

# VulnWatcher – Swiss made Vulnerability Management schützt Ihre IT-Infrastruktur vor unerlaubten Zugriffen

## IT-Infrastrukturen haben sicherheitsrelevante Schwachstellen!

IT-Systeme (Hard- und Software) von Schweizer Unternehmen und Privatpersonen weisen bei Verbindungen ins Internet erschreckend viele, teilweise sicherheitsrelevante Schwachstellen auf. Der Swiss Vulnerability Report ermittelte im Durchschnitt pro aktive IP-Adresse über 70 potenzielle Einfallstore für Malware (Viren, Würmer, Botnets, Trojaner, etc.), Hacker, Datendiebe, Geheimdienste und Wirtschaftsspione, welche Daten Ihres Computersystems verändern, entwenden oder zerstören können. Gegen 95% dieser Schwachstellen betreffen die weit verbreiteten Linux-Systeme. Besondere Gefährdungen wurden in öffentlichen Verwaltungen, im Gesundheitswesen, bei Internet-Service-Providern und Finanzdienstleistern geortet. Gefährdet sind aber grundsätzlich alle internet basierten IT-Systeme: eine undichte Stelle genügt! Und es werden täglich mehr...

## Sicherheitslücken können erkannt und behoben werden!

Schwachstellen sind Sicherheitslücken, die durch fehlerhafte oder falsch konfigurierte Systeme, fehlerhafte Programmcodes oder nicht aktualisierte Infrastrukturen entstehen. Sie gefährden die Integrität, Verfügbarkeit und Vertraulichkeit von Computersystemen. Damit Sicherheitslücken in einer Software rechtzeitig erkannt und geschlossen werden können, ist die regelmässige, vorbeugende Prüfung der Betriebssysteme und der Applikationen unerlässlich. Firewalls und Antivirus-Programme sichern Ihre Systeme ungenügend ab. Laufende Veränderungen der IT-Konfiguration durch neu eingeführte Programme, Updates usw. sowie der angeschlossenen Systeme und die stetig wachsende Zahl von potentiellen Schwachstellen destabilisieren den Sicherheitszustand jedes IT-Systems.

## Die effiziente Lösung: VulnWatcher

Vulnerability Management (Schwachstellen Management) ist ein zyklischer, sich stetig wiederholender Prozess, der die Identifizierung, Klassifizierung und Behebung von Schwachstellen in der gesamten IT-Infrastruktur ermöglicht. Vulnerability Management hat die Verringerung der Anfälligkeit der IT Infrastruktur auf Angriffe von innen und aussen zum Ziel, bevor Angriffe Schaden anrichten können.

VulnWatcher ist die proaktive Sicherheitsmassnahme und damit ein tragender Baustein des IT-Sicherheitskonzeptes. Mit VulnWatcher werden Schwachstellen in einem Netzwerk inventarisiert, identifiziert und nach Priorität zur Behebung vorbereitet, bevor sie missbraucht werden können - und das in einem fortlaufenden Prozess!

## VulnWatcher schützt KMU und grosse Unternehmen

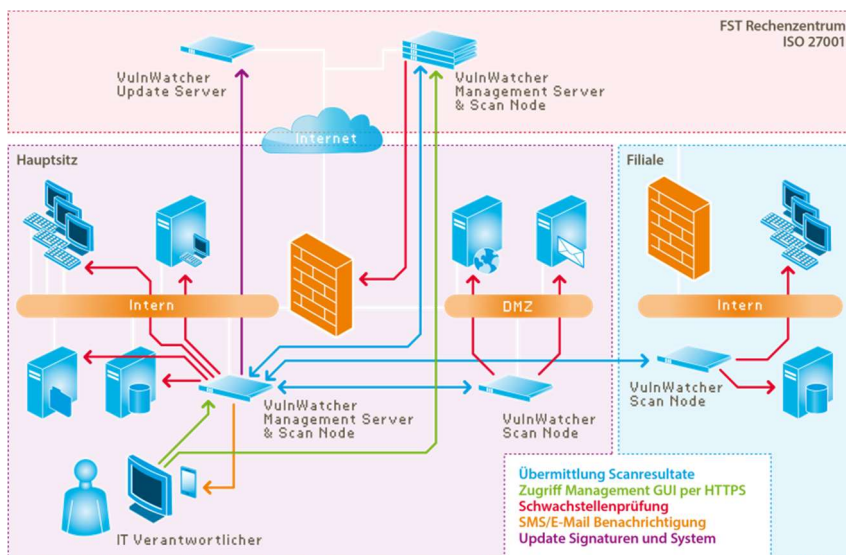
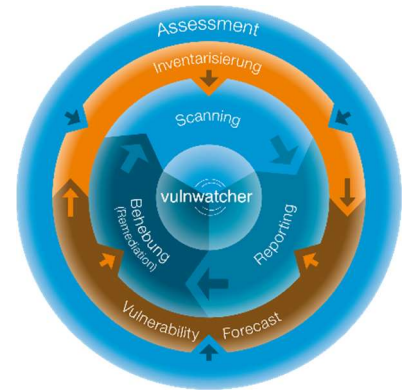
VulnWatcher kann und sollte in jeder IT Infrastruktur regelmässig zum Einsatz kommen.

VulnWatcher ist unabhängig von Betriebssystemvorgaben oder Technologien einsetzbar.

VulnWatcher überprüft alle in der IT Infrastruktur integrierten Hardware-Komponenten und die installierte Software auf Schwachstellen.

