datomo®
MOBILE
DEVICE MANAGEMENT

Mobiler Bedrohungsschutz

(MTD)

Version 19.11.2025 – Aktualisiert 06.01.2026

Übersicht

1 Integration des Mobilen Bedrohungsschutzes (MTD)

Mobile Threat Defense (MTD) ist eine Sicherheitslösung, die entwickelt wurde, um mobile Geräte vor verschiedenen Cyberbedrohungen wie Malware, Phishing, unsicheren Netzwerkverbindungen und risikobehafteten Geräteeinstellungen wie Jailbreaking oder Rooting zu schützen. MTD überwacht kontinuierlich das Geräteverhalten, App-Aktivitäten und den Netzwerkverkehr, um diese Bedrohungen in Echtzeit zu erkennen und zu blockieren – so bleiben sensible Daten auf mobilen Endgeräten stets sicher.

Die Integration von MTD in datomo MDM ermöglicht eine zentralisierte Sicherheitsverwaltung und -durchsetzung. Diese Lösung bietet Administratoren eine vereinfachte Möglichkeit, Bedrohungen zu überwachen und Reaktionen wie automatische Gegenmaßnahmen durchzuführen, die den Nutzerkomfort nicht beeinträchtigen. Die Nutzer profitieren von nahtloser Hintergrundsicherung ohne zusätzliche Interaktion.

Zusammengefasst bieten MTD-Lösungen folgende Vorteile:

- Echtzeit-Erkennung und automatische Abwehr von Bedrohungen auf mobilen Geräten,
- Erhöhte Transparenz und Kontrolle für Administratoren über ein einzelnes Dashboard,
- Schutz vor Malware, Phishing, Netzwerkangriffen sowie riskanten Gerätezuständen,
- Unterstützung bei Compliance-Anforderungen und Verhinderung von Datenverlust,
- Eine reibungslose Nutzererfahrung mit unsichtbar laufender Sicherheit.

Die Integration der **Pradeo Mobile Threat Defense**-Lösung mit der **datomo MDM-Plattform** ist darauf ausgelegt, einen robusten Schutz zu bieten, während gleichzeitig die Verwaltung und Interaktion für Anwender einfach und unkompliziert bleibt. So werden unternehmensweite mobile Umgebungen gesichert, ohne dass Arbeitsabläufe oder die Produktivität der Nutzer beeinträchtigt werden.

Die Integration wird unterstützt auf **Android-Geräten** mit Version 8.0 oder höher sowie auf **iOS- oder iPadOS-Geräten** mit Version 14.0 oder höher.

2 Integration aktivieren

Um die Integration mit der **Pradeo Mobile Threat Defense**-Lösung zu starten, ist ein Lizenzschlüssel erforderlich. Wenden Sie sich hierfür an den Support unter mdm@dotoso.de.

Nach Erhalt des Lizenzschlüssels müssen folgende Netzwerkeinstellungen konfiguriert werden:

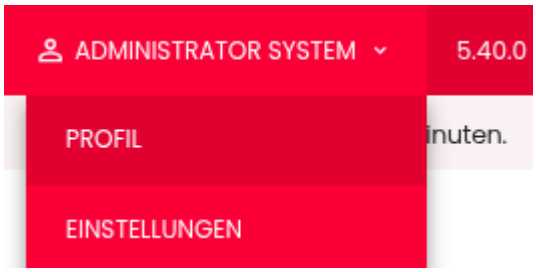
Port 443 muss geöffnet sein, um die Kommunikation mit folgenden Pradeo-Servern zu ermöglichen:

- **Outbound (Egress) IP:** 145.239.45.193
- **Inbound (Ingress) IP:** 162.19.108.112
- **Hostname:** https://m201.pradeo-security.com

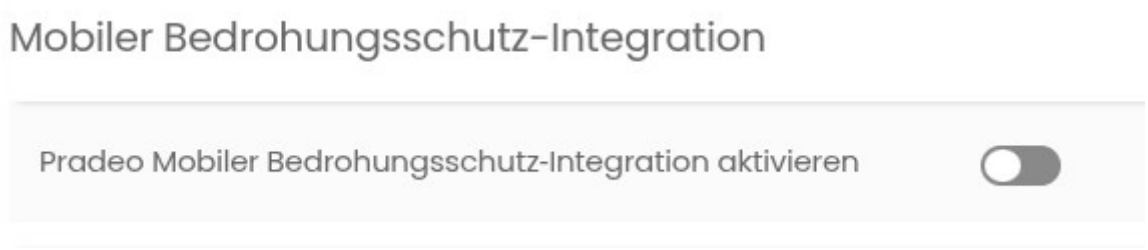
Danach kann der Lizenzschlüssel in den Organisationseinstellungen hinterlegt werden. Der letzte Schritt ist die Aktivierung spezifischer Bedrohungskategorien in der Richtlinie, wodurch die Lizenzierung auf den Geräten freigeschaltet wird. Weitere Details finden Sie unten.

