

# redNET Secure Client/Server

## Leistungsbeschreibung

### 1 Einleitung

Unser redNET Secure Client basiert auf dem mehrfach ausgezeichneten Antivirus-Programm von F-Secure. Die Software erkennt und entfernt schädliche Inhalte wie Viren, Würmer, unerwünschte Internet-Inhalte und mehr, aus dem E-Mail- und Daten-Verkehr.

Ein redNET Secure Client arbeitet als Filter zwischen dem Internet und dem Netzwerk des Kunden. Er verfügt über ein Regelwerk, welches die Filtereigenschaften gemäss der Security Policy und dem Netz und den Systemvoraussetzungen des Kunden abbildet. Mögliche Angriffe, welche sich auf IP/ICMP (Netzwerk-Layer) oder TCP/UDP (Transport-Layer) beziehen, werden innerhalb des Secure Client erkannt und abgewehrt. Dies gilt für Angriffe auf den Secure Client und die zu schützenden Netzwerke.

### 2 Leistungsumfang

redNET Secure Client ist ein Softwaredienst.

- Grundkonfiguration und Nutzung des Secure Client
- Automatische Updates der Secure Client Software
- Automatische Updates der Secure Client Signaturen
- Sicherung der aktuellen Secure Client-Konfiguration
- Permanente Überwachung Ihrer Secure Clients

#### 2.1 Definitionen

##### 2.1.1 Grundkonfiguration

Die Grundkonfiguration des Secure Clients erfolgt auf Basis der Standardkonfiguration und der mit dem Kunden abgestimmten Security Policy.

##### 2.1.2 Automatische Update der Software

Updates werden, wenn dies aus Sicherheitsgründen oder zum Bereitstellen neuer Funktionen nötig ist, zeitnah eingespielt, sobald der Hersteller der eingesetzten Komponente solche zur Verfügung stellt. redIT hat keinen Einfluss auf die Bereitstellung von Updates durch einen Hersteller.

##### 2.1.3 Automatisches Update der Signaturen

redIT verwendet die offiziell zur Verfügung gestellten Signaturen des Herstellers und stellt den Secure Client auf ein automatisches Update ein, um Funktionsweise und Tüchtigkeit der Signaturen des Herstellers zu gewährleisten. redIT hat keinen Einfluss auf die Bereitstellung von Updates durch einen Hersteller.

### 2.2 Leistungen im Detail

#### 2.2.1 Konfigurationsänderungen

Eine Änderung an der Konfiguration kann nur schriftlich per E-Mail an [redNET.services@redIT.ch](mailto:redNET.services@redIT.ch) erfolgen. Für die Bestätigung wird redIT den Kunden telefonisch kontaktieren. redIT wird Konfigurationsänderungen nur von den auf der Security Policy aufgeführten Personen akzeptieren. Änderungen können nur innerhalb der Betriebszeiten durchgeführt werden. Die Reaktionszeit beträgt werktags acht Stunden. Der Kunde hat nicht die Möglichkeit, die Konfiguration selber zu verändern.

### 2.2.2 Haftung

Datentransfers, welche nicht den Secure Client durchlaufen, entziehen sich der Kontrolle durch den Secure Client. Ebenso kann der Secure Client keine verschlüsselten oder mehrfach komprimierten Inhalte nach schadhafte Bedrohungen untersuchen. Der Service gewährleistet nicht die Sicherheit des Kundennetzwerkes sondern stellt einen Sicherheitsmechanismus zur Verfügung. Ein Secure Client kann keinen Schutz vor unbekanntem Angriffen geben.

## 3 Service Levels

Garantierte Verfügbarkeit	99.5%
Monitoring/Alarmierung	7x24h (falls Option Monitoring/Alarmierung)
Störungsannahme	7x24h
Reaktionszeiten (Mo – Fr von 08.00 – 12.00 und 13.00 – 17.00)	Max. 2h
Reaktionszeiten (Mo – Fr von 17.00 – 08.00, Sa, So, Feiertage)	Max. 4h (falls Option Pikettbereitschaft)

Im Störfall ist der Helpdesk von Montag bis Freitag von 08.00 – 12.00 und 13.00 – 17.00 Uhr (ausgenommen gesamtschweizerische und lokale Feiertage) unter Telefon 0848 000 801 erreichbar. Ausserhalb dieser Zeiten können Sie jederzeit eine E-Mail an: [redNET.services@redIT.ch](mailto:redNET.services@redIT.ch) absetzen.

### 3.1 Reaktionszeit

Die Reaktionszeit ist der Zeitraum zwischen der Störungsmeldung durch den Kunden und der Bestätigung der Störungsannahme durch das für die Störungsbehebung verantwortliche Team.

### 3.2 Wartungsarbeiten an den redIT Anlagen

Die periodische Wartung an den Support- und Überwachungseinrichtungen der redIT kann eine geplante Unterbrechung dieser Services bewirken. Die Wartungen werden während einem definierten Zeitraum, dem so genannten Wartungsfenster durchgeführt und mindestens 2 Tage im Voraus angekündigt. Die Wartungsfenster sind auf den ersten und dritten Mittwoch des Monats von 18.00 bis 06.00 Uhr festgelegt.

In dringenden Fällen kann eine ungeplante Wartung ausserhalb des offiziellen Wartungsfensters notwendig sein. In solchen Fällen werden die Kunden über den Beginn und das voraussichtliche Ende der Wartung sofort informiert.