Lumension SECURITY™

Schluss mit

DATENVERLUST UND MALWARE

Stellen Sie effizienten Schutz vor Datenverlust und Malware durch policybasierte Endpunktsicherheit bereit.

Endpunkt-Sicherheitslösung

74 Prozent der von einem Unternehmen erlittenen finanziellen Einbußen sind auf Virusattacken, nicht autorisierten Zugriff auf das Netzwerk, verlorene/gestohlene Laptops und mobile Hardware, Diebstahl interner Daten oder geistigen Eigentums zurückzuführen. Dem Schutz Ihrer Endpunkte kommt daher vorrangige Bedeutung zu.[1]

Glücklicherweise ist das kein Ding der Unmöglichkeit. Mit der Common Criteria EAL2-zertifizierten Endpunkt-Sicherheitslösung von Lumension Security steht eine policybasierte Anwendungs- und Gerätekontrolle bereit, die Ihr Unternehmen proaktiv vor Datenbedrohungen schützt, einschließlich Datenverlust, Malware und Spyware.

Sanctuary® von Lumension unterstützt ein Sicherheitskonzept, bei dem ausschließlich bekannte und sichere Anwendungen und Geräte auf Netzwerkservern, Terminal-Services-Servern, Thin Clients, Laptops und Desktops ausgeführt werden dürfen:

- Eliminierung des Risikos von Datendiebstahl oder Datenverlust aufgrund nicht autorisierter Anwendungen und Geräte
- Verhinderung der Ausführung unbekannter/bösartiger Codes, einschließlich Malware, Spyware, Zero-Day-Bedrohungen und aller anderen zerstörerischen Viren
- Gewährleistung der Konformität mit kontinuierlich weiterentwickelten Regelungen und Vorschriften in Bezug auf Datenschutz und interne Kontrollen (u. a. Sarbanes Oxley, HIPAA, GLBA)
- Bewahrung der IT-Systemintegrität sowie Verbesserung der IT-Systemleistung und der Netzwerkbandbreite
- Reduzierung der TCO für die Endpunktsicherheit
- Steigerung der Endbenutzerproduktivität

Lösungsübersicht

- Eliminierung des Risikos von Datenverlust, Malware und Spyware sowie Verbesserung der IT-Sicherheit und der Netzwerkbandbreite
- Reduzierung des Arbeits- und Kostenaufwands in Verbindung mit der Unterstützung von Endpunkt-Technologien sowie Gewährleistung der Konformität mit geltenden Regelungen
- Uneingeschränkte Kontrolle über alle mobilen Medien und Endpunkt-Peripheriegeräte sowie über den gesamten Port-Zugriff
- Lückenloser Schutz vor Malware und unerwünschten Anwendungen
- Konsequente Umsetzung angemessener Richtlinien zur Anwendungs- und Gerätenutzung

Anwendungs- und Gerätekontrolle für Ihre Endpunkte

Unternehmen müssen sich kontinuierlich mit Problemen rund um Sicherheit und Support auseinandersetzen, wenn es um Endpunktbenutzer und deren Laptops und PCs geht. Sanctuary gewährleistet Endpunktsicherheit durch den Rückgriff auf ein geradezu einmaliges, überaus einfaches und positives Sicherheitskonzept: Ausschließlich autorisierte Anwendungen können ausgeführt werden und nur autorisierten Geräten wird der Zugriff auf Netzwerkserver, Terminal-Services-Server, Thin Clients, Laptops oder PCs genehmigt. Daraus ergibt sich das Beste für beide Welten – das Sicherheits- und Systemmanagement gestaltet sich um einiges einfacher, das Unternehmen verfügt weiterhin über die benötigte Flexibilität.

Zum Schutz Ihres Unternehmens vor bekannten wie auch vor unbekannten Bedrohungen vereint Sanctuary die bereits bewährten Fähigkeiten seiner Module zur Anwendungs- und Gerätekontrolle und stellt damit die einzige Endpunkt-Sicherheitslösung bereit, die eine zentrale Verwaltung, Überwachung und Kontrolle aller Anwendungen und Geräte im Netzwerk eines Unternehmens ermöglicht.

Sanctuary® Application Control
Policybasierte Kontrolle der Anwendungsnutzung im Hinblick auf den Schutz der Endpunkte vor Bedrohungen wie Malware und Spyware sowie vor unerwünschter oder nicht lizenzierter Software.

