



DESKTOP AUTHORITY®

OPTION ZUR SPYWARE-ERKENNUNG UND -ENTFERNUNG

Einem aktuellen Gartner-Bericht* zufolge, sind 20 bis 40% aller Helpdesk-Anfragen in Unternehmen auf Spyware und Adware-Infektionen zurückzuführen.

Administratoren, die die Aufgabe haben, Spyware auf Desktops zu erkennen und zu entfernen, benötigen eine zentrale, leistungsstarke Lösung, damit die Spyware sich nicht festsetzen kann. Mithilfe der integrierten Option zur Spyware-Erkennung und -Entfernung (SDR – Spyware Detection and Removal) von Desktop Authority kann die Anti-Spyware-Technologie unternehmensweit eingesetzt werden.

Ohne Anti-Spyware-Lösungen mit Verwaltungsfunktionen für Unternehmen verlassen sich viele Administratoren auf die Sicherheit des Umkreisnetzwerks und hoffen, dass keine Probleme auftreten. Viele der vorhandenen Anti-Spyware-Lösungen sind auf Einzelbenutzer zugeschnitten und verfügen nicht über zentralisierte Funktionen zur Verwaltung und Berichterstellung. Die Verwendung von Anti-Spyware-Produkten für Einzelbenutzer in einem Unternehmensnetzwerk ist in der Administration sehr zeitaufwändig, schränkt die Sichtbarkeit von Spyware ein und bietet keine Garantie für konsistente Ergebnisse auf allen Desktops.

INTEGRIERTE LÖSUNG

Die SDR-Option von Desktop Authority ist vollständig in die benutzerfreundliche Desktop Authority-Verwaltungskonsolle integriert. Administratoren, die bereits mit der Verwaltung von Clientcomputern mit Desktop Authority vertraut sind, müssen sich lediglich mit einer neuen Funktion vertraut machen und

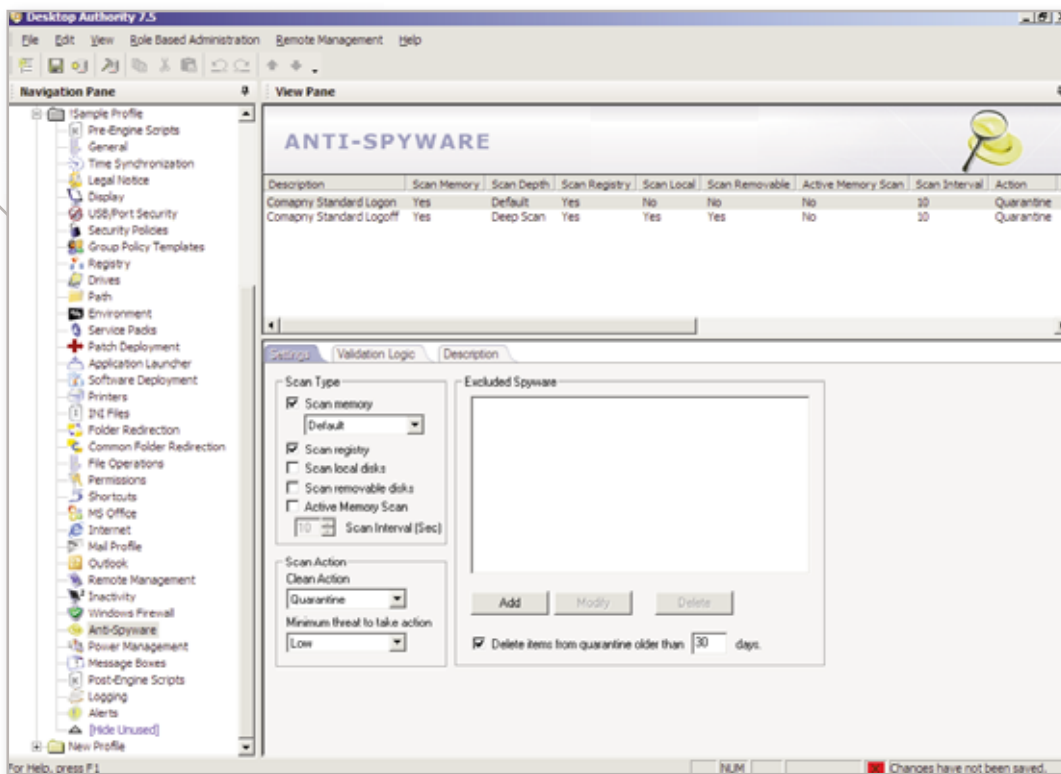
nicht mit einer vollständig neuen Lösung. SDR profitiert außerdem von der patentierten *Validation Logic*-Technologie von ScriptLogic. Diese Technologie ermöglicht eine hochpräzise Kontrolle darüber, wann, wo und wie die einzelnen Ebenen der Spyware-Bedrohung erkannt und entfernt werden.

FLEXIBLE VERWALTUNG

Neben der Verwendung von *Validation Logic* enthält SDR die folgenden Verwaltungselemente, mit der die Optionen des Administrators bei der Art der Handhabung von Spyware erweitert werden:

- **Scantypen: Arbeitsspeicher, lokale Laufwerke, Wechselmedien, Registrierung, aktives Durchsuchen des Arbeitsspeichers (Echtzeit).**
- **Scanaktionen: Protokoll, Isolation, Entfernen**
- **Bedrohungsebenen: Harmlos bis schwerwiegend**
- **Erkennungsausschlüsse**

Durch den unternehmensweiten Einsatz der SDR-Option von Desktop Authority verfügen Administratoren über zentrale Steuerungsmöglichkeiten zum Entfernen von Spyware.



*Gartner-Bericht vom 27.06.05, „Antivirus Vendors Strike Back with Anti-Spyware Products“

© 2006 ScriptLogic Corporation. Alle Rechte vorbehalten. Desktop Authority und das ScriptLogic-Logo sind eingetragene Marken der ScriptLogic Corporation in den USA und/oder anderen Ländern. Weitere in diesem Dokument erwähnte Produkt- und Firmenamen können geschützte Marken ihrer jeweiligen Inhaber sein.

09-06

HAUPTVORTEILE

Zentrale Verwaltung

Mit einer einzigen Verwaltungskonsolle können Sie SDR-Option von einem zentralen Standort aus auf allen Desktops konfigurieren.

Zentrale Berichterstattung

Clients senden Berichte zur Spyware-Erkennung, damit Administratoren eine ausführliche Übersicht über die Spyware im Netzwerk erhalten.

Erhöhte Produktivität

Administratoren können Spyware automatisch erkennen, entfernen oder isolieren lassen, damit die Ausfallzeit und Anfälligkeit für das Eindringen, Datendiebstahl und andere Angriffe verringert werden.

HAUPTFUNKTIONEN

Umfassende Spyware-Erkennung

SDR aktualisiert die Datenbank der Spyware-Definitionen automatisch und deckt somit ein breites Spektrum an Spyware-Typen und -Bedrohungen ab.

Integrierte Verwaltung

SDR ist vollständig in Desktop Authority integriert. Somit ist die Spyware-Erkennung und -Entfernung so einfach wie jede andere Aufgabe.

Präzise Verwaltungsauswahl

Die patentierte *Validation Logic*-Technologie von ScriptLogic ermöglicht eine hochpräzise Auswahl der Benutzer und Computer, für die SDR verfügbar sein soll. Jede Kombination von Benutzern und Computern kann somit unterschiedlich behandelt werden, z. B. durch das Durchsuchen nach verschiedenen Bedrohungsebenen, durch verschiedene Ausschlusslisten oder durch unterschiedliche Scanintensitäten.



Geplantes und aktives Durchsuchen des Arbeitsspeichers

SDR ermöglicht das Durchsuchen des Arbeitsspeichers in Echtzeit und unterstützt geplante vollständige Scans des Laufwerks und der Registrierung.

SYSTEMANFORDERUNGEN

Verwaltung

Desktop Authority 6.5 oder höher.

Clientunterstützung

Windows 98/Me/2000/XP.

LIZENZIERUNG

Die SDR-Option wird als jährliches **Abonnement** separat von Desktop Authority lizenziert.

DR.
MORAWIETZ
OFFICES OF TWARE & SYSTEMHAUS
Schwanheimer Straße 144a
64625 Bensheim
Telefon: +49 (6251) 10 58-0
ScriptLogic@MORAWIETZ.de
www.morawietz.com

