

Leistungsbeschreibung -- Endpoint Security Mobile (CrowdStrike)

EXT IT GmbH -- Vahrenwalder Str. 271, 30179 Hannover

Hinweis: Diese Leistungsbeschreibung richtet sich ausschließlich an Unternehmer i.S.d. § 14 BGB. Verträge mit Verbrauchern i.S.d. § 13 BGB werden nicht geschlossen.

1. Servicebezeichnung

Endpoint Security Mobile (CrowdStrike)

2. Servicebeschreibung

Der Service Endpoint Security Mobile umfasst die Lizenzierung, Bereitstellung und den Betrieb der Bedrohungserkennung für mobile Endgeräte (iOS/iPadOS und Android) auf Basis von CrowdStrike. Die Schutzanwendung erkennt Phishing- und Schadlinks, schadhafte Anwendungen sowie unsichere Netzwerkverbindungen und bewertet fortlaufend den Sicherheitszustand des Geräts.

Der Service ist **eigenständig buchbar** -- auch für Geräte, die der Auftraggeber selbst über ein eigenes Mobile Device Management verwaltet (z.B. Microsoft Intune). Er kann alternativ als Zusatzleistung innerhalb des Services Managed Service MDM in den Stufen Silber und Gold gebucht werden; in der Stufe Platin ist er bereits enthalten (abrufbar unter ext-it.tech/leistungen). Der Leistungsumfang ist in allen Fällen identisch.

2.1 Abgrenzung zu Endpoint Security für Clients und Server

Dieser Service ist **nicht** mit dem Service Endpoint Security (CrowdStrike MDR Complete) für Windows-Clients und Server identisch und ersetzt ihn nicht.

iOS/iPadOS und Android lassen den Systemzugriff, den eine vollständige Endpoint Detection and Response erfordert, nicht zu. Dieser Service leistet daher **keine** prozessbasierte Bedrohungserkennung und **keine** Managed Detection & Response mit 24/7-Analystenteam. Erbracht wird die in Abschnitt 3.1 beschriebene Bedrohungserkennung auf Anwendungs-, Netzwerk- und Konfigurationsebene.

3. Leistungsumfang

3.1 Basisleistungen

- Lizenzierung der CrowdStrike-Schutzanwendung für die vereinbarte Anzahl mobiler Endgeräte
- Bereitstellung und Betrieb des CrowdStrike-Mandanten (Tenant) für den Auftraggeber
- Bereitstellung der Konfiguration für die Verteilung der Schutzanwendung über das Mobile Device Management (siehe §5.1)
- Erkennung und Abwehr von Phishing- und Schadlinks
- Erkennung schadhafter und unsicherer Anwendungen auf dem Gerät
- Erkennung unsicherer Netzwerkverbindungen (z.B. manipulierte WLAN-Zugangspunkte, abgefangene Verbindungen)
- Erkennung manipulierter Geräte (Jailbreak, Root) und veralteter Betriebssystemstände
- Fortlaufende Bewertung des Gerätesicherheitszustands
- Weiterleitung sicherheitsrelevanter Meldungen an den vom Auftraggeber benannten Ansprechpartner
- On- und Offboarding von Geräten im CrowdStrike-Mandanten

3.2 Enthaltene Tätigkeiten

Tätigkeit	Beschreibung	Intervall
Bereitstellung	Einrichtung des Mandanten und der Verteilkonfiguration für das MDM	Bei Onboarding
Richtlinienpflege	Pflege der Erkennungs- und Reaktionsrichtlinien gemäß Herstellerempfehlung	Laufend
Bedrohungserkennung	Prüfung von Links, Anwendungen, Netzwerkverbindungen und Gerätezustand	Kontinuierlich
Meldungsweiterleitung	Weitergabe sicherheitsrelevanter Meldungen an den Ansprechpartner des Auftraggebers	Bei Vorfall
On-/Offboarding	Anlage und Entfernung von Geräten im CrowdStrike-Mandanten	Bei Bedarf

3.3 Haftung

Die Buchung dieses Services hat keinen Einfluss auf die gemäß §7 AGB geregelte Haftung. Eine darüber hinausgehende Haftung von EXT IT für Schäden aus Schadsoftware, Phishing oder Kompromittierungen wird durch den Service nicht begründet. Der Service reduziert das Risiko einer Kompromittierung, kann sie jedoch nicht ausschließen.

