der globalen Reduzierung der Betriebskosten, bedingt durch ein konsolidiertes Management sowie einen stärkeren allgemeinen Sicherheitsstatus und die notwendige Flexibilität zur proaktiven Beseitigung von Problemen mit weniger Mitarbeiterressourcen.

„Die Verwaltung einer heterogenen Netzwerkumgebung über 20 verschiedene Standorte ist für unsere IT-Mitarbeiter endlich kein Fulltimejob mehr: Lumension hat zu einer erheblichen Risikobegrenzung und zur Reduzierung der IT-Sicherheitsprobleme beigetragen. Diese robuste Lösung zeichnet sich durch hohe Leistungsstärke aus und ermöglicht eine umfassende Beurteilung, Remediation und kontinuierliche Überwachung. Unser Netzwerk profitiert von einem lückenlosen Schutz rund um die Uhr ohne jede Beeinträchtigung unserer Rechenumgebung.“

Jim Czyzewski – Leitender Spezialist für Informationssysteme, MidMichigan Medical Center

Die versteckten Kosten und fehlenden Funktionen punktorientierter Patching-Produkte

In Bezug auf „kostenlose“ Lösungen besagt ein altes Diktum aus Verbraucherkreisen: „Denke immer daran: Erscheint dir etwas zu gut, um wahr zu sein, dann ist es das wahrscheinlich auch.“

Nur Betriebssysteme und Anwendungen von Microsoft

Die meisten kostenlosen Tools statten Unternehmen mit allen Basisfunktionen für das Patching aus, jedoch nur für Betriebssysteme und Anwendungen von Microsoft. Und dabei bleibt es dann auch. Für andere Anwendungen und Betriebssysteme wird keine Unterstützung geboten. Doch selbst die homogensten Microsoft-Umgebungen umfassen eine Vielzahl verschiedener Anwendungen von Drittherstellern, für die ebenfalls regelmäßige Beurteilungen und Patch-Ausgaben erforderlich sind. Nur so kann eine effiziente Beseitigung kritischer Schwachstellen und eine Konformität mit geltenden Regelungen und Konformitätsstandards gewährleistet werden. Die heutigen IT-Umgebungen sind zu vielfältig und heterogen, um auf Anwendungen wie Acrobat Reader, QuickTime von Apple oder die Java Runtime Engine von Sun, einem Enabler betriebssystemunabhängiger Anwendungen, verzichten zu können. Bei der Implementierung von Richtlinien zur Anwendungskontrolle in einem Unternehmen darf darüber hinaus nicht vernachlässigt werden, dass die Benutzer ggf. persönliche Produktivitäts- oder Unterhaltungsanwendungen installiert haben, wie z. B. iTunes von Apple – und das bedeutet eine weitere Diver-

sifizierung der bereits bestehenden Vielfalt bekannter Anwendungen, für die ein Patching durchzuführen ist. Damit haben Unternehmen nicht nur das Patching Windows-spezifischer und anderer Betriebssysteme und Anwendungen zu bewältigen, sondern auch das Patching benutzerspezifischer Anwendungen.

Bedarf an zusätzlichen punktorientierten Produkten selbst in reinen Windows-Umgebungen

Es lässt sich einfach nicht vermeiden, dass mit Nicht-Microsoft-Anwendungen kritische Schwachstellen eingeführt werden. Deshalb ist in Unternehmen, die sich ausschließlich auf Microsoft-Patches beschränken, zwangsläufig ein nicht erfüllter Bedarf gegeben – und die Notwendigkeit, reaktiv in zusätzliche Technologie zu investieren und möglicherweise sogar Mitarbeiter zur Behebung dieses Mankos abzustellen. Wird in diesem Fall der Einsatz eines „kostenlosen“ Tools beschlossen, dann sind letztendlich unzählige punktorientierte Produkte erforderlich, um den Anforderungen eines effizienten Patch Managements gerecht zu werden. Der Rückgriff auf eine konsolidierte Lösung hingegen ermöglicht direkt die effektive Verwaltung des gesamten unternehmensweiten Bedarfs, und das bei gleichzeitiger Reduzierung der betriebsbezogenen TCO.

