

Verbesserte Cyber-Abwehr mit DriveLock Device Control

Ausgangssituation

FEV, ein weltweit führender Engineering-Dienstleister im Automobilsektor und Innovationsmotor für verschiedene Branchen, stand vor großen Herausforderungen in Bezug auf die Sicherheit von USB-Speichergeräten. Im Jahr 2022 sah sich das Unternehmen häufig mit Fällen von eindringender Malware, Datenexfiltration und nicht autorisierten Softwareinstallationen über externe Geräte konfrontiert. Diese Sicherheitsbedrohungen, insbesondere die Raspberry-Robin-Malware, die schnell Daten über USB-Geräte exfiltriert, erforderte die Suche nach einer robusten Sicherheitslösung.



„Wir sahen uns mit erheblichen Sicherheitsbedrohungen durch USB-Geräte konfrontiert, insbesondere durch Malware, die Daten schnell und unauffällig exfiltriert. Unsere bestehenden Lösungen waren unzureichend“, sagt René Tieben, Global Manager bei FEV.

Die wichtigsten Ziele zur Bewältigung dieser Herausforderungen waren:

- › Volle Kontrolle und bessere Transparenz über externe Speichergeräte.
- › Schnelle Reaktion auf Vorfälle wie Malware oder Datenverlust.
- › Einhaltung von Branchenvorschriften wie TISAX und anderen kundenspezifischen Sicherheitsanforderungen.

Auswahl der Lösung

FEV leitete einen gründlichen Evaluierungsprozess ein, einschließlich einer Ausschreibung, um die besten verfügbaren Sicherheitslösungen zu ermitteln. Die Organisation zog mehrere Optionen in Betracht, entschied sich aber schließlich für DriveLock aufgrund der einfachen Handhabung, der effektiven Bereitstellung und der Kosteneffizienz im Vergleich zu anderen Produkten.

„Wir brauchten eine professionelle Lösung, die eine granulare Kontrolle und einen schnellen Einsatz ermöglichte. DriveLock erfüllte all diese Kriterien und war preislich wettbewerbsfähig“, so Tieben.

Prozess der Umsetzung

DriveLock wurde nahtlos in die Infrastruktur von FEV implementiert, wobei interne Tools für schnelle und transparente Updates genutzt wurden.

*Marco Barberis, Technical Lead Engineer bei FEV, erläutert:
„Der Implementierungsprozess war unkompliziert, und die Updates werden nahtlos integriert. Wir können sicherstellen, dass auf 90 Prozent unserer Geräte immer der neueste Agent läuft.“*

FEV begann mit der Sicherung von 8.000 Geräten und steigerte die Zahl allmählich auf 10.000, einschließlich der Geräte aus laufenden Betriebssystemmigrationen sowie neu eingeführter Hardware.

Wichtige Schritte bei der Umsetzung:

- » **Erstinstallation:** FEV nutzte Software Packaging Manager, um DriveLock und andere Security-Tools auf den ersten Geräten zu installieren und so eine reibungslose Integration ohne Probleme zu gewährleisten.
- » **Monitoring und Updates:** Transparente Updates für DriveLock Agenten sorgen dafür, dass neueste Sicherheitspatches automatisch eingespielt werden.
- » **Skalierbarkeit:** Von initial 8.000 Geräten wurde auf 10.000 erweitert, darunter neue Geräte wie auch auf Windows 11 migrierte.

DriveLocks Device Control bietet mehrere entscheidende Vorteile:



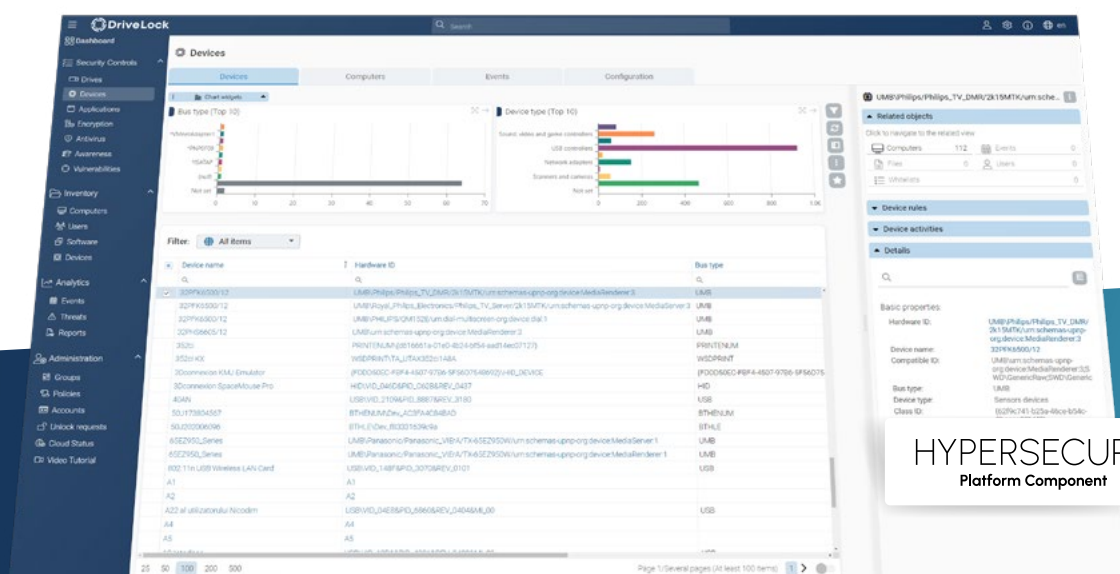
FEV hat nun vollständige Kontrolle und Echtzeit-Überwachung aller externen Speichergeräte und reduzierte damit das Risiko von Malware-Infektionen deutlich.

