# ReddFort
# App-Protect


reddFort

# App-Protect

**Immer dann, wenn es darum geht, sicherheitskritische Anwendungen innerhalb Ihres Unternehmens zu schützen, kommt das ReddFort-Sicherheitssystem App-Protect zum Einsatz. App-Protect bietet eine patentierte Lösung, die aus zwei logischen Einheiten besteht: dem Basisschutz und der sicheren Schutzhülle „Guarded Desktop".**

Der Basisschutz, der alle auf dem Client installierten Programme durch eine gesicherte und verschlüsselte Datenbasis gegen Kompromittierung schützt, verhindert somit die Ausführung von nicht autorisierten Programmen. Dieser Schutz startet vor Betriebssystemstart, wodurch Veränderungen an der Installationsbasis nicht mehr möglich sind. Alle Programme und Prozesse, die nicht in der Datenbasis registriert sind, egal wie diese auf den Client gelangt sind (E-Mail, Internet, Netzwerk, Laufwerke), werden noch vor dem Hochladen erkannt und kommen nicht zur Ausführung.

Kernstück von ReddFort App-Protect ist der Guarded Desktop, in dem sensible und kritische Programme ausgeführt werden können. Der Guarded Desktop erzeugt eine gesicherte Anwendungsumgebung in Form eines zweiten Desktops. Dabei wird eine isolierte – nicht virtuelle – Umgebung „sandbox" erzeugt, innerhalb derer zuvor registrierte Anwendungen ausgeführt werden. Während der Laufzeit wird sichergestellt, dass aktive Anwendungen nur auf zulässige und unverfälschte Systemkomponenten zurückgreifen. Jegliche Abweichung der Anwendungen wird bemerkt und verhindert.

## Folgende Angriffsszenarien können durch den Einsatz von App-Protect verhindert werden:

- System-wide Hooks (Beispiel: Vertauschung eingegebener Zeichen)
- Kopieren des Bildschirminhaltes über die DirectX- oder Win32-API-Schnittstelle
- Kopieren des Inhaltes von Passworteingabefeldern
- Kopieren/Schreiben des Inhaltes beliebiger Felder
- Library-Injection: Einbetten von DLLs in den virtuellen Speicher eines Prozesses
- Keylogger: Aufzeichnung von Tastenanschlägen
- Message-Corruption: Lesen/Schreiben von Daten in Handles
- Simulation von Eingaben und Kommandos an andere Fenster
- IAT-Hooking (Beispiel: Daten werden beim Speichern verschlüsselt)

## Ihre Vorteile im Überblick:

- Kein Zugriff von außen auf sicherheitskritische Anwendungen und Prozesse
- Alle im „GuardedDesktop" laufenden Anwendungen sind für mögliche Angreifer unsichtbar, Tastatur- und Mausbefehle können nicht mitgeschnitten werden
- Der bestehende Desktop und der „GuardedDesktop" sind voneinander unabhängig und kommunizieren nicht miteinander. Mögliche Angriffe auf den Client oder Server können also keinen Schaden verursachen.
- Jeglicher Angriff auf Programmdateien wird verhindert
- Zentrales Management und integrierte Softwareverteilung
- Komplexe Architektur, aber einfach in der Handhabung

**Systemvoraussetzungen:**
Internetverbindung (für die Produktaktivierung und die Updatefunktion)
Prozessor: mindestens 800 MHz
RAM: 512 MB für 32 Bit oder 1 GB für 64 Bit
Festplattenspeicher: 3 GB für 32-Bit-Betriebssysteme oder 6 GB für 64-Bit-Betriebssysteme

**Unterstützte Betriebssysteme:**
Windows Vista x86/x64
Windows 7 x86/x64
Windows 8 x86/x64
Windows 8.1 x86/x64
Windows 10 x86/x64

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

reddFort

**ReddFort Software GmbH**

Neuensaaler Str. 70, 51515 Kürten
Fon: +49 2206 908066, Fax: +49 2296 908068
E-Mail: info@reddfort.de

www.reddfort.de