

# ApplicationWatch

Wissen Was  
Wirklich Läuft!



**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](http://www.itWatch.de)  
[info@itWatch.de](mailto:info@itWatch.de)

## Haben Sie noch den Überblick?

Anwendungen tun nicht immer das, was der Anwender oder das Unternehmen will. Schadsoftware hat viele Ausprägungen, z.B.:

- ⦿ „Spielsoftware“, die einfach nur Zeit kostet
- ⦿ Software mit Schadsoftwareanteilen wie ein Mail-Plug-In oder eine modifizierte DLL, die eine Blindkopie jeder Mail in das Internet lädt
- ⦿ Lizenzrechtlich bedenkliche Software, z.B. Kopierprogramme, welche das Copyright aushebeln
- ⦿ Ressourcen werden entgegen der Unternehmensrichtlinie genutzt, z.B. WebEx, Skype oder 0900-Dialer, die hohe Kosten verursachen
- ⦿ Brennprogramme, die den Datenklau unterstützen
- ⦿ Angriffssoftware, welche automatisch Schwachstellen in den Firmennetzen analysiert und ausnutzt oder Passworte und Schlüssel ausspäht

Das sind nur einige Gründe, den Überblick zu behalten, wer welche Anwendungen in Ihrem Unternehmen zu welchem Zweck nutzt. Die unerwünschten Aktionen gilt es zu blockieren!

## Zentrales Echtzeitmonitoring

**ApplicationWatch** liefert Ihnen alle Anwendungen (auch portable Apps!) inklusive Nutzungsstatistiken zu Häufigkeit und Verwendungsdauer, die Lokation von der gestartet wurde und den Ort der Ausführung mit Zeitpunkt wann gestartet und beendet. Der Versuch verbotene Anwendungen auszuführen steht im Log. Sie können aber auch nur die neuen - noch unbekannt - Anwendungen in Echtzeit an die Zentrale melden.

## Data Loss Prevention (DLP)

Unsichere Anwendungen dürfen vertrauliche Inhalte nicht lesen und keine ausführbaren Dateien modifizieren oder dürfen nur in einer „unsicheren zentralen Schleuse“ gestartet werden. Ein Browser darf nur bestimmte Plug-Ins aus dem Internet laden und keine sensiblen Daten ins Internet hochladen. Aktiver Code, egal woher dieser stammt und wie er verpackt ist, wird automatisch in einer „unsafe Area“ ausgeführt, ohne dabei die produktive Umgebung zu gefährden. Den Rechneraum und die Inhalte überwacht itWatch. Skype darf nur auf seine Konfigurationsdaten zugreifen! Schützen Sie so auch alte Anwendungen - Client Server oder lokal - ohne den Code anzufassen vor neuen Angriffen. Geben Sie vertrauenswürdigen Anwendungen - z.B. Ihren CAD Programmen - die Zugriffsrechte, die der Anwender nicht hat und schützen damit Ihre Daten vor dem unberechtigten Mitnehmen.

**Mit ApplicationWatch bestimmen Sie, welche Programme dem Anwender in welcher Situation auf welchem PC zur Verfügung stehen, wo diese ausgeführt werden (Virtualisierung) - und auf welche Dateien diese Anwendung zugreifen darf. ApplicationWatch verhindert Malware, Spyware, malicious Code und nichtlizenzierte Software und protokolliert kritische Zugriffe der Anwendungen.**

- ⦿ IST-Zustand aller ausgeführten Anwendungen mit Nutzungsstatistiken erlaubt kosteneffizientes Black-List-Blocking neben White-List
- ⦿ Einfaches Ausschalten sämtlicher Schadsoftware



... und Sie definieren was läuft!

- ⦿ Kein Upload vertraulicher Daten über Browser oder ftp, protokollieren von sensiblen Email-Anhängen

...und vieles mehr unter [www.itWatch.de](http://www.itWatch.de)

## Black- und White-List-Blocking

Sie können je Arbeitsplatz und Nutzungsszenario zwischen White-List und Black-List wählen. Im Black-List-Modus erlaubt es das Alerting der „neuen“ noch unbekannt Anwendungen, sofort zu reagieren und neue Anwendungen sofort auf die „Black-List“ zu setzen. Applikationen nur situationsbezogen zulassen, z.B. Skype nur im Hotel, oder eine Selbstfreigabe für Anwendungen, die dann sofort unter vollständigem Monitoring liegen oder virtualisiert werden - das erlaubt den kostengünstigen Betrieb.

## Schutz für alle Arbeitsplätze

Die Kontrolle der portablen Anwendungen (portable Apps) ist auch unter CITRIX® möglich - bei beliebigen Thin oder Zero Clients. Die **Endpoint Security Suite** der **itWatch** schützt auch vor Anwendungs-Plug-Ins, z.B. WebEx im Internet Explorer, und setzt zusammen mit **XRyWatch** einen eigenen Rechneraum für jede Anwendung durch.