



Die itWatch entwickelt seit 10 Jahren in Deutschland IT-Sicherheits Innovationen auf Basis eines Software Patents. Das Software Patent 10152121.9-53 trägt beim deutschen Patentamt den Titel "Regelbasierte Verarbeitungskontrolle mobiler Information". Grundgedanke ist es, Grundschutz nach BSI (und erweiterten Schutz), Compliance, Security Awareness in Echtzeit und die dafür nötigen Werkzeuge des Systemsmanagements aus einer Hand mit zentralem Management zur Verfügung zu stellen, um Kosteneffizienz im Betrieb zu ermöglichen.

Die Endpoint Security Suite der itWatch umfasst folgende Module:

- 👁️ [DeviceWatch](#), mit dem Sie alle Devices (externe und eingebaute Geräte) und alle Ports (USB etc.) kosteneffizient und sicher nutzen können - auch die situationsbezogene Freigabe von Netzwerkverbindungen ist enthalten - z.B. WLAN nur "unterwegs" erlauben.
- 👁️ [XRayWatch](#), mit dem Sie Dateien beim Austausch mit mobilen Datenträgern oder Netzwerkshares inhaltlich kontrollieren, protokollieren und bei Bedarf blockieren
- 👁️ [PDWatch](#), mit dem Sie Verschlüsselung beim Export von Dateien auf beliebige Datenträger erzwingen können; die Verwendung eines oder mehrerer Unternehmensschlüssel schützt sicher vor Datenlecks (Data Loss); der persönliche Schlüssel erlaubt den sicheren Transport auf Drittsysteme
- 👁️ [ApplicationWatch](#) meldet alle "neuen" Anwendungen in Echtzeit – auch portable Anwendungen. Verbote benutzer- und gruppenspezifisch natürlich mit Black- und White-List möglich, Plug-Ins – wie z.B. WebEx als plug-In in den Internetexplorer - können dediziert verboten oder erlaubt werden. Als weltweite Alleinstellung kann der Rechteraum der Anwendung unabhängig von den Benutzerrechten definiert werden – mit mehr oder weniger Rechten als der Benutzer.
- 👁️ [CDWatch](#), organisiert die Nutzung von CDs/DVDs im Netz einfach und sicher
- 👁️ [DEvCon](#), mit dem Sie Ihre Sicherheitsrichtlinien und die Freiräume für Ihre VIPs zwischen reiner Awareness und vollständiger Blockade automatisch organisieren können - übrigens ganz ohne Consulting! (siehe auch [Presse-Artikel](#) unten); die DEvCon verfügt zusätzlich über Echtzeit-Monitoring und Reporting sowie viele weitere Mehrwerte.

Die Fact Sheets zu diesen Modulen (der Einfachheit halber haben wir Ihnen diese als Links hinterlegt) oder weitere technische Details senden wir Ihnen natürlich auch gerne zu. Sie finden diese unter anderem auf unserer Website www.itWatch.de.

Technische Innovationen der itWatch Endpoint Security

- 👁️ **Schleusenfunktion lokal:** Entschlüsselung und Dekomprimierung in einer lokalen Quarantäne -- erst dann können die Inhalte im Klartext geprüft werden. Je nach Ergebnis werden die Dateien geblockt und sicher gelöscht, Zur Prüfung an Dritte weitergeleitet oder frei gegeben. Kein Zugriff der Benutzer während der Überprüfung. Der Rechner kann nicht durch Schadcode infiziert werden. Zusätzliche Hardware und lange Wege sind unnötig.
- 👁️ **Spyware bleibt draußen:** Angreifer schleusen Schadcode verborgen in eigentlich erlaubten Dateiformaten über Email, Web oder auch USB-Sticks und durch die Ausnutzung von Schwachstellen in Programmen vom Benutzer unbemerkt in das Unternehmen ein. Dieser wird unter Nutzerrechten im Hintergrund ausgeführt und überträgt die sensiblen Daten verschlüsselt ins Internet. itWatch blockt den Schadcode, egal über welchen Weg er auf den PC kommt. [Mehr...](#)
- 👁️ **Effiziente Festplatten-Verschlüsselung:** Die Verschlüsselung der Nutzdaten bringt den Schutz vor Diebstahl und Verlust ohne die Softwareverteilung zu behindern. Applikationskontrolle stellt die Integrität der gestarteten Anwendungen sicher. [Mehr...](#)
- 👁️ **Mandantenfähige Administration:** Die Administration hierarchisch nach Standorten oder Sparten organisieren und dezentralen Administratoren unterschiedliche Aufgaben und Berechtigungen zuweisen.
- 👁️ **Data Loss Prevention:** Der Verfassungsschutz meldet vermehrte Computerspionage-Angriffe. Das Einschleusen von Schadcode nimmt in der Angriffsstatistik die ersten Plätze ein. ItWatch schützt gegen alle diskutierten Angriffe (Ink, dpf, IE, zip ...). [Mehr...](#)

Ebenso auf unserer Webseite finden Sie die folgenden Artikel und Anwenderberichte, die einige der angesprochenen Themen illustrieren:

