



Agrarfrost GmbH

Projektdokumentation

Zum Abschlussprojekt der Ausbildung zum
Fachinformatiker – Systemintegration

**Ablösung der bestehenden USB-Kontrollsoftware
durch ein neues USB-Sicherheits- und
Richtlinienmanagementsystem**

Prüfung: Winter 2025

Prüfungsteilnehmer:

Paul Tiemann
XXXXXXXXXX
XXXXXXXXXX

Ausbildungsbetrieb:

Agrarfrost GmbH
Aldrup 3
27793 Aldrup

Projektverantwortlicher:

XXXX XXXX

Inhaltsverzeichnis

1. Projektbeschreibung.....	1
1.1 Einleitung.....	1
1.2 Ausbildungsbetrieb.....	1
1.3 Aufgabenstellung	1
1.4 Projektteam.....	1
1.5 Projektumfang.....	1
2. Planungsphase.....	2
2.1 Ablauf der Planungsphase	2
2.2 IST-Analyse	2
2.2.1 Ermittlung der Geräteanzahl.....	2
2.3 SOLL-Konzept	2
2.4 Marktüberblick	3
2.4.1 CrowdStrike – „Falcon Device Control“	3
2.4.2 ManageEngine – „Device Control Plus“	3
2.4.3 Netwrix – „Endpoint Protector“.....	4
2.4.4 Microsoft Active Directory – „Gruppenrichtlinie“	4
2.5 Lösungskonzepte im Überblick	4
2.6 On Premise oder Cloud.....	4
3. Angebots und Testphase	5
3.1 Kontaktaufnahme mit ausgewählten Anbietern und Funktionsumfang.....	5
3.1.1 Endpoint Protector.....	5
3.1.2 CrowdStrike Falcon Device Control	5
3.1.3 Manage Engine - Device Control Plus	5
3.2 Vorbereitung der Testumgebung	6
3.3 Netzwerkumgebung	6
3.4 Installation und Einrichtung	6
3.4.1 Manage Engine	6
3.4.2 Einrichtung der Gruppenrichtlinie.....	6
3.4.3 CrowdStrike.....	7
3.5 Testphase in Testumgebung.....	7
3.5.1 Manage Engine	7
3.5.2 Gruppenrichtlinie	7
3.7 Angebotsvergleich.....	8
3.7.1 Kostenübersicht.....	8
3.7.2 Nutzwertanalyse	9
3.7.3 Auswertung.....	10
3.8 Wirtschaftlichkeitsbetrachtung.....	10

3.9 Vorstellung der Angebote und Entscheidung	11
4. Implementierungsphase	11
4.1 Installation und Konfiguration	11
4.2 Deinstallation des Agenten (altes USB-Kontrollsystem)	11
4.3 Richtlinie für Sperrung und Freigabe von USB-Geräten	12
4.4 Anwenderdokumentation	12
5. Projektabschluss	12
5.1 Vergleich Projektantrag	12
5.2 Fazit	12
6. Anhang	13
Angebote	13
CrowdStrike	13
Endpoint Protector	15
ManageEngine	16
Zeitplan	17
Herleitung von Server-, Hypervisor- und Wartungskosten	17
Glossar	18
Tabellenverzeichnis	19
Abbildungsverzeichnis	19
Quellen	19

1. Projektbeschreibung

1.1 Einleitung

Das Projekt „Ablösung der bestehenden USB-Kontrollsoftware durch ein neues USB-Sicherheits- und Richtlinienmanagementsystem“ wurde im Rahmen der Berufsausbildung zum Fachinformatiker für Systemintegration durchgeführt. Diese Dokumentation enthält die Tätigkeiten und Ergebnisse dieses Projekts.

1.2 Ausbildungsbetrieb

Agrarfrost GmbH ist ein 1967 gegründetes, familiengeführtes Unternehmen mit Hauptsitz in Aldrup bei Wildeshausen und einem weiteren Werk in Oschersleben. Das Unternehmen ist Hersteller von tiefgekühlten Kartoffelprodukten wie Pommes Frites, Kroketten und Wedges, dazu kommen Chips und Kartoffelflocken. Jährlich verarbeitet Agrarfrost die Rohware zu rund 215.000 Tonnen fertigem Produkt. Das Unternehmen beschäftigt rund 650 Mitarbeiter an den Standorten Aldrup und Oschersleben.

Als IT-Abteilung betreuen wir nicht nur die beiden Produktionsstandorte, sondern auch die IT-Infrastruktur der Tochterunternehmen an diversen Lagerstandorten in ganz Norddeutschland.

1.3 Aufgabenstellung

Die konsequente Kontrolle der USB-Schnittstellen ist für Unternehmen unerlässlich, da diese Ports eine kritische physische Schwachstelle im IT-Sicherheitssystem darstellen und weit über die Risiken unachtsamer Mitarbeiter hinausgehen. Ein ungesicherter USB-Anschluss ermöglicht nicht nur den unkontrollierten und schnellen Diebstahl sensibler Unternehmens- und Kundendaten in großem Umfang, sondern dient auch als direktes Einfallstor für gefährliche Malware wie Ransomware oder "BadUSB". Diese Angriffe nutzen manipulierte Geräte, um Sicherheitsvorkehrungen zu umgehen und Malware direkt in die Systeme einzuschleusen, was zu Störungen oder gar Totalausfällen der IT-Systeme führen kann. Vor dem Hintergrund sich verschärfender gesetzlicher Vorgaben und der Notwendigkeit, die digitale Betriebskontinuität zu gewährleisten, ist die Implementierung einer strikten USB-Kontrolle eine präventive Maßnahme zum Schutz der gesamten IT-Infrastruktur.

Da der Support des alten, hierzu verwendeten Systems nicht erneuert wird, soll im Rahmen dieses Projekts ein Neues ausgewählt und implementiert werden.

1.4 Projektteam

Das Projektteam bestand aus Herrn XXXX (Informationssicherheitsbeauftragter) als Projektverantwortlichen und mir.

1.5 Projektumfang

Der zeitliche Umfang des Projektes beträgt 40 Stunden.