2.1 Lizenzschlüssel eingeben

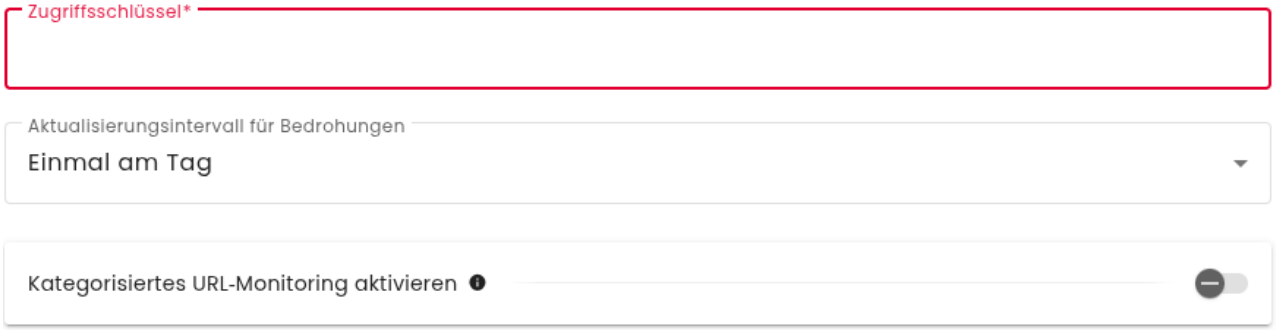
Nach Erhalt des Schlüssels melden Sie sich in **datomo MDM** an und navigieren zu den Organisationseinstellungen über **Benutzer → Einstellungen**.



Aktivieren Sie anschließend die Integration für mobilen Bedrohungsschutz:



Geben Sie im modalen Fenster den Lizenzschlüssel ein. Wählen Sie als Nächstes das Intervall für die Bedrohungsaktualisierung aus, das die Häufigkeit der Bedrohungsscans von Geräten definiert.



Mögliche Intervalloptionen sind

- 5 Minuten,
- 15 Minuten,
- 30 Minuten,
- 1 Stunde,
- 4 Stunden,
- 12 Stunden,
- einmal täglich,
- einmal wöchentlich oder
- einmal monatlich.

Die Auswahl hängt von spezifischen Bedürfnissen und betrieblichen Szenarien ab. Der empfohlene Wert ist einmal täglich.

Auf Android-Geräten wird das Intervall mit hoher Genauigkeit und minimaler Toleranz ausgeführt. Auf Apple-Geräten (iOS/iPadOS) hängt das Verhalten von den Systemressourcen ab, die der Anwendung zugewiesen sind, da eine dauerhafte Hintergrundausführung aus Designgründen nicht unterstützt wird. Nur kurze Hintergrundaufgaben sind erlaubt.

Mehrere interne Mechanismen sind implementiert, um das präziseste Ausführungsintervall zu ermöglichen.