Sogar Microsoft musste feststellen, dass in 9 von 10 Fällen neuer softwarebasierter Sicherheitslücken die Ursache bei benutzerspezifischer Produktivitätssoftware zu suchen ist¹.

1. Microsoft Security Intelligence Report: Januar bis Juni 2008, Vinny Gullotto, et al.

Unternehmen sollten deshalb eine Risikobegrenzung anhand verschiedener Angriffsvektoren in Betracht ziehen. Die nachstehende Tabelle illustriert die Bandbreite einer potenziellen Bedrohung je nach Technologie.

Schnittstelle mit Sicherheitsmanko	Prozentsatz
Windows-Betriebssystem und Micro-soft-Anwendungen	38%
Apple und Apple-Anwendungen	24%
Andere Anwendungen für Windows ²	29%
Netzwerk, Netzwerkbetriebssystem und Netzwerktechnologien	7%
Unix und reine Linux-Plattformen und -Anwendungen	3%

US-CERT – Technische Cyber-Sicherheitswarnungen 2006-2008³

Bei einer exklusiven Schwerpunktsetzung auf Microsoft-Anwendungen bleibt ein bedenkliches Sicherheitsmanko bestehen, das gezielt beseitigt werden kann.

Keine Konsolidierung der Prozesse

Auch wenn sich viele Unternehmen bei der Wahl ihrer Betriebssysteme ausschließlich auf Windows beschränken, implementieren im Gegensatz dazu zahlreiche Unternehmen eine ganze Reihe verschiedener Betriebssysteme (z. B. MAC OS X, Sun Solaris, HP-UX, Red Hat Enterprise und SUSE Linux). Der Einsatz einer umfassenden Patch-Management-Lösung ermöglicht den Unternehmen die Deckung des betriebssystemspezifischen Patching-Bedarfs für ihre gesamte, diversifizierte IT-Umgebung – und das bei begrenztem Arbeitsaufwand und reduzierten Betriebskosten.

Keine Gewährleistung der Konformität mit geltenden Regelungen

Die breite Palette der unterstützten Anwendungen und Betriebssysteme kann sich auch im Hinblick auf bestehende Konformitätsanforderungen als von grundlegender Bedeutung erweisen. Wenn beispielsweise das unternehmensinterne Kontrollsystem für die finanzielle Konformität eines Unternehmens auf der IT-/Anwendungssicherheit basiert, dann müssen laut SOX, Abschnitt 404, ggf. eine ganze Reihe Kriterien höchster Stufe per Audit beurteilt werden. Eine Audit-Checkliste für die SOX 404-Konformität beinhaltet eventuell auch die Anforderung, dass der Patching-Prozess auf alle Produkte erweitert wird, die im IT-Kontrollsystem zur Anwendung kommen. Wenn Ihr Tool ausschließlich Microsoft-Anwendungen verwaltet, dann wird es für die Audit-Liste nicht genehmigt. In diesem Fall müssen andere Patching-Methoden für die nicht unterstützten Anwendungen angegeben werden, damit die Konformitätsanforderungen erfüllt werden können.

Nur begrenzte Identifizierung nicht verwalteter Komponenten

Da kostenlose Tools in der Regel nur für die Verwaltung reiner Windows-Systeme konzipiert wurden, greifen sie bei der Suche nach den in der IT-Umgebung implementierten Komponenten umfassend auf Active Directory zurück. Nicht verwaltete oder gefährliche Geräte werden in diesem Fall nicht für eine weitere Prüfung erfasst. Durch diesen Mangel an Visibilität bzw. Intelligenz entstehen gefährliche Blindpunkte, die unzureichend verwaltete Komponenten extrem anfällig für potenzielle Angriffe zurücklassen und damit selbst intensivste Versuche einer standardisierten Umsetzung von Sicherheitsrichtlinien untergraben.