4. Leistungsabgrenzung

Folgende Leistungen sind **nicht** im Service enthalten und können gesondert beauftragt werden:

- Managed Detection & Response mit 24/7-Analystenteam sowie prozessbasierte Endpoint Detection and Response (siehe §2.1) -- für Windows-Clients und Server siehe Endpoint Security (abrufbar unter ext-it.tech/leistungen)
- Verwaltung der mobilen Endgeräte (Enrollment, Betriebssystem-Updates, Richtlinien, Monitoring) -- siehe Managed Service MDM (abrufbar unter ext-it.tech/leistungen)
- Bereitstellung eines Mobile Device Management, sofern der Auftraggeber kein eigenes betreibt (siehe §5.1)
- Verteilung der Schutzanwendung auf die Geräte, sofern der Auftraggeber sein Mobile Device Management selbst betreibt
- Schutz von Windows-Clients, macOS-Geräten und Servern
- Forensische Untersuchungen und Incident Response
- Wiederherstellung von Systemen und Daten nach einem Sicherheitsvorfall
- Backup und Datensicherung
- Anwender-Support und Schulungen
- Security-Awareness-Maßnahmen für Endanwender

5. Voraussetzungen und Mitwirkungspflichten

5.1 Mobile Device Management erforderlich

Die Schutzanwendung lässt sich auf iOS/iPadOS und Android nur über ein Mobile Device Management verteilen und konfigurieren. Der Service setzt daher voraus, dass die Geräte

- über den Service Managed Service MDM der EXT IT verwaltet werden **oder**
- über ein eigenes Mobile Device Management des Auftraggebers verwaltet werden (z.B. Microsoft Intune).

Im zweiten Fall stellt EXT IT die Verteilkonfiguration bereit; die Verteilung auf die Geräte und deren Verwaltung obliegen dem Auftraggeber. Ohne ein Mobile Device Management kann der Service nicht erbracht werden.

5.2 Technische Voraussetzungen

- iOS/iPadOS oder Android in einer vom Hersteller der Schutzanwendung unterstützten Version (aktuelle Systemanforderungen auf Anfrage)
- Internetverbindung der Geräte für die Kommunikation mit der CrowdStrike-Plattform
- Zulassung der erforderlichen Netzwerkverbindungen zur CrowdStrike-Cloud, soweit der Auftraggeber Netzwerkzugriffe einschränkt

5.3 Mitwirkungspflichten des Auftraggebers

- Benennung eines fachlichen Ansprechpartners mit Entscheidungsbefugnis, der sicherheitsrelevante Meldungen entgegennimmt
- Verteilung der Schutzanwendung, sofern der Auftraggeber sein Mobile Device Management selbst betreibt
- Information über Zu- und Abgänge von Geräten
- Sicherstellung, dass die Schutzanwendung auf den Geräten nicht deaktiviert oder entfernt wird
- Unverzügliche Rückmeldung bei Rückfragen zu Bedrohungsmeldungen
- Bereitstellung einer zentralen E-Mail-Adresse (z.B. Verteiler oder Funktionspostfach) für sicherheitsrelevante Informationen

5.4 Beschäftigtendatenschutz und Mitbestimmung

Die Schutzanwendung prüft aufgerufene Adressen und die auf dem Gerät installierten Anwendungen. Auf Geräten von Beschäftigten ist das mitbestimmungspflichtig und bedarf einer eigenen Rechtsgrundlage. Der Auftraggeber ist datenschutzrechtlich Verantwortlicher und stellt vor Inbetriebnahme sicher, dass

- eine Rechtsgrundlage für die Verarbeitung besteht,
- die Beteiligungsrechte einer bestehenden Arbeitnehmervertretung gewahrt sind, insbesondere nach § 87 Abs. 1 Nr. 6 BetrVG,
- die betroffenen Personen gemäß Art. 13 DSGVO informiert wurden und
- bei privat mitgenutzten Geräten eine wirksame Nutzungsvereinbarung vorliegt.

Bei privat mitgenutzten Geräten empfiehlt EXT IT die Einrichtung eines getrennten Arbeitsprofils; die Schutzanwendung wirkt dann nur im verwalteten Bereich.