Die letzte Sektion im Modalfenster ist **Kategorisiertes URL-Monitoring**

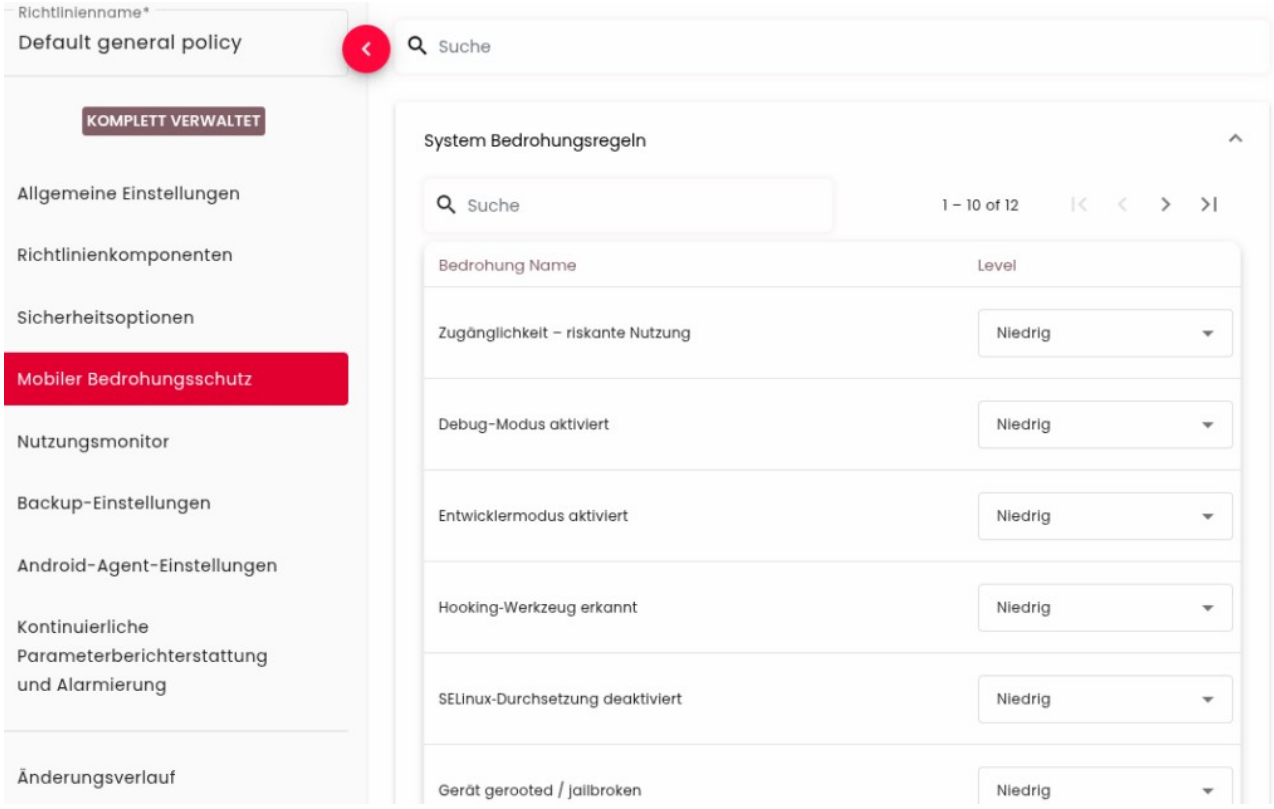
Diese Funktion aktiviert Web-Inhalt-Filterung basierend auf einer Liste riskanter URLs, die von der MTD-Lösung bereitgestellt wird. Im Allgemeinen erhöht sie die Webbrowsing-Sicherheit durch automatische Filterung von Webseiten. Die Funktion ist nur bei Geräten im Betreuten Modus (supervised) unterstützt. Die URL-Liste wird regelmäßig gemäß dem definierten ausgewählten Intervall aktualisiert. Verfügbare Intervalle:

- 1 Tag,
- 2 Tage,
- 3 Tage,
- 7 Tage,
- 14 Tage und
- 30 Tage.

Weitere Infos finden Sie im Abschnitt zu kategorisierten URLs. Speichern Sie anschließend Ihre Einstellungen.

2.1 Lizenz auf den Geräten aktivieren

Nach Konfiguration der Integrations-Einstellungen erfordert die vollständige Integration die Aktivierung des bereitgestellten Zugriffsschlüssels auf den zu schützenden Geräten. Das Eingeben des Schlüssels aktiviert einen neuen Tab im Richtlinienbereich namens **Mobiler Bedrohungsschutz**.



Der Tab enthält folgende Abschnitte:

- System-Bedrohungsregeln
- Netzwerk-Bedrohungsregeln
- Globale Anwendungsbedrohungen
- Bedrohregelliste pro Anwendung
- Schadsoftware- und Virusscan für Anwendungen aktivieren

Weitere Details zu jedem Abschnitt finden Sie in den folgenden Teilen dieses Dokuments. Zunächst schließen wir den Integrationsprozess ab, indem sichergestellt wird, dass der Lizenzschlüssel auf dem Gerät aktiv wird.

Aktivieren Sie dazu mindestens einen der Schalter aus der Richtlinien speichern Sie die Richtlinie. Bei der nächsten Richtlinien-Aktualisierung wird eine Operation namens **Aktivierung der Pradeo**

Lizenz ausgelöst, wodurch der Integrationsprozess abgeschlossen ist, das Gerät in MTD registriert und die Bedrohungserkennung initiiert wird.

3 Mobiler Bedrohungsschutz-Abschnitt in Richtlinien

Im MTD-Tab kann der Benutzer verfügbare Funktionen konfigurieren und beobachtete Bedrohungen definieren. Er enthält auch Details zu Intervalloperationen und den dahinterstehenden Mechanismen. MTD wird über alle Richtlinientypen hinweg unterstützt: Vollständig verwaltet, BYOD/WPC und COSU (dediziertes Gerät / Kiosk-Modus).