2. Bezieht sich sowohl auf Windows als auch auf zahlreiche Betriebssystemanwendungen.

3. Quelle:US-CERT (www.us-cert.gov), „Technical Cyber Alerts“ (Technische Cyber-Warnungen), Stand 31. Oktober 2008

Erforderliche Mitgliedschaft in einer Domain

Die kostenlosen Tools setzen voraus, dass alle verwalteten Windows-Systeme Mitglied derselben Domain sind. Allerdings kann in vielen IT-Umgebungen einfach nicht garantiert werden, dass sämtliche kritischen Windows-Systeme effektiv über Active Directory verwaltet werden. All diejenigen Komponenten, die nicht über die Domain verwaltet werden, werden von den kostenlosen Tools nicht berücksichtigt. Und das bedeutet, dass alle Unternehmen, die mit isolierten Workgroups arbeiten, diese Tools in ihrer Umgebung nicht implementieren können.

Überaus lückenhafte Inventur der Systemsoftware und -hardware

Da sich kostenlose Patching-Tools auf Windows-Patches beschränken, erfassen sie keinerlei Inventurdaten zu installierter Dritthersteller-Software und lokaler Hardware. Dieser lückenhafte Kontext begrenzt die Nützlichkeit dieser Tools um einiges – außerdem ist für die Sammlung dieser Informationen eine zusätzliche Lösung erforderlich.

Keine Verwaltung der Systemkonfigurationen

Das Patch Management ist lediglich eine Komponente einer umfassenden Schwachstellenmanagement-Strategie. Gartner zufolge lassen sich 65 Prozent aller Netzwerkeinbrüche auf Systemfehlfunktionen zurückführen – bei Weitem die häufigste Ursache für Probleme in Verbindung mit der Netzwerksicherheit.⁴ Ebenso viele bekannte Schwachstellen, die verwaltet werden müssen, damit ein sicherer, fortlaufender Betrieb gewährleistet

werden kann, werden durch Fehler bei den Sicherheitskonfigurationseinstellungen verursacht. Der große Nachteil kostenloser Patch-Management-Tools liegt darin, dass diese weder sicherheitsspezifische Best Practices noch native Funktionen zur Beurteilung und Remediation von Fehlkonfigurationen bereitstellen.

Insgesamt höhere Arbeits- und Produktkosten

Selbst Gartner hat sich mit dem problematischen Bedarf an zahlreichen punktorientierten Produkten und zusätzlichen Mitarbeiterressourcen für die Verwaltung kostenloser Patch-Management-Tools beschäftigt. Einem neueren Gartner-Bericht⁵ zufolge setzen einige Unternehmen auch weiterhin kostenlose Patch-Management-Tools ein, die sich als vorwiegend manuell und damit arbeitsintensiv erweisen, und sehen sich dadurch letztendlich mit erheblich höheren Arbeitskosten für die Content-Analyse, das Testing und die Implementierung konfrontiert.

Eine komplette Patch-Management-Lösung – die richtige Lösung

Lumension stellt eine komplette Patch-Management-Lösung bereit, die Unterstützung für eine breit gefächerte Palette an Dritthersteller-Anwendungen sowie für alle gängigen Betriebssysteme bietet. Durch diesen universellen Deckungsbereich lassen sich die versteckten Kosten in Verbindung mit punktorientierten Patching-Produkten vollständig ausgrenzen – denn die Schwachstellenbeurteilung und Patch-Implementierung können über eine zentrale Managementkonsole konsolidiert

4. John Pescatore, Gartner Fellow

5. Gartner: „The Patch Management Market: Collision or Coexistence?“ (Der Patch-Management-Markt: Kollision oder Koexistenz?) Ronni Colville, März 2008

werden. Damit wird den Unternehmen die Möglichkeit gegeben, wesentlich mehr mit wesentlich weniger Mitarbeiterressourcen zu erreichen.