2. Planungsphase

2.1 Ablauf der Planungsphase

Das Projekt begann mit einem Kick-Off-Meeting zwischen dem Informationssicherheitsbeauftragten Herrn XXXX und mir. Im Zentrum dieses Treffens stand die Erörterung der dringenden Notwendigkeit einer USB-Kontroll-Software, primär zur Eindämmung potenziellen Informationsabflusses und zur Abschottung eines Einfallstors für Malware im Unternehmensnetzwerk. Nach dieser Bedarfsanalyse wurde mir die Gesamtverantwortung für die Durchführung des Projekts übertragen. Die erste Phase sah die detaillierte Analyse der aktuellen Ist-Situation vor, um daraus die konkreten Probleme abzuleiten. Basierend darauf sollten die detaillierten Anforderungen an eine USB-Kontrolllösung definiert und in einem Soll-Konzept zusammengefasst werden. Danach erfolgte die zeitliche und strukturelle Planung des Projektablaufs. Darauf aufbauend wurde die Auswahl potenzieller Anbieter vorgenommen, deren Produkte gegen die erstellten Soll-Anforderungen geprüft werden sollten.

2.2 IST-Analyse

Derzeit ist ein Tool zur Sperrung der USB-Anschlüsse im Einsatz, das über eine On-Premise-Lösung einer internationalen IT-Sicherheitsfirma betrieben wird. Diese Lösung ist Teil eines Endpoint Detection and Response (EDR)-Ökosystems, für das wir mittlerweile einen anderen Anbieter im Einsatz haben. Das aktuell genutzte System stellt somit ein Überbleibsel einer früheren Sicherheitsarchitektur dar und beschränkt sich ausschließlich auf die Sperrung der USB-Ports für Massenspeicher. Der bestehende Vertrag und somit die zugehörige Lizenz für dieses System sollen nicht verlängert werden, wodurch künftig keine neuen Updates oder Supportleistungen mehr bereitgestellt werden.

2.2.1 Ermittlung der Geräteanzahl

Die Preise für eine Software zur Kontrolle der USB-Ports sind von der Anzahl der Endgeräte anhängig. Diese Anzahl wurde aus dem IT-Asset Management System ermittelt und umfasst alle Desktop-Computer und Notebooks. Die Server Systeme müssen nicht berücksichtigt werden, da sie virtualisiert in einer separaten Infrastruktur ohne USB-Anschluss existieren.

Gerätekategorie	Anzahl
Desktops	XX
Notebooks	XX
Gesamt	<u>XX</u>

Tabelle 1 - Ermittlung der Geräteanzahl

2.3 SOLL-Konzept

Am Ende des Projektes soll ein USB-Sicherheits- und Richtlinienmanagementsystem implementiert sein, welches standardmäßig alle USB-Massenspeicher blockiert. Spezifische USB-Geräte, Gerätegruppen oder Endgeräte sollen zeitlich begrenzt für die Nutzung der gesperrten USB-Ports freigegeben werden können. Die Freigabe nach Nutzerkonten ist optional. Die Verwaltung des Systems soll zentralisiert und browserbasiert über eine

anwenderfreundliche Weboberfläche möglich sein. Das neue USB-Kontrollsystem soll möglichst ohne einen neuen Agenten auf den Endgeräten funktionieren. Wenn ein neuer Agent zum Einsatz kommen sollte, muss dieser kompatibel mit Microsoft Windows sein, andere Betriebssysteme sind wünschenswert, aber nicht notwendig. Zudem sollte der Agent möglichst wenig Systemressourcen benötigen. Das System soll nicht mit bereits vorhandenen Sicherheitssystemen in Konflikt treten und es soll nicht zu Funktionsdopplungen kommen.

2.4 Marktüberblick

Eine ausführliche Marktanalyse hat ergeben, dass es zwar eine große Menge an Anbietern gibt, viele davon aber Teil eines weitaus umfassenderen Ökosystems an IT-Sicherheitslösungen sind, so bieten z.B. Sophos und SentinelOne Tools zur Kontrolle der USB-Geräte an, diese sind aber Teil eines (anderweitig schlicht nicht freigeschalteten) vollwertigen EDR-Systems. Da hierfür bereits ein System vorhanden ist und es Bedenken hinsichtlich potenzieller Kompatibilitätsprobleme und technischer Konflikte gibt, wurden diese Anbieter ausgeschlossen und es wurde sich auf Anbieter fokussiert, die reine USB-Kontrolltools anbieten. Als potentielle Kandidaten wurden CrowdStrike, als Anbieter unseres aktuellen EDR-Systems und ManageEngine, sowie Endpoint Protector als alleinstehende Systeme ausgewählt. Eine passende OpenSource Lösung wurde nicht gefunden. Ebenso wurde die Verwaltung der USB-Ports über die Verteilung von Gruppenrichtlinien über das Active Directory getestet. Ausgenommen der Sperrung über Gruppenrichtlinien erfüllen alle Produkte die Mindestanforderungen (Weboberfläche, temporäre Freigabe, etc.).

2.4.1 CrowdStrike – „Falcon Device Control“

Falcon Device Control ist CrowdStrikes Lösung für die Verwaltung von an das Endgerät angeschlossenen Geräten. Es umfasst nicht nur USB-Massenspeicher, sondern auch Human Interface Devices, wie Tastaturen oder Bluetooth-Geräte. Ebenso lässt sich überwachen, welche Daten transferiert wurden. Die Steuerung auf dem Endgerät geschieht durch einen lokal installierten Agenten, der die Richtlinien aus der Cloud bezieht. Die Verwaltung erfolgt über ein Webinterface im Browser.

Da CrowdStrike bereits für Endpoint Protection und als Schwachstellenscanner im Unternehmen eingesetzt wird und die Erweiterung um den Punkt Device Control unkompliziert vorgenommen werden kann, wurde dieser Anbieter in die Auswahl aufgenommen.

Der CrowdStrike Falcon Sensor ist mit Windows, Mac und Linux Systemen kompatibel und deckt damit alle im Einsatz befindlichen Endgeräte ab, zudem ist er bereits auf allen Endgeräten installiert.