Sanctuary® Device Control
Policybasierte Kontrolle der Nutzung mobiler Geräte im Hinblick auf eine Steuerung des ein- und abgehenden Datenflusses an den Endpunkten.

Die Herausforderung Endpunktsicherheit

Die Sicherheitslandschaft ist im Wandel begriffen: An Stelle der breit angelegten, spektakulären Attacken am Unternehmensperimeter kommt es immer häufiger zu gezielten Bedrohungen an den Unternehmensendpunkten, die seit jeher einen niedrigeren Sicherheitsgrad aufweisen. Datenlecks und Sicherheitsbedrohungen – ob versehentlich oder vorsätzlich entstanden – treten großteils an den Endpunkten auf und sind häufig auf interne Fehler oder Nachlässigkeiten zurückzuführen.

Nicht verwaltete mobile Medien und Anwendungen an den Endpunkten können die herkömmlichen Sicherheitsmaßnahmen leicht umgehen und die Offenlegung von Daten fördern, sodass diese schnell in falsche Hände geraten. Die traditionellen Sicherheitslösungen haben sich als Schutzwall gegen diese stetig wachsende Flut der Sicherheitsbedrohungen an den Endpunkten als ineffizient erwiesen, da sie auf Symptome reagieren, nachdem eine Bedrohung bereits eingeführt wurde – und der Bedrohung nicht proaktiv von Anfang an Einhalt gebieten.

Das belegt allein die Tatsache, dass 62 Prozent der Unternehmen, die über eine Antivirus-Lösung verfügen, eine Infizierung zu verzeichnen hatten.[2] Darüber hinaus gehen 70 Prozent aller Computerattacken, IT-Sicherheitseinbrüche und Datendiebstähle von innerhalb der Firewall aus,[2] wodurch erneut ersichtlich wird, dass Endpunkte einen perfekten Eingangspunkt für Malware darstellen. Inzwischen können Sicherheitsbedrohungen wie Malware ebenfalls über mobile Medien an den Endpunkten eingeschleust werden.

Durch die konsequente Umsetzung angemessener Policies zur Anwendungs- und Gerätenutzung richten Sie an den Endpunkten einen effizienten Schutz ein und verhindern dadurch, dass diese als Datenschleuse missbraucht werden: Kritische Daten können damit nicht mehr ausgeführt werden und Sicherheitsbedrohungen, wie z. B. Malware, werden am Eindringen in das Netzwerk gehindert. Die Ausgrenzung bekannter Sicherheitsbedrohungen aus dem Netzwerk ist kein Problem – das Problem liegt bei den verborgenen Bedrohungen, die an den Endpunkten lauern und ein neues Konzept erforderlich machen.

Lückenlose Umsetzung der Policies

Sanctuary lässt alle autorisierten Anwendungen und mobilen Geräte zu, die innerhalb eines Unternehmens zum Einsatz kommen. Das von Sanctuary unterstützte positive Modell ermöglicht ausschließlich die Ausführung autorisierter Anwendungen und gestattet nur autorisierten Geräten den Zugriff auf Laptops, PCs, Server, Terminal-Services-Server und Thin Clients. Anwendungen, die nicht explizit autorisiert wurden, können standardmäßig nicht ausgeführt werden. Dasselbe gilt für nicht autorisierte Geräte, auf die der Zugriff standardmäßig verweigert wird. Die mit Sanctuary erstellten Policies lassen sich bedarfsgerecht für einzelne Benutzer oder Benutzergruppen wie auch für einzelne Computer verwalten.

Einfachheit, Schnelligkeit und Flexibilität bei Administration und Management

Policies zur Anwendungs- und Gerätekontrolle lassen sich in kürzester Zeit über eine zentrale Konsole erstellen und anhand zweier einfacher Schritte anwenden: Mithilfe von Sanctuary identifiziert der Administrator problemlos alle betroffenen Geräte und Anwendungen und weist dann Zugriffsberechtigungen auf höchster Ebene oder bis auf die gewünschte Detailebene zu, d. h. er kann Benutzern, Benutzergruppen oder einem bestimmten Computer Zugriffsberechtigungen für eine Geräteklasse, ein spezifisches Gerät oder eine Anwendung einräumen. Sanctuary verknüpft die Anwendungs- und Geräte-Policies mit den in Microsoft® Windows® Active Directory™ oder Novell® eDirectory™ gespeicherten Benutzer- und Benutzergruppendaten und trägt dadurch zu einer wesentlichen Vereinfachung der Verwaltung der Anwendungs- und Geräteressourcen an den Endpunkten bei.