Die komplette Patch-Management-Lösung von Lumension bildet das Fundament für eine wesentlich erfolgreichere und kosteneffektivere Implementierung im Vergleich zu den kostenlosen Patch-Management-Tools, und das unter mehreren Gesichtspunkten:

- » Umfassende Unterstützung für heterogene Umgebungen, einschließlich zahlreicher Betriebssysteme und einer breit gefächerten Palette an gängigen Dritthersteller-Anwendungen
- » Konsolidierung der verschiedenen Prozesse mit einer einzigen Lösung
- » Erfüllung der Anforderungen an das Patch- und Schwachstellenmanagement zur Gewährleistung der Konformität
- » Automatisierte Identifizierung aller Komponenten in der IT-Umgebung, einschließlich nicht verwalteter und gefährlicher Geräte
- » GUI-basiertes Authoring-Tool für benutzerspezifischen Content-Bedarf
- » Beurteilung der Sicherheitskonfigurationen und Patches
- » Reduzierung der TCO für das Patch Management

„Lumension stellt eine grundlegend sicherheitsorientierte Anzeige des Netzwerks bereit. Dadurch erhalten wir zum einen einen wesentlich besseren Einblick in das Netzwerk und zum anderen einen optimalen Gesamtüberblick über

das System. Wir können uns Änderungen im Geschäftsverlauf in wesentlich kürzerer Zeit anpassen und ermöglichen der IT-Abteilung dadurch eine rundum proaktive und flexible Vorgehensweise, und das bedeutet gesteigerte Produktivität bei der Arbeit.“

Anthony Sica, Geschäftsführer des Bereichs IT, Shiseido

Lumension stellt jedoch nicht nur eine umfassende Lösung für das Patch Management bereit, sondern darüber hinaus auch Funktionen zur Gewährleistung der Policy-Konformität. Das Lumension Security Configuration Management™ ermöglicht ein Open-Standards-basiertes Konfigurationsmanagement sowie die Überwachung und Beurteilung von Rechensystemen, damit die Konformität mit geltenden Regelungen bzw. spezifischen unternehmensinternen Richtlinien gewährleistet werden kann. Des Weiteren ermöglicht Lumension seinen Kunden eine effiziente Nutzung der Sicherheitscontent-Datenbank des National Institute for Security and Technology (NIST). Administratoren können die Best Practices des NIST überprüfen und im Vergleich dazu ihren eigenen Konformitätsstatus beurteilen.

Wenn in Unternehmen benutzerspezifischer Content benötigt wird, der speziell auf die Unternehmensumgebung zugeschnitten sein muss, dann steht mit dem Lumension Developers Kit™ eine Benutzeroberfläche bereit, die den Authoring-Prozess um einiges vereinfacht, und das ohne extensive Schulung oder besonderen Arbeitsaufwand. In Verbindung mit dem flexiblen Konzept der Erfassung und Verwaltung auch Domain-externer Komponenten bedeutet das eine drastische Reduzierung

der Komplexität und des Overhead eines erfolgreichen Patch-Management-Prozesses.

Das konsolidierte Management und die Flexibilität des Produktangebots von Lumension ermöglichen eine Steigerung der Betriebseffizienz bei gleichzeitiger Reduzierung der TCO aufgrund des geringeren Ressourcen- und Zeitbedarfs bei der Verwaltung des Patch-Management-Prozesses. Neben den zahlreichen erweiterten Funktionen stellt die preisgekrönte Patch-Management-Lösung von Lumension ebenfalls hoch detaillierte Funktionen bereit und bietet damit eine wesentlich größere Vielseitigkeit im Vergleich zu der heute auf dem Markt verfügbaren kostenlosen Software. Nachstehend eine kleine Auswahl der gebotenen Funktionen:

- » Möglichkeit zur Durchführung assistentbasierter Multi-Patch-Implementierungen
- » Unterstützung für eine Einführung in mehreren Stufen
- » Möglichkeit zur Definition schmaler Installationsfenster
- » Automatische Initiierung von Basisvorgängen, z. B. Patch-Priorisierung und Datensicherung
- » Flexibles Arbeiten für Endbenutzer mit minimalen Betriebsunterbrechungen durch die Möglichkeit zur verzögerten Patch-Implementierung oder einer Installation mit oder ohne verzögertem Neustart
- » Verfeinerung der Verwaltung (d. h. rollenbasierte Zugriffskontrolle zusätzlich zur Zuweisung einfacher Lese- und Schreibberechtigungen)
- » Rapide Schwachstellenbeurteilungen, unabhängig von der Verteilung von Gruppenlinienobjekten (GPOs)
- » Betriebssystemübergreifende Methoden zur Rechnergruppierung, einschließlich der Gruppierung nach IP-Adressbereichen und Active Directory-Attributen
- » Integration von Active Directory zur Vereinfachung des Patch-Management-Mechanismus in Anlehnung an das GPO-Management

