

Leistungsbeschreibung – Managed Antivirus

Das Systemhaus 2F-IT bietet ihren Kunden einen Service zur aktiven und kontinuierlichen Betreuung des Antivirenmanagements und stellt eine Next Generation Endpoint Protection Software zur Verfügung, die Clients und Server im Netzwerk umfassend gegen modernste Bedrohungen absichert.

Folgende Funktionen werden bereitgestellt:

Next Generation Endpoint Protection:

- ✓ Antivirus
- ✓ Verhaltensanalysen
 - Ermittelt verdächtige Verhaltensweisen und kann so Malware aufspüren, die speziell entwickelt wurde, um traditionelle Lösungen zu überlisten.
- ✓ Traffic Detection
 - Nimmt eine Vorfilterung des gesamten HTTP-Datenverkehrs vor und verfolgt verdächtigen Datenverkehr sowie den Dateipfad des Prozesses, der den schädlichen Datenverkehr sendet.
- ✓ Web Control
 - Web-Filterung auf Basis von Kategorien, die sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks durchgesetzt wird.
- ✓ Application Control
 - Point-and-Click-Blockierung von Anwendungen basierend auf einer Kategorie oder einem Namen.
- ✓ Device Control
 - Verwalteter Zugriff auf Wechselmedien und mobile Geräte
- ✓ Data Control
 - Data Loss Prevention (DLP) mit vorkonfigurierten oder individuellen Regeln.

Intercept X*:

- ✓ Kombination aus modernen und traditionellen Techniken
 - Deep-Learning-Technologie (neuronale Netzwerke)
 - Bei der in Intercept X integrierten künstlichen Intelligenz handelt es sich um ein neuronales Netzwerk – eine erweiterte Form des

maschinellen Lernens. Dieses Netzwerk ist in der Lage, sowohl bekannte als auch unbekannte Malware komplett ohne Signaturen zu erkennen.

- Dank Deep Learning ist Intercept X intelligenter, skalierbarer und leistungsstärker als Sicherheitslösungen, die sich allein auf herkömmliches Machine Learning oder eine signaturbasierte Erkennung verlassen.

- Exploit Prevention
 - blockiert die Exploits und Verfahren, die zur Verbreitung von Malware, zum Diebstahl von Zugangsdaten und zum Aushebeln von Erkennungsmechanismen genutzt werden. So haben Hacker und Zero-Day-Angriffe keine Chance mehr, in Ihr Netzwerk zu gelangen.
- CryptoGuard Anti-Ransomware
 - Schützt Endpoints vor Ransomware-Angriffen
 - Setzt verschlüsselte Dateien automatisch in ihren Ursprungszustand zurück, ohne dass Daten verloren gehen.
 - Stoppt lokale und Remote-Dateiverschlüsselungen.
- Forensische Systembereinigung
- Grafische Malware Auswertung
- Protokollierung der Malware (Dateien, Prozesse, Pfade, Registrywerte)

Was leistet 2F-IT:

✓ **Verwaltung und Monitoring**

- 2F-IT installiert eine Endpoint-Protection Software und überprüft regelmäßig den Virenschutz auf Aktualität und Integrität.
- 2F-IT konfiguriert die Endpoint Protection Software Richtlinien und Einstellungen nach best practice und passt diese bei Bedarf an individuelle Anforderungen ihrer Kunden an.
- Falls ein Neustart des Client oder Server notwendig sein sollte, wird dies nach Absprache durch 2F-IT oder selbständig vom Kunden durchgeführt.
- Software und Lizenzen werden von 2F-IT ihren Kunden zur Verfügung gestellt und aktualisiert.

✓ **Reaktion auf Vorfälle bei Clients und Servern:**

- Nach einer Alarmierung bei kritischen Vorfällen wie Virusfund, Botnet Erkennung, Verschlüsselungstrojaner oder ähnlich, meldet sich 2F-IT bei ihren Kunden, um die Fehlerbehebung abzustimmen. Dies kann per E-Mail oder telefonisch erfolgen.
Die Fehlerbeseitigung ist nicht Bestandteil dieses Leistungspakets und wird separat abgerechnet.

Der Kunde wurde darauf hingewiesen, dass der Einsatz einer Antiviren-Software nicht bedeutet, dass jegliche Schadsoftware vom System ferngehalten werden kann. Es gibt immer einen zeitlichen Verzug zwischen Bekanntwerden einer neuen Schadsoftware und dem Anpassen der Software durch den Hersteller. In dieser Zeit ist der Schutz gegen diese Schadsoftware möglicherweise nicht gegeben.

Die Beseitigung eines Virenbefalls und dessen Folgen sind nicht Bestandteil des Paketes und werden separat abgerechnet.

- **Monatlicher Bericht über Monitoring**

- Der Kunde erhält auf Wunsch einen monatlichen Bericht über Antivirus-Ergebnisse und Alarmierungen per E-Mail.

Alle nicht explizit in dieser Leistungsbeschreibung ausgewiesenen Leistungen sind optionale Leistungen und nicht Bestandteil dieser Leistungsbeschreibung.

*Intercept X ist nur in den Paketen Premium und Intercept X enthalten.