Automatische Identifizierung von Anwendungen und Geräten

Sanctuary ermöglicht die Identifizierung aller zum Einsatz kommenden Anwendungen und Geräte durch den Rückgriff auf eine Audit-Option ohne Nutzungssperre sowie auf verschiedene Scanning-Tools. Dadurch kann die aktuelle Situation im Detail erfasst und bewertet werden, die anschließende Definition und Verwaltung der geeigneten Policies gestalten sich auf dieser Grundlage um einiges einfacher.

Detaillierte Definition der Berechtigungen im Rahmen der Gerätekontrolle

Um das Risiko eines Netzwerkzugriffs durch nicht autorisierte Geräte vollständig zu beseitigen, stehen für die Anwendung der Gerätepolicies unterschiedlichste Kriterien zur Verfügung – zeitliche Begrenzung, Verschlüsselung, Datenvolumen, Datenübertragung und vieles andere mehr. Darüber hinaus ermöglicht Sanctuary die Kontrolle des Typs der Dateien, die auf mobile Geräte übertragen bzw. von dort eingelesen werden können. Dadurch lässt sich das Risiko eines Eindringens unerwünschter Dateien in das Netzwerk sowie eines Abflusses kritischer Dateien aus dem Netzwerk grundlegend begrenzen. Je nach Art der Tätigkeit der Benutzer – online oder offline – können zudem separate Policies definiert und angewendet werden.

Kontrollierte Verschlüsselung

Mobile Medien können verschlüsselt werden, sodass ein sicherer Betrieb und Transport möglich wird, d. h. die Gefahr des Zugriffs durch nicht autorisierte Benutzer auf vertrauliche Daten wird ausgegrenzt. Die Benutzer können auf ihre verschlüsselten Daten auch von Rechnern aus zugreifen, auf denen die Sanctuary-Clientsoftware nicht installiert wurde. Anhand zentraler wie auch dezentraler Verschlüsselungsschemata erhalten die Sanctuary-Administratoren die erforderliche Flexibilität, um mobile Medien von einem zentralen Standpunkt aus zu verschlüsseln oder ganz im Gegenteil Benutzern die selbstständige Verschlüsselung ihrer mobilen Medien zu ermöglichen. Damit – und das ist von ganz entscheidender Bedeutung – lässt sich die Nutzung der verschlüsselten Medien umfassend kontrollieren.

Flexible Autorisationsregeln

Administratoren können vertrauenswürdige Benutzer dazu berechtigen, Autorisierungen für ihre eigenen Anwendungen zu erteilen. Durch diese Möglichkeit ist absolute Flexibilität gegeben, wobei der Administrator durch Warnmeldungen stets auf dem Laufenden gehalten wird.

Detaillierte Audit-Funktionen

Durch den Rückgriff auf die zum Patent angemeldete bidirektionale I/O-Shadowing-Technologie von Sanctuary werden die Namen bzw. der Inhalt aller Dateien aufgezeichnet, die von Disketten, CDs/DVDs und mobilen Geräten eingelesen bzw. darauf geschrieben werden. Jede versuchte Anwendungsausführung bzw. jeder versuchte Gerätezugriff kann aufgezeichnet und geprüft werden. Dazu stehen flexible Filter-, Sortier- und Anzeigeoptionen sowie gespeicherte, benutzerspezifische Abfragevorlagen zur Verfügung. Darüber hinaus werden sämtliche Administratoraktionen protokolliert, einschließlich aller Policy-Einstellungsänderungen. Dadurch steht ein kompletter Audit-Trail für die Umsetzung der Policies bereit.

Bewährte Sicherheit

Aufgrund seiner Implementierung auf Kerneltreiber-Ebene ist Sanctuary absolut unzugänglich. Das bedeutet, dass Sanctuary von den Benutzern weder abgeschaltet noch in irgendeiner Form umgangen werden kann.