6. Service Level

Es gelten die Servicezeiten, Reaktionszeiten und Verfügbarkeitszusagen gemäß §6a der Allgemeinen Geschäftsbedingungen (abrufbar unter ext-it.tech/agb/). Abweichende Vereinbarungen können im jeweiligen Einzelauftrag getroffen werden.

Die Bedrohungserkennung auf dem Gerät läuft fortlaufend. Leistungen der EXT IT GmbH (z.B. Rückfragen, Konfigurationsänderungen, Bereitstellung) werden innerhalb der Servicezeiten gemäß §6a AGB erbracht. Eine Bearbeitung von Meldungen rund um die Uhr ist nicht Gegenstand dieses Services (siehe §2.1).

Für die Verfügbarkeit der CrowdStrike-Plattform gelten die Zusagen des Herstellers; EXT IT gibt hierfür keine eigene Verfügbarkeitszusage ab.

7. Vergütung

Modell	Beschreibung
Monatliche Pauschale	Pro geschütztem mobilen Endgerät
Staffelpreise	Mengenrabatte möglich ab definierten Schwellwerten

Ersteinrichtung	Einmalige Einrichtungspauschale oder Abrechnung nach Aufwand gemäß Angebot
Zusatzaufwände	Über den Leistungsumfang hinausgehende Tätigkeiten nach Aufwand gemäß vereinbartem Stundensatz

Aktuelle Preise erhalten Sie auf Anfrage oder in Ihrem individuellen Angebot.

8. Vertragliche Grundlagen

Dokument	Abruf
Allgemeine Geschäftsbedingungen	ext-it.tech/agb/
Auftragsverarbeitungsvertrag	ext-it.tech/avv
Produktspezifische AVV-Anlage 2 -- Endpoint Security Mobile	ext-it.tech/avv

9. Datenschutz (AVV)

Im Rahmen des Services Endpoint Security Mobile werden personenbezogene Daten des Auftraggebers verarbeitet (z.B. Gerätekennungen, Benutzerkennungen, IP-Adressen, installierte Anwendungen, aufgerufene und blockierte Adressen sowie Bedrohungsindikatoren). Die Verarbeitung erfolgt auf Grundlage des Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DSGVO.

Die Prüfung aufgerufener Adressen betrifft das Verhalten von Beschäftigten. Die Verantwortung für Rechtsgrundlage, Mitbestimmung und Information der Betroffenen liegt beim Auftraggeber (siehe §5.4).

Alle relevanten Datenschutz-Dokumente sind unter ext-it.tech/avv abrufbar:

- AVV-Rahmenvertrag
- Produktspezifische Anlage 2 -- Endpoint Security Mobile
- Technisch-organisatorische Maßnahmen (Anlage 1)
- Zentrale Unterauftragsverarbeiter-Liste (Anlage 3)

Der AVV wird automatisch Vertragsbestandteil bei Beauftragung (siehe §1 Abs. 2 AVV).

10. Laufzeit und Kündigung

Es gelten die Regelungen des §10 der Allgemeinen Geschäftsbedingungen (abrufbar unter ext-it.tech/agb/). Abweichende Laufzeiten und Kündigungsfristen können im jeweiligen Einzelauftrag individuell vereinbart werden.

Produktspezifische Ergänzung: Die Lizenzierung erfolgt in Laufzeiten des Herstellers. Die für den Auftraggeber maßgebliche Mindestlaufzeit wird im Angebot bzw. Einzelauftrag ausgewiesen; ohne eine solche Ausweisung gilt §10 Abs. 1 und 2 AGB. Eine Reduzierung der lizenzierten Geräte ist, soweit im Einzelauftrag nichts anderes vereinbart ist, zum jeweiligen Verlängerungstermin (§10 Abs. 2c AGB) möglich. Wird der Service als Zusatzleistung zu Managed Service MDM gebucht, gilt die Mindestlaufzeit für diese Zusatzleistung gesondert; die monatliche Abrechnung bleibt hiervon unberührt.

Änderungshistorie

Version	Datum	Änderung	Verantwortlich
1.0	2026-09-02	Erstveröffentlichung	Geschäftsführung

Stand: 2026-09-02