VulnWatcher kann als Software-as-a-Service (SaaS) zur externen Prüfung der IT Infrastruktur eingesetzt werden. In diesem Fall ist keine zusätzliche Hard- oder Software in die IT Infrastruktur zu integrieren und zu betreiben. Die Überprüfung der IT Infrastruktur auf Schwachstellen kann jederzeit und unmittelbar vorgenommen werden.

VulnWatcher-on-an-Appliance wird vorwiegend zur internen Prüfung der IT Infrastruktur eingesetzt. Dazu wird zusätzliche Hard- und Software (eine sog. Appliance) in die zu überprüfende IT Infrastruktur integriert.



VulnWatcher-on-an-Appliance ermöglicht es, eine IT Infrastruktur von innen und von aussen zu überprüfen und zu überwachen. Kombinierte externe und interne Prüfung ergeben einen umfassenden und zuverlässigen Schutz vor Schwachstellen.

Zudem kann VulnWatcher auch in einer virtualisierten Umgebung implementiert werden (VulnWatcher-on-Virtual-Machine).

### Was ist der konkrete Nutzen von VulnWatcher?

- Erhöhung der Compliance & IT-Sicherheit durch regelmässige Schwachstellenüberwachung (proaktive Verifizierung, Bewertung und Behebung von Schwachstellen)
- Verbesserung der Effizienz des IT-Systems
- Schutz der Unternehmensdaten vor unerlaubtem Zugriff und dadurch Investitionsschutz mit mittel- und langfristigen Kosteneinsparungen sowie Vermeidung von Imageschäden und Ertragseinbussen
- Prozessoptimierung durch automatisierte Scans mit integrierter individuell definierbarer Risikobeurteilung, Alarmierung und Tracking-System
- Sichere Datenhaltung unternehmensintern oder in unserem VulnWatcher-Rechenzentrum in der Schweiz
- Ständig aktualisierter, integrierter Feed mit über 100'000 IT-Schwachstellen
- Stufengerechtes Reporting bis hin zum IT-Revisionsbericht

### VulnWatcher Versionen und Merkmale

	Professional	Enterprise
Scan extern/intern	Externe Scans	Externe und interne Scans
Anzahl Benutzer	Max. 5 Benutzer	unlimitiert
Lizenzmodell	Host und Scan Credit Max. 100 Host Credits / 100 Scan Credits	Host und Scan Credits unlimitiert
Mandantenfähigkeit	Ja	Ja
Reporting	Standard-Reports	Individuelle und Standard-Reports
Scan Engines	OpenVAS	OpenVAS , Arachni, Nessus (Optional) und Hydra
VulnWatcher-on-an-Appliance	Nein	Ja
VulnWatcher-on-Virtual Machine	Nein	Ja
Schnittstellen zu externen Applikationen	Nein	Ja
Assessment	Top 1000 Ports Ohne Historie	Keine Limitierung Mit Historie
Web Application Scanning	Ja	Ja
Benutzerdefinierte Reports	Nein	Ja

### Kernfunktionalität

- Zentrale Administration
- Integriertes Ticket-System und Schnittstellen zu externen Ticket-Systemen
- Einfaches, skalierbares Lizenzmodell
- Rollenbasierte Gruppenrichtlinien (ACL)
- Leistungsfähige Inventarisierung und Assessment der IT Infrastruktur (IPv4/IPv6)
- Diverse Schnittstellen für eine optimale Integration in die bestehende Umgebung
- Zuverlässige Erkennung von Schwachstellen und Elimination von False Positives und False Negatives
- Rescan von einzelnen Schwachstellen
- Standardisierte oder voll-individualisierte Risikoberechnung und Priorisierung
- Benachrichtigung von Personen und Gruppen per SMS und E-Mail gemäss individuell definierten Schwellenwerten
- Tägliche Aktualisierung der Schwachstellen-Datenbank
- Skalierbare Lösung mit definierbarer Kommunikationsrichtung für Scanner
- VulnWatcher-on-an-Appliance voll skalierbar und clusterfähig
- Integriertes Backup
- Lifetime\* Support für Appliance und Software (\* lifetime: solange Appliance und Software genutzt werden)

### Weitere Informationen

Verkauf: [sales@first-security.com](mailto:sales@first-security.com)  
 Support: [support@first-security.com](mailto:support@first-security.com)  
 Internet: <http://www.first-security.com>

Der Einsatz von VulnWatcher ermöglicht es unseren Kunden, das Gefahrenpotential, welchem die IT Infrastruktur täglich ausgesetzt ist, zu erfassen, zu bewerten, zu bearbeiten und zu vermindern. VulnWatcher-as-a-Service prüft und überwacht den Perimeter der IT Infrastruktur vor unerlaubtem Zugriff von aussen. Mit VulnWatcher-on-an-Appliance und VulnWatcher-on-Virtual-Machine kann die IT Infrastruktur von aussen wie auch von innen überprüft und überwacht werden.

### Über First Security Technology (FST): Swiss Made Vulnerability Management!

FST gegründet 2001 mit Sitz in Chur ist der führende Hersteller von Schwachstellen-Management-Lösungen in der Schweiz. FST entwickelt Sicherheitslösungen als Software-as-a-Service, Virtual-Machine-basierend oder als Appliance und vertreibt diese über ein Netz von ausgewiesenen Händlern und Distributoren. FST's Sicherheitslösungen umfassen vollautomatische Schwachstellenerkennung, IT Infrastruktur-Assessment, Schwachstellenbeseitigung und -überwachung sowie IT Compliance erfüllende Reporting-Mechanismen.

Weitere Informationen: <http://www.first-security.com>