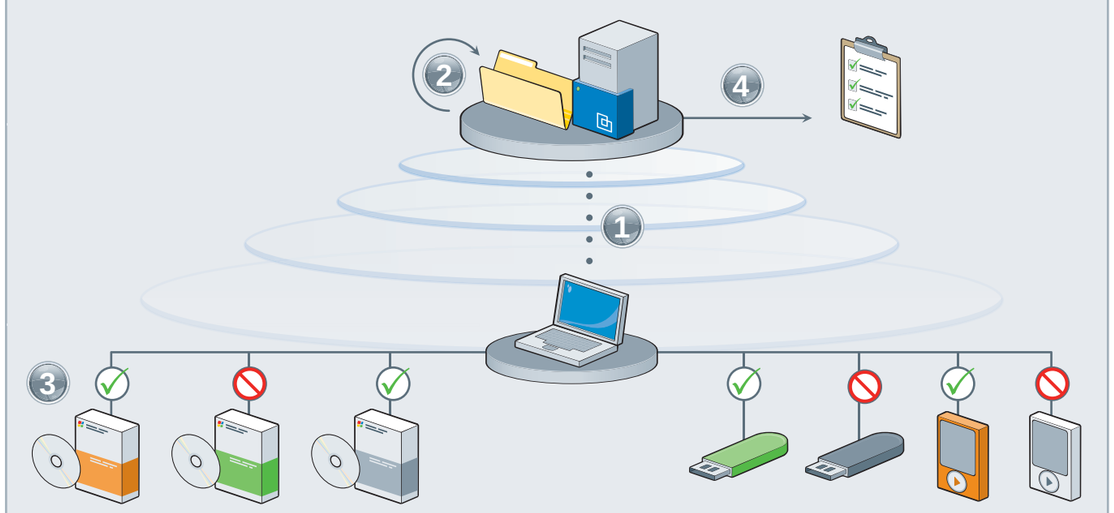
Unternehmensspezifische Skalierbarkeit

Sanctuary wurde für eine bedarfsgerechte Skalierung in weitläufigen und komplexen Umgebungen konzipiert und weist aus diesem Grund eine 3-tier-Architektur mit Datenbank, Anwendungsserver(n) und Client auf.

Common Criteria EAL2-Zertifizierung

Die Zertifizierungseinrichtung Common Criteria Evaluation and Validation Scheme (CCEVS) hat die Konformität der Endpunkt-Sicherheitslösung von Lumension mit den vorgegebenen Sicherheitsanforderungen bestätigt.

Und so funktioniert's



1. Identifizierung: Erfassung aller exe-Dateien und Geräte, Sammlung der Profile und Anordnung in vordefinierten Dateigruppen.

2. Auswertung: Zuweisung von Ausführungsberechtigungen nach Anwendungs- und Geräte- sowie nach Benutzer- und/oder Benutzergruppenattributen.

3. Umsetzung: Wenn ein Benutzer die Ausführung einer Anwendung oder den Zugriff auf ein Gerät anfordert, wird die OS-Anforderung auf Kernel-Ebene vom Sanctuary-Treiber abgefangen. Der gesamte Prozess des Policy Enforcement verläuft für den Endbenutzer vollständig transparent.

   Bei Anwendungen erfolgt die Generierung und Verifizierung der Signatur, die dann mit der zentral oder lokal autorisierten Liste der zugelassenen Dateien verglichen wird. Kann keine Übereinstimmung zwischen der exe-Datei und der autorisierten Dateiliste festgestellt werden, dann wird die Ausführung der Datei verweigert. Wenn die Datei in der Liste der zulässigen Dateien enthalten ist, wird ihre Ausführung genehmigt.

   Dieses Konzept gilt ebenfalls für alle Geräte. Der Treiber prüft die Benutzerberechtigungen durch den Rückgriff auf die Zugriffskontrollliste (ACL) für die entsprechende Geräteklasse oder das betroffene Gerät. Verfügt der Benutzer über die erforderliche Berechtigung, dann erhält er Zugriff auf das Gerät. Wird das Gerät jedoch nicht erkannt oder verfügt der Benutzer nicht über die erforderliche Berechtigung, dann wird der Zugriff verweigert.

4. Auditing: Sanctuary zeichnet sämtliche Versuche der Anwendungsausführung und des Gerätezugriffs, alle Administratoraktionen und alle auf mobile Geräte geschriebenen bzw. davon ausgelesenen Daten auf.

Zusatzprodukte

Sanctuary® Application Control: Server Edition

Damit steht eine Serversicherheitssoftware bereit, die umfassende Unterstützung bei der Umsetzung von Policies zur Anwendungsnutzung bietet – für den standardmäßigen Schutz missionskritischer Server (d. h. Mailserver, CRM-Anwendungen, Webserver und andere missionskritische Datenbankserver) vor nicht autorisierten, illegalen oder unerwünschten Anwendungen und die Verhinderung jeder Unterbrechung des Geschäftsablaufs.

