

XRayWatch

...und Sie sehen ALLES



itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de
info@itWatch.de

Datenlecks schließen

Wissen Sie welche Daten ausgetauscht werden? Mit **XRayWatch** schützt man firmeneigene Informationen vor dem Datenklau und das Firmennetz gegen kritische oder unerlaubte Inhalte, z.B. *Ink, pdf, embedded executables*.

Proaktiver Schutz vor dem Verbotenen

Unerlaubte Dateien sollen nicht in Ihr Netz kommen, im Klartext oder eingebettet in andere Objekte (verschlüsselte zip-Archive)? Mit **XRayWatch** definieren Sie, wer oder welche Anwendung welche Daten von wo lesen und wohin schreiben darf - im Netzwerk, lokal auf der Festplatte oder auf mobilen Datenträgern unter CITRIX®, auf Thin oder Fat Clients.

Überwachung des Erlaubten

Benutzer lesen und verändern Informationen. Verbote behindern dabei häufig das Tagesgeschäft und die Business Prozesse. Für sensible Information ist daher eine Beweis-sicherung erforderlich: Wer hat die Login.exe mit einem Trojaner gepatcht oder die Inhalte der Börsenmeldung vor der Veröffentlichung gelesen und mitgenommen? **XRay-Watch** beantwortet die dringlichen Fragen schnell und effizient.

Sicheres Löschen

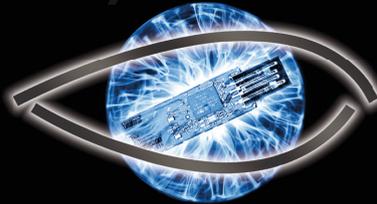
XRayWatch ermöglicht das sichere Löschen von Dateien, Ordnern und deren Metainformationen von Datenträgern, so dass diese auch forensisch nicht mehr rekonstruiert werden können.

XRayWatch überwacht die Dateizugriffe aller Benutzer und Anwendungen nach zentralen Richtlinien. Auf Netzwerkshares, lokalen Directories oder mobilen Datenträgern wie USB-Sticks, CD/DVD etc. werden die Rechte von Benutzern und Anwendungen unabhängig voneinander definiert. Weil die Namen der Dateien trügerisch sein können, bietet XRayWatch die detaillierte inhaltliche Kontrolle aller Dateien und die detaillierte Protokollierung aller Zugriffe. Zusammen mit PDWatch kann man definieren, wo und wann eine Verschlüsselung erzwungen wird.

👁️ Wer darf welche Dateien mit welcher Anwendung an welchem Ort wie bearbeiten ?

👁️ Eine generelle Unternehmensrichtlinie kann auf Basis von White-List oder Black-List beliebig verfeinert werden.

XRayWatch



und Sie sehen einfach ALLES

👁️ Dateiinhalte und nicht nur -namen werden geprüft
Virtualisierte Schleusen senken die Kosten

...und vieles mehr unter www.itWatch.de

Sichere Schleuse für den Rest

Lokale Schleusenfunktion: Entschlüsselung und Dekomprimierung in einer lokalen Quarantäne - dann werden die Inhalte im Klartext geprüft. Je nach Ergebnis, werden die Dateien geblockt und sicher gelöscht, freigegeben oder zur Ausführung an eine zentrale Schleuse weitergeleitet.

Zentrale Schleuse: Identisch zur ReCoBS-Definition des BSI wird die Ausführung von der Anzeige getrennt. Die Inhalte werden durch **XRayWatch** sowohl auf dem Remote controlled System als auch auf dem Client des Anwenders nach den zentralen Vorgaben kontrolliert, so dass kein Schadcode ins interne Netz gerät und der Anwender trotzdem alle aktiven Inhalte sicher nutzen kann.

Inhalte prüfen - nicht Dateinamen

Unternehmen überprüfen auf den Firewalls und Mail-Gateways die Inhalte der ausgetauschten Dateien. Warum nur dort? Umbenennung ist zwecklos: **XRayWatch** bietet mit seiner Pattern Prüfung die semantisch und syntaktisch beliebig genaue Prüfung der Inhalte einer Datei. Diese ist kundenseitig beliebig modifizierbar. Plug-ins erlauben das Einhängen von Drittprodukten - „Unternehmensvertraulich“ im Header und das unverschlüsselte Mitnehmen dieser Dateien ist verboten.

Compliance

§9 des BDSG fordert besonderen Schutz bei der Speicherung von personenbezogenen Daten auf portablen Datenträgern. Mit **XRayWatch** erkennen Sie die personenbezogenen Daten, verbieten die Auslagerung oder erzwingen eine Verschlüsselung z.B. mit **PDWatch**.

Lokaler Safe

Mit **XRayWatch** kontrollieren Sie, welche Daten in den Safe gehen und welche entnommen werden. Der Benutzer hat nur mit vertrauenswürdigen Anwendungen Zugriff auf die Daten im lokalen Safe. Mit **PDWatch** und **XRayWatch** setzen Sie komplexeste **Data Loss Prevention (DLP)** Anforderungen um.