UNITED ENDPOINT
PROTECTOR

UNITED ENDPOINT PROTECTOR

HANDBUCH

1.4

Inhaltsverzeichnis

1. Einführung

Der United Endpoint Protector (UEP) ist ein universelles Sicherheitssystem für Microsoft Windows zum Schutz vor Cyberbedrohungen. Das System vereinheitlicht den Betrieb von unabhängigen Sicherheitsanbietern und stellt diese auf Knopfdruck zur Verfügung. Dazu ist der United Endpoint Protector (UEP) mit unterschiedlichen Anti-Malware-Technologien ausgestattet, die mit Hilfe von Technologielizenzen freigeschalten werden können. Nach der Freischaltung können die gewünschten Anbieter in den jeweiligen Sicherheitsfunktionen jederzeit aktiviert und miteinander kombiniert werden.

Die Inbetriebnahme des United Endpoint Protectors (UEP) umfasst die folgenden Schritte:

1. Installieren Sie den United Endpoint Protector anstelle Ihres bisherigen Antiviren-Produktes. (siehe Kapitel 2)
2. Schalten Sie die gewünschten Anbieter mit Hilfe von Technologielizenzen frei, die Sie von uns zugeschickt bekommen. (siehe Kapitel 3)
3. Aktivieren Sie die gewünschten Anbieter über die jeweilige Technologieoberfläche in den Sicherheitsfunktionen. (siehe Kapitel 9)
4. Erstellen Sie eine Aktualisierungsaufgabe, um die aktiven Anbieter mit den neuesten Informationen zu aktualisieren. (siehe Kapitel 4)

Dieses Handbuch soll Ihnen bei der Installation und dem Betrieb des United Endpoint Protectors (UEP) auf Ihrem Windows Computer helfen. Mit den folgenden Kapiteln leiten wir Sie Schritt für Schritt durch diesen Vorgang und erläutern mögliche Strategien.

2. Installation

Der United Endpoint Protector (UEP) kann mit Hilfe des Installationspaketes „uepsetup.msi“ auf einem Windows Computer installiert werden, welches Sie von der Tabidus Webseite herunterladen können. Abhängig vom Installationsumfeld, beschreiben die nachstehenden Punkte die erforderlichen Schritte für die Installation des UEP.

Vor der Installation des UEP auf produktiven Maschinen sollte dessen Funktionsweise und Konfiguration auf Testgeräten überprüft werden! Abhängig vom Einsatzgebiet, der zur Verfügung stehenden Hardware und dem Betrieb bestehender Softwarekomponenten, können spezielle Anpassungen für den UEP erforderlich sein.

2.1. Systemvoraussetzungen

Bevor Sie eine Installation des United Endpoint Protectors (UEP) auf einem Computersystem durchführen, stellen Sie bitte sicher, dass die folgenden Voraussetzungen gegeben sind:

- Das Betriebssystem des Computers ist eines der folgenden:
  - Microsoft Windows 10
  - Microsoft Windows 11
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022

- Die Hardware des Computers besitzt mindestens die folgenden Ressourcen:
  - Intel kompatibler Prozessor (4 Cores empfohlen)
  - 4 GB Arbeitsspeicher
  - 2 GB freier Festplattenspeicher

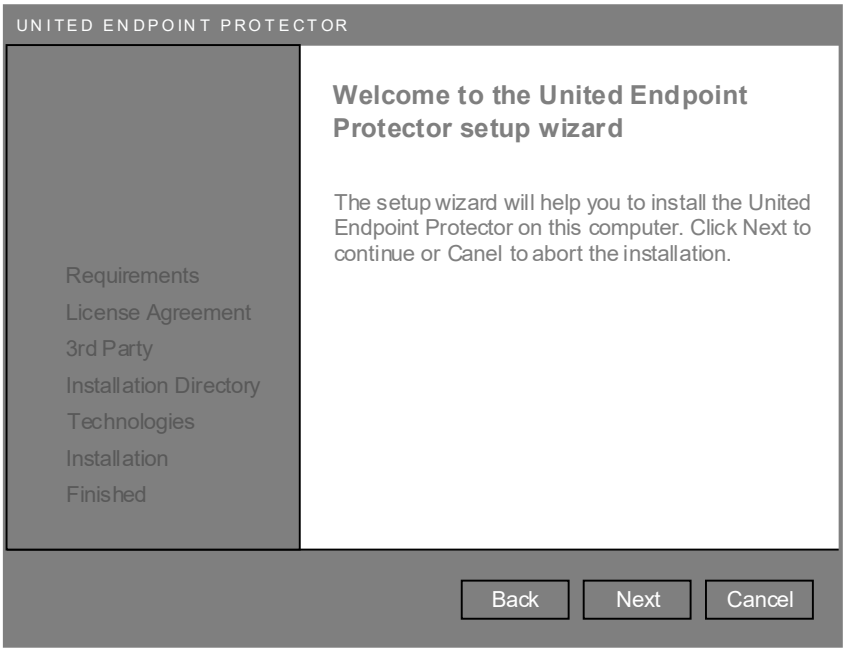
- Lokale Administratorrechte für den Installationsvorgang stehen zur Verfügung.

- Keine andere Anti-Virus-Software ist auf dem Gerät installiert.

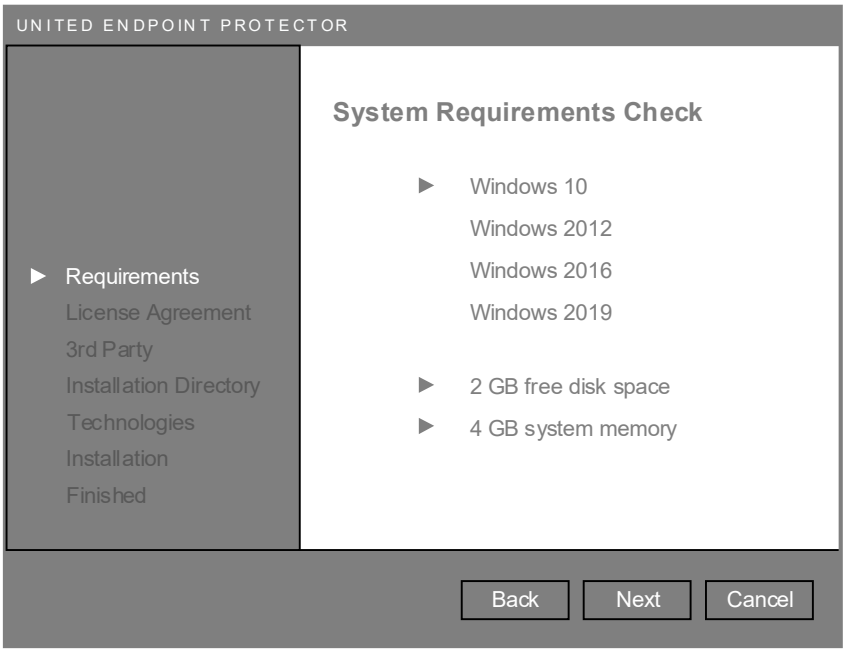
2.2. Lokale Installation

Die lokale Installation eignet sich für die Inbetriebnahme des United Endpoint Protectors (UEP) auf einzelnen Computersystemen. Achten Sie vor dem Beginn der Installation, dass die unter Punkt 2.1 angeführten Voraussetzungen gegeben sind.

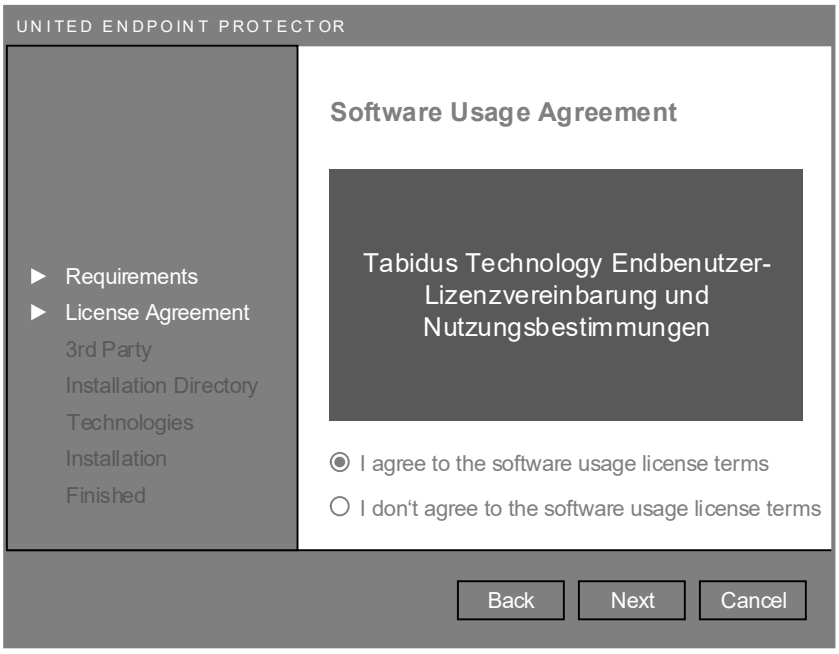
Für den Start der lokalen Installation führen Sie die „uepsetup.msi" mit lokalen Administratorrechten aus. Nach kurzer Zeit erscheint ein Willkommen-Fenster. Klicken Sie auf „Next" um mit der Installation zu beginnen.



Der nächste Schritt überprüft automatisch die Einhaltung der Systemvoraussetzungen in Hinblick auf Betriebssystem, Festplattenspeicher und Arbeitsspeicher. Sollte das Computersystem die Vorgaben erfüllen, können Sie die Installation mit „Next" fortsetzen. Andernfalls brechen Sie den Versuch bitte mit „Cancel" ab.



Lesen Sie sich im nächsten Schritt sorgfältig die EULA für den Einsatz des United Endpoint Protectors durch. Diese finden Sie auch auf unserer Webseite unter https://www.tabidus.com/de/eula/. Um mit der Installation fortzufahren ist Ihre Zustimmung zu den Bedingungen erforderlich. Anschließend können Sie mit „Next" fortsetzen.

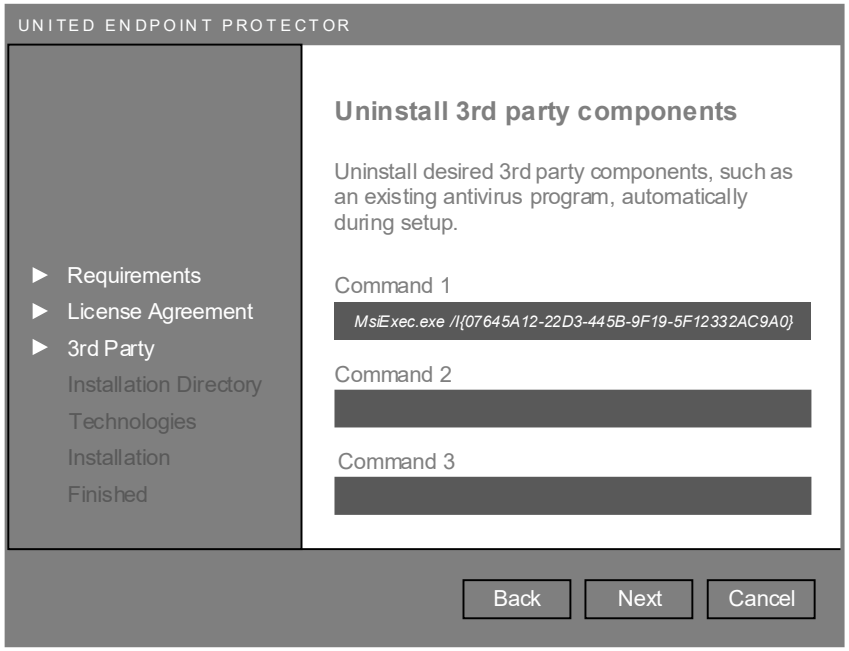


Sollte sich auf dem Computersystem noch eine andere Sicherheitssoftware befinden, die noch nicht entfernt wurde, kann diese automatisch durch den Installationsvorgang deinstalliert werden. Dazu können Sie in diesem Schritt bis zu drei Befehlszeilenkommandos angeben die ausgeführt werden sollen. Diese Vorgehensweise eignet sich besonders für einen schnellen Produktwechsel, ohne lange Ausfallszeiten.

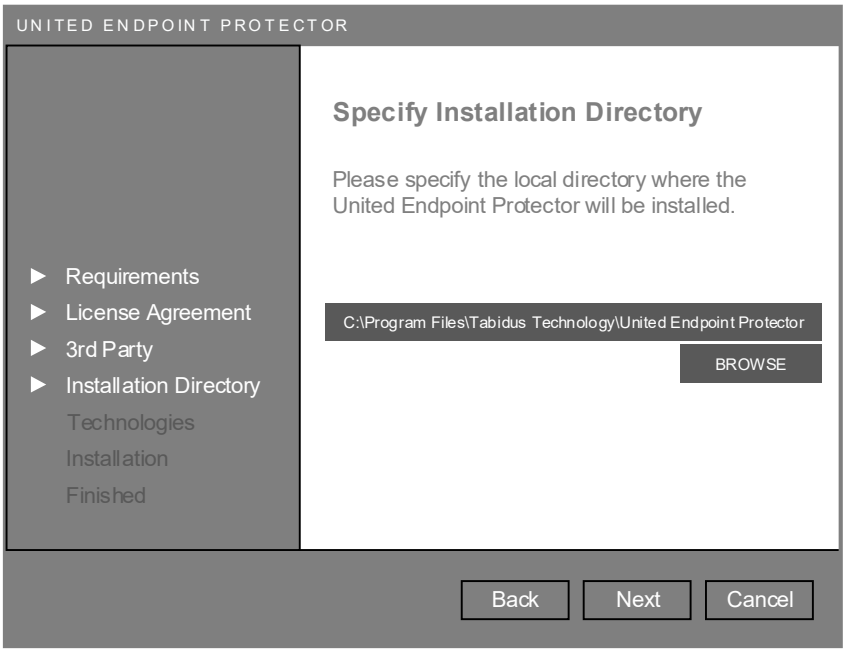
In vielen Fällen können geeignete Deinstallationsbefehle in der Windows Registry unter HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall gefunden werden. Suchen Sie dort nach der gewünschten Komponente und überprüfen Sie ob ein „UninstallString" Eintrag vorhanden ist. Dieser könnte zum Beispiel wie folgt aussehen: *MsiExec.exe /I{07645A12-22D3-445B-9F19-5F12332AC9A0}*
Kopieren Sie den String in eines der Texteingabefelder des Setups. Beachten Sie dabei, dass Ihre Sicherheitssoftware unter Umständen Selbstschutzmechanismen aktiviert hat die eine Deinstallation verhindern. Im Zweifelsfall wenden Sie sich bitte an Ihren bisherigen Anbieter für genaue Informationen zur Deinstallation des Produktes.

Unter Windows Server 2016 und 2019 können Sie die Windows Defender Rolle bei Bedarf mit dem folgenden Befehl deinstallieren: *Uninstall-WindowsFeature -Name Windows-Defender*

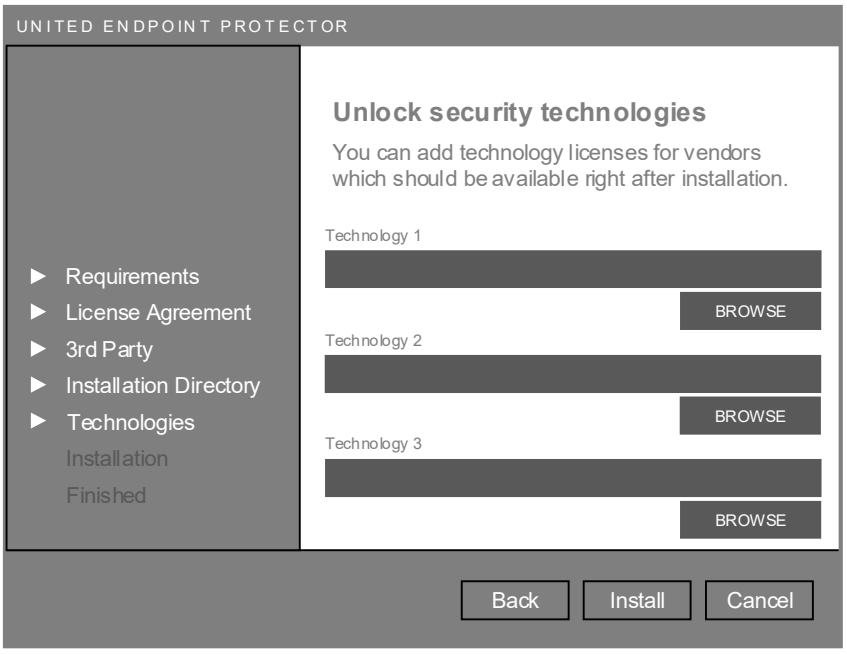
Diese Angaben sind optional. Sollten Sie keine Komponenten deinstallieren wollen, klicken Sie auf „Next" um fortzufahren.



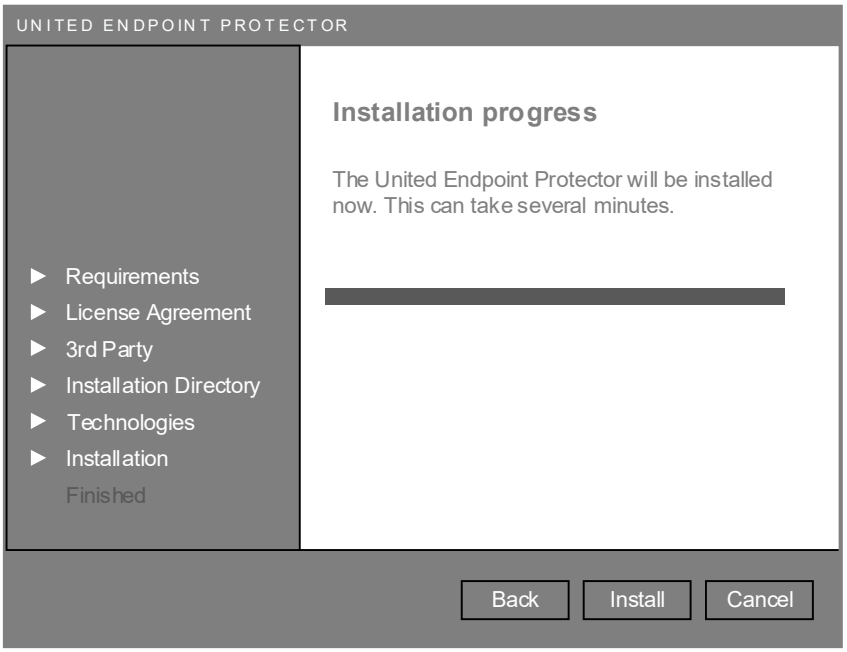
Legen Sie im nächsten Schritt das gewünschte Installationsverzeichnis fest, in das der UEP installiert werden soll. Mit Hilfe der „Browse“ Schaltfläche können Sie ein anderes Verzeichnis auswählen. Klicken Sie anschließend auf „Next“ um fortzufahren.



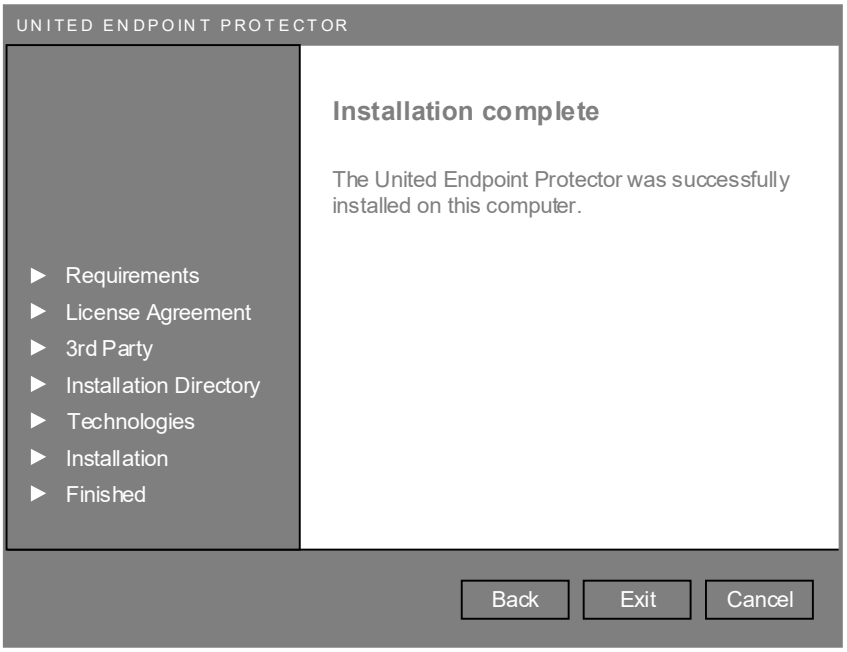
Wenn Sie bestimmte Sicherheitsanbieter bereits unmittelbar nach der Installation zur Verfügung stellen wollen, können Sie die entsprechenden Technologielizenzen (siehe Kapitel 3) im nächsten Schritt angeben. Andernfalls steht Ihnen diese Option auch jederzeit nach der Installation zur Verfügung. Klicken Sie anschließend auf „Install“ um den Installationsprozess zu starten.



Während des Installationsprozesses werden alle festgelegten Angaben berücksichtigt und der United Endpoint Protector (UEP) auf dem Computersystem installiert. Dieser Vorgang kann mehrere Minuten dauern.



Abschließend wird Ihnen das Installationsergebnis mitgeteilt. Sollte während des Vorgangs ein Fehler aufgetreten sein, steht Ihnen im Anschluss ein detailliertes Installationsprotokoll zur Verfügung.



2.3. Software Verteilung

Zur Installation des United Endpoint Protectors (UEP) auf mehreren Computersystemen, eignet sich eine Form der Softwareverteilung. Neben verschiedenen Drittanbieterlösungen, stellt auch Microsoft eine Funktion zur Verteilung von MSI-Paketen via Active Directory bereit.

Um eine unbeaufsichtigte, automatische Installation von UEP durchzuführen, kann die „uepsetup.msi" mit den folgenden Parametern gestartet werden.

accepteula=true	Akzeptiert die Bedingungen der Endbenutzer-Lizenzvereinbarung und Nutzungsbestimmungen, wie sie unter https://www.tabidus.com/de/eula/ zu finden sind.
uninstall1="" uninstall2="" uninstall3=""	Ermöglicht die Deinstallation von Drittanbieter-Komponenten, zum Beispiel bestehende Sicherheitssoftware, während des Installationsvorganges, wie unter Punkt 2.2 beschrieben.
installdir=""	Legt das Installationsverzeichnis fest in das der UEP installiert werden soll.
tech1="" tech2="" tech3=""	Ermöglicht die Angabe gewünschter Technologielizenzen, um bestimmte Sicherheitsanbieter bereits nach der Installation zur Verfügung zu stellen, wie unter Punkt 2.2 beschrieben.
/qn	Unterdrückt die Anzeige des Installationsvorganges und führt diesen im Hintergrund aus.
/qb	Unterdrückt eine Interaktion mit dem Installationsvorgang und stellt eine Fortschrittsanzeige dar. Dieser Parameter ist verpflichtend zu verwenden, wenn /qn nicht genutzt wird.

Beispiel:

msiexec /i uepsetup.msi accepteula=true uninstall1="MsiExec.exe /I{07645A12-22D3-445B-9F19-5F12332AC9A0}" uninstall2="MsiExec.exe /I{01395A12-11AA-3F91-8FE9-11117452A1111}" installdir="D:\Program Files\UEP" tech1="E:\licenses\mylicense.dat" tech2="E:\licenses\secondlicense.dat" /qb

2.4. Deinstallation

Um den United Endpoint Protector (UEP) zu deinstallieren, muss dessen Selbstschutz (siehe Kapitel 5.1) zuvor deaktiviert werden. Anschließend kann die Deinstallationsroutine in der Systemsteuerung von Windows unter „Programme und Features“ aufgerufen werden. Alternativ ist eine Deinstallation mit Hilfe des Befehls „MsiExec.exe /X{*GUID*}“ möglich, der in der Windows Registry unter HKLM\SOFTWARE\Microsoft\CurrentVersion\Uninstall\{*GUID*} zu finden ist.

2.5. Benutzeroberfläche

Zur Überprüfung der Arbeitsweise und Konfiguration des United Endpoint Protectors (UEP) steht die Benutzeroberfläche (uepconsole.exe) zur Verfügung. Diese kann über das System-Tray-Icon von Tabidus oder dem Startmenü von Windows aufgerufen werden.

UEP Benutzeroberfläche

Das wichtigste Bedienelement der Oberfläche ist das Hauptmenü, in der oberen linken Ecke. Über dieses können alle Funktionen des UEP aufgerufen werden.

- **Status**
  Statusanzeige aller wichtigen Betriebsparameter, um den Zustand und die Arbeitsweise des UEP auf einen Blick kontrollieren zu können (siehe Kapitel 13).

- **Dateisicherheit**
  Echtzeit-Überwachung aller Dateizugriffe auf der lokalen Festplatte, Netzlaufwerke und Wechseldatenträger (siehe Kapitel 5).

- **Speicherschutz**
  Forensische Überprüfung des Arbeitsspeichers mit verschiedenen Methoden (siehe Kapitel 6).

- **Registry Sicherheit**
  Echtzeit-Überwachung aller Zugriffe auf die Microsoft Windows-Registry und andere Application HIVES' (siehe Kapitel 7).

- **Auf Anforderung**
  Erstellung und Verwaltung von Scan-Aufgaben zur zeitgesteuerten Überprüfung bestimmter Bereiche des Computersystems (siehe Kapitel 8).

- **Aktualisieren**
  Statusanzeige der Sicherheitstechnologien und Verwaltung der Aufgaben zur Aktualisierung der Technologien (siehe Kapitel 4).

- **Lizenzen**
  Lizenzverwaltung zur Freischaltung von gewünschten Sicherheitsanbietern und Überwachung deren Laufzeit (siehe Kapitel 3).

Jeder Menüeintrag besitzt ein Untermenü, in dem alle zugehörigen Konfigurationsoptionen zu den Funktionen bereitgestellt sind. Nähere Informationen zu deren genaue Funktionsweise und Betrieb werden in den entsprechenden Kapiteln erläutert. Sollten Infektionen erkannt werden, wird deren Anzahl ebenfalls im Hauptmenü eingeblendet.

Mit einem Klick auf einen Menüeintrag, wird die jeweilige Oberfläche im Hauptfenster aufgerufen. Abhängig von der Funktion, wird im unteren Bereich der Oberfläche eine Menüleiste mit weiteren Bedienelementen dargestellt.

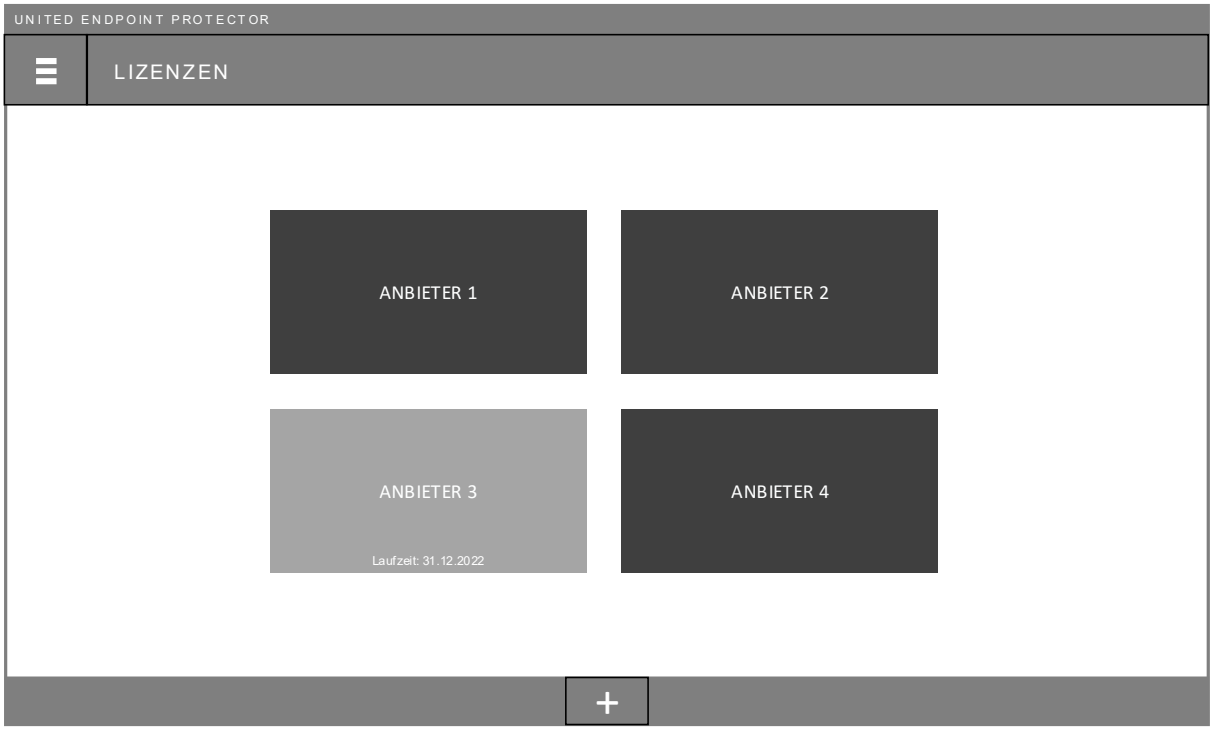
Falls der UEP durch das United Control Center (UCC) zentral verwaltet wird, kann der Zugriff auf die Benutzeroberfläche gesperrt sein. In diesem Fall erscheint beim Aufruf der Oberfläche eine Passworteingabeaufforderung. Erst durch die Eingabe des Passwortes, welches durch Ihren Administrator festgelegt wurde, wird der Zugriff auf die verschiedenen Funktionen freigegeben.

In der rechten oberen Ecke der Benutzeroberfläche befindet sich eine Schaltfläche zur Sprachauswahl. Mit dieser können Sie die Anzeige der Oberfläche jederzeit zwischen den Sprachen Englisch und Deutsch ändern.

Die Benutzeroberfläche ist ein Werkzeug für die Bedienung des UEP. Die Schutzfunktion des UEP ist nicht von deren Ausführung abhängig. Auch bei geschlossener Oberfläche ist der UEP voll funktionstüchtig und führt die konfigurierten Schutzfunktionen aus.

3. Lizenzverwaltung

Mit der Lizenzverwaltung steuern Sie, welche Sicherheitsanbieter zum Schutz eingesetzt werden sollen. Klicken Sie im Hauptmenü auf „Lizenzen“, um die Übersicht aller verfügbaren Anbieter zu öffnen. Mit Hilfe von Technologielizenzen, die Sie von uns erhalten, können Sie die gewünschten Anbieter freischalten. Welche Anbieter bereits freigeschalten wurden und wie lange Ihnen der jeweilige Anbieter zur Verfügung steht, wird Ihnen auf dieser Übersichtsseite angezeigt.



Lizenzen -> Übersicht

3.1. Anbieter freischalten

Zur Freischaltung eines Sicherheitsanbieters klicken Sie im Hauptmenü auf „Lizenzen“, um die Lizenzübersicht zu öffnen. Klicken Sie anschließend auf das Hinzufügen-Icon in der unteren Menüleiste und wählen Sie die vorhandene Technologielizenz aus. Sollten Sie noch keine Technologielizenzen besitzen, nehmen Sie bitte Kontakt mit uns auf.

Bei erfolgreicher Freischaltung verändert sich das Logo des jeweiligen Anbieters innerhalb weniger Sekunden und die Laufzeit der Lizenz wird sichtbar. Zusätzlich wird ein neuer Untermenüpunkt bei „Lizenzen" im Hauptmenü hinzugefügt, über den Sie Details zu Ihrer Lizenz einsehen können. An dieser Stelle besteht auch die Möglichkeit eine Lizenz bei Bedarf zu löschen.

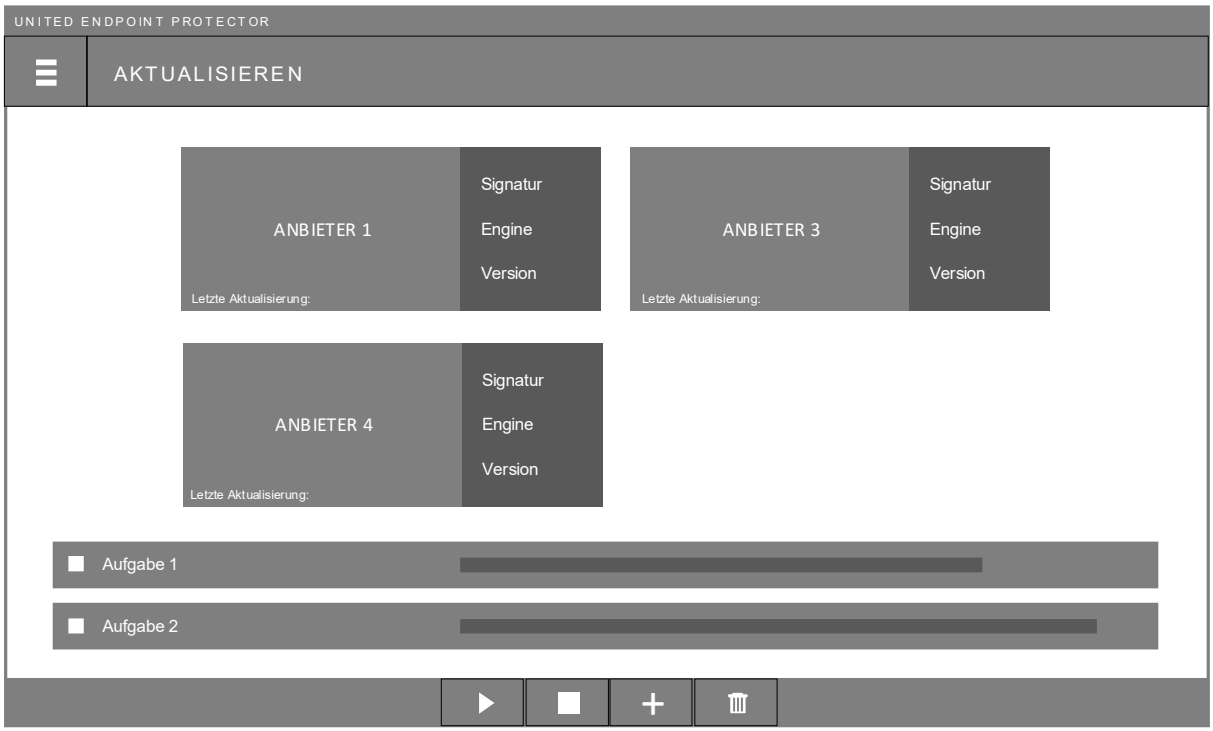
3.2. Lizenzende und Verlängerung

Wenn das Ablaufdatum einer Technologielizenz erreicht ist, löscht sich diese automatisch und der jeweilige Anbieter schaltet sich ab. Wir empfehlen Ihnen daher rechtzeitig, vor Laufzeitende, eine neue Lizenz für den Anbieter zu erwerben, um die Sicherheit Ihres Endgerätes nicht zu gefährden.

Sie können jederzeit mehrere Lizenzen für einen Sicherheitsanbieter, mit unterschiedlichen Laufzeiten, hinzufügen. Um eine ungewollte Abschaltung eines Anbieters zu verhindern, empfehlen wir daher eine weitere Lizenz vor Ablauf hinzuzufügen. Zum Zeitpunkt, an dem die bisherige Lizenz endet, löscht sich diese und die neue Lizenz übernimmt automatisch.

4. Aktualisieren

Abhängig von den ausgewählten Sicherheitsanbietern und deren technischen Ansätzen, benötigen die Technologien fortlaufende Aktualisierungen, um ihr volles Schutzpotenzial zu erzielen. Der United Endpoint Protector (UEP) ist deshalb mit einem automatischen Updatesystem ausgestattet, mit dessen Hilfe die freigeschalteten Anbieter mit Aktualisierungen versorgen werden können. Klicken Sie dafür im Hauptmenü auf „Aktualisieren“ um die Aktualisierungsübersicht zu öffnen.



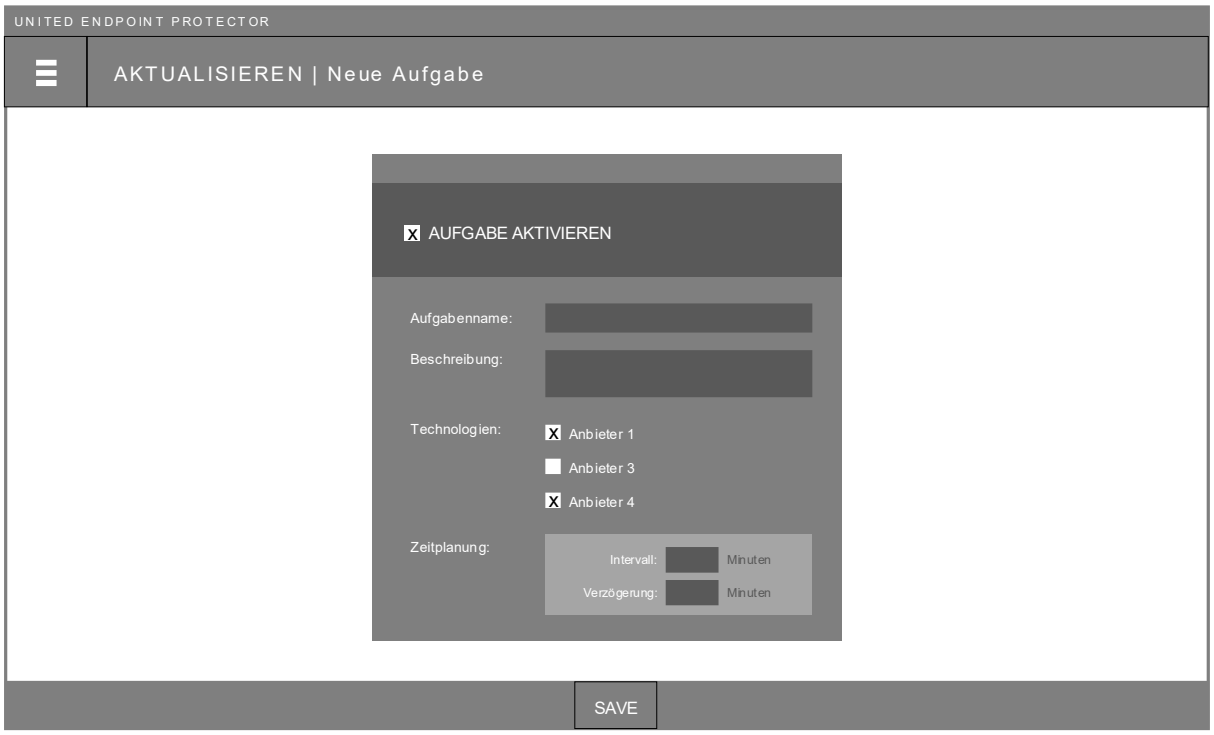
Aktualisieren -> Übersicht

Im oberen Bereich der Oberfläche werden die freigeschalteten Anbieter und deren Status angezeigt. Abhängig vom jeweiligen Anbieter können sich die zu aktualisierenden Komponenten unterscheiden. Pro Anbieter wird der Zeitpunkt angegeben wann die letzte Aktualisierung stattgefunden hat. Liegt dieser Zeitpunkt nicht innerhalb der letzten 24 Stunden, wird dies durch rote Schriftfarbe gekennzeichnet.

Im unteren Bereich werden eine oder mehrere Aktualisierungsaufgaben dargestellt, die sie nach Belieben erstellen können (siehe Kapitel 4.1). Durch Auswahl einer Aufgabe mittels Kontrollkästchen, werden verschiedene Icons in der darunterliegenden Menüleiste verfügbar. Mit diesen können Sie Aufgaben manuell starten, stoppen oder bei Bedarf löschen. Pro Aufgabe wird der Zeitpunkt der letzten Ausführung angezeigt. Mit einem Klick auf das Expander-Symbol können Sie detaillierte Informationen über die laufende Ausführung anzeigen lassen.

4.1. Aufgabe erstellen

Zur Erstellung einer Aktualisierungsaufgabe klicken Sie im Hauptmenü auf „Aktualisieren“, um die Aktualisierungsübersicht zu öffnen. Anschließend klicken Sie auf der unteren Menüleiste auf das Hinzufügen-Icon. Daraufhin öffnet sich die Konfigurationsoberfläche der Aufgabe.



Aktualisieren -> Aufgabe

Auf der Konfigurationsoberfläche können Sie die folgenden Einstellungen vornehmen, um die Aufgabe festzulegen:

Aufgabe aktivieren	Aktiviert die automatische Ausführung der Aufgabe nach angegebenen Zeitplan. Wird die Aufgabe nicht aktiviert, steht diese zur manuellen Ausführung bereit.
Aufgabenname	Eine beliebige Bezeichnung zur Benennung der Aufgabe. Diese erscheint in der Aktualisierungsübersicht, sowie im Untermenü von „Aktualisieren“ im Hauptmenü.
Beschreibung	Ein beliebiger Text der für Dokumentationszwecke optional eingetragen werden kann. Dieser Text wird nur in der Konfigurationsoberfläche der Aufgabe angezeigt.

Technologien	Abhängig von den freigeschalteten Anbietern und ob für diese automatische Aktualisierungen existieren, werden diese angeführt. Mit Hilfe der Kontrollkästchen können Sie festlegen, welche Anbieter durch diese Aufgabe aktualisiert werden sollen. Sie können mehrere Anbieter mit einer gemeinsamen Aufgabe aktualisieren lassen. Der UEP ladet alle Aktualisierungen gleichzeitig herunter und übernimmt diese hintereinander in den laufenden Betrieb der Technologien, um Unterbrechungen der Sicherheit zu verhindern.
Zeitplanung	Legt den Zeitplan für die automatische Ausführung der Aufgabe fest. „Intervall" definiert die Anzahl der Minuten, wann die Aufgabe erneut ausgeführt werden soll. „Verzögerung" beschreibt den Zeitraum, wann die Aufgabe starten soll, falls die letzte reguläre Ausführung nicht stattgefunden hat. Das ist zum Beispiel der Fall, wenn der Computer ausgeschalten war. Die Verzögerung gibt in diesem Fall die Anzahl der Minuten an, wann die erste Ausführung nach dem Einschalten des Computers stattfinden soll.

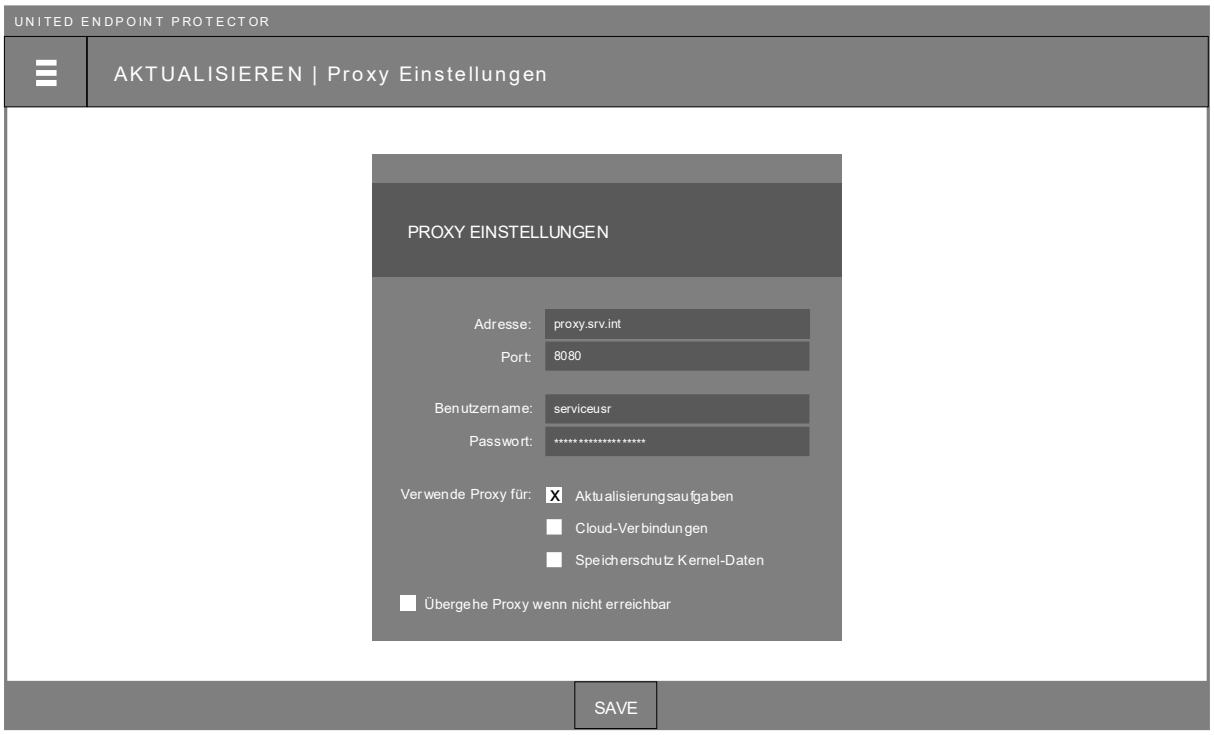
Nachdem alle Einstellungen vorgenommen wurden, kann die Aufgabe mit dem Speicher-Icon in der unteren Menüleiste gespeichert werden. Damit wird die Aufgabe in der Aktualisierungsübersicht sichtbar und kann dort überwacht werden. Die Konfigurationsoberfläche der Aufgabe kann jederzeit im Untermenü von „Aktualisieren" im Hauptmenü wieder aufgerufen werden.

Für das Herunterladen der Aktualisierungen baut der United Endpoint Protector (UEP), falls er nicht durch das United Control Center (UCC) zentral verwaltet wird, eine Verbindung zu den Servern der jeweiligen Anbieter auf.

Anbieter	URL
Avira	http://oem.avira-update.com
Cyren	http://oem.avdl.ctmail.com
IKARUS	http://*.ikarus.at

4.2. Proxy Einstellungen

Sollte für eine Internetverbindung ein Proxy-Server eingesetzt werden, können Sie die erforderlichen Verbindungsdaten in den Proxy-Einstellungen eintragen. Diese können Sie im Untermenü von „Aktualisieren“ über den Punkt „Proxy“ aufrufen.



Aktualisieren - Proxy

Die folgenden Proxy-Einstellungen können in der Konfigurationsoberfläche vorgenommen werden:

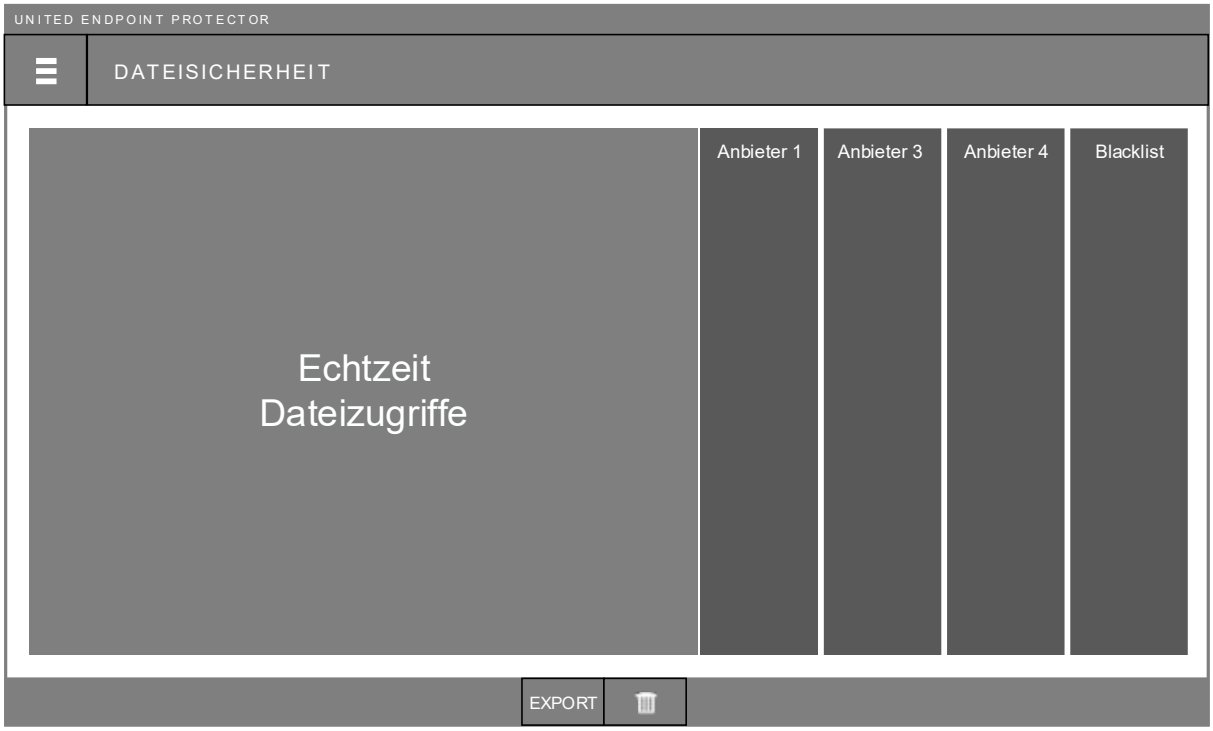
Adresse	Name oder IP-Adresse des zu verwendenden Proxy-Servers.
Port	Port des zu verwendenden Proxy-Servers.
Benutzername Passwort	Authentifizierung gegenüber dem Proxy-Server. Unterstützt wird dazu Basic-Authentication.
Verwende Proxy für	Legt die Verbindungsarten fest für die der Proxy-Server genutzt werden soll. „Aktualisierungsaufgaben“ bezieht sich auf jeden Verbindungsaufbau zu einem Update-Server eines Anbieters.

	„Cloud-Verbindungen“ bezieht sich auf alle Verbindungen einer Technologie zur Cloud des jeweiligen Anbieters, falls die entsprechende Funktion aktiviert wurde. „Speicherschutz Kernel-Daten“ bezieht sich auf den Verbindungaufbau der Speicherschutz-Funktion zum Microsoft Symbol-Server.
Übergehe Proxy wenn nicht erreichbar	Legt fest, ob der Proxy-Eintrag ignoriert werden soll falls dieser nicht erreichbar ist. Das ist zum Beispiel der Fall, wenn ein mobiles Gerät das Unternehmensnetzwerk verlässt.

5. Dateisicherheit

Die Dateisicherheit ermöglicht die Überwachung und Überprüfung aller Dateizugriffe auf der lokalen Festplatte, auf Netzlaufwerke und auf Wechseldatenträger in Echtzeit. Zur Erkennung von bösartigen Dateien können Sie jeden freigeschalteten Anbieter, in beliebigen Kombinationen, in dieser Schutzfunktion einsetzen.

Klicken Sie im Hauptmenü auf „Dateisicherheit“, um den Dateisicherheits-Monitor zu öffnen. Der Monitor stellt in Echtzeit alle Dateizugriffe dar, sowie das Untersuchungs- und Säuberungsergebnis der aktiven Anbieter.

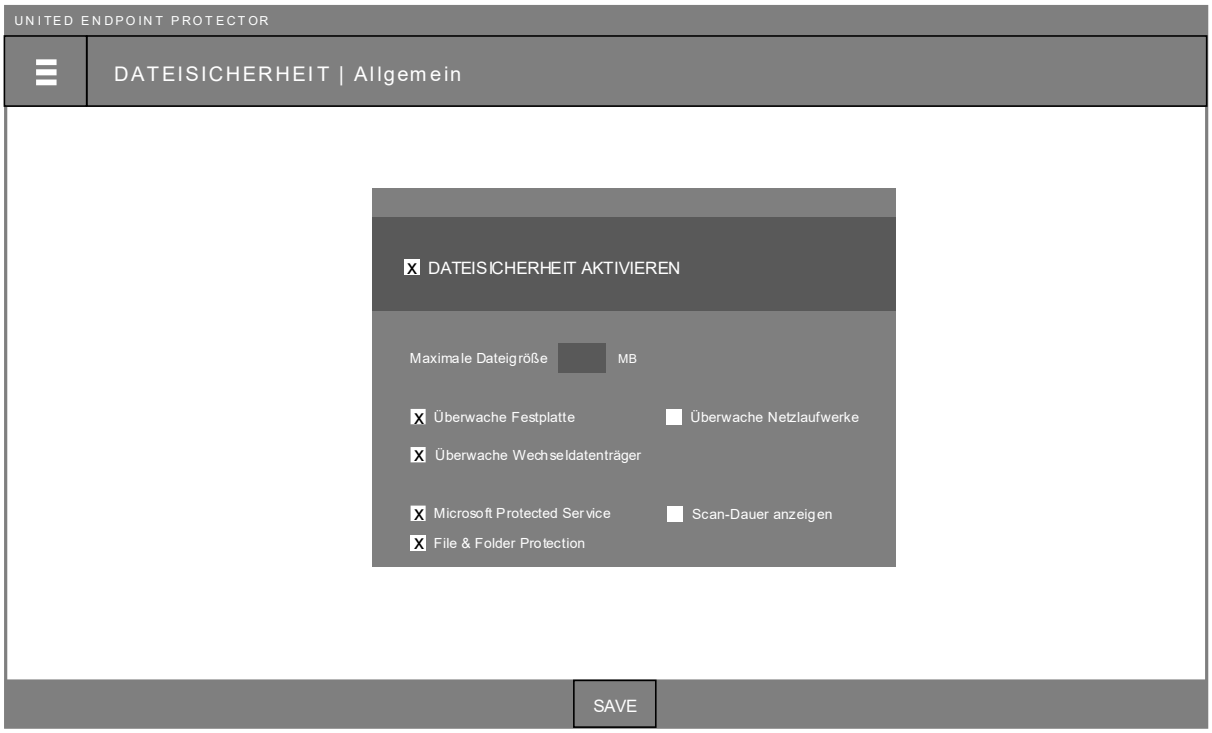


Dateisicherheit -> Monitor

Auf der Benutzeroberfläche werden die letzten 10.000 Zugriffe dargestellt, die Sie mit Hilfe der Filterleiste in Echtzeit durchsuchen können. Mit dem Export-Icon, in der unteren Menüleiste, können Sie alle aufgezeichneten Zugriffe in eine XLS-Datei exportieren. Das Lösch-Icon erlaubt hingegen die manuelle Löschung aller aufgezeichneten Daten. Eine automatische Löschung findet durch das Beenden des United Endpoint Protector Dienstes bzw. in regelmäßigen Abständen, wenn Daten älter als 24 Stunden sind, statt.

5.1. Allgemeine Einstellungen

Die Funktionsweise der Dateisicherheit kann über die allgemeinen Einstellungen festgelegt werden. Klicken Sie dazu im Untermenü von „Dateisicherheit“ auf „Allgemein“.



Dateisicherheit -> Allgemein

Auf der Konfigurationsoberfläche können die folgenden Einstellungen vorgenommen werden:

Dateisicherheit aktivieren	Aktiviert oder deaktiviert die Überwachung der Dateizugriffe.
Maximale Dateigröße	Legt die maximale Größe der Dateien in Megabyte fest die überwacht werden sollen.
Überwache Festplatte	Aktiviert oder deaktiviert die Überwachung von Dateizugriffen auf der lokalen Festplatte.
Überwache Netzlaufwerke	Aktiviert oder deaktiviert die Überwachung von Dateizugriffen auf Netzlaufwerke.
Überwache Wechseldatenträger	Aktiviert oder deaktiviert die Überwachung von Dateizugriffen auf Wechseldatenträger, wie zum Beispiel USB-Sticks.

Scan-Dauer anzeigen	Zeigt im Monitor der Dateisicherheit die Zeitdauern an, die für die Überprüfung der Dateizugriffe erforderlich sind.
Microsoft Protected Service	Aktiviert oder deaktiviert den Schutz des United Endpoint Protectors (UEP) durch das Betriebssystem. Windows verhindert dabei jegliche Manipulation an Prozessen und dem Dienst des UEP.
File & Folder Protection	Aktiviert oder deaktiviert den Manipulationsschutz für die Dateien des United Endpoint Protectors (UEP). Der Schutz blockiert alle nicht autorisierten Zugriffe auf das Installationsverzeichnis des UEP. Um gewünschten Prozessen einen Zugriff auf die Dateien trotz aktiviertem Selbstschutz zu gewähren, können dafür Ausnahmen erstellt werden (siehe Kapitel 12.1).

5.2. Strategie

Die Überwachung der Dateizugriffe ist eine wichtige Sicherheitsfunktion um Bedrohungen aufzuspüren und Infektionen zu verhindern. Wir empfehlen dafür die Aktivierung von mehreren Sicherheitsanbietern, um eine zuverlässige Identifizierung von Schadcode zu gewährleisten.

Um beim Einsatz dieser Schutzfunktion eine optimale Verträglichkeit mit dem Betriebssystem und anderen Programmen zu erzielen, ist die Bearbeitungsgeschwindigkeit der Zugriffe entscheidend. Im United Endpoint Protector können Sie mehrere Technologien gleichzeitig nutzen, die ihre Untersuchungen parallel durchführen. Die gesamte Bearbeitungsdauer eines Zugriffs entspricht dabei jener des jeweils langsamsten Anbieters. Für die Dateisicherheit eignen sich daher besonders Anbieter mit einem hohen Datendurchsatz.

Zur Beurteilung der Geschwindigkeit können Sie in den allgemeinen Einstellungen (siehe Kapitel 5.1) die Anzeige der Scan-Dauern aktivieren. Damit werden im Dateisicherheitsmonitor die einzelnen Bearbeitungszeiten aller Anbieter sichtbar, samt einer Berechnung der Durchschnittswerte. Mit dieser Hilfestellung können passende Anbieter für diese Funktion identifiziert werden.

Neben der Auswahl passender Anbieter, hat auch die Festlegung der maximal zu untersuchenden Dateigröße eine Auswirkung auf die Gesamtleistung. Je größer eine Datei ist, desto mehr Zeit wird für deren Überprüfung benötigt. Die Größe sollte daher so klein wie möglich, aber so groß wie nötig gewählt sein. Ein Mittelwert von 10 MB wird von vielen Sicherheitsanbietern empfohlen, kann aber nach eigenem Ermessen festgelegt werden.

Der Einsatz von Ausnahmeregeln stellt eine weitere Optimierungsmöglichkeit dar (siehe Kapitel 12). Mit gezielten Ausnahmen für die Zugriffsüberwachung kann deren Arbeitslast verringert und ungewünschte Verzögerungen vermieden werden.

6. Speicherschutz

Der Speicherschutz ermöglicht die Überprüfung des Arbeitsspeichers eines Computers. Das ist eine wichtige Sicherheitsfunktion, um die aktive Ausführung von schadhaftem Code festzustellen und zu stoppen. Für diese Aufgabe stehen verschiedene forensische Methoden von Rekall Forensics zur Verfügung, mit denen der Arbeitsspeicher aus unterschiedlichen Blickwinkeln betrachtet und auch versteckte Code-Ausführungen sichtbar gemacht werden können. Die offengelegten Daten können anschließend von gewünschten Sicherheitsanbietern beurteilen lassen, um Bedrohungen festzustellen.

Klicken Sie im Hauptmenü auf „Speicherschutz", um den Speicherschutz-Monitor zu öffnen. Dieser zeigt das Ergebnis der letzten bzw. laufenden Überprüfung des Arbeitsspeichers an.

Speicherschutz -> Monitor

Im oberen Bereich des Monitors werden die verschiedenen forensischen Methoden dargestellt, die während der Überprüfung durchlaufen werden. Durch farbliche Markierungen wird der Fortschritt angezeigt, sowie die Zeitdauer der Untersuchung und die Anzahl der entdeckten Prozesse. Darunter werden Statusinformationen dargestellt, die den letzten Untersuchungszeitpunkt bzw. die aktuell untersuchte Datei ausgeben.

Im unteren Bereich wird das detaillierte Untersuchungsergebnis aufbereitet. Dies umfasst Informationen zu den entdeckten Prozessen, deren geladene Dateien, sowie das Untersuchungsergebnis der eingesetzten Sicherheitsanbieter.

In der unteren Menüleiste kann eine Untersuchung manuell gestartet oder gestoppt, das Untersuchungsergebnis in Form eines Baumes visualisiert oder in eine XLS-Datei exportiert werden.

6.1. Ausführung

Die Untersuchung des Arbeitsspeichers kann manuell oder in einem zeitlichen Intervall erfolgen. Zu Beginn einer Untersuchung wird die Version des Windows-Kernels überprüft. Sollte sich diese seit der letzten Untersuchung geändert haben (z.B. durch Windows-Updates), wird eine Verbindung zum Microsoft Symbolserver (https://msdl.microsoft.com/download/symbols) aufgebaut, um benötigte Kernel-Daten herunterzuladen. Diese dienen als Landkarte für den Windows-Kernel und werden von den forensischen Methoden benötigt, um die Speicherbereiche und Eintrittspunkte korrekt zu identifizieren.

Wenn für die Internetverbindung ein Proxy-Server eingesetzt wird, kann dieser im Hauptmenü unter „Aktualisieren –> Proxy" festgelegt werden (siehe Kapitel 4.2). Dabei ist darauf zu achten, dass bei „Verwende Proxy für" die Option „Windows Kernel-Daten" aktiviert ist. Sollte keine Internetverbindung aufgebaut werden können oder Microsoft die Kernel-Daten für die aktuelle Windows Version noch nicht veröffentlicht haben, können die forensischen Methoden nicht arbeiten. In diesem Fall schaltet der Speicherschutz in einen Notbetrieb. Dieser nutzt statt den forensischen Methoden traditionelle Windows-API's zur Feststellung bekannter Prozesse und führt deren Untersuchung durch. Symbolisiert wird der Notbetrieb durch graue Pfeile im Speicherschutz-Monitor.

6.2. Allgemeine Einstellungen

Die Funktionsweise des Speicherschutzes kann über die allgemeinen Einstellungen festgelegt werden. Klicken Sie dazu im Untermenü von „Speicherschutz" auf „Allgemein".

Speicherschutz -> Allgemein

Auf der Konfigurationsoberfläche können die folgenden Einstellungen vorgenommen werden:

Speicherschutz aktivieren	Aktiviert die automatische Überprüfung des Arbeitsspeichers basierend auf der festgelegten Zeitplanung. Wird sie nicht aktiviert, steht sie zur manuellen Ausführung bereit.
Forensische Methode	Definiert die forensischen Methoden, die bei der Überprüfung verwendet werden sollen. Nicht aktivierte Methoden werden übersprungen.
Zeitplanung	Legt den Zeitplan für die automatische Ausführung der Untersuchung fest. „Scan-Intervall" definiert die Anzahl der Minuten wann die Untersuchung, nach Abschluss des vorangegangenen Laufes, erneut ausgeführt werden soll. „Verzögerung" beschreibt den Zeitraum, wann die Aufgabe starten soll, falls die letzte reguläre Ausführung nicht stattgefunden hat. Das ist zum Beispiel der Fall, wenn ein Computer ausgeschalten war. Die Verzögerung gibt in diesem Fall die Anzahl der Minuten an, wann die erste Ausführung nach dem Einschalten des Computers stattfinden soll.
Ressourcennutzung	Ermöglicht die zu verwendende CPU-Belastung während einer Untersuchung festzulegen. Dabei gilt es zu bedenken: Je stärker die CPU genutzt wird, desto kürzer dauert eine Untersuchung. Je weniger eine CPU genutzt wird, desto länger dauert eine Untersuchung.
Maximale Dateigröße	Diese Einstellmöglichkeit hat eine doppelte Funktion. Zum einen legt sie die maximale Größe einer Datei für die Untersuchung durch Sicherheitsanbieter fest. Ist eine entdeckte Datei größer als der angegebene Wert, wird sie nicht überprüft. Zum anderen legt dieser Wert die maximale Größe des Speicherbereiches eines Prozesses für die Untersuchung fest. Ist der verwendete Speicherbereich eines aktiven Prozesses kleiner als der angegebene Wert, wird dieser vollständig aus dem Speicher extrahiert und zur Überprüfung herangezogen. Ist der Speicherbereich größer, findet keine Extraktion statt und nur die referenzierte ausführbare Datei wird untersucht.

Scan-Dauer anzeigen	Zeigt im Monitor des Speicherschutzes die Zeitdauern der Sicherheitsanbieter an, die für die Überprüfung der gefundenen Dateien erforderlich sind.

6.3. Strategie

Die Überprüfung des Arbeitsspeichers auf bösartige Code-Ausführungen ist eine wichtige Sicherheitsfunktionen. Einem regulären Prozessstart geht zwar ein Dateizugriff voraus, der durch die Dateisicherheit überprüft werden kann, jedoch findet diese Überprüfung nur zum Zeitpunkt des Prozessstarts statt. Wenn zu diesem Zeitpunkt die Erkennungsrate durch die ausgewählten Sicherheitsanbieter noch nicht zur Verfügung steht, der startende Prozess selbst nicht bösartig ist (wie zum Beispiel bei File-Less-Malware) oder Code auf andere Wege eingeschleust wird, kann es zu einer Infektion kommen. Wir empfehlen daher die Untersuchung des Arbeitsspeichers in regelmäßigen Zeitintervallen durchführen zu lassen.

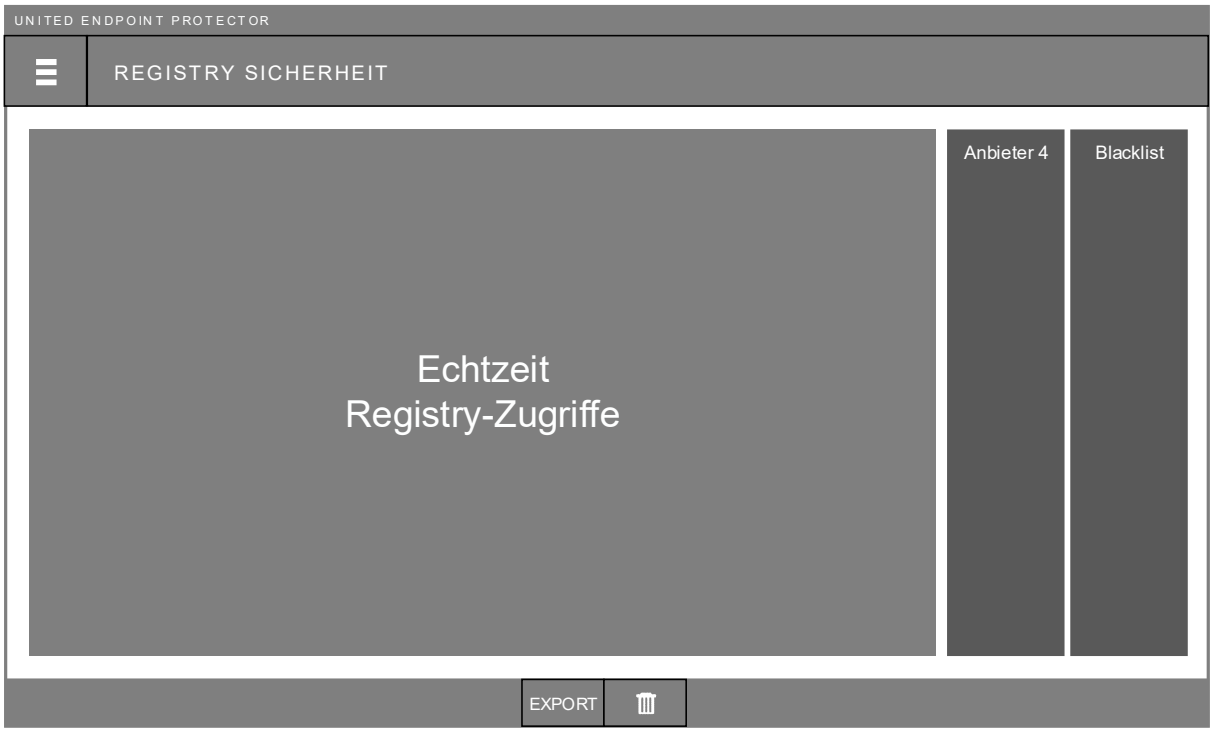
Als mögliche Alternative oder Ergänzung zu den intervallmäßigen Überprüfungen, können Sie diese auch durch einen Auf-Anforderung-Scan (siehe Kapitel 8) mit anderen Zeitplanungsoptionen durchführen lassen. Eine weitere Möglichkeit ist die Untersuchung des Arbeitsspeichers mit einer Scan-Aktion (siehe Kapitel 11) zu verbinden. Identifiziert zum Beispiel die Dateisicherheit eine bösartige Datei auf der Festplatte, kann als Reaktion darauf eine Speicherüberprüfung ausgelöst werden, um aktuell ausgeführten, bösartigen Code zu erkennen.

Bei der Wahl der Sicherheitsanbieter kommt es, im Vergleich zur Dateisicherheit, nicht auf den Datendurchsatz an. Es können daher auch langsamere Anbieter oder zeitaufwendigere Untersuchungstechniken zum Einsatz kommen. Eine mögliche Strategie könnte daher sein besonders schnelle Anbieter in der Dateisicherheit und langsamere Anbieter für den Speicherschutz zu nutzen. Auch die Vielfalt an Anbieter und Techniken könnte damit erweitert werden.

7. Registry Sicherheit

Die Registry Sicherheit ermöglicht in Echtzeit alle Zugriffe auf die Microsoft Windows Registry, sowie auf andere Application Hives, zu überwachen. Diese sind ein beliebtes Ziel von Malware, um schadhafte Manipulationen vorzunehmen, eigene Daten abzuspeichern oder sich in das System einzunisten. Neben der Überwachung der Zugriffe können Sie verfügbare Sicherheitsanbieter zur Beurteilung der Zugriffe nutzen oder mit Hilfe der Blacklist (siehe Kapitel 10) einen präventiven Schutz errichten.

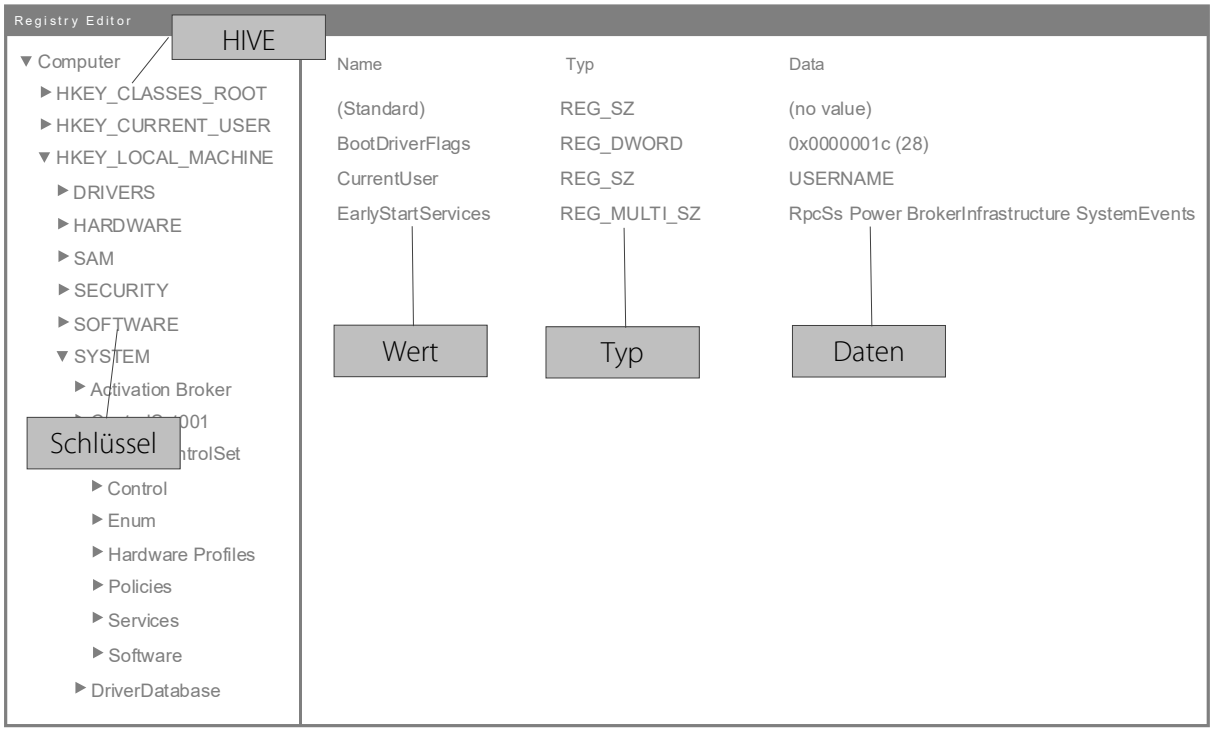
Klicken Sie im Hauptmenü auf „Registry Sicherheit", um den Registry-Sicherheit-Monitor zu öffnen. Der Monitor stellt in Echtzeit alle Zugriffe dar, sowie die jeweilige Sicherheitseinschätzung und das Säuberungsergebnis der aktivierten Anbieter.



Registry Sicherheit -> Monitor

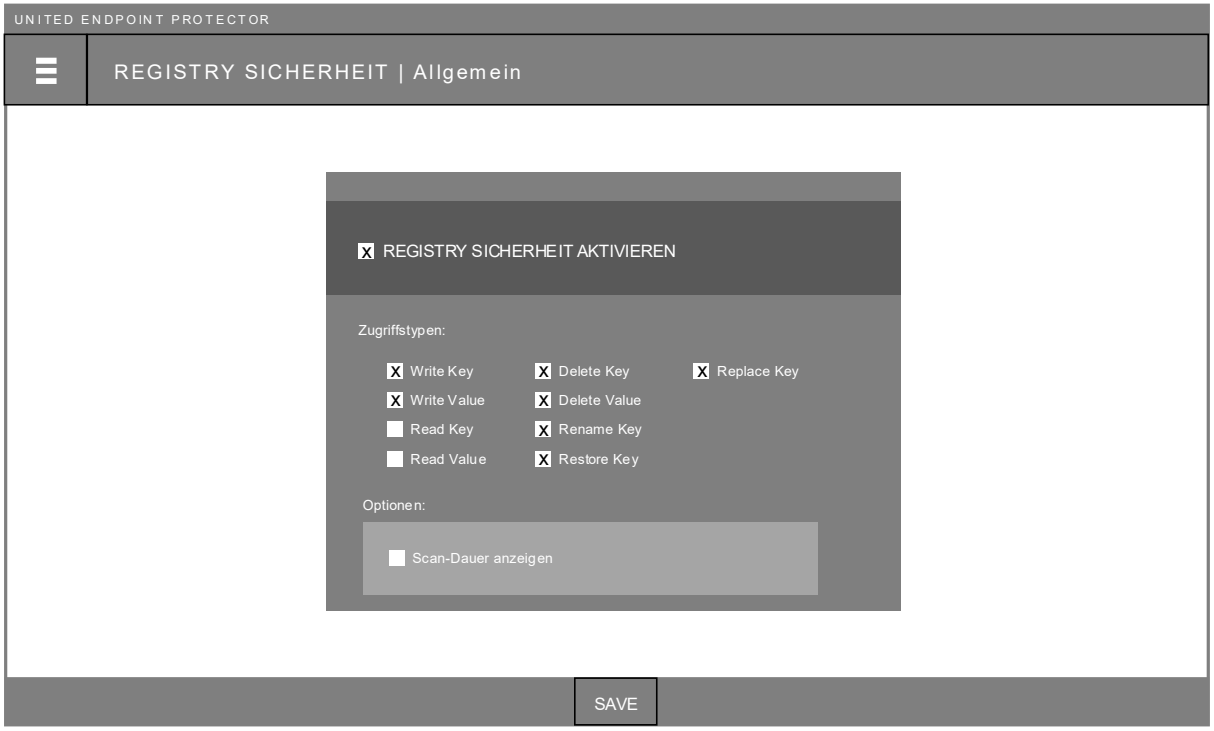
Auf der Benutzeroberfläche werden die letzten 10.000 Zugriffe dargestellt, die Sie mit Hilfe der Filterleiste in Echtzeit durchsuchen können. Mit dem Export-Icon in der unteren Menüleiste können Sie alle aufgezeichneten Zugriffe in eine XLS-Datei exportieren. Das Lösch-Icon erlaubt hingegen die manuelle Löschung aller aufgezeichneten Daten. Eine automatische Löschung findet durch das Beenden des United Endpoint Protector Dienstes bzw. in regelmäßigen Abständen, wenn Daten älter als 24 Stunden sind, statt.

Zum besseren Verständnis der angezeigten Registry-Daten, erläutert die nachstehende Darstellung die Begriffe am Beispiel des Windows Registry Editors.



7.1. Allgemeine Einstellungen

Die Funktionsweise der Registry Sicherheit kann über die allgemeinen Einstellungen festgelegt werden. Klicken Sie dazu im Untermenü von „Registry Sicherheit“ auf „Allgemein“.



Registry Sicherheit -> Allgemein

Auf der Konfigurationsoberfläche können die folgenden Einstellungen vorgenommen werden:

Registry Sicherheit aktivieren	Aktiviert oder deaktiviert die Überwachung der Registry-Zugriffe.
Zugriffstypen	Legt die Art der Zugriffe fest die überwacht werden sollen.
Scan-Dauer anzeigen	Zeigt im Monitor der Registry Sicherheit die Zeitdauern an, die für die Überprüfung der Registry-Zugriffe erforderlich sind.

7.2. Strategie

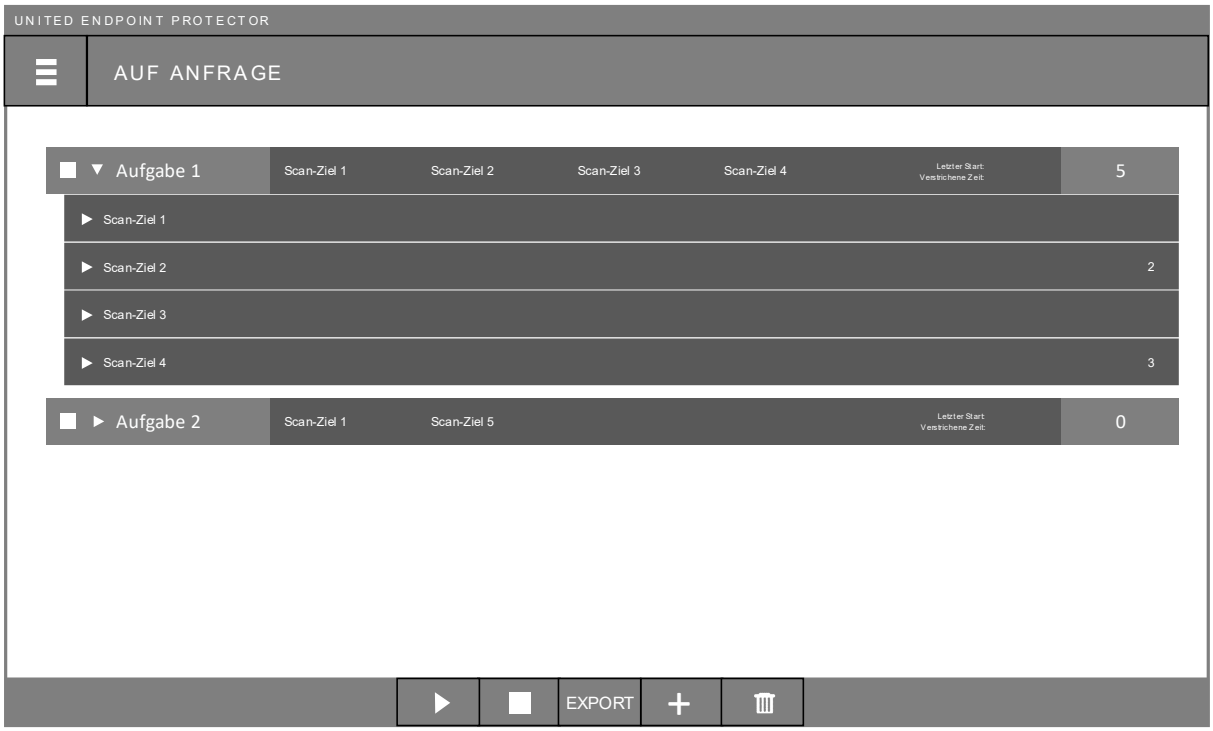
Die Überwachung der Registry-Zugriffe kann ein wichtiges Hilfsmittel zur Aufspürung und Entfernung von Bedrohungen sein. Eine wichtige Entscheidung ist dabei die Arten der Zugriffe festzulegen die überwacht werden sollen. Registry-Zugriffe treten in einer größeren Anzahl als Dateizugriffe auf und folglich benötigt deren Überprüfung mehr Systemressourcen. Wir empfehlen daher die Überwachung auf jene Zugriffe zu beschränken, die Änderungen an der Registry vornehmen und folglich eine potentielle Gefahr darstellen. Andere Zugriffe wie „Read Key" oder „Read Value" können bei Bedarf überwacht werden, jedoch mit einem spürbaren Effekt auf die Systemleistung.

Die Bewertung ob ein Zugriff bösartig ist oder nicht kann durch Sicherheitsanbieter durchgeführt werden, wenn Anbieter verfügbar sind die dies unterstützen. In jedem Fall kann die Blacklist (siehe Kapitel 10) genutzt werden, um spezifische Zugriffe zu blockieren. Eine mögliche Strategie kann dabei die Erfassung von bekannten, bösartigen Aktivitäten sein, um einen manuellen Schutz zu realisieren. Eine andere Möglichkeit ist die Errichtung eines präventiven Schutzes. Beispielsweise könnte die Änderung der Startseite eines Web-Browsers nur für bestimmte Prozesse erlaubt werden (Blockierung mit der Blacklist und festlegen von erlaubten Prozessen über Ausnahmen).

8. Auf-Anforderung Scans

Auf-Anforderung Scans erlauben zeitlich geplante Untersuchungen von verschiedenen Bereichen des Computers zu erstellen. Diese können genutzt werden, um bislang nicht entdeckte Bedrohungen aufzuspüren und eine weitere Sicherheitsebene einzuführen.

Klicken Sie dazu im Hauptmenü auf „Auf Anforderung“, um die Übersicht der Auf-Anforderung-Scans zu öffnen. Auf dieser Übersicht werden alle erstellen Scan-Aufgaben dargestellt. Für jede Aufgabe werden die überprüften Scan-Ziele, die Anzahl der gefundenen Bedrohungen, sowie Informationen über die letzte Ausführung dargestellt. Mit Hilfe der Expander kann das letzte bzw. laufende Untersuchungsergebnis im Detail angezeigt werden. Eine erneute Ausführung der Scan-Aufgabe löscht das vorangegangene Untersuchungsergebnis.

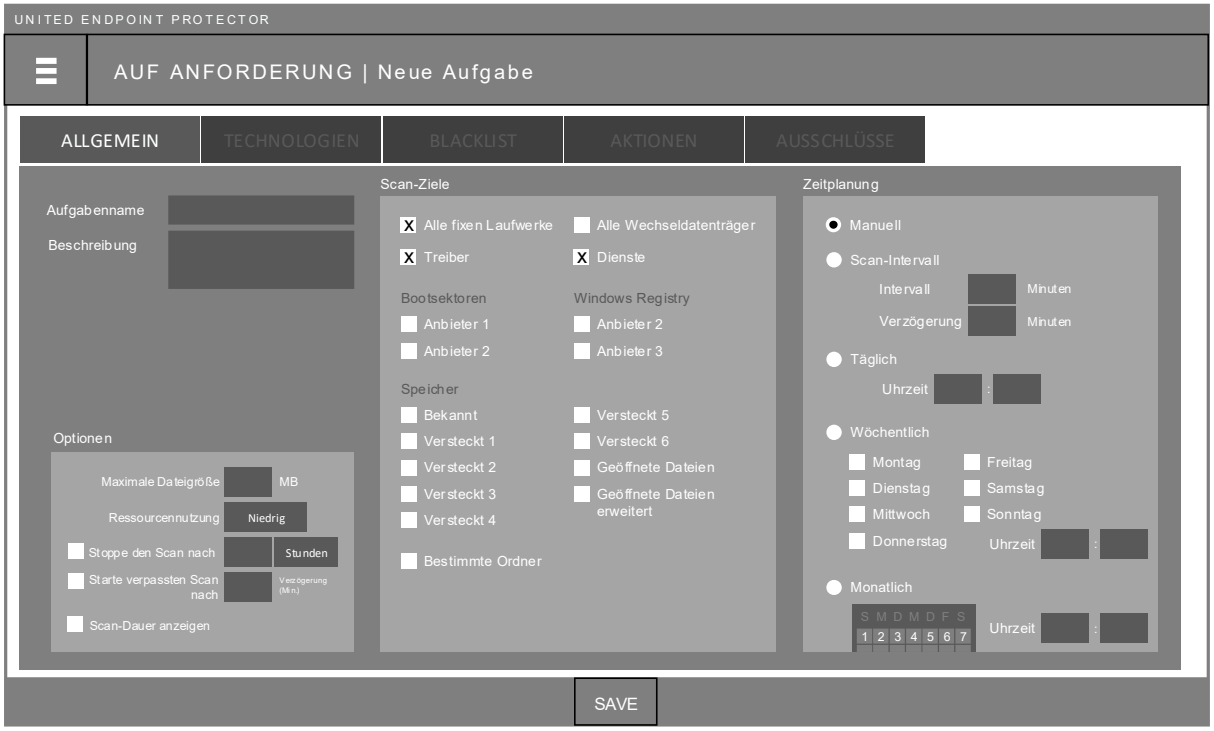


Auf Anfrage -> Übersicht

Durch Auswahl einer Aufgabe über das zugehörige Kontrollkästchens stehen in der unteren Menüleiste verschiedene Funktionen zur Verfügung. Mit diesen können Aufgaben manuell gestartet oder gestoppt, das letzte Untersuchungsergebnis in eine XLS-Datei exportiert oder eine Aufgabe gelöscht werden.

8.1. Erstellen einer Scan-Aufgabe

Zur Erstellung einer neuen Scan-Aufgabe klicken Sie im Hauptmenü auf „Auf Anfrage“ und klicken in der unteren Menüleiste auf das Hinzufügen-Icon. Daraufhin öffnet sich die Konfigurationsoberfläche für eine neue Aufgabe.



Auf Anfrage –> Scan-Aufgabe -> Allgemein

Neben der Vergabe eines beliebigen Namens für die Aufgabe und einer optionalen Beschreibung, können auf dieser Konfigurationsoberfläche die folgenden Scan-Ziele ausgewählt werden:

Alle fixen Laufwerke	Nutzt forensische Methoden, um alle Daten auf allen lokalen Festplatten sichtbar zu machen und mit ausgewählten Sicherheitsanbietern zu überprüfen.
Alle Wechseldatenträger	Nutzt forensische Methoden, um alle Daten auf angeschlossenen Wechseldatenträgern (z.B. USB-Sticks, externe Festplatten) sichtbar zu machen und mit ausgewählten Sicherheitsanbietern zu überprüfen.
Treiber	Nutzt forensische Methoden, um alle im System registrierten Gerätetreiber sichtbar zu machen und mit ausgewählten Sicherheitsanbietern zu überprüfen.

Dienste	Nutzt forensische Methoden, um alle im System registrierten Windows Dienste sichtbar zu machen und mit ausgewählten Sicherheitsanbietern zu überprüfen.
Bootsektoren	Abhängig von den freigeschalteten Sicherheitsanbietern besteht die Möglichkeit Master- und Volume Boot Records zu untersuchen. Dabei entscheidet der jeweilige Anbieter über den Umfang der Untersuchung.
Windows Registry	Im Vergleich zur Registry Sicherheit besteht auch die Möglichkeit, abhängig von verfügbaren Sicherheitsanbietern, die Windows Registry zeitlich geplant zu überprüfen. Dabei entscheidet der jeweilige Anbieter welche Teile der Registry untersucht werden.
Speicher	Ermöglicht die gleiche Überprüfung des Arbeitsspeichers wie der Speicherschutz, allerdings mit anderen Zeitplanungsoptionen.
Bestimmte Ordner	Erlaubt ein oder mehrere spezifische Ordner mit gewünschten Sicherheitsanbietern zu untersuchen, auf Basis forensischer Methoden.

Neben der Festlegung der gewünschten Scan-Ziele kann mit Hilfe der nachstehenden Zeitplanungsoptionen der Zeitpunkt der Überprüfung festgelegt werden:

Manuell	Es findet keine automatische Ausführung dieser Aufgabe statt, sondern diese kann über die „Auf-Anforderung – Übersicht" manuell gestartet werden.
Scan-Intervall	Die Aufgabe wird im angegebenen Minuten-Intervall wiederholt. Sollte die letzte reguläre Ausführung nicht stattgefunden haben, weil der Computer beispielsweise abgeschaltet war, legt die Verzögerung fest wann die nächste Ausführung stattfinden soll.
Täglich	Die Aufgabe wird jeden Tag zur angegebenen Uhrzeit (24 Stunden Format) ausgeführt.

Wöchentlich	Die Aufgabe wird jede Woche, zu den angegebenen Wochentagen, zur angegebenen Uhrzeit (24 Stunden Format), ausgeführt.
Monatlich	Die Aufgabe wird jeden Monat, zu den angegebenen Tagen des Monats, zur angegebenen Uhrzeit (24 Stunden Format), ausgeführt.

Zusätzlich können für die Ausführung der Aufgabe die folgenden Optionen festgelegt werden:

Maximale Dateigröße	Legt die maximale Größe einer Datei fest, um durch die Sicherheitsanbieter überprüft zu werden. Jede Datei die größer als der angegebene Wert ist wird ignoriert. Im Falle des Scan-Ziels „Speicher" definiert dieser Wert auch die maximale Größe des Speicherbereiches eines Prozesses für die Extraktion.
Ressourcennutzung	Ermöglicht die zu verwendende CPU-Belastung während einer Untersuchung festzulegen. Dabei gilt es zu bedenken: Je stärker die CPU genutzt wird, desto schneller ist die Aufgabe abgeschlossen. Je weniger die CPU genutzt wird, desto länger ist die Laufzeit der Aufgabe.
Stoppe den Scan nach	Gibt die Anzahl der Stunden oder Minuten an wann die Aufgabe automatisch gestoppt werden soll.
Starte verpassten Scan nach	Legt fest ob eine Scan-Aufgabe, die den regulären Ausführungszeitpunkt verpasst hat, nachgeholt werden soll. Die Verzögerung gibt dabei den Zeitpunkt an, wann die nächste Ausführung stattfinden soll.
Scan-Dauer anzeigen	Zeigt in den detaillierten Darstellungen der Scan-Ziele in der „Auf-Anforderung Übersicht" die Zeitdauern an, die für die Überprüfung der Dateien erforderlich waren.

8.2. Strategie

Die Hauptaufgabe von Auf-Anforderung-Scans ist die Errichtung von Kontrollinstanzen, die noch nicht entdeckte Bedrohungen aufspüren sollen. Auch als mögliche Reaktion auf eine bereits erkannte Bedrohung (siehe Kapitel 11) können Scan-Aufgaben zum Einsatz kommen. Der maximale Nutzen wird dabei durch den Einsatz von anderen oder zusätzlichen Sicherheitsanbietern erzielt, die aus bestimmten Gründen, in anderen Sicherheitsfunktionen, vielleicht nicht zum Einsatz kommen. Im Vergleich zur Dateisicherheit kommt es bei der Wahl der Anbieter für einen Auf-Anforderung-Scan nicht auf den Datendurchsatz an. Folglich können auch zeitintensivere Untersuchungstechniken in diesem Anwendungsgebiet genutzt werden.

Wir empfehlen den Einsatz von zwei verschiedenen Auf-Anforderung-Scans:

Hot-Spot Scan

Dieser Scan hat die Aufgabe die wichtigsten Bereiche eines Computers, die häufig von Malware genutzt werden, zu überprüfen. Dazu zählen die Scan-Ziele „Treiber", „Dienste", „Bootsektor" und „Windows Registry". Auch einzelne Verzeichnisse wie der Windows-Ordner, Temp-Verzeichnisse oder der Profilordner von Benutzern, könnten für diese Aufgabe in Frage kommen. Abhängig von der Anzahl an ausgewählten Scan-Zielen und welche Systemressourcen auf dem Computersystem zur Verfügung stehen (CPU-Kapazität, Geschwindigkeit der Festplatte), sollte diese Überprüfung in einem Zeitintervall von wenigen Stunden stattfinden. Die Ressourcensteuerung kann dabei auf die Gegebenheiten angepasst werden, um negative Auswirkungen für den Endanwender zu vermeiden.

Vollständiger Scan

Dieser Scan hat die Aufgabe die lokalen Festplatten zu überprüfen. Dazu eignet sich das Scan-Ziel „Alle fixen Laufwerke". Ziel dieser Überprüfung ist schadhafte Dateien, die zum Zeitpunkt des Zugriffs durch die Dateisicherheit nicht identifiziert wurden, zu entdecken und zu entfernen. Abhängig von der verfügbaren Datenmenge kann diese Prüfung mehrere Stunden in Anspruch nehmen. Es sollte daher ein Zeitpunkt gewählt werden, der sich mit dem IT-Betrieb gut vereinbaren lässt. Für Server eignen sich dafür meist die Wochenend- oder Nachtstunden, wohingegen Workstations zu Zeitpunkten überprüft werden müssen an denen diese eingeschalten sind. In diesem Fall empfehlen wir eine niedrige Ressourcennutzung, um negative Auswirkungen für den Endanwender zu vermeiden.

9. Technologien

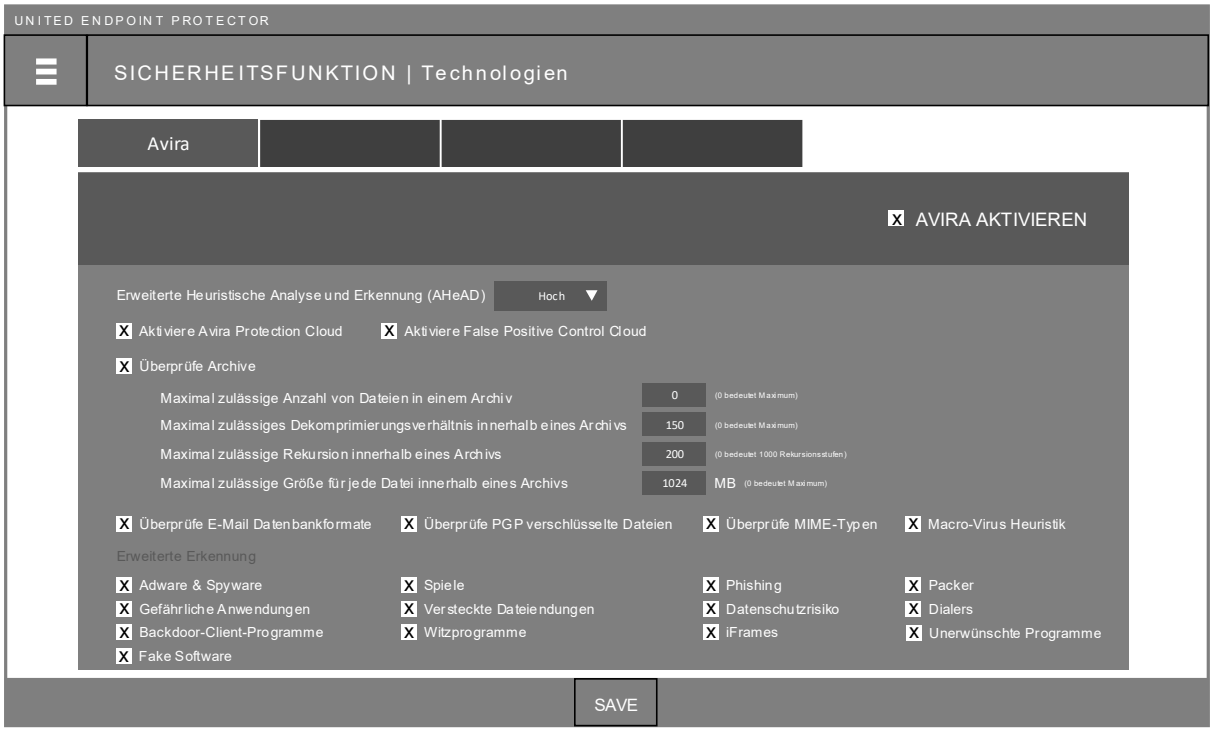
Abhängig von den freigeschalteten Sicherheitsanbietern (siehe Kapitel 3), stehen Ihnen die entsprechenden Konfigurationsoberflächen für die Technologien zur Verfügung. Mit deren Hilfe können Sie verschiedene Einstellungen für den jeweiligen Anbieter vornehmen. Für eine maximale Flexibilität stehen Ihnen die Oberflächen in jeder Sicherheitsfunktion einzeln bereit, um separate Einstellungen für den jeweiligen Anwendungszweck vornehmen zu können.

Die Oberflächen befinden sich im jeweiligen Untermenü der Sicherheitsfunktionen im Hauptmenü. Die wichtigste Einstellungsmöglichkeit ist die Aktivierung der verschiedenen Technologien. Mit dieser können Sie für jede Sicherheitsfunktion festlegen welche Sicherheitsanbieter, in welchen Kombinationen, die jeweiligen Daten überprüfen sollen.

Nachstehend erläutern wir die Einstellungsmöglichkeiten für die im United Endpoint Protector (UEP) verfügbaren Anbieter.

9.1. Avira

Folgende Konfigurationsoptionen stehen für die Technologie von Avira zur Verfügung:



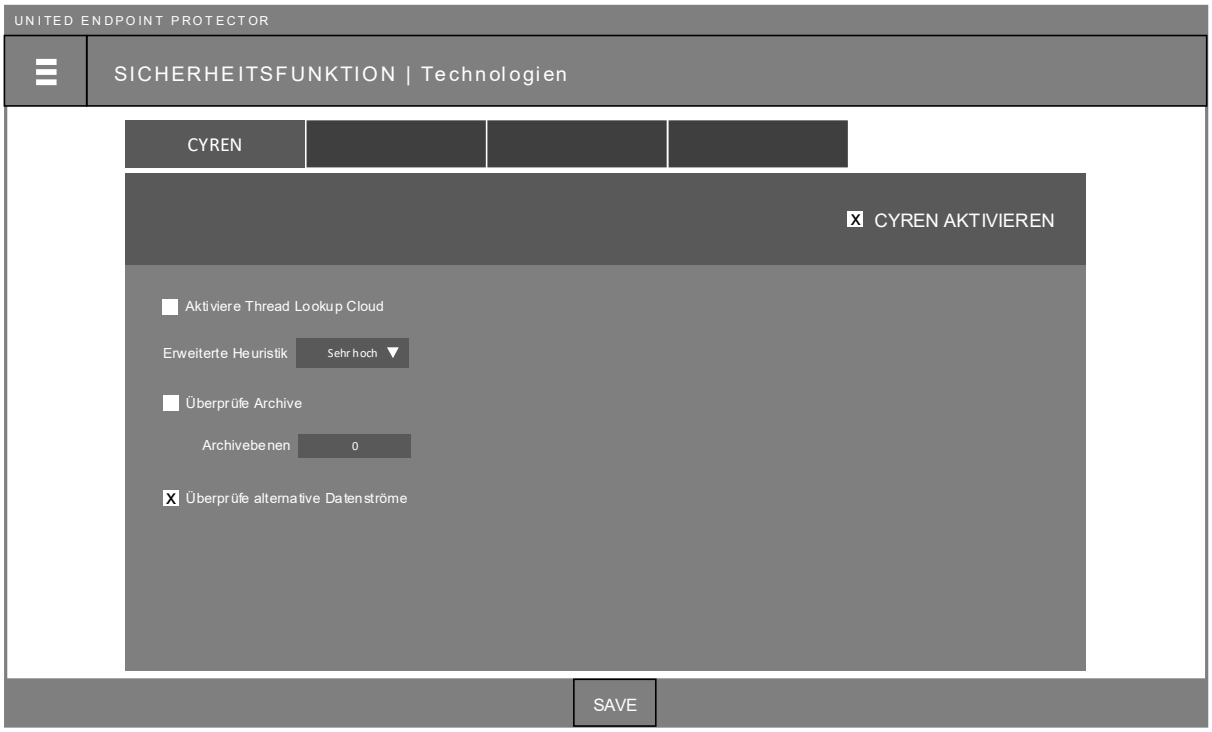
Technologien -> Avira

AVIRA Aktivieren	Aktiviert oder deaktiviert die Datenüberprüfung durch Avira in der jeweiligen Sicherheitsfunktion.
Erweiterte Heuristische Analyse und Erkennung (AHeAD)	Aktiviert oder deaktiviert die heuristische Erkennung von Bedrohungen und legt dessen Empfindlichkeitsstufe fest.
Aktiviere Avira Protection Cloud	Aktiviert die zusätzliche Bedrohungserkennung durch die Avira-Cloud. Wenn diese Funktion aktiviert ist werden PE, non-PE und weitere Dateitypen, nach einer lokalen Überprüfung, zusätzlich durch die Cloud bewertet. Dafür wird von der Datei ein HASH-Wert gebildet und an *.compute.amazonaws.com über Port 443 bzw. 80 übermittelt. Sollte der HASH-Wert noch unbekannt sein, wird die vollständige Datei zur detaillierten Analyse übertragen. Wenn für die Internetverbindung ein Proxy-Server eingesetzt wird, können Sie diesen in den Proxy-Einstellung (siehe Kapitel 4.2) eintragen. Achten Sie darauf die Funktion „Cloud-Verbindungen" in den Proxy-Einstellungen zu aktivieren. Die aktivierte Verwendung der Cloud wird im Kopf der Avira-Spalte in der jeweiligen Sicherheitsfunktion durch ein Cloud-Icon symbolisiert.
Aktiviere False Positive Control Cloud	Aktiviert einen zusätzlichen Schutz vor Fehlalarmen (False-Positves) durch Unterstützung der Avira-Cloud. Wenn diese Funktion aktiviert ist und bei einer lokalen Überprüfung eine Bedrohung festgestellt wurde, wird der HASH-Wert der Datei, samt weiteren Informationen (Dateiname, Bedrohungsname, Dateigröße, Erstellungs- und Änderungsdatum etc.) an *.compute.amazonaws.com über Port 443 bzw. 80 übermittelt. Diese Informationen werden in der Cloud genutzt, um die korrekte Erkennung der Bedrohung zu bestätigen und im Falle eines Fehlers zu korrigieren. Wenn für die Internetverbindung ein Proxy-Server eingesetzt wird, können Sie diesen in den Proxy-Einstellung (siehe Kapitel 4.2) eintragen. Achten Sie darauf die Funktion „Cloud-Verbindungen" in den Proxy-Einstellungen zu aktivieren.
Überprüfe Archive	Aktiviert oder deaktiviert die Überprüfung von Archiven, wie zum Beispiel ZIP-Dateien, auf enthaltene, bösartige Dateien.
Maximal zulässige Anzahl von Dateien in einem Archiv	Legt die maximale Anzahl von Dateien innerhalb eines Archivs fest die überprüft werden sollen.

Maximal zulässiges Dekomprimierungsverhältnis innerhalb eines Archivs	Legt das maximale Dekomprimierungsverhältnis innerhalb eines Archivs fest, um die Überprüfung durchzuführen.
Maximal zulässige Rekursion innerhalb eines Archivs	Legt die maximale Rekursionstiefe innerhalb eines Archivs fest das überprüft werden soll.
Maximal zulässige Größe für jede Datei innerhalb eines Archivs	Legt die maximale Dateigröße innerhalb eines Archivs fest die überprüft werden soll.
Überprüfe E-Mail Datenbankformate	Schließt Dateien in die Untersuchung ein, die ein E-Mail Datenbankformat aufweisen (z.B. EML).
Überprüfe PGP verschlüsselte Dateien	Schließt Dateien in die Untersuchung ein die eine PGP Verschlüsselung aufweisen.
Macrovirus Heuristik	Aktiviert oder deaktiviert die heuristische Überprüfung von Macros in Office-Dokumenten.
Überprüfe MIME-Typen	Schließt Dateien in die Untersuchung ein, die einen MIME-Datentyp aufweisen.
Erweiterte Erkennung	Legt zusätzliche Bedrohungsarten fest, die bei der Beurteilung von Dateien in Betracht gezogen werden sollen.

9.2. Cyren

Folgende Konfigurationsoptionen stehen für die Technologie von Cyren zur Verfügung:



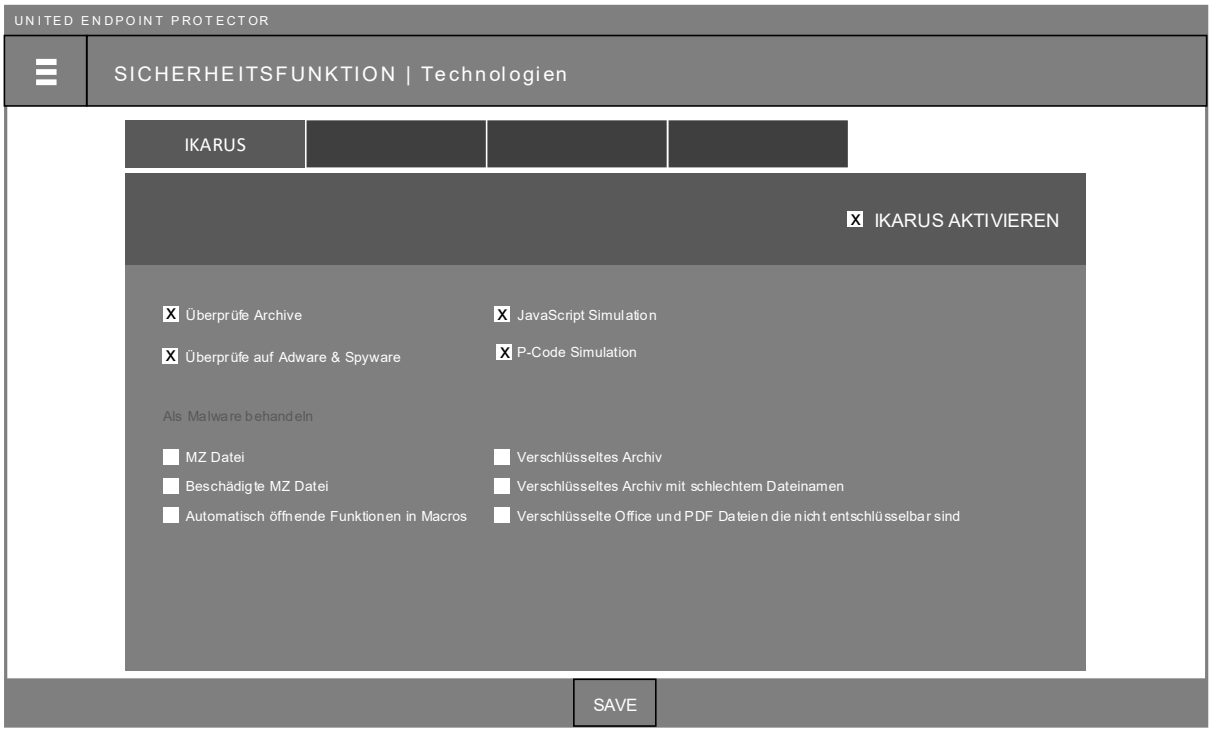
Technologien -> CYREN

CYREN Aktivieren	Aktiviert oder deaktiviert die Datenüberprüfung durch Cyren in der jeweiligen Sicherheitsfunktion.
Aktiviere Thread Lookup Cloud	Aktiviert die zusätzliche Bedrohungserkennung durch die Cyren Thread Lookup Cloud. Wenn diese Funktion aktiviert ist werden PE Dateien, nach einer lokalen Überprüfung, zusätzlich durch die Cloud bewertet. Dafür wird von der Datei ein HASH-Wert gebildet und mit zusätzlichen Informationen (Signatur-Version, Engine-Version, ausgelöster Regelname, License-ID) an 84.39.152.194 via Port 443 übermittelt. Die aktivierte Verwendung der Cloud wird im Kopf der Cyren-Spalte in der jeweiligen Sicherheitsfunktion durch ein Cloud-Icon symbolisiert.
Erweiterte Heuristik	Aktiviert oder deaktiviert die heuristische Erkennung von Bedrohungen und definiert deren Empfindlichkeitsstufe.

Überprüfe Archive	Aktiviert oder deaktiviert die Überprüfung von Archiven, wie zum Beispiel ZIP-Dateien, auf enthaltene, bösartige Dateien.
Archivebenen	Legt die maximale Anzahl an Archivebenen fest, die bei der Überprüfung berücksichtigt werden sollen.
Überprüfe alternative Datenströme	Aktiviert oder deaktiviert die Untersuchung von alternativen Datenströmen von Dateien.

9.3. IKARUS

Folgende Konfigurationsoptionen stehen für die Technologie von IKARUS zur Verfügung:



Technologien -> IKARUS

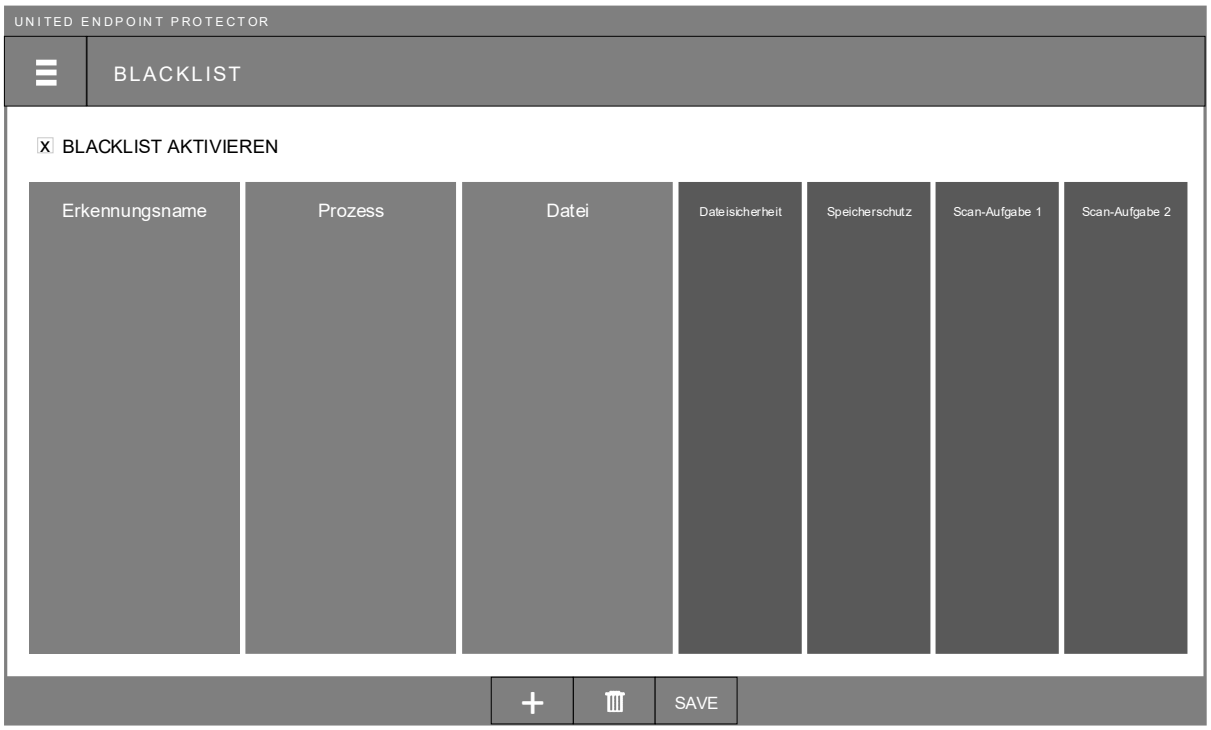
IKARUS Aktivieren	Aktiviert oder deaktiviert die Datenüberprüfung durch IKARUS in der jeweiligen Sicherheitsfunktion.
Überprüfe Archive	Aktiviert oder deaktiviert die Überprüfung von Archiven, wie zum Beispiel ZIP-Dateien, auf enthaltene, bösartige Dateien.
Überprüfe auf Adware & Spyware	Aktiviert oder deaktiviert die Bedrohungskategorie „Adware & Spyware“ bei der Beurteilung von Dateien.
JavaScript Simulation	Aktiviert oder deaktiviert die virtuelle Ausführung von Java Scripts zur Feststellung von Bedrohungen.
P-Code Simulation	Aktiviert oder deaktiviert die virtuelle Ausführung von Pseudo-Maschine-Codes zur Feststellung von Bedrohungen.
Als Malware behandeln	Ermöglicht bestimmte Dateiarten als Bedrohung anzusehen, unabhängig von deren Sicherheitsstatus.

10. Blacklist

Neben dem Einsatz von professionellen Sicherheitsanbietern, steht Ihnen die Blacklist in allen Sicherheitsfunktionen zur Verfügung. Mit dieser können Sie manuelle Erkennungen festlegen. Dafür stehen Ihnen im United Endpoint Protector (UEP) zwei verschiedene Listen zur Verfügung, in denen Sie Dateien und Zugriffe definieren können, die als bösartig betrachtet werden sollen.

10.1. Datei-Blacklist

Die Datei-Blacklist ist eine globale Liste von Einträgen zur manuellen Erfassung von Datei- und Prozess-basierten Bedrohungen. Diese Liste kann im jeweiligen Untermenü der Sicherheitsfunktionen „Dateisicherheit" und „Speicherschutz", sowie auf der Konfigurationsoberfläche von Scan-Aufgaben (siehe Kapitel 8.1) aufgerufen werden.



Sicherheitsfunktion –> Blacklist (Global)

Mit den Schaltflächen in der unteren Menüleiste können Einträge der Liste hinzugefügt, bestehende entfernt und die vorgenommenen Änderungen gespeichert werden. Im oberen Bereich der Oberfläche kann die Blacklist für die jeweilige Sicherheitsfunktion aktiviert werden. Diese wird in den Übersichten der Sicherheitsfunktionen auf die gleiche Weise dargestellt wie andere Technologien. Im Fall eines Auf-Anforderung-Scans aktiviert sich die Blacklist automatisch, sobald mindestens ein Eintrag für die Scan-Aufgabe aktiviert wurde.

Jeder Listeneintrag kann aus den folgenden Angaben bestehen, die mit einem logischen UND verknüpft sind:

Erkennungsname	Ein beliebiger Begriff zur Benennung der Bedrohung. Diese Bezeichnung wird im Falle einer Erkennung als Bedrohungsname dargestellt.
Prozess	Ein Name oder eine Pfadangabe zu einem Prozess dessen Dateizugriffe als Bedrohung angesehen werden sollen. Dieser kann mit einem Datei-Eintrag kombiniert, sowie mit Hilfe des Wildcards *, festgelegt werden. Im Falle der „Speichersicherheit" bezieht sich diese Angabe auf einen erkannten Hauptprozess.
Datei	Ein Name oder eine Pfadangabe zu einer Datei die als Bedrohung angesehen werden soll. Dieser kann mit einem Prozess-Eintrag kombiniert, sowie mit Hilfe des Wildcards *, festgelegt werden. Im Falle der „Speichersicherheit" bezieht sich diese Angabe auf eine Datei die von einem Hauptprozess verwendet wird.
Sicherheitsfunktion	Mit der Aktivierung der jeweiligen Kontrollkästchen wird festgelegt, in welchen Sicherheitsfunktionen der Eintrag erkannt werden soll. „Dateisicherheit" und „Speicherschutz" stehen immer zur Verfügung. Weitere Spalten können, abhängig von erstellten Scan-Aufgaben, zur Verfügung stehen.

Beispiele für Einträge:

Erkennungsname:	Malware 1	Jede Datei auf die der Prozess C:\Program Data\dummy.exe zugreift wird als Bedrohung „Malware 1" angesehen.
Prozess:	C:\Program Data\dummy.exe	
Datei:		

Erkennungsname:	Malware 2	Jede Datei mit der Endung „.encrypt", die sich in einem Ordner „tmp" befindet, wird als Bedrohung „Malware 2" angesehen.
Prozess:		
Datei:	*\tmp*.encrypt	

Erkennungsname:	Malware 3	Jede Datei die mit „tmp" beginnt und sich in einem Unterordner von „C:\Users\"
Prozess:	C:\windows*\shh.exe	

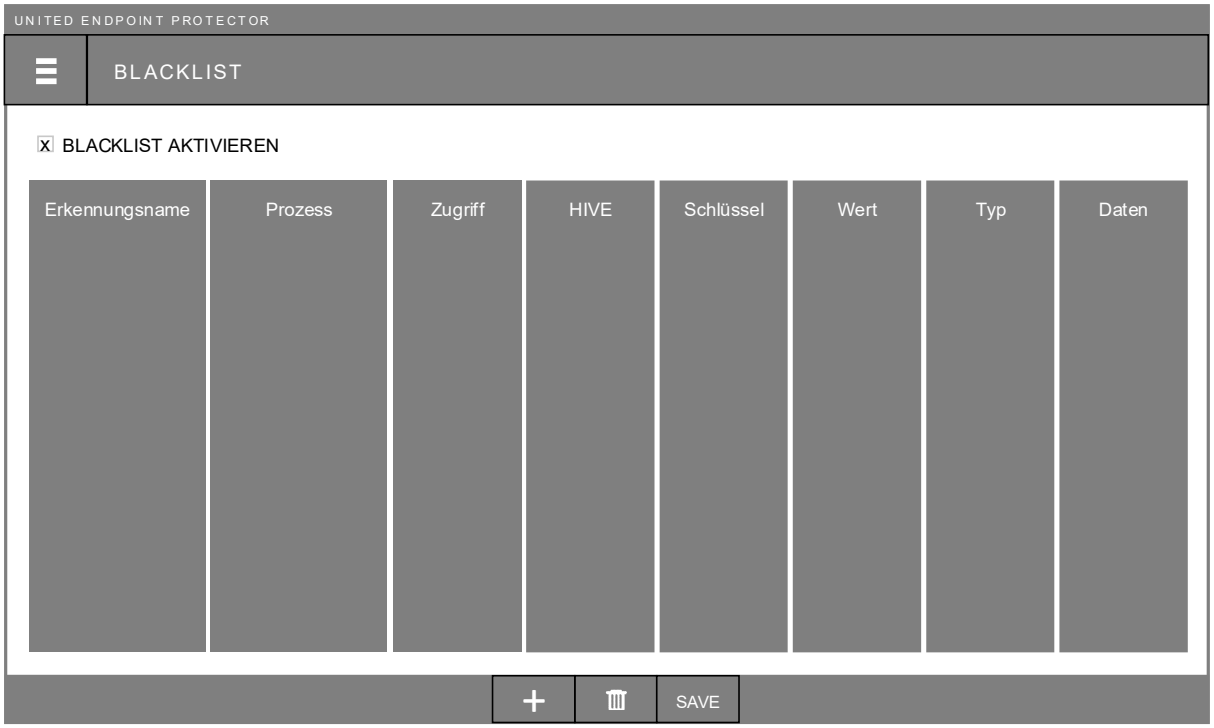
Datei:	C:\Users*\tmp*.*	befindet und auf die ein Prozess „shh.exe“, der sich in einem Unterverzeichnis von „C:\windows\“ befindet, wird als Bedrohung „Malware 3“ angesehen.

ACHTUNG!

Ein falscher Eintrag, wie zum Beispiel die Behandlung jeder EXE-Datei als Bedrohung, kann zur Beschädigung des Computersystems führen! Wir empfehlen daher sehr vorsichtig und gewissenhaft mit Blacklist-Einträgen umzugehen und diese vor einem produktiven Einsatz gründlich zu Testen.

10.2. Registry-Blacklist

Die Registry-Blacklist ist eine spezielle Liste zur manuellen Erfassung von schadhaften Windows Registry Manipulationen. Diese Liste kann im Untermenü von „Registry Sicherheit“ im Hauptmenü aufgerufen werden.



Sicherheitsfunktion –> Blacklist (Registry Sicherheit)

Mit den Buttons in der unteren Menüleiste können Einträge der Liste hinzugefügt, bestehende entfernt und die vorgenommenen Änderungen gespeichert werden. Mit dem Kontrollkästchen „Blacklist aktivieren“ wird die Blacklist für die Registry Sicherheit aktiviert und in der Registry-Übersicht dargestellt.

Jeder Listeneintrag kann aus den folgenden Angaben bestehen die mit UND verknüpft sind:

Erkennungsname	Ein beliebiger Begriff zur Benennung der Bedrohung. Diese Bezeichnung wird im Falle einer Erkennung als Bedrohungsname dargestellt.
Prozess	Ein Name oder eine Pfadangabe zu einem Prozess dessen Registry-Zugriffe als Bedrohung angesehen werden sollen. Dieser kann mit allen anderen Angaben kombiniert und mit Hilfe des Wildcards *, festgelegt werden.
Zugriff	Legt die Art des Zugriffes auf die Registry fest der als Bedrohung angesehen werden soll.
HIVE	Der Name des HIVE's auf den der Zugriff stattfindet. Neben den Microsoft eigenen HIVE's können auch Application HIVE's (/A) festgelegt werden. Die Verwendung des Wildcards * ist erlaubt.
Schlüssel	Der Name des Schlüssels auf den zugegriffen wird und als Bedrohung angesehen werden soll. Die Verwendung des Wildcards * ist erlaubt.
Wert	Der Name des Wertes auf den zugegriffen wird und der als Bedrohung angesehen werden soll. Die Verwendung des Wildcards * ist erlaubt.
Typ	Der Typ des Wertes auf den der Zugriff stattfindet.
Daten	Die Daten des Wertes auf die zugegriffen und als Bedrohung angesehen werden soll. Die Verwendung des Wildcards * ist erlaubt.

Beispiele für Einträge:

Erkennungsname:	Malware abc	Jeder Zugriff des Prozesses C:\Program Data\dummy.exe wird als Bedrohung „Malware abc“ angesehen.
Prozess:	C:\Program Data\dummy.exe	
Zugriff:		
HIVE:		
Schlüssel:		
Wert:		
Typ:		
Daten:		

Erkennungsname:	Malware xyz	Jeder Zugriff auf einen Wert „Dummy“, der sich unterhalb von HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet befindet, wird als Bedrohung „Malware xyz“ angesehen.
Prozess:		
Zugriff:		
HIVE:	HKEY_LOCAL_MACHINE	
Schlüssel:	SYSTEM\CurrentControlSet*	
Wert:	Dummy	
Typ:		
Daten:		

Erkennungsname:	Tmp80	Jeder Wert den der Prozess „tmp80.exe“ unterhalb von HKEY_LOCAL_MACHINE \SOFTWARE\ erstellt, wird als Bedrohung „Tmp80“ angesehen.
Prozess:	*\tmp80.exe	
Zugriff:	Write Value	
HIVE:	HKEY_LOCAL_MACHINE	
Schlüssel:	SOFTWARE*	
Wert:		
Typ:		
Daten:		

ACHTUNG!

Ein falscher Eintrag, wie zum Beispiel die Behandlung jedes Zugriffes auf einen HIVE als Bedrohung, kann zur Beschädigung des Computersystems führen! Wir empfehlen daher sehr vorsichtig und gewissenhaft mit Blacklist-Einträgen umzugehen und diese vor einem produktiven Einsatz gründlich zu Testen.

10.3. Strategie

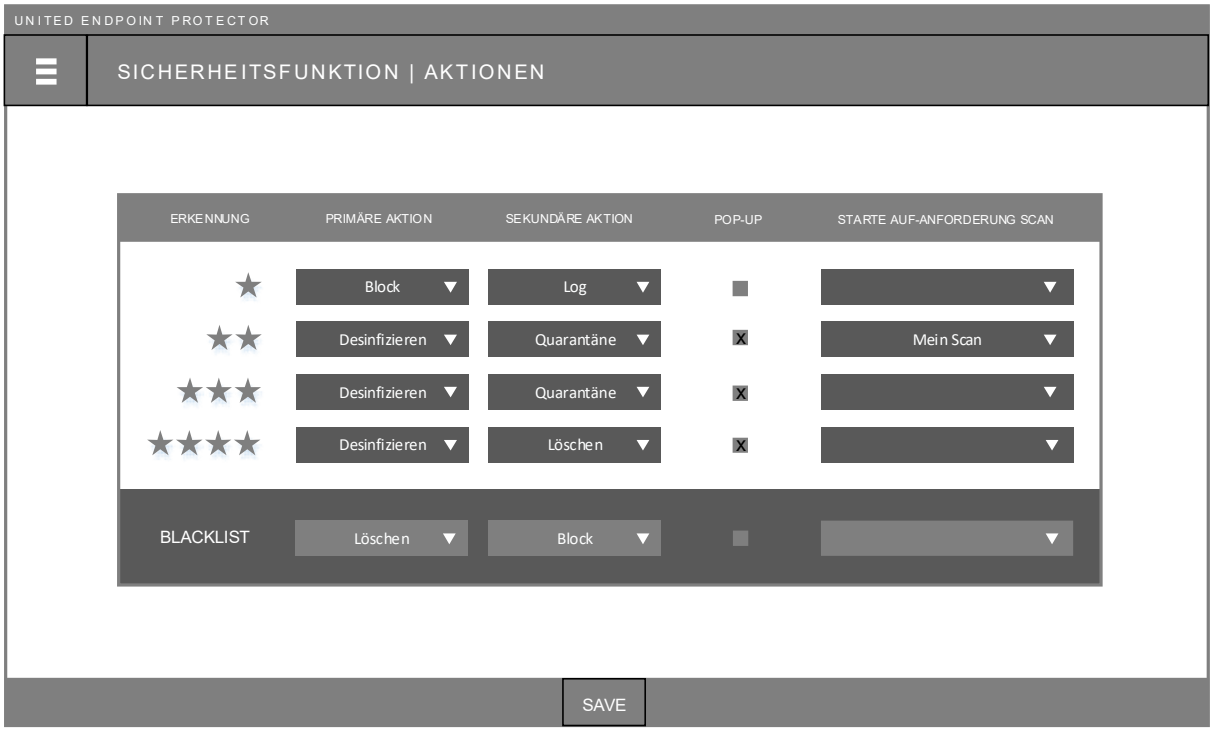
Die Blacklist ist ein flexibles Werkzeug, das hauptsächlich in zwei Bereichen Anwendung findet. Einerseits zur manuellen Bekämpfung von Bedrohungen, die von den eingesetzten Sicherheitstechnologien nicht erkannt werden. Andererseits zur Errichtung von präventiven Schutzmaßnahmen, um unerwünschte Vorgänge bereits im Vorfeld zu unterbinden.

Anzeichen wie neue Dateien mit verdächtigen Dateinamen, laufende Prozesse mit suspekten Bezeichnungen oder ungewöhnliches Verhalten des Computersystems, können auf eine Bedrohung hindeuten, die von den eingesetzten Sicherheitstechnologien nicht erkannt wurden. In diesem Fall können Einträge auf der Blacklist vorgenommen werden, um diese Symptomatiken mit einer gewünschten Aktion zu behandeln. Die Informationen der verschiedenen Sicherheitsfunktionen können helfen, um passende Blacklist-Einträge zu definieren. In jeder Sicherheitsfunktion kann festgelegt werden, ob die Blacklist aktiv und mit welcher Aktion Blacklist-Erkennungen behandelt werden sollen (siehe Kapitel 11).

Es gibt verschiedene Szenarien in denen die Blacklist auch zur Errichtung von präventiven Schutzmaßnahmen eingesetzt werden kann. Soll beispielsweise verhindert werden, dass die Startseite eines Webbrowsers geändert wird, könnten Änderungsversuche des entsprechenden Registry-Wertes durch die Blacklist verhindert werden. Auch die Ausführung oder Installation von unerwünschten Applikationen kann mit der Blacklist verhindert oder aufgezeichnet werden.

11. Aktionen

Der United Endpoint Protector (UEP) ist mit einer Reihe von möglichen Aktionen ausgestattet, um identifizierte Bedrohungen unschädlich zu machen. Für jede Sicherheitsfunktion steht dafür eine eigene Konfigurationsoberfläche, im jeweiligen Untermenü des Hauptmenüs zur Verfügung, um die gewünschten Reaktionen festzulegen.



Sicherheitsfunktion -> Aktionen

Die durchzuführenden Aktionen werden pro Übereinstimmung an Sicherheitstechnologien festgelegt. Abhängig davon, wie viele Sicherheitsanbieter eine Bedrohung identifizieren, kann eine primäre und eine sekundäre Aktion automatisch durchgeführt werden:

Log	Meldet die gefundene Bedrohung, führt jedoch keine weiteren Schritte zur Bereinigung aus.
Block	Steht in den Echtzeit-Funktionen „Dateisicherheit“ und „Registry-Sicherheit“ zur Verfügung und verhindert die Durchführung des Zugriffes.
Desinfizieren	Ruft die Säuberungsmethode, die der jeweilige Sicherheitsanbieter zur Verfügung stellt auf, um die Bedrohung zu entfernen. Sollten

	mehrere Anbieter die Bedrohung melden, werden die Methoden nach dem Zufallsprinzip hintereinander gestartet. Sollte der erste Anbieter die Bedrohung nicht vollständig entfernen, kann ein weiterer Anbieter dies durchführen.
Quarantäne	Verschiebt die identifizierte Datei in die Quarantäne des UEP und isoliert diese dort (siehe Kapitel 11.1).
Löschen	Löscht die identifizierte Datei. Beachten Sie, dass dabei keine Sicherheitskopie angefertigt wird!

Die sekundäre Aktion wird immer dann aufgerufen, wenn die Primäre nicht erfolgreich war. Zusätzlich kann für jede identifizierte Bedrohung festgelegt werden, ob auf dem Computersystem ein Benachrichtigungsfenster geöffnet werden soll. Als weitere Reaktion auf eine identifizierte Bedrohung, kann ein existierender Auf-Anforderung-Scan (siehe Kapitel 8) automatisch gestartet werden. Im Falle einer Blacklist-Erkennung können gesonderte Aktionen festgelegt werden.

In den Sicherheitsfunktionen werden die Untersuchungs- und Säuberungsergebnisse in den jeweiligen Spalten der Sicherheitsanbieter dargestellt. Die folgenden Ausgaben können dabei stattfinden:

OK	Der Sicherheitsanbieter hat den Zugriff erfolgreich überprüft und diesen als Sauber eingestuft.
- - -	Der Sicherheitsanbieter konnte den Zugriff nicht überprüfen. Wenn Sie mit der Maus über den Eintrag fahren, wird der Grund dafür angezeigt.
Bedrohungsname	Der Sicherheitsanbieter hat bei dem vorliegenden Zugriff eine Bedrohung festgestellt und konnte diese erfolgreich neutralisieren. Wenn Sie mit der Maus über den Eintrag fahren, wird die durchgeführte Aktion angezeigt.
Bedrohungsname	Der Sicherheitsanbieter hat bei dem vorliegenden Zugriff eine Bedrohung festgestellt, konnte diese jedoch nicht erfolgreich neutralisieren. Das kann unteranderem der Fall sein, wenn die Aktion „Log“ oder „Block“ festgelegt wurde. Wenn Sie mit der Maus über den Eintrag fahren, wird der genaue Status angezeigt.
Self Protection	Es wurde ein Zugriff auf Tabidus eigene Komponenten festgestellt, der nicht durch eine Ausnahmeregelung (siehe Kapitel 12) erlaubt wurde. Das kann auftreten, wenn der Selbstschutz von UEP aktiviert ist (siehe Kapitel 5.1).

11.1. Quarantäne

Wenn eine Bedrohung festgestellt und die Aktion „Quarantäne“ ausgewählt wurde, wird die Datei in das Quarantäneverzeichnis von UEP verschoben (…\Tabidus Technology\United Endpoint Protector\quar\) und dort isoliert. Die Verwaltungsoberfläche der Quarantäne kann im Untermenü von „Status“ im Hauptmenü aufgerufen werden.

Status -> Quarantäne

Die Oberfläche stellt alle Objekte dar die sich in der Quarantäne befinden. Für jedes Objekt wird der Zeitpunkt der Isolation, die dafür verantwortliche Sicherheitsfunktion, der ursprüngliche Speicherort, sowie die Untersuchungsergebnisse der Sicherheitsanbieter dargestellt. Mit der unteren Menüleiste können bestehende Objekte auf den ursprünglichen Speicherort wiederhergestellt oder Objekte endgültig aus der Quarantäne gelöscht werden. Mit Hilfe des Refresh-Buttons kann die Darstellung aktualisiert werden.

11.2. Strategie

Die wichtigste Entscheidung bei der Festlegung der automatischen Aktionen ist ein Abwiegen zwischen einem potentiellen False-Negative (der Nicht-Behandlung einer Bedrohung) und einem False-Positive (die fälschliche Behandlung einer Bedrohung). Beides sind mögliche Nebenerscheinungen, die bei der Identifizierung von Bedrohungen auftreten können. Abhängig davon welches Szenario in der jeweiligen Umgebung und im jeweiligen Einsatzgebiet die größere Gefahr darstellt, sollten die Aktionen passend gewählt werden.

Handelt es sich beispielsweise um ein besonderes Computersystem, auf dem eine spezielle Software betrieben wird, die für die Produktion entscheidend ist und auf dem kein Anwender frei arbeitet, ist ein potentieller False-Positive womöglich die größere Gefahr. In diesem Fall könnte die Aktion, wenn nur ein einzelner Anbieter eine Bedrohung identifiziert, auf „Block" oder „Log" gesetzt werden. Negative Auswirkungen eines Fehlalarms würden damit mit hoher Wahrscheinlichkeit vermieden werden. Sollte dennoch eine echte Bedrohung auftreten, könnte eine Benachrichtigung angezeigt und diese nach eigener Beurteilung manuell entfernt werden. Sind sich hingegen zwei oder mehr Anbieter bei der Einstufung einer Bedrohung einig, könnte eine automatische „Desinfizierung" oder „Quarantäne" in Betracht gezogen werden.

Handelt es sich hingegen um eine einfache Arbeitsmaschine, die keine außerordentlich wichtige Funktion ausübt und werden auf dieser beispielsweise oft Fremddaten verarbeitet, ist ein potentieller False-Negative die größere Gefahr. In diesem Fall könnte bereits bei der Identifizierung durch einen einzelnen Hersteller die Aktionen „Desinfizierung" und „Quarantäne" angebracht sein. Sollten sich sogar zwei oder mehr Anbieter einig sein, könnte auch ein „Löschen" in Frage kommen.

Die Wahl ob oder bei wie vielen übereinstimmenden Anbietern dem Anwender ein Benachrichtigungsfenster angezeigt werden soll, kann von der Art des Anwenders und ob dieser mit einer solchen Benachrichtigung etwas anfangen kann, abhängig gemacht werden.

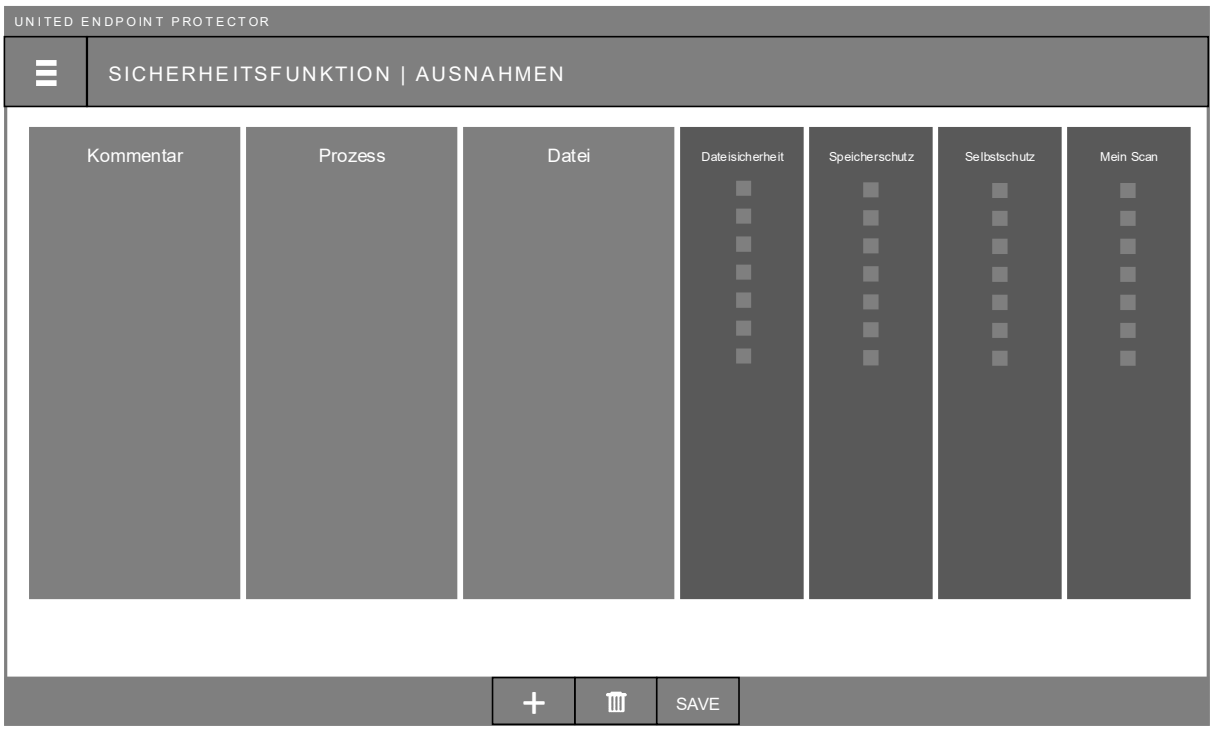
Eine automatische Ausführung eines Auf-Anforderung-Scans, ausgelöst durch die Erkennung einer ersten Bedrohung, ist eine gute Möglichkeit für einen erweiterten Schutz. Wird beispielsweise durch die Dateisicherheit eine bösartige Datei identifiziert, könnte sich zu diesem Zeitpunkt auch ein schadhafter Prozess im Arbeitsspeicher befinden oder ein bösartiger Windows-Dienst installiert sein. Die unmittelbare Überprüfung durch einen „Hot-Spot Scan" oder gar der gesamten Festplatte, könnte weitere Bestandteile der Bedrohung, vielleicht durch andere Anbieter oder intensivere Untersuchungstechniken, aufdecken.

12. Ausnahmen

Die Überprüfung von Dateien und Registry-Zugriffen auf mögliche Bedrohungen kann in bestimmten Situationen zu Geschwindigkeitseinbußen des Computersystems führen. Der United Endpoint Protector (UEP) erlaubt deshalb gewünschte Zugriffe von der Überprüfung auszuschließen, um negative Auswirkungen auf besondere Vorgänge zu verhindern. Dafür stehen zwei verschiedene Listen zur Ausnahme von Datei- und Registry-Zugriffen zur Verfügung.

12.1. Datei-Ausnahmen

Im Untermenü der Sicherheitsfunktionen „Dateisicherheit“ und „Speicherschutz“, sowie auf der Konfigurationsoberfläche von Auf-Anforderung-Scans, kann die globale Liste für Datei-Ausnahmen aufgerufen werden.



Sicherheitsfunktion -> Ausnahmen

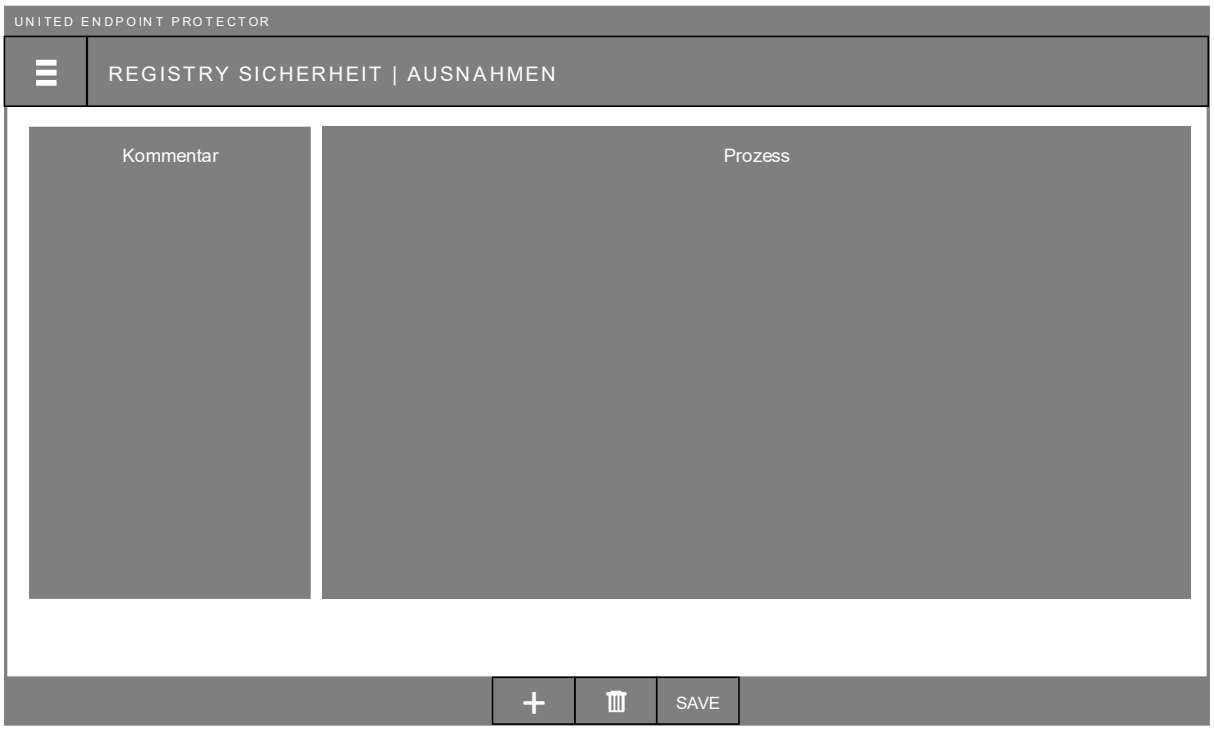
Mit der unteren Menüleiste können neue Einträge der Liste hinzugefügt, bestehende Einträge gelöscht, sowie die vorgenommenen Änderungen gespeichert werden. Jeder Eintrag beschreibt eine Datei, einen Ordner oder einen spezifischen Zugriff, der von der Überprüfung ausgeschlossen werden soll. Passend zu jedem Eintrag kann mit Hilfe der Kontrollkästchen festgelegt werden, in welcher Sicherheitsfunktion die jeweilige Ausnahme gelten soll. Neben der „Dateisicherheit“ und dem „Speicherschutz“ können Ausnahmen für den Selbstschutz (siehe Kapitel 5.1) festgelegt werden (Prozesse die auf Tabidus eigene Komponenten zugreifen dürfen), sowie für jede erstellte Scan-Aufgabe.

Jeder Eintrag kann aus den folgenden Angaben bestehen:

Kommentar	Eine beliebige Bezeichnung zur Beschreibung der Ausnahme. Beispielsweise kann das dazugehörige Programm oder der Grund für die Ausnahme genannt werden.
Prozess	Der Name oder eine Pfadangabe zu einem Prozess, dessen Dateizugriffe nicht überprüft werden sollen. Die Verwendung des Wildcards * ist erlaubt. Eine Prozess-Definition kann mit einer Datei-Definition kombiniert werden.
Datei	Die Pfadangabe zu einer Datei oder einem Ordner der nicht überprüft werden soll. Die Verwendung des Wildcards * ist erlaubt. Eine Datei-Definiton kann mit einer Prozess-Definition kombiniert werden.
Sicherheitsfunktion	Aktivierung der Sicherheitsfunktionen für die der Eintrag gelten soll.

12.2. Registry-Ausnahmen

Im Untermenü von „Registry Sicherheit“ kann die zweite Liste aufgerufen werden, mit der die Erfassung von Ausnahmen für Registry-Zugriffe möglich ist. Diese erlaubt Prozesse festzulegen, deren Zugriffe auf die Windows Registry nicht überwacht werden sollen.



Registry Sicherheit -> Ausnahmen

Jeder Eintrag kann aus den folgenden Angaben bestehen:

Kommentar	Eine beliebige Bezeichnung zur Beschreibung der Ausnahme. Beispielsweise kann das dazugehörige Programm oder der Grund für die Ausnahme genannt werden.
Prozess	Der Name oder eine Pfadangabe zu einem Prozess, dessen Dateizugriffe nicht überprüft werden sollen. Die Verwendung des Wildcards * ist erlaubt.

12.3. Strategie

Jede Ausnahme von der Überwachung durch eine Sicherheitsfunktion ist ein potentielles Sicherheitsrisiko. Der Einsatz von Ausnahmeregelungen sollte daher nur aus wichtigen Gründen erfolgen. Mögliche Gründe könnten die Beeinträchtigung einer bestimmten Applikation oder die starke Belastung eines bestimmten Vorganges sein, der zu einem hohen CPU-Verbrauch führt. Klassische Beispiele sind dafür das eingesetzte Backup-System oder besondere Server-Applikationen wie Datenbankserver. Diese verursachen durch ihren Betrieb sehr viele Dateizugriffe, deren Überwachung negative Auswirkungen haben kann.

Um das potentielle Sicherheitsrisiko durch eine Ausnahme so gering wie möglich zu halten, sollte diese so präzise wie möglich beschrieben werden. Anstatt eines einfachen Dateinamens, der Mehrdeutigkeiten zulässt, ist eine genauere Beschreibung des Speicherortes (Pfad) zu empfehlen. Grundsätzlich können Ausnahmen in drei verschiedenen Arten erfolgen:

- **Datei & Ordner Ausnahme**
  Ist eine Ausnahme die nur den Pfad zu einer Datei oder einem ganzen Ordner beinhaltet der nicht überwacht werden soll. Das kann beispielsweise im Falle eines Fehlalarms (False-Positive) eine temporäre Hilfe sein. In anderen Fällen kann dies zwar ein potentielles Problem beheben, doch durch die große Mehrdeutigkeit (Wer greif aller auf diese Datei oder diesen Ordner zu?) gilt diese Ausnahmeform als die unsicherste und sollte vermieden werden. Wenn eine solche Ausnahme dennoch notwendig ist, sollte diese durch einen Auf-Anforderung-Scan regelmäßig überprüft werden.

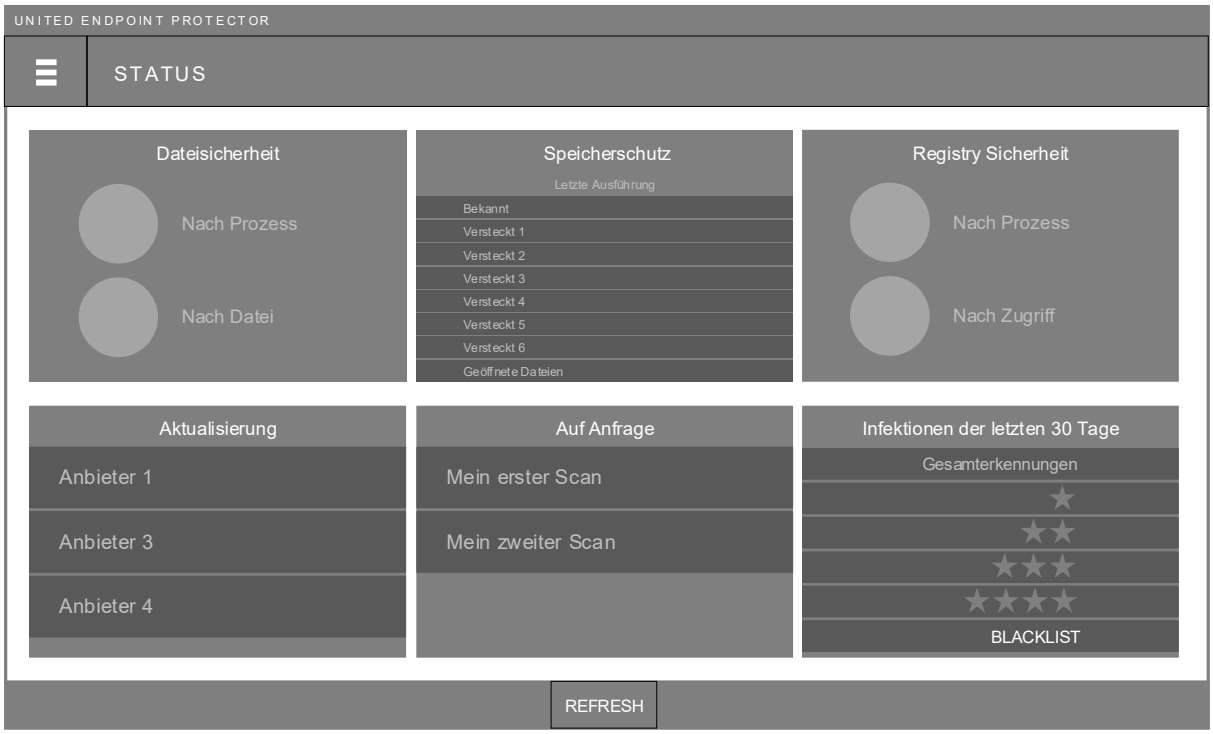
- **Prozessausnahme**
  Ist eine Ausnahme die nur den Pfad zu einem Prozess beinhaltet. Dem Start des Prozesses geht ein lesender Zugriff auf die zugehörige EXE-Datei voraus, die von der Ausnahmeregelung nicht betroffen ist. Jeglicher Zugriff den dieser Prozess jedoch anschließend durchführt, wird von der Überprüfung ausgeschlossen. Diese Form der Ausnahme ist sicherer, da der Prozess beim Startvorgang überprüft wird und die Identität der Zugriffe bekannt ist. Da jedoch auch ein vermeintlich gutartiger Prozess während der Ausführung manipuliert oder Fremddaten verarbeiten kann, sollten keine Hoch-Risikoprozesse wie iexplorer.exe, explorer.exe, svchost.exe oder ähnliche ausgeschlossen werden.

- **Prozess & Datei Ausnahme**
  Hierbei handelt es sich um eine Kombination aus Prozess- und Datei & Ordner-Ausnahme. Das ist die sicherste Form einer Ausnahme, die am wenigsten Mehrdeutigkeiten zulässt. Von der Überwachung ausgenommen ist nur jener Vorgang, wenn ein festgelegter Prozess auf eine festgelegte Datei oder Ordner zugreift. Greift der angegebene Prozess auf ein anderes Ziel oder greift ein anderer Prozess auf die angegebene Datei oder Ordner zu, ist dies nicht mehr von der Ausnahme betroffen.

Die Notwendigkeit Ausnahmen festzulegen kann sich auch auf den Betrieb des Selbstschutzes des United Endpoint Protectors (UEP) beziehen (siehe Kapitel 5.1). Der Selbstschutz blockiert jegliche Zugriffe auf Tabidus eigene Dateien, Ordner und Prozesse, um potentiell bösartige Manipulationen am UEP zu verhindern. Sollte jedoch ein Vorgang aus gutem Grund einen solchen Zugriff benötigen, muss dieser als Ausnahme eingetragen und für die Funktion „Selbstschutz" aktiviert werden.

13. Dashboard

Zur Überwachung aller wichtigen Operationsparameter und auftretenden Events, steht das Status-Dashboard zur Verfügung. Dieses kann im Hauptmenü mit einem Klick auf „Status“ aufgerufen werden.



Die Daten des Dashboards lassen sich mit dem Refresh-Button in der unteren Menüleiste aktualisieren. Folgende Informationen können dort abgelesen werden:

- **Dateisicherheit**
  Zeigt alle durch die Dateisicherheit überprüften Zugriffe der letzten 24 Stunden bzw. seit dem letzten Neustart an. Die Daten werden „nach Prozess“ und „nach Datei“ sortiert. Im Kopfbereich wird die Anzahl der aufgetretenen Infektionen angezeigt. Mit einem Klick auf die jeweilige Überschrift öffnet sich die entsprechende Detailansicht, um alle verfügbaren Daten darzustellen. Diese Informationen können genutzt werden, um Optimierungen an der Konfiguration der Dateisicherheit (z.B. festlegen von Ausnahmen - siehe Kapitel 12) vorzunehmen.

- **Speicherschutz**
  Stellt den Status des Speicherschutzes dar. Neben dem Zeitpunkt der letzten Ausführung, werden die durchlaufenen, forensischen Methoden und die von ihnen gefundenen Prozesse im Speicher dargestellt. Im Kopfbereich wird die Anzahl der entdeckten Infektionen angezeigt.

- **Registry Sicherheit**

  Zeigt alle durch die Registry Sicherheit überprüften Zugriffe der letzten 24 Stunden bzw. seit dem letzten Neustart an. Die Daten werden „nach Prozess" und „nach Zugriff" sortiert. Im Kopfbereich wird die Anzahl der aufgetretenen Infektionen angezeigt. Mit einem Klick auf die jeweilige Überschrift öffnet sich die entsprechende Detailansicht, um alle verfügbaren Daten darzustellen. Diese Informationen können genutzt werden, um Optimierungen an der Konfiguration der Registry Sicherheit (z.B. festlegen von Ausnahmen - siehe Kapitel 12) vorzunehmen.

- **Aktualisierung**

  Zeigt alle freigeschalteten Sicherheitsanbieter an (siehe Kapitel 3). Pro Anbieter wird deren Aktualität der automatischen Aktualisierungen, die über eine Aktualisierungs-Aufgabe (siehe Kapitel 4) empfangen werden, dargestellt. Der Status ist Grün, wenn die letzte Aktualisierung innerhalb der letzten 24 Stunden stattgefunden hat. Andernfalls wird dies mit einem roten Kreuz angezeigt.

- **Auf Anforderung**

  Zeigt alle erstellten Scan-Aufgaben (siehe Kapitel 8) an. Für jede Aufgabe wird der Zeitpunkt, sowie die Anzahl der gefundenen Bedrohungen, der letzten Ausführung angezeigt. Mit einem Klick auf den Aufgabennamen, wird die Übersicht der Auf-Anforderungs-Scans geöffnet.

- **Infektionen der letzten 30 Tage**

  Stellt alle identifizierten Bedrohungen der letzten 30 Tage dar. Neben der Gesamtanzahl werden diese zusätzlich nach der Zahl an übereinstimmenden Sicherheitsanbietern dargestellt, welche die Bedrohung entdeckt haben. Mit einem Klick auf einen Eintrag, wird die entsprechende Detailansicht geöffnet, die alle verfügbaren Daten anzeigt.

14. Drittanbieter Lizenzen

Der United Endpoint Protector (UEP) verwendet, neben den integrierten Sicherheitsanbietern, die folgenden Open-Source Komponenten zur Durchführung verschiedener Aufgaben. Diese sind über die nachfolgenden Lizenzen verfügbar.

14.1. Rekall Forensic

Rekall Forensic steht in Form der uepmemanalyser.exe im UEP zur Verfügung und stellt forensische Daten des Arbeitsspeichers zur weiteren Verarbeitung bereit. Der Source Code kann über folgenden Link eingesehen werden: https://github.com/google/rekall

Copyright (C) 2007-2011 Volatile Systems Copyright 2012-2016 Google Inc. All Rights Reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

14.2. WinPmem

WinPmem ist ein Kernel-Mode-Treiber der von Rekall Forensic genutzt wird, um Zugriff auf den Arbeitsspeicher des Computers zu erlangen. Der Source Code kann über folgenden Link eingesehen werden: https://github.com/google/rekall/tree/master/tools/windows/winpmem

WinPmem steht über die Apache License Version 2.0 zur Verfügung, deren Lizenzvereinbarung unter folgendem Link gefunden werden kann: https://github.com/google/rekall/blob/master/tools/windows/winpmem/LICENSE

14.3. The Sleuth Kit

Die Auf-Anforderung-Scans des UEP verwenden einzelne Libraries des Sleuth Kits zur forensischen Untersuchung von Datenträgern. Der Source Code kann über folgenden Link gefunden werden: http://www.sleuthkit.org/sleuthkit/download.php

The source code in TSK are distributed under several licenses. Each source code file identifies the license that applies to its contents.

Some of the files in TSK core (non-framework) have roots in The Coroner's Toolkit (TCT) and are distributed under the IBM Public License. These files are limited to the file system code and mainly for the FFS and Ext2 file systems. Files that have been created since the fork are released under the Common Public License. This includes all other files in the library. Note that the Common Public License is a generic form of the IBM Public License.

The framework code is distributed under the Common Public License.