

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

Präsentation des Abschlussprojektes
Paul Tiemann
2026





Agenda

- Vorstellung von Agrarfrost
- Projektbeschreibung
- Projektplanung
- Angebots und Testphase
- Implementierungsphase
- Projektabschluss



Agrarfrost GmbH



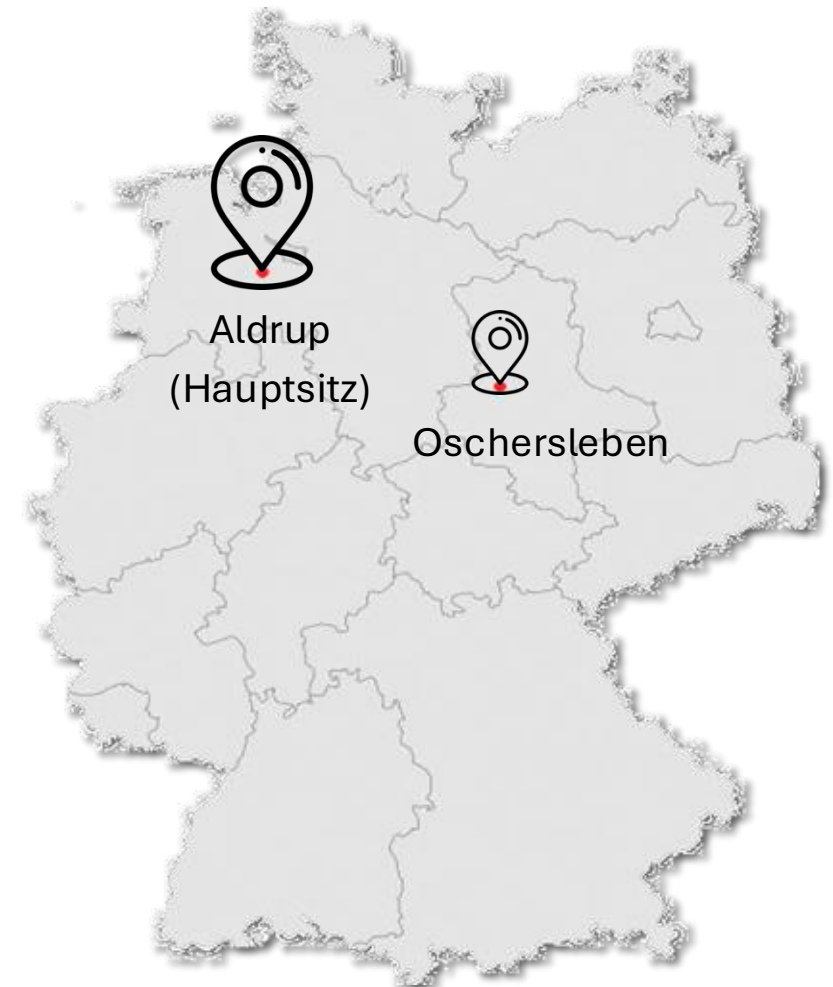
- Gründung 1967
- Familienunternehmen
- Lebensmittelindustrie
 - Kartoffelprodukte



- Ca. 800 Mitarbeiter in der Unternehmensgruppe



- 215.000 Tonnen / Jahr



Was ist ein USB-Sicherheits- und Richtlinienmanagementsystem?

- Einsatz von Wechselmedien in einem Unternehmensnetzwerk
- Zentrale Zugriffskontrolle (White- und Blacklisting)
- Schutz vor Datenabfluss und Malware
- Möglichkeit für Überwachung und Audit-Logging

Projektbeschreibung

Problemstellung

- USB-Schnittstellen sind Einfallstor für Malware
- Abfluss sensibler Daten
- Kontrolle der Mitarbeiter nicht realistisch

➤ Technische Lösung nötig

Aufgabenstellung

- Implementierung einer strikten USB-Kontrolle auf technischer Ebene



IST-Analyse

- Altes System ist Teil einer alten EDR-Lösung
- Vertrag ausgelaufen, keine Verlängerung geplant
- Ca. 750 relevante Geräte



SOLL-Konzept

Anforderungen an die Lösung

- Freigabe/Sperrung nach:
 - USB-Gerät, Gerätegruppe, Endgerät
 - Optional: Nutzerkonto
- Anwenderfreundliche Bedienung
- Zentrale, browserbasierte Verwaltung
- Kein oder ressourcensparsamer Agent