„Wir haben die Malware-Infektionen durch externe Geräte um 99,9 Prozent reduziert. Das hat erhebliche Ressourcen freigesetzt und die Sicherheit insgesamt signifikant verbessert“, so Tieben.

Darüber hinaus unterstützt DriveLock die Einhaltung von TISAX und anderen vertraglichen Vereinbarungen, die eine strenge Kontrolle über externe Speichergeräte verlangen.

„DriveLock ermöglicht es uns, die Einhaltung dieser Richtlinien und vertraglichen Verpflichtungen transparent und effektiv nachzuweisen“, fügt Tieben hinzu.

Die umfassenden Überwachungsfunktionen ermöglichen zudem eine schnelle Reaktion auf Vorfälle und detaillierte Audits. „DriveLocks umfassende Überwachungs- und Incident-Response-Tools sparen uns so jedes Jahr Hunderte von Stunden“, sagt Tieben.



HYPERSECUR
Platform Component

Herausforderungen und Lösungen

Bei der anfänglichen Implementierung gab es kleinere Probleme, wie z. B. die Sicherstellung der richtigen Spracheinstellungen für Benutzerbenachrichtigungen und den Umgang mit nicht konformen USB-Geräten mit nicht standardisierten Seriennummern. Diese Probleme wurden gelöst, indem die Meldungen auf Englisch standardisiert und problematische Geräte ausgeschlossen wurden.

„Eine Herausforderung war die Verwaltung der Spracheinstellungen für Benutzerbenachrichtigungen, die wir durch die Verwendung von Englisch als Standardsprache gelöst haben“, erklärt Barberis.

Eine weitere Herausforderung war der Umgang mit nicht-konformen USB-Geräten, die keine korrekten Seriennummern hatten, was ihre Erkennung und Verwaltung durch DriveLock erschwerte. Dieses Problem wurde durch den Ausschluss dieser Geräte von der Zulassungsliste entschärft.

Einhaltung der Vorschriften und Berichterstattung

Die Einhaltung von Compliance-Anforderungen ist für Unternehmen, die in regulierten Branchen tätig sind, von entscheidender Bedeutung. Die Lösungen von DriveLock sind darauf ausgelegt, die Einhaltung von Standards wie TISAX, ISO-Zertifizierungen und EU-Vorschriften wie NIS2 zu unterstützen. Die robusten Berichts- und Überwachungsfunktionen erleichtern FEV den Nachweis der Compliance bei Audits.

René Tieben: „Mit DriveLock können wir unsere Compliance-Bemühungen transparent nachweisen. Es ist beruhigend, ein so robustes Tool zu haben, das wir Auditoren vorlegen können und das sicherstellt, dass wir unsere vertraglichen Verpflichtungen erfüllen.“

Schlussfolgerung

DriveLock's Device Control hat die Cyberabwehr der FEV erheblich verbessert, indem es eine robuste Kontrolle, verbesserte Compliance und eine effiziente Reaktion auf Vorfälle ermöglicht. Die nahtlose Integration und die benutzerfreundliche Administration haben DriveLock zu einem unverzichtbaren Bestandteil der Sicherheitsstrategie von FEV gemacht.

„DriveLock hat unsere Ziele erreicht und im Laufe der Zeit zusätzliche Vorteile gebracht, was es zu einem unverzichtbaren Werkzeug in unserem Cyber-Defense-Arsenal macht“, so Tieben abschließend.

Die umfassenden Sicherheitslösungen von DriveLock haben sich bei FEV und vielen anderen Unternehmen, die vor ähnlichen Herausforderungen stehen, bewährt.

Verbessern Sie Ihren Cyber-Schutz, erreichen Sie Compliance und optimieren Sie Ihre Endpoint Security mit DriveLock.

Falls Sie Fragen haben oder weitere Details zur Implementierung und den Vorteilen von DriveLock für Ihre Organisation erfahren möchten, wenden Sie sich bitte an unser Team. Wir stehen Ihnen jederzeit für eine Beratung und Unterstützung zur Verfügung.

Telefon: +49 89 546 49-0
E-Mail: info@drivelock.com

Weitere Informationen zu den Sicherheitslösungen von DriveLock finden Sie hier:

DRIVELOCK.COM

**ÜBERZEUGEN
SIE SICH**

Jetzt unverbindlich
30 Tage gratis testen