2.4.2 ManageEngine – „Device Control Plus“

ManageEngine stellt mit Device Control Plus ein eigenständiges System zur Kontrolle von USB-Geräten bereit. Device Control Plus gibt es, anders als bei CrowdStrike, nur als On-Premise Lösung. Auch hier erfolgt die Verwaltung über eine Weboberfläche und auf dem Endgerät wird ein Agent benötigt.

2.4.3 Netwrix – „Endpoint Protector“

Endpoint Protector von Netwrix ist ein eigenständiges System, wobei Netwrix auch eine Vielzahl weiterer Produkte anbietet. Es gibt hier sowohl eine On-Premise Lösung, als auch die Möglichkeit des Betriebs in der Cloud. Hier wird ebenfalls ein Agent auf dem Endgerät benötigt.

Neben der Funktionen USB-Geräte zu blockieren, bietet Endpoint Protector weitere Möglichkeiten. So ist es möglich, auf Speichermedien übertragene Daten zu untersuchen und je nach Art oder Inhalt zu blockieren oder die Verschlüsselung der Geräte zu erzwingen.

2.4.4 Microsoft Active Directory – „Gruppenrichtlinie“

Das Blockieren der USB-Ports lässt sich auch über Gruppenrichtlinien, welche über das Active Directory verteilt werden, umsetzen. Dies erfüllt einige der Anforderungen nicht, wie die Verwaltung über eine Weboberfläche oder eine zeitliche Begrenzung der Freigaben. Dennoch wurde diese Lösung in Betracht gezogen, weil sie keine zusätzlichen Lizenzgebühren verursachen würde und somit eine kostengünstige Alternative darstellt. Ebenso braucht diese Windows-native Lösung keinen Agenten.

Freigaben für bestimmte Endgeräte oder USB-Geräte lassen sich durch Änderung der Richtlinien verteilen. Mit lokal ausgeführten Skripten zur Identifizierung der USB-Geräte lassen sich die benötigten Informationen einfach auslesen.

2.5 Lösungskonzepte im Überblick

1.	2.	3.	4.
CrowdStrike - Falcon Device Control	ManageEngine – Device Control Plus	Netwrix - Endpoint Protector	Active Directory - Gruppenrichtlinie
Cloud	On Premise	Cloud oder On Premise	On Premise (AD)

Tabelle 2 - Lösungskonzepte im Überblick

2.6 On Premise oder Cloud

Sowohl der Betrieb in der Cloud als auch On Premise sind prinzipiell möglich. Die Cloud-Lösung punktet durch niedrige Startkosten, schnelle Implementierung und einfache Skalierbarkeit, da der Anbieter die Wartung und Updates übernimmt. Sie benötigt jedoch eine stabile Internetverbindung und erfordert eine sorgfältige Prüfung der Datenschutz-Compliance bei externer Speicherung, insbesondere falls eine Inhaltsüberwachung der USB-Geräte stattfindet.

Im Gegensatz dazu bietet die On-Premise-Lösung die vollständige Datenhoheit und höchste Anpassbarkeit und ist unabhängig vom Internet, was für streng regulierte Branchen entscheidend ist. Allerdings sind hier die Anfangsinvestitionen für Hardware höher, die Implementierung ist aufwendiger, und das Unternehmen muss die gesamte Wartung selbst tragen, was bei einer wachsenden Zahl der Geräte die Komplexität erhöht.

Meine Empfehlung ist aufgrund des kleinen Teams eine weniger wartungsintensive Cloud-Variante.

3. Angebots und Testphase

3.1 Kontaktaufnahme mit ausgewählten Anbietern und Funktionsumfang

Um Angebote zu bekommen, wurden CrowdStrike, ManageEngine und Netwrix (Endpoint Protector) direkt kontaktiert.

3.1.1 Endpoint Protector

Da mit dem Anbieter Netwrix, dem Hersteller der Lösung Endpoint Protector, bislang noch keine Geschäftsbeziehung bestand, wurde der Erstkontakt über das auf der Unternehmenswebseite bereitgestellte Formular initiiert. Die Reaktion erfolgte zeitnah: Eine Vertreterin meldete sich daraufhin telefonisch bei uns. Im Rahmen dieses ersten Austauschs wurden die grundlegenden Projektinteressen abgestimmt und umgehend ein Termin für ein vertiefendes Erstgespräch mit Produktdemonstration vereinbart. Dieses Meeting fand in Form einer Webdemonstration statt, um uns einen umfassenden Einblick in die Funktionen und Möglichkeiten von Endpoint Protector im Hinblick auf unsere spezifischen Anforderungen an die USB-Kontrolle zu geben.

Als spezialisiertes Produkt im Bereich der Kontrolle von USB-Ports und Geräten bot Endpoint Protector die umfangreichsten Features. So gibt es die Möglichkeit die Sperrung von USB-Geräten mithilfe eines generierten Codes zu umgehen, falls das Gerät keine Verbindung zum Server aufbauen kann. Änderungen der Rechte oder Richtlinien, wie temporäre Freigaben werden innerhalb kürzester Zeit an das Endgerät übertragen. Zusätzlich lassen sich weitere Features als Erweiterungen buchen: EasyLock, welches USB-Speichermedien verschlüsselt oder Content Aware Protection, welches übertragene Dateiinhalte untersucht und nur die Übertragung bestimmter Dateien oder Formate erlaubt oder sogar bestimmte Inhalte blockieren kann.

3.1.2 CrowdStrike Falcon Device Control

Der Kontakt mit CrowdStrike erfolgte über einen bereits bestehenden Kontakt, verzögerte sich seitens CrowdStrike aber urlaubsbedingt erheblich. Nach der anfänglichen Verzögerung wurde ein Online-Meeting vereinbart, bei dem, wie bei Endpoint Protector, die Funktionen vorgestellt und Fragen geklärt wurden.

Der Funktionsumfang von Falcon Device Control war im Unterschied zu Endpoint Protector mehr auf das wesentliche beschränkt, so gibt es nicht die Möglichkeit eine Sperrung ohne Cloudanbindung zu Umgehen. Auch eine nutzergebundene Rechteverwaltung ist nicht möglich, ohne das Modul Privileged Access zusätzlich zu kaufen. Standardmäßig enthalten ist aber die Möglichkeit zu erfassen, welche Dateien übertragen werden.