- 👁️ [DLP und Endpoint Security - Lösungen](#)
 - stellt die Zusammenhänge zwischen IT-Sicherheit, gesetzlichen Rahmenbedingungen, Compliance und Unternehmenskultur dar.
- 👁️ [Null Administration - volle Sicherheit](#)
 - beschreibt die Möglichkeiten, Compliance ohne täglichen Aufwand in der Administration zu realisieren, wenn dem VIP oder "erwachsenen" Benutzer gewisse Freiräume automatisiert zugestanden werden
- 👁️ [Security Awareness in Echtzeit](#)
 - schult den Nutzer "wenn nötig" also "on demand", schafft gleichzeitig Compliance und reduziert den administrativen Aufwand
- 👁️ [Verschlüsselung unterwegs](#)
 - Zeigt die Anforderungen des neuen Bundesdatenschutzgesetzes und Lösungen bei dem Transport mobiler Daten
- 👁️ [Verschlüsselung: Transparent UND sicher?](#)
 - Wie transparent darf eine sichere Verschlüsselung sein – welche Transparenz ist für die sichere Verwendung durch den Anwender erforderlich?
- 👁️ [Endpoint Security - leicht](#)
 - Beschreibt best practices bei der Projektierung mit den verschiedenen Phasen „Einsammeln von Information“, Zieldefinition, „Weicher roll-out“ und "Scharfschalten“, und der Integration in das Risk-Management.

- 🔗 Datenschutzverstöße sicher vermeiden
 - Die Hauptursachen für Verstöße gegen den Datenschutz sind verbesserte Angriffsverfahren der Täter, mangelndes Risikobewusstsein oder technische Kenntnis der Anwender, aber auch vorsätzlicher Datendiebstahl von internen Mitarbeitern. Strategien zur Vermeidung gemäß der Empfehlungen des BSI werden dargestellt
- 🔗 Das Ende der Dienstvereinbarung
 - Die Angriffe der letzten Zeit (Ink, Stuxnet, pdf-Exploit,...) haben gezeigt, dass technische Unterstützung notwendig Dienstvereinbarungen unterlegen müssen
- 🔗 Mehr Kontrolle – weniger Kosten
 - Ein **Anwenderbericht** der ivv – (IT-Dienstleister für öffentlich-rechtliche Versicherungsunternehmen)
- 🔗 Flexible Lösung für umfassenden Netzwerkschutz
 - Ein **Anwenderbericht** der Deutschen Rückversicherung (Rückversicherungsunternehmen mit Sitz in Düsseldorf und Zürich)

DeviceWatch wurde in Deutschland ohne den Zukauf von Fremdanteilen entwickelt, so dass das Know-how und alle Rechte bei der itWatch GmbH, München, liegen. Einen Auszug unserer Referenzkunden legen wir bei. Mehrere Einzelinstallationen umfassen jeweils weit über 100.000 Clients. Nach mehrmonatigen Sicherheitsprüfungen hat DeviceWatch die Tests für eine Verschlusssache-Umgebung im militärischen Bereich mit „Keine Verletzbarkeit“ bestanden und es wurde eine Vollausrüstung bestellt. Neben Installationen in VS-NfD klassifizierten Umgebungen gibt es auch mehrere tausend Lizenzen in Umgebungen, die bis zu geheim klassifiziert sind. Die Sparda Bank und Landesbank Baden Württemberg haben sich nach ausführlichen Marktuntersuchungen für den Kauf von je 10.000 Lizenzen entschieden. Das Bayerische Landeskriminalamt hat nach einer öffentlichen Ausschreibung eine flächendeckende Ausstattung für alle Polizeistationen in Bayern bestellt (20.000 Arbeitsplätze). Bei allen öffentlichen Ausschreibungen (z.B. Bundesministeriums der Justiz, Deutsche Rentenversicherung, Straßen NRW, Rhein Neckar Kreis, Wasserschiffahrtsämter ...) zur Portkontrolle hat DeviceWatch den Zuschlag erhalten. Die Allianz AG hat für ihren Außendienst 40.000 Lizenzen PDWatch zur Verschlüsselung von Daten auf mobilen Medien seit 2005 im produktiven Einsatz – ohne Mitarbeiterschulung und ohne Fehlermeldungen.

itWatch hat mit der Endpoint Security Suite viele internationale Projekte gewonnen, z. B. mit über 100.000 Lizenzen die größte Device & Content Control Projektierung öffentlicher Auftraggeber in Europa, Benchmark aller Standorte eines europäischen Unternehmens mit 130.000 Mitarbeitern. Die Ausschreibung von General Electric für über 300.000 PCs haben wir als "bestes Produkt" gewonnen. Auf Grund der hohen Mehrwerte und der Zufriedenheit mit den Produkten hat sich die Polizei Sachsen in 2009 zu einem Upgrade auf eine hochwertige Lizenz für über 10.000 Arbeitsplätze entschlossen. Aktuell befindet sich das Produkt nach einer mehrmonatigen Marktevaluierung und einer folgenden Sicherheitsprüfung im Roll-Out bei der Bundeswehr auf 100.000 Arbeitsplätzen.