Sanctuary® Application Control: Terminal Services Edition

Damit wird ebenfalls die Umsetzung von Policies zur Anwendungsnutzung gewährleistet – für den standardmäßigen Schutz kritischer Windows- oder Citrix-basierter Terminal-Services-Umgebungen vor nicht autorisierten, illegalen oder unerwünschten Anwendungen.

Sanctuary® for Embedded Devices

Damit steht eine einfache und überaus effiziente Kontrolle der Netzwerkkonfiguration aller Windows-Embedded-Geräte bereit, und das ausgehend von einem zentralen Standort. Sanctuary unterstützt fortschrittlichstes Policy Enforcement in Bezug auf die Geräte- und Anwendungsnutzung für Thin-Client-Vorrichtungen, die die Plattformen Windows Embedded for Point of Service (WEPOS) und Windows XP Embedded unterstützen, wie z. B. PoS-Terminals im Einzelhandel, Geldautomaten, Gaming-Geräte, Thin Clients und andere netzwerkbasierte Systeme.

Unsere Kunden kommen zu Wort

„Sanctuary bietet eine einzige, nahtlose Ansicht aller Geräte und Anwendungen, die über Unternehmensendpunkte auf das Netzwerk zugreifen bzw. Zugriffsversuche unternehmen. Damit steht ein neuer, umfassender Einblick in das Netzwerk bereit, wie er bisher nicht möglich gewesen war."

John C. Lincoln Health Network

„Mit Sanctuary Device Control wird sichergestellt, dass kein Gerät ohne entsprechende Genehmigung eingesetzt werden kann, ungeachtet des jeweils verwendeten Anschlusses. Device Control ist ein überaus leistungsstarkes, benutzerfreundliches Produkt – und genau aus diesen Gründen hat sich Barclays für diese Lösung entschieden."

Barclays

„Mit Sanctuary kann ich eine explizite Liste derjenigen Anwendungen aufstellen, deren Ausführung auf den Rechnern in unserer Bank zugelassen ist. Alle anderen exe-Dateien – und dazu gehört auch bösartiger Code – können einfach nicht ausgeführt werden. Damit bin ich dank Sanctuary allen potenziellen Problemen stets um einen Schritt voraus. Für die Leitung der Bank, die Auditoren und letztendlich auch für unsere Kunden bedeutet das die Gewissheit, über den bestmöglichen Schutz zu verfügen."

First National Bank Bosque County

Auch erhältlich bei Lumension

Die Schwachstellenmanagement-Lösung von Lumension ermöglicht Unternehmen eine effiziente Verwaltung des gesamten Schwachstellenzyklus. Dazu wurden ein Scanner zur unternehmensweiten Schwachstellenbeurteilung und die auf Nummer 1 platzierte Patch- und Remediation-Lösung in einer zentralen Management- und Reporting-Konsole vereint.

Mehr zu Lumension

Lumension Security profiliert sich als führendes, internationales Unternehmen im Bereich Sicherheitsmanagement und stattet weltweit bereits mehr als 5.100 Kunden und 14 Millionen Knoten mit einer einheitlichen Sicherheit und Kontrolle für sämtliche unternehmensinternen Endpunkte, Anwendungen und Geräte aus. Lumension ermöglicht Unternehmen ein effizientes Risikomanagement an den Endpunkten durch die Bereitstellung hochmoderner policybasierter Lösungen. Dazu gehören Schwachstellenmanagement, endpunktorientiertes Policy Enforcement und extensives Reporting zur Policy-Konformität.

Sie wünschen sich absolute Kontrolle über Ihre Endpunkte?

Wie lässt sich eine akzeptable Nutzung von Anwendungen und Geräten in Ihrem Unternehmen durchsetzen? Konkrete Informationen diesbezüglich erhalten Sie bei Ihrer örtlichen Lumension-Handelsvertretung, Ihrem Lumension-Fachhändler oder auf unserer Website: www.lumension.com.

Quellen:

1. 2006, CSI/FBI-Studie zu Computerverbrechen und -sicherheit
2. Studie der Yankee Group aus dem Jahr 2005 zu den "Leaders" (Vorreiter) und "Laggards" (Trödler) im Bereich Sicherheit

Lumension SECURITY™

Lumension Security - Luxembourg
Atrium Business Park
Z.A. Bourmicht
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364 11 / www.lumension.com