Richtlinie für den Umgang mit USB-Geräten

- Sperren aller Massenspeicher
- Antrag für Freigabe über Ticketsystem



Anbieterübersicht

**CROWDSTRIKE**

Falcon Device Control

- Bereits Anbieter für EDR im Konzern
- Agent bereits installiert
- Cloud

ManageEngine

Device Control Plus

- Günstiger Anbieter
- On Premise

**ENDPOINT
PROTECTOR**

by CoSoSys

- Spezialisierter Anbieter
- Cloud oder On Premise

Microsoft
Active Directory

- Praktisch keine Kosten
- Umfassende AD-Struktur bereits vorhanden
- Kein Agent
- On Premise



Testphase



CROWDSTRIKE Falcon Device Control

- Agent bereits installiert
- Richtlinien und Gruppen intuitiv zu erstellen
- Aktualisierung in Echtzeit



Device Control Plus

- Einfache Installation
- Einfache Anleitung für erste Schritte
- Unvollständige Übersetzung
- langes Aktualisierungsintervall
- Zusätzlicher Agent



ENDPOINT PROTECTOR

by CoSoSys

- Großer Funktionsumfang
- Offline Freigabe
- Weitere optionale Features buchbar
- Aktualisierung in Echtzeit
- Zusätzlicher Agent



Active Directory

- Erstellen als Computerrichtlinie
- Aktualisierungsintervall zu lange
- Zu viele Anforderungen nicht erfüllt



Kosten pro Jahr

Kostenart	CrowdStrike Falcon Device Control	ManageEngine Device Control Plus	Netwrix Endpoint Protector (On-Prem/Cloud)
Kosten Techniker/Support	XXXX €	XXXX €	- €
Lizenzkosten Endgeräte	XXXX €	XXXX €	XXXX / XXXX€
Lizenzkosten Server (On-Premise)	- €	XXXX €	XXXX / XXXX €
Kosten für Server, Backups, etc.	- €	XXXX €	XXXX / XXXX €
Summe	XXXX €	XXXX €	XXXX / XXXX €



Angebotsvergleich

		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%	38	4,05	20	2,5	30	3,55	15	2,05



Kaufentscheidung



CROWDSTRIKE

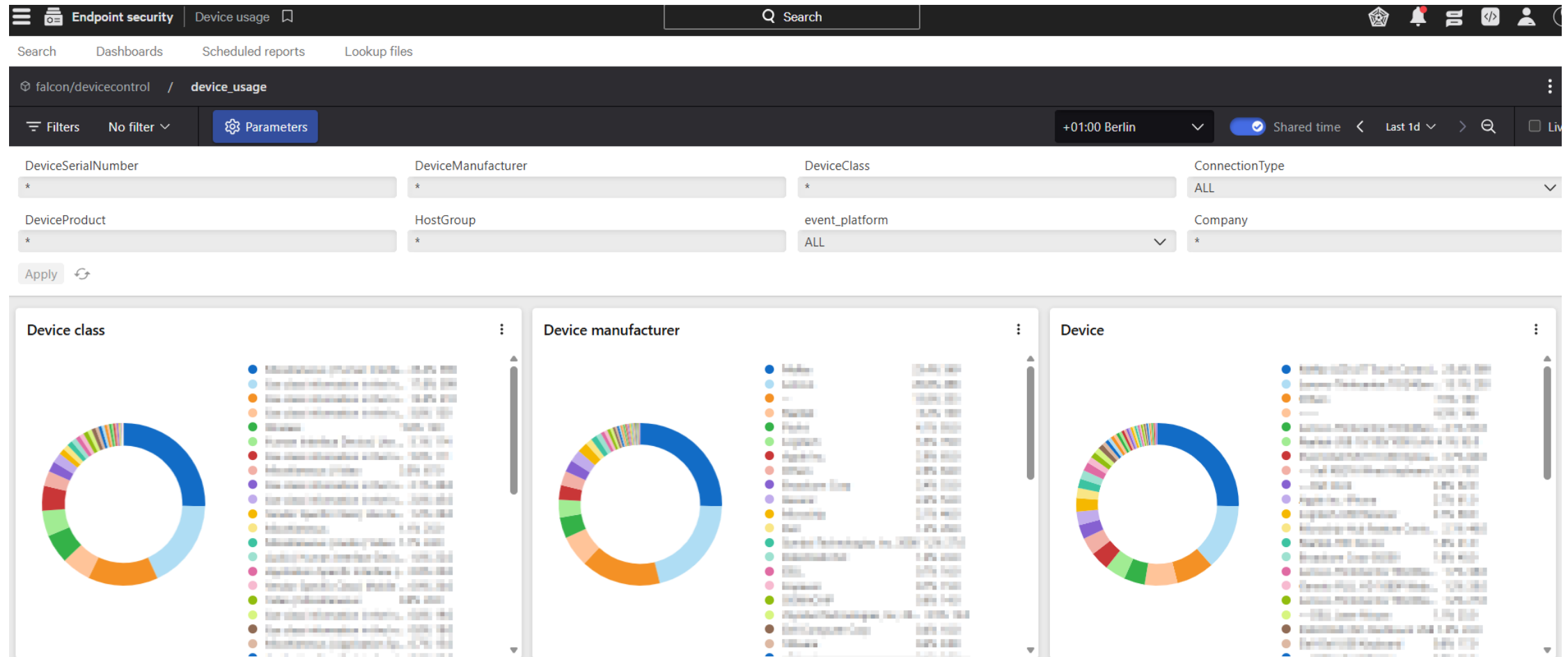
Falcon Device Control




Realisierungsphase

- Aktivierung Anfang Januar
- Agent bereits installiert
- Richtlinien und Gruppen können sofort erstellt werden
- Deinstallation des alten Systems



Dashboard – Device usage



Device policies



 Endpoint security | [Device policies](#) > Windows 

Q Search



Device policies

Platform

 Windows 

3 Windows policies

[Edit precedence](#)[Create policy](#)

Precedence	Status	Name	ID	USB Mode	PCIe Mode	Last Modified	Applied hosts	Pending hosts
1	Enabled	TEST 2	0087b5c9d22746...	Monitor and enforce	Monitor only	Jan. 7, 2026 08:33:40	2	0
2	Enabled	TEST	9755dac0eaa14c...	Monitor and enforce	Monitor only	Jan. 6, 2026 14:59:52	2	0
	Enabled	Default (Windows)	b39a09eec3fa41...	Monitor and enforce	Monitor only	Jan. 11, 2023 16:25:05	635	101

Einstellungen - Auswahl

The screenshot displays the 'Settings' application with the 'USB devices' tab selected. The 'Mass storage' device class is chosen, and the 'Full block' permission is selected. A modal dialog titled 'Add device exception' is open in the center. This dialog allows users to specify how to find devices (Combined ID or Manual entry), enter a combined ID, select a device class (currently 'Mass storage'), and choose permissions (Read, write, execute; Read and write only; Read only; Full block). A red box highlights the 'Make temporary exception' checkbox, which is currently unchecked. At the bottom of the dialog, there is a 'Description' text area and 'Cancel' and 'Add exception' buttons. In the background, the 'Permissions' section of the settings is visible, showing a list of permissions with a red box highlighting the '+ Add exception' button.

Settings **USB devices** PCIe devices

Device Class

Any class

Audio/Video

Imaging

Mass storage

Permissions

- ☐ Read, write, execute
- ☐ Read and write only
- ☐ Read only
- ☒ Full block

Specific device exceptions in this class

Vendor ID	Vendor name	Product ID
-----------	-------------	------------

Add device exception

Choose how to find devices for this policy

- ☒ Combined ID
- ☐ Manual entry

For USB devices observed in your environment, copy the combined ID from the [USB device usage dashboard](#) and paste it below.

Combined ID

Device class

Mass storage

Permissions

- ☒ Read, write, execute
- ☐ Read and write only
- ☐ Read only
- ☐ Full block
- ☐ Make temporary exception

Description

Cancel Add exception

Cancel Save

Permissions

Full access

Full access

Full block

+ Add exception

ns	Created	Last modified	A...
----	---------	---------------	------

Fazit



Passende Lösung
ausgewählt



Lösung implementiert



Richtlinien erstellt und
Funktionen erprobt



ToDo:
unternehmensweite
Umsetzung



**Vielen Dank für Ihre
Aufmerksamkeit!**