Abschluss

Während „kostenlose“ Tools als Lösung für das Patch Management überaus verlockend wirken, bedingt eine detaillierte Analyse der Anforderungen eines Unternehmens letztendlich die Wahl einer umfassenderen Patch-Management-Lösung, die eine Reduzierung der langfristigen Risiken und eine Optimierung der Betriebskosten ermöglicht.

Funktion	Schwachstellenmanagement von Lumension	Kostenlose punktorientierte Patching-Produkte
Patching von Microsoft-Betriebssystemen	✓	✓
Unterstützung für Anwendungen und Betriebssysteme von Drittherstellern	✓	✗
Konsolidierung der Patch-Management-Prozesse	✓	✗
Erfassung nicht verwalteter Komponenten	✓	✗
Unterstützung für andere als Active-Directory-basierte Umgebungen	✓	✗
PatchLink Security Configuration Management™	✓	✗
Lückenlose Systeminventur-Erfassung	✓	✗
GUI-basiertes benutzerspezifisches Authoring-Tool	✓	✗
Reduzierung der benötigten Mitarbeiterressourcen	✓	✗
Senkungen der TCO für das Patch Management	✓	✗
Detaillierte Patching-Kontrolle	✓	✗
Komplettlösung ohne Bedarf an zusätzlichen punktorientierten Produkten	✓	✗

Funktionsvergleich zwischen Lumension und kostenloser Patch-Software

„Wir können nunmehr in kürzester Zeit die Rechner identifizieren, die mit Patches ausgestattet wurden und eine verwaltbare Automationsebene in Bezug auf die Anwendung erforderlicher Patches erreicht haben. Seit der Implementierung von Lumension und dem Einsatz der zentralisierten Managementfunktionen haben wir keinerlei bedeutende Virusattacken erfahren. Kritische Patches lassen sich schnell und problemlos auf sämtliche Rechner in unserem gesamten dezentralen Netzwerk anwenden.“

Mike Walder, Support Consultant, East Sussex Council

Mehr zu Lumension

Lumension, ist ein weltweit führendes Unternehmen im Bereich operationelle Endpunktsicherheit. Lumension entwickelt, integriert und vertreibt Sicherheitssoftwarelösungen, die Unternehmen den effizienten Schutz sensibler Informationen und die bedarfsgerechte Verwaltung kritischer Risiken für ihre Netzwerke und Endpunkte ermöglichen.

Über 5.100 Lumension-Kunden rund um den Globus profitieren von optimaler Sicherheit und einer erfolgreichen IT-Strategie dank der bewährten und preisgekrönten Lösungen von Lumension – dazu gehören Schwachstellenmanagement, Endpunktschutz, Datensicherheit, Reporting und Konformitätsgarantie. Lumension ist zudem für seinen ausgezeichneten Kundenservice bekannt und stellt Supportleistungen rund um die Uhr bereit, 24 Stunden am Tag, 365 Tage im Jahr.

Der Hauptsitz des Unternehmens befindet sich in Scottsdale, Arizona (USA). Darüber hinaus verfügt Lumension über Zweigniederlassungen auf der ganzen Welt, u. a. in Virginia und Florida (USA), in Luxemburg, Großbritannien, Spanien, Australien, Indien, Hongkong und Singapur. Lumension: IT-Sicherheit und Erfolgsgarantie. Weitere Informationen finden Sie auf der Website

www.lumension.com.



Internationaler Hauptsitz

15.580 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260 – USA

Telefon: +1.888.725.7828

Fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance