

Kontrolle über vertrauliche Daten im Unternehmen hat höchste Priorität

Der Verlust vertraulicher Daten wie Kundendatenbanken, geistigem Eigentums, Finanz- oder Rechtsdokumenten, Marktforschungs- oder persönlicher Daten kann Unternehmen jeder Größe treffen. Die unternehmerische Nachhaltigkeit und Effizienz eines Unternehmens hängen im großen Maße davon ab, wie gut solche Informationen geschützt sind.

Üblicherweise wird dem Thema Datenverlust mit der Einführung betriebsinterner Maßnahmen begegnet - wie beispielsweise durch unterschriebene Vereinbarungen zur Verschwiegenheitspflicht oder durch den Einsatz interner technischer Mittel und Richtlinien für den Umgang mit Informationen (zum Beispiel das Verbot, am Arbeitsplatz USB-Speicher oder das Internet zu benutzen). Diese Maßnahmen decken jedoch nicht die Vielzahl der Kanäle ab, über die Daten in fremde Hände gelangen können.

Laut Analysen von InfoWatch gingen über 48 Prozent aller registrierten Datenverluste im ersten Halbjahr 2009 auf das Benutzen von tragbaren Geräten (wie Laptops), portabler Speichermedien (wie Flash-Laufwerke) und auf das Ausdrucken von Dokumenten zurück. Neben E-Mails, Internetforen und Instant Messengers (wie MSN oder AOL IM) sind die am häufigsten betroffenen Wege, über die sowohl unbeabsichtigte als auch vorsätzliche Datendiebstähle passieren, portable Laufwerke, oder sonstige Speichermedien und Dokumente, die vom Benutzer ausgedruckt werden.

InfoWatch Device Monitor schützt vertrauliche Informationen

InfoWatch Device Monitor wird an den Arbeitsplätzen der Benutzer installiert und überwacht die üblichen Wege, über die vertrauliche Daten abhanden kommen können. Die Lösung ermöglicht es, unbeabsichtigte Datenverluste, aber auch vorsätzliche Datendiebstähle per mobiler Datenträger und sonstiger Speichermedien und Kommunikations-Ports zu erkennen und die Benutzung von Input-/Outputgeräten im Einklang mit den Security-Policies des Unternehmens zu begrenzen.

InfoWatch Device Monitor überwacht:

- das Kopieren von Daten auf portable Medien (Disketten, USB-Sticks und andere Geräte, die per LPT, COM oder andere Kommunikations-Ports verbunden werden)
- den Zugang zu CD- und DVD-Laufwerken
- die Benutzung von Geräten, die drahtlos angesteuert werden (IRDA, Bluetooth)
- den Zugang zu Smartphones, PDAs (mit Windows Mobile oder Palm OS), Laptops, Netbooks und anderen tragbaren Geräten
- das Drucken von Daten

Überblick über die Lösung

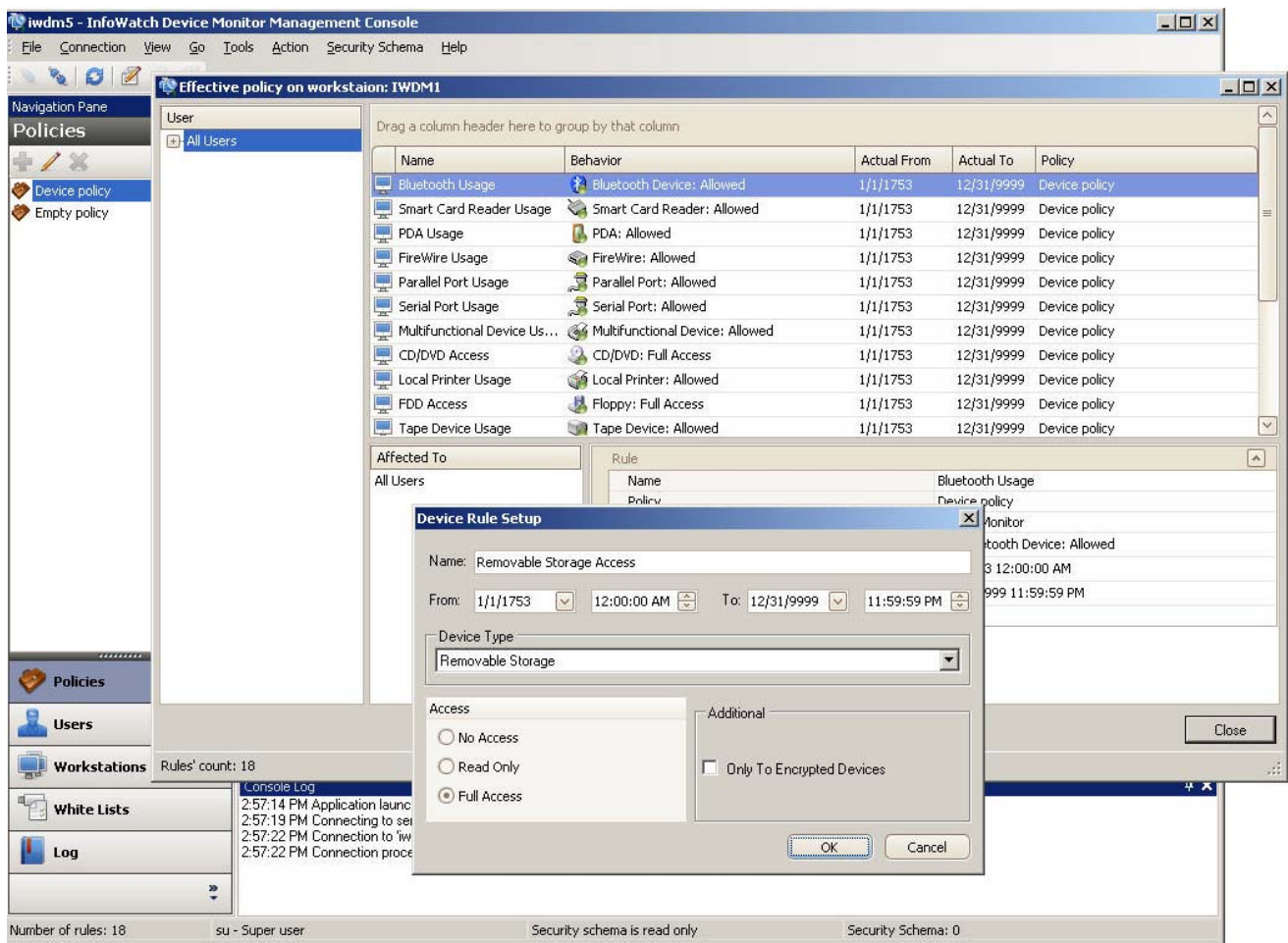
InfoWatch Device Monitor verfügt über eine Client-Server-Architektur. Der Client wird an den Arbeitsplätzen der Benutzer installiert und über die zentrale InfoWatch Device Monitor-Konsole administriert. Ist der Arbeitsplatz mit dem installierten Client im Unternehmensnetzwerk verbunden, wird eine spezifische Liste mit Security-Policies übertragen. **InfoWatch Device Monitor** ist in der Lage, für einen spezifischen Benutzer oder eine Benutzergruppe eine Sicherheitsliste mit genehmigten Geräten zu erstellen. Diese Liste wird auf der Basis von Gerätemodellen oder deren einzigartiger Seriennummer zusammengestellt. Der Zugang zu den Geräten der Sicherheitsliste wird immer gewährt.

Werden Daten auf tragbare Geräte oder Speichermedien kopiert oder auch an einen Drucker gesendet, fertigt **InfoWatch Device Monitor** Schattenkopien aller betroffenen Dateien an. Diese Daten werden zu einem zentralen Analyse-Server gesendet, der die Entscheidung darüber fällt, ob die übertragenen Daten vertrauliche Informationen beinhalten. Nach der Prüfung werden die Daten in einem InfoWatch Storage-Archiv gesichert.

Dank der Integration mit Microsofts Active Directory ermöglicht **InfoWatch Device Monitor** die Anwendung der Security-Policies für Benutzer oder Benutzergruppen aus dem Corporate Directory. Der **InfoWatch Device Monitor** Client kann zentral an alle Arbeitsplätze über Microsofts Active Directory oder mit eigenen, remote bedienbaren Installationswerkzeugen verteilt werden.

InfoWatch Device Monitor belastet den Prozessor des lokalen Computers nur sehr gering und unterbricht die tägliche Arbeit des Benutzers in keiner Weise.

Die Lösung verfügt über spezielle Selbstschutz-Tools und kann weder deinstalliert noch gestoppt werden, auch nicht von privilegierten Benutzern wie Systemadministratoren.



InfoWatch Device Monitor

Zusammenfassung

Informationssicherheit außerhalb des Unternehmensnetzwerks

InfoWatch Device Monitor wendet Security-Policies an, indem es Schattenkopien von vertraulichen Daten erstellt, die auf externe Laufwerke oder portable Speichermedien kopiert oder ausgedruckt werden, auch dann, wenn der Benutzer vorübergehend nicht mit dem Unternehmensnetzwerk verbunden ist. Nachdem die Arbeitsstation wieder mit dem Unternehmensnetzwerk verbunden ist, werden die gesicherten Daten an den InfoWatch Device Monitor Server übermittelt, der diese dann analysiert und detaillierte Reports darüber erstellt. Auf diese Weise stellt **InfoWatch Device Monitor** die Kontinuität der Anwendung von Security-Policies des Unternehmens und die Effizienz des Informationsschutzes auch im Falle der Mitarbeiter sicher, die sich außerhalb des Unternehmensnetzwerks befinden.

InfoWatch Device Monitor gibt dem Unternehmens-Management vollständige Kontrolle über die Kanäle, auf denen Daten nach außen gelangen können. Die meisten Unternehmen, die mit der Implementierung von **InfoWatch Device Monitor** begonnen haben, rüsten diese Lösung schließlich zu einem umfassenden Informationssicherheits-System wie **InfoWatch Traffic Monitor** auf.

InfoWatch Traffic Monitor verwaltet alle netzwerkbasieren Informationskanäle wie E-Mail, Internetforen, Chats, Instant Messengers und viele andere.

Kontakt:

www.infowatch.de
Tel.: +7 (495) 22 900 22
sales@infowatch.com
sales-oem@infowatch.com

Partner-Kontakte:

Österreich und Schweiz: sales-ach@infowatch.com, +49 (8152) 969340
Deutschland: sales-de@infowatch.com, +49 (4207) 689933
Benelux und Mittelmeerstaaten: sales-be@infowatch.com, +32 47792090