3.1.3 Manage Engine - Device Control Plus

ManageEngine stellt unter Angabe der Mail-Adresse direkt eine 30-tägige Testversion mit einer grundlegenden Dokumentation und Anleitungen zur Verfügung. Diese wurde heruntergeladen und in einer Testumgebung installiert. Die Anfrage eines Angebots war über ein Formular sowohl auf der Website, als auch auf der Weboberfläche des Produktes möglich. Hier fiel ManageEngine Device Control direkt negativ auf, da über die

Weboberfläche nur eine Fehlermeldung als Antwort kam, dass es aktuell „technische Probleme“ gäbe. Dieser Fehler bestand während der gesamten Testphase von 30 Tagen.

3.2 Vorbereitung der Testumgebung

Für die Installation der Testversion von ManageEngine wurden mehrere Mini-PCs mit Intel Core i5-8500T, 32GB RAM und 500GB Festplattenspeicher gewählt, einer als Server, die andere für den Agent. Diese Computer entsprechen dem Standardcomputer in der Produktivumgebung.

Die Sperrung der USB-Ports über eine Gruppenrichtlinie wurde mit einer Testgruppe auf dem Active Directory und einem Testcomputer umgesetzt. Die Richtlinie wurde erstellt und mit der Testgruppe verknüpft. Danach wurde der Computer in die Testgruppe verschoben.

3.3 Netzwerkumgebung

Für den Test des Produktes von ManageEngine musste keine Änderung am vorhandenen Netzwerk vorgenommen werden, da sich sowohl Server, als auch Endgerät im selben Testnetzwerk befanden.

Für die Kommunikation des CrowdStrike Agenten und der Cloud gibt es bereits entsprechende Regeln, somit musste auch hier nichts geändert werden.

Gleiches gilt für die Verteilung von Gruppenrichtlinien.

3.4 Installation und Einrichtung

3.4.1 Manage Engine

Die bereitgestellte Installationsdatei war in Windowsumgebungen einfach ausführbar und konnte auf den Standardeinstellungen belassen werden. Danach liefen die benötigten Dienste im Hintergrund. Die Weboberfläche war sofort unter der IP-Adresse des Servers auf dem Port XXXX (HTTP) und Port YYYY (HTTPS) erreichbar. Diese Ports entsprechen den Standardeinstellungen während der Installation, können aber angepasst werden.

Der Agent steht danach in der Weboberfläche als Download bereit und wurde auf dem Endgerät installiert. Auch dies verlief problemlos.

3.4.2 Einrichtung der Gruppenrichtlinie

Für das Blockieren von Wechselmedien wurde unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Wechselmedienzugriff* die Option „Alle Wechselmedienklassen. Jeglichen Zugriff verweigern“ aktiviert. Das Richtlinienobjekt wurde dann mit der bereits bestehenden Testgruppe verknüpft und das Testgerät in die Gruppe verschoben.

Computerkonfiguration (Aktiviert)	
Richtlinien	
Administrative Vorlagen	
Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.	
System/Wechselmedienzugriff	
Richtlinie	Einstellung
Alle Wechselmedienklassen: Jeglichen Zugriff verweigern	Aktiviert

Abbildung 1 – Richtlinie zum Blockieren von Wechselmedien

3.4.3 CrowdStrike

Der Agent von CrowdStrike ist bereits auf allen relevanten Endgeräten installiert und Firewall Regeln existieren bereits. Da es sich um eine Cloudlösung handelt, muss auch dort nur die entsprechende Funktion seitens CrowdStrike freigeschaltet werden.

3.5 Testphase in Testumgebung

3.5.1 Manage Engine

Nach der Installation meldete sich der Agent direkt beim Server und wird in der Weboberfläche angezeigt. Dort wurde durch die relativ intuitive Oberfläche, eine knappe, bebilderte Anleitung zum Erstellen einer Gruppe und dem Zuordnen von Richtlinien das erste Endgerät in Betrieb genommen. Nach diesem ersten Tutorial stand das Programm in seiner vollen Vielfalt zur Verfügung. Das Erstellen weiterer Gruppen und Zuordnen von Richtlinien blieb weiterhin intuitiv und erfolgte über den Reiter „Richtlinien“, das Zuordnen von Endgeräten zu den Gruppen versteckt sich aber unter dem Reiter „Administrator“. Zudem fiel schnell auf, dass die deutsche Übersetzung noch unfertig war. So sind einige Überschriften oder Schaltflächen noch auf Englisch.

Negativ fiel während des Tests auf, dass eine Änderung der Richtlinien oder Gerätezuordnung nicht sofort an das Endgerät übertragen wurden, sondern erst mit dem regulären Aktualisierungsintervall. Dieses war standardmäßig auf 90 Minuten eingestellt, bei zwei verwalteten Endgeräten wurde ein Intervall von 15 Minuten vorgeschlagen. Manuell ließ sich eine Aktualisierung über den Reiter „Einblicke“ im Geräte-Manager für einzelne Endgeräte starten.

Positiv war, dass auf einigen Reitern Anleitungen aus der Wissensdatenbank des Herstellers verlinkt waren, ebenso häufig gestellte Fragen zu den unter den jeweiligen Reitern zu findenden Optionen. Diese Artikel waren nur in englischer Sprache verfügbar.

3.5.2 Gruppenrichtlinie

Da wir für Ausfallsicherheit mehrere Active Directory Server betreiben und Endgeräte die nötigen Daten von dem ersten verfügbaren Server beziehen, kann es mehrere Minuten dauern, bis Änderungen übermittelt werden. Dies war auch bei dem Testgerät der Fall. Zudem handelt es sich bei der verwendeten Richtlinie um eine Computerrichtlinie, welche erst mit einem Neustart des Endgerätes aktiv werden. Mit dem Befehl „gpupdate /force“ wurde eine Aktualisierung auf dem Endgerät erzwungen und das Testgerät neugestartet.

Die Richtlinie funktionierte und ein USB-Massenspeicher konnte nicht mehr verwendet werden. Für eine Freischaltung muss das Endgerät in eine Gruppe mit deaktivierter Richtlinie geschoben werden oder dem Gerät eine Ausnahmerichtlinie zugeteilt werden, die weiteren Schritte sind wie bereits oben beschrieben: Updaten der Richtlinien und Neustart.

Eine Erstellung dieser Richtlinie als Benutzerrichtlinie anstatt einer Computerrichtlinie wäre ebenso möglich, wurde aber nicht getestet, ebenso eine etwas granularer Einstellung als „Jeglichen Zugriff verweigern“. Die lange Zeit bis zur Verteilung und die Nichterfüllung von weiteren Anforderungen (fehlende Weboberfläche, komplexe Bedienung, keine zeitbegrenzte Freigabe) waren bereits ein ausreichendes Ausschlusskriterium.




Einstellung	Status	Kommentar
 Zeit (in Sekunden) bis zur Erzwungung des Neustarts festlegen	Nicht konfigur...	Nein
 CD und DVD: Ausführungszugriff verweigern	Nicht konfigur...	Nein
 CD und DVD: Lesezugriff verweigern	Nicht konfigur...	Nein
 CD und DVD: Schreibzugriff verweigern	Nicht konfigur...	Nein
 Benutzerdefinierte Klassen: Lesezugriff verweigern	Nicht konfigur...	Nein
 Benutzerdefinierte Klassen: Schreibzugriff verweigern	Nicht konfigur...	Nein
 Diskettenlaufwerke: Ausführungszugriff verweigern	Nicht konfigur...	Nein
 Diskettenlaufwerke: Lesezugriff verweigern	Nicht konfigur...	Nein
 Diskettenlaufwerke: Schreibzugriff verweigern	Nicht konfigur...	Nein
 Wechseldatenträger: Ausführungszugriff verweigern	Nicht konfigur...	Nein
 Wechseldatenträger: Lesezugriff verweigern	Nicht konfigur...	Nein
 Wechseldatenträger: Schreibzugriff verweigern	Nicht konfigur...	Nein
 Alle Wechselmedienklassen: Jeglichen Zugriff verweigern	Aktiviert	Nein
 Alle Wechselmedien: Jeglichen direkten Zugriff in Remotesit...	Nicht konfigur...	Nein
 Bandlaufwerke: Ausführungszugriff verweigern	Nicht konfigur...	Nein
 Bandlaufwerke: Lesezugriff verweigern	Nicht konfigur...	Nein
 Bandlaufwerke: Schreibzugriff verweigern	Nicht konfigur...	Nein
 WPD-Geräte: Lesezugriff verweigern	Nicht konfigur...	Nein
 WPD-Geräte: Schreibzugriff verweigern	Nicht konfigur...	Nein

Abbildung 2 – weitere Einstellungen der Richtlinie

3.7 Angebotsvergleich

3.7.1 Kostenübersicht

Die Angebote wurden für 750 Endgeräte eingeholt. Für ManageEngine war zudem noch die Angabe der Anzahl der „Techniker“ (Administratoren) nötig, welche mit fünf angegeben wurde. Die aufgeführten Kosten beziehen sich jeweils auf die Kosten für ein Jahr. Bei allen angegebenen Preisen wurden die Nettopreise zum Vergleich gezogen. Bei Netwrix handelte es sich nicht um ein verbindliches, formales Angebot, sondern nur eine Information, das den Bruttopreis darstellt. Da das Active Directory bereits unabhängig von diesem Projekt besteht und auch bestehen bleiben wird und der durch die Gruppenrichtlinie verursachte Mehraufwand als vernachlässigbar einzustufen ist, werden hierfür keine Kosten angesetzt.

Überraschend ist hier, dass CrowdStrike als Cloudvariante der günstigste Anbieter ist.

Kostenart	Produkt		
	CrowdStrike Falcon Device Control	ManageEngine Device Control Plus	Netwrix Endpoint Protector (On-Prem/Cloud)
Lizenzkosten Techniker	- €	XXX €	- €
Lizenzkosten Endgeräte	XXX €	XXX €	XXX/XXX€
Lizenzkosten Server (On-Premise)	- €	XXX €	XXX/XXX €
Kosten für Server, Backups, Service	XXX €	XXX €	XXX/XX €
Summe	<u>XXXX €</u>	<u>XXXX €</u>	<u>XXXX/XXXX€</u>

Tabelle 3 – Kosten pro Jahr

3.7.2 Nutzwertanalyse

Als Nächstes wird eine Nutzwertanalyse der verschiedenen Softwarelösungen durchgeführt, um die am besten geeignete Lösung für unsere Anforderungen zu identifizieren und die Rechtfertigung eines eventuellen Aufpreises zu prüfen.

Basierend auf den zuvor definierten Anforderungen wurden Bewertungskriterien festgelegt und gewichtet. Diese Kriterien sind in die folgenden Hauptbereiche unterteilt: Agent, Funktionsumfang, intuitive Bedienbarkeit und anwenderfreundliche GUI, Berichte und Protokollierung, Wartungsaufwand, Reaktionsgeschwindigkeit (Zeit bis Änderungen am Endgerät ankommen), Support und Kosten.

Die relative Gewichtung der Kriterien erfolgte auf einer Prozentskala. Die Erfüllung der Kriterien durch die Softwarelösung wurde mit einer Punktzahl von 0 bis 5 bewertet, wobei 5 Punkte für eine vollständige Erfüllung und 0 Punkte für eine Nichterfüllung vergeben wurden.

		CrowdStrike		ManageEngine		Endpoint Protector		Gruppenrichtlinie	
Kriterium	Gewichtung	Punkte	Ergebnis	Punkte	Ergebnis	Punkte	Ergebnis	Punkte	Ergebnis
Agent	10%	4	0,4	2	0,2	2	0,2	5	0,5
Funktionsumfang	10%	4	0,4	3	0,3	5	0,5	1	0,1
Intuitivität / GUI	10%	4	0,4	2	0,2	4	0,4	1	0,1
Berichte	10%	4	0,4	3	0,3	4	0,4	0	0
Wartung	10%	5	0,5	3	0,3	5	0,5	2	0,2
Reaktionsgeschwindigkeit	15%	5	0,75	2	0,3	5	0,75	1	0,15
Support	15%	4	0,6	2	0,3	4	0,6	0	0
Kosten	20%	3	0,6	3	0,6	1	0,2	5	1
Gesamt	100%	33	<u>4,05</u>	20	<u>2,5</u>	30	<u>3,55</u>	15	<u>2,05</u>

Tabelle 4 - Qualitativer Angebotsvergleich

3.7.3 Auswertung

CrowdStrike (Gesamtpunktzahl: 4,05)

CrowdStrike geht als Gesamtsieger aus der Bewertung hervor. Die Lösung zeichnet sich durchweg durch hohe Qualität aus und erzielt in fast allen Kategorien 4 oder 5 von 5 möglichen Punkten. Die größten Stärken liegen in der Reaktionsgeschwindigkeit bei der Übertragung neuer Richtlinien und als Cloudlösung bei der Wartung, wo sie mit der vollen Punktzahl überzeugt. Auch bei dem Kriterium Agent schneidet CrowdStrike gut ab, da der Agent bereits vorhanden ist. Für den leicht über die Mindestanforderungen herausgehenden Funktionsumfang, eine gute GUI (für die seitens CrowdStrike bereits eine verbesserte Version 2.0 in Arbeit ist), ausführlichen Berichten und dem bisher guten Support werden sehr gute Werte erreicht. Selbst bei dem schwächsten Punkt, den Kosten, schneidet CrowdStrike gut ab und wird nur von der kostenfreien Gruppenrichtlinie unterboten.

Endpoint Protector (Gesamtpunktzahl: 3,55)

Endpoint Protector bietet in den Kernbereichen Funktionsumfang, Wartung und Reaktionsgeschwindigkeit eine Spitzenperformance und erreicht hier entsprechend Höchstbewertungen. Auch die GUI war intuitiv und der Support wirkte gut, wobei im Gegensatz zu CrowdStrike natürlich langfristig die Erfahrung fehlt. Die größte Schwäche dieser Lösung sind jedoch die Kosten. Mit einem 80 Prozent höherem Preis für die On-Premise Variante und dem zwei-einhalbfachen Preis für die Cloudvariante im Vergleich zu dem Angebot von CrowdStrike erreicht Endpoint Protector in dieser wichtigen Kategorie die schlechteste Bewertung unter allen Tools. Auch der zusätzliche Agent verschlechtert die Bewertung.

ManageEngine (Gesamtpunktzahl: 2,5)

Die primäre Stärke ist der Bereich Kosten die nur geringfügig höher sind als die günstigste Alternative (CrowdStrike) und damit zu den besten Werten des Produkts gehört. Demgegenüber stehen jedoch deutliche Schwächen in fast allen funktionalen und Service-Kategorien. Besonders niedrig sind die Bewertungen für Intuitivität / GUI, Reaktionsgeschwindigkeit und Support (vgl. 3.5.1).

Gruppenrichtlinie (Gesamtpunktzahl: 2,05)

Die Gruppenrichtlinie ist als native Windows-Lösung die kostengünstigste Option. Ihre größten Stärken sind Kategorien Agent und Kosten, da sie ohne zusätzliche Lizenzkosten und als fester Bestandteil des Betriebssystems zur Verfügung steht. Allerdings ist sie in fast allen anderen Bereichen, die professionelle USB-Kontroll-Tools auszeichnen, stark eingeschränkt. Schwächen zeigen sich besonders bei den nicht existenten Berichten, der Reaktionsgeschwindigkeit und der fehlenden (Web-)GUI. Sie ist somit funktional den kommerziellen Lösungen klar unterlegen.

3.8 Wirtschaftlichkeitsbetrachtung

Die wirtschaftlichen Auswirkungen, die eine fehlende USB-Kontrolle haben kann, ist in den meisten Fällen schwer zu bewerten, da nicht genau bemessen werden kann, welche Schäden der Abfluss von Informationen verursacht. Ebenso lassen sich Reputationsschäden nur schwer vorhersagen und vorab bemessen. Dahingegen ist eine genaue Berechnung von finanziellen Schäden durch einen Ransomware Angriff, der zu einem Totalausfall führt, sehr einfach. Die durchschnittliche Ausfallzeit bei einem Ransomware Angriff liegt bei etwa 23 Tagen, die geringste anzunehmende Zeit liegt bei einem Tag.

Bei einem Jahresumsatz im dreistelligen Millionenbereich bei Agrarfrost würde schon ein eintägiger Ausfall die Kosten der teuersten Lösung (Endpoint Protector Cloud) für Jahrzehnte rechtfertigen. Die günstigeren Lösungen schneiden entsprechend noch besser ab.

3.9 Vorstellung der Angebote und Entscheidung

Aufgrund der langen Wartezeit auf eine Antwort des Anbieters CrowdStrike, welcher bereits zu Projektbeginn als möglicher Favorit galt, verzögerte sich die Entscheidungsfindung stark. Das Angebot lag erst am 26.11.2025 vor, somit fand die Vorstellung vor dem Leiter der IT-Abteilung, dem Informationssicherheitsbeauftragten und den Kollegen erst am 28.11.2025 statt. Es wurden die Funktionsumfänge der einzelnen Lösungen vorgestellt, deren Stärken und Schwächen benannt und Kosten verglichen. Dabei wurde Falcon Device Control von CrowdStrike empfohlen. Aufgrund der überzeugenden Argumente haben die Verantwortlichen für die empfohlene Lösung die Kaufentscheidung getroffen.

4. Implementierungsphase

Aufgrund der bereits genannten Verzögerungen beschreibt dieser Abschnitt die noch zu erledigenden Schritte. Geplant ist ein Abschluss der Implementation bis Mitte Januar 2026. Die in diesem Abschnitt beschriebenen Schritte sind noch durchzuführen.

4.1 Installation und Konfiguration

Als Software as a Service (SaaS) muss Falcon Device Control seitens CrowdStrike für Agrarfrost freigeschaltet werden, es muss kein Server erstellt werden. Die Agenten sind bereits vorhanden.

Es bleibt das Erstellen von Richtlinien und die Zuweisung der Endgeräte entsprechend der weiter unten genannten Regeln.

4.2 Deinstallation des Agenten (altes USB-Kontrollsystem)

Die Deinstallation des alten Agenten ist nicht über die Systemsteuerung von Windows möglich, sondern benötigt entweder einen speziellen Deinstallationscode, der von der Serveranwendung für jeden Agent einzeln generiert werden muss oder erfolgt automatisiert über die alte Weboberfläche. Dazu wird in der Weboberfläche des alten USB-Kontrollsystems unter dem Reiter „Client Task ausführen“ die bereits bestehende Aufgabe „DLP Uninstall“ ausgewählt, dann werden die entsprechenden Endgeräte angegeben. Nachdem diese Aufgabe erfolgreich beendet wurde, wird das Endgerät aus der Liste der verwalteten Geräte gelöscht und bei der Bestätigung ein Haken bei „Agent löschen“ gesetzt. Nach kurzer Zeit ist der Agent vom Endgerät entfernt, dies geschieht im Hintergrund. Dieser Vorgang wird bei allen Endgeräten in mehreren Chargen mit über einen längeren Zeitraum durchgeführt, um den Server und das Netzwerk nicht zu überlasten. Dies wurde vorab an mehreren Geräten getestet.

4.3 Richtlinie für Sperrung und Freigabe von USB-Geräten

USB-Geräte, die keine Speicher sind, wie z.B. Tastaturen, Mäuse oder Webcams sind standardmäßig freigegeben. Massenspeicher (USB-Sticks, externe Festplatten, etc.) sind standardmäßig gesperrt. Eine Freigabe kann schriftlich mit Begründung und Zeitraum über das Ticketsystem beantragt werden und wird individuell geprüft. Ausgenommen sind hierbei die Firmen-iPhones, da diese von den Mitarbeitern bei Rundgängen zur Dokumentation mithilfe von Fotos genutzt werden und die einfache Übertragung auf den Computer möglich sein soll.

4.4 Anwenderdokumentation

Die Anwenderdokumentation wird in der internen Wissensdatenbank erstellt.

5. Projektabschluss

5.1 Vergleich Projektantrag

Es ergaben sich während der Durchführung einige Unterschiede zum Projektantrag. Auf der einen Seite haben einige Abschnitte deutlich mehr Zeit in Anspruch genommen als ursprünglich geplant. Die Anbietersuche dauerte aufgrund der hohen Anzahl der angebotenen Lösungen bedeutend länger als geplant und streckte sich durch eine erste Bewertung noch weiter. Außerdem nahm die Kontaktaufnahme mit den Anbietern durch Onlinemeetings weit mehr Zeit ein als ursprünglich gedacht. Die Testphase inklusive Angebotsvergleich war zu kurz bemessen. Auch die Projektdokumentation nahm mehr Zeit als geplant ein.

Auf der anderen Seite verschiebt sich die Implementierungsphase aufgrund der bereits genannten Probleme nach hinten, wobei diese weniger Zeit in Anspruch nehmen wird, als ursprünglich geplant. Dies liegt daran, dass die gewählte Lösung bereits verwendet wird und somit keine Zeit für das Installieren von Agenten oder eines Servers benötigt wird.

5.2 Fazit

Mit der erfolgreichen Ablösung der Altanwendung durch Falcon Device Control wurde im Unternehmen ein modernes USB-Sicherheits- und Richtlinienmanagementsystem etabliert. Die neue Lösung ermöglicht eine granularere Kontrolle über alle Wechseldatenträger und anderer USB-Geräte, wodurch die Gefahr des Datenabflusses sowie das Risiko von Malware-Einschleusungen signifikant reduziert werden. Das System erfüllt alle definierten Anforderungen und zukünftig wird das Unternehmen die erweiterte Funktionalität nutzen, um die Sicherheitsrichtlinien kontinuierlich anzupassen und die Konformität der Endgeräte im Umgang mit sensiblen Daten nachhaltig zu gewährleisten.

6. Anhang

Angebote
CrowdStrike

[illegible][illegible]

Konto		Saldo	Umsatz	Saldo
1	Saldo			
2	Saldo			
3	Saldo			
4	Saldo			
5	Saldo			
6	Saldo			
7	Saldo			
8	Saldo			
9	Saldo			
10	Saldo			
11	Saldo			
12	Saldo			
13	Saldo			
14	Saldo			
15	Saldo			
16	Saldo			
17	Saldo			
18	Saldo			
19	Saldo			
20	Saldo			
21	Saldo			
22	Saldo			
23	Saldo			
24	Saldo			
25	Saldo			
26	Saldo			
27	Saldo			
28	Saldo			
29	Saldo			
30	Saldo			
31	Saldo			
32	Saldo			
33	Saldo			
34	Saldo			
35	Saldo			
36	Saldo			
37	Saldo			
38	Saldo			
39	Saldo			
40	Saldo			
41	Saldo			
42	Saldo			
43	Saldo			
44	Saldo			
45	Saldo			
46	Saldo			
47	Saldo			
48	Saldo			
49	Saldo			
50	Saldo			
51	Saldo			
52	Saldo			
53	Saldo			
54	Saldo			
55	Saldo			
56	Saldo			
57	Saldo			
58	Saldo			
59	Saldo			
60	Saldo			
61	Saldo			
62	Saldo			
63	Saldo			
64	Saldo			
65	Saldo			
66	Saldo			
67	Saldo			
68	Saldo			
69	Saldo			
70	Saldo			
71	Saldo			
72	Saldo			
73	Saldo			
74	Saldo			
75	Saldo			
76	Saldo			
77	Saldo			
78	Saldo			
79	Saldo			
80	Saldo			
81	Saldo			
82	Saldo			
83	Saldo			
84	Saldo			
85	Saldo			
86	Saldo			
87	Saldo			
88	Saldo			
89	Saldo			
90	Saldo			
91	Saldo			
92	Saldo			
93	Saldo			
94	Saldo			
95	Saldo			
96	Saldo			
97	Saldo			
98	Saldo			
99	Saldo			
100	Saldo			

Endpoint Protector

netwrix

Endpoint Protector		Netwrix		Status		Informationen		Details	
Endpoint	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse
192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
Endpoint Protector									
Endpoint Protector									
Endpoint Protector									

Endpoint Protector		Netwrix		Status		Informationen		Details	
Endpoint	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse	Hostname	IP-Adresse
192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
Endpoint Protector									
Endpoint Protector									
Endpoint Protector									

Endpoint Protector

Endpoint Protector

Endpoint Protector

Endpoint Protector

ManageEngine



Zeitplan

Phase	SOLL	IST	Differenz
Planungsphase	5	10	+5
Besprechung des Problems	1	1	
IST-Analyse	1	1	
Anforderungen ermitteln, SOLL-Konzept entwickeln	1	2	+1
Anbietersuche, Auswahl an Produkten zum Testen	2	6	+4
Angebots und Testphase	8	18	+10
Kontaktaufnahme mit Anbietern	1	4	+3
Installation und Konfiguration von Testversionen	4	9	+5
Auswertung der Testphase, Angebotsvergleich	2	3	+1
Angebote vorstellen, Festlegung für ein Angebot	1	2	+1
Implementierungsphase	20	2	-18
Installation und Konfiguration	8	1	-7
Funktionstest bei ausgewählten Netzwerkkomponenten	2	0	-2
Fehlerbehebung und Bewertung der Testphase	3	0	-3
Finale Ausbreitung der Software	3	0	-3
interne System- und Anwenderdokumentation	3	1	-2
Abnahme der Software	1	0	-1
Projektabschluss	7	10	+3
Vorstellung	1	1	
Bewertung des Projekts	1	1	
IHK -Projektdokumentation	5	8	+3
Gesamt	40	40	0

Tabelle 5 – Zeitplan

Herleitung von Server-, Hypervisor- und Wartungskosten

Abschreibungskosten Server			
Geräte	Anschaffungskosten	Abschreibung pro Jahr	Pro Server
Dell Hardware	XXXX €	XXXX €	XXXX €
Backup Server	XXXX €	XXXX €	XXXX €
Wartung (VMWare, Bandlaufwerke, etc.)		XXXX €	XXXX €
Jährlich gesamt			XXXX €

Tabelle 6 - Kosten

Um die Kosten eines einzelnen Servers pro Jahr zu berechnen, wurde zunächst die Abschreibung der gesamten Virtualisierungsumgebung auf 5 Jahre betrachtet. Anschließend wurde dies durch die Anzahl an Server geteilt. Hinzu kommen die Kosten für das Backup-System, wobei ebenfalls von einer Abschreibung von 5 Jahren ausgegangen ist.

Glossar

Active Directory

Active Directory (AD) ist ein von Microsoft entwickelter Verzeichnisdienst für Windows-Domänennetzwerke, der zur zentralen Verwaltung von Benutzern, Computern und anderen Netzwerkressourcen dient.

Cloud

Cloud Computing beschreibt die Bereitstellung von IT-Ressourcen wie Rechenleistung, Speicher und Anwendungen über das Internet ("die Cloud") als Dienst, wobei Nutzer diese nach Bedarf beziehen und bezahlen.

DLP

DLP (Data Loss Prevention) bezeichnet Sicherheitsstrategien und Tools, die verhindern sollen, dass sensible Daten das Unternehmensnetzwerk verlassen oder unbefugt verwendet werden, sei es versehentlich oder böswillig.

EDR

EDR (Endpoint Detection and Response) ist eine Sicherheitslösung, die kontinuierlich Endgeräte überwacht, Daten sammelt, verdächtige Aktivitäten analysiert und darauf reagiert, um Bedrohungen zu erkennen und einzudämmen.

GUI

Die GUI (Graphical User Interface) ist eine grafische Benutzeroberfläche, die es Benutzern ermöglicht, mit elektronischen Geräten oder Software über visuelle Elemente wie Fenster, Icons und Menüs zu interagieren, anstatt Befehle über Text einzugeben.

On Premise

On-Premise beschreibt die lokale Installation und den Betrieb von Software und IT-Infrastruktur direkt in den Räumlichkeiten und unter der Kontrolle des jeweiligen Unternehmens.

SaaS (Software as a Service)

SaaS ist ein Lizenz- und Bereitstellungsmodell, bei dem die Software zentral von einem Anbieter gehostet und über das Internet (meist per Webbrowser) gegen ein Abonnement zur Verfügung gestellt wird, wodurch der Endnutzer keine lokale Installation oder Wartung benötigt. Es handelt sich dabei um die Bereitstellung einer fertigen Anwendung über die Cloud.

USB

USB (Universal Serial Bus) ist ein standardisiertes, serielles Bussystem zur Verbindung von externen Geräten (wie Speichersticks oder Tastaturen) mit einem Computer oder anderen Hosts und dient der Datenübertragung sowie der Stromversorgung.

Tabellenverzeichnis

Tabelle 1 – Ermittlung der Geräteanzahl.....	2
Tabelle 2 – Lösungskonzepte im Überblick.....	4
Tabelle 3 – Kosten pro Jahr.....	9
Tabelle 4 – Qualitativer Angebotsvergleich	9
Tabelle 5 – Zeitplan	17
Tabelle 6 – Kosten.....	17

Abbildungsverzeichnis

Abbildung 1 – Richtlinie zum Blockieren von Wechselmedien	7
Abbildung 2 – weitere Einstellungen der Richtlinie	8

Quellen

Webseite Agrarfrost

<https://www.agrarfrost.de/>

Website ManageEngine Device Control Plus

<https://www.manageengine.com/de/device-control/>

Website CrowdStrike Falcon Device Control

<https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-device-control/>

Website Endpoint Protector Device Control

<https://www.endpointprotector.de/solutions/device-control>

Andere Quellen

https://de.wikipedia.org/wiki/Active_Directory

https://de.wikipedia.org/wiki/Cloud_Computing

https://en.wikipedia.org/wiki/Endpoint_detection_and_response

https://de.wikipedia.org/wiki/Data_Loss_Prevention

<https://de.wikipedia.org/wiki/On-Premises>

https://de.wikipedia.org/wiki/Universal_Serial_Bus

<https://de.wikipedia.org/wiki/Software-as-a-Service>

https://de.wikipedia.org/wiki/Grafische_Benutzeroberfl%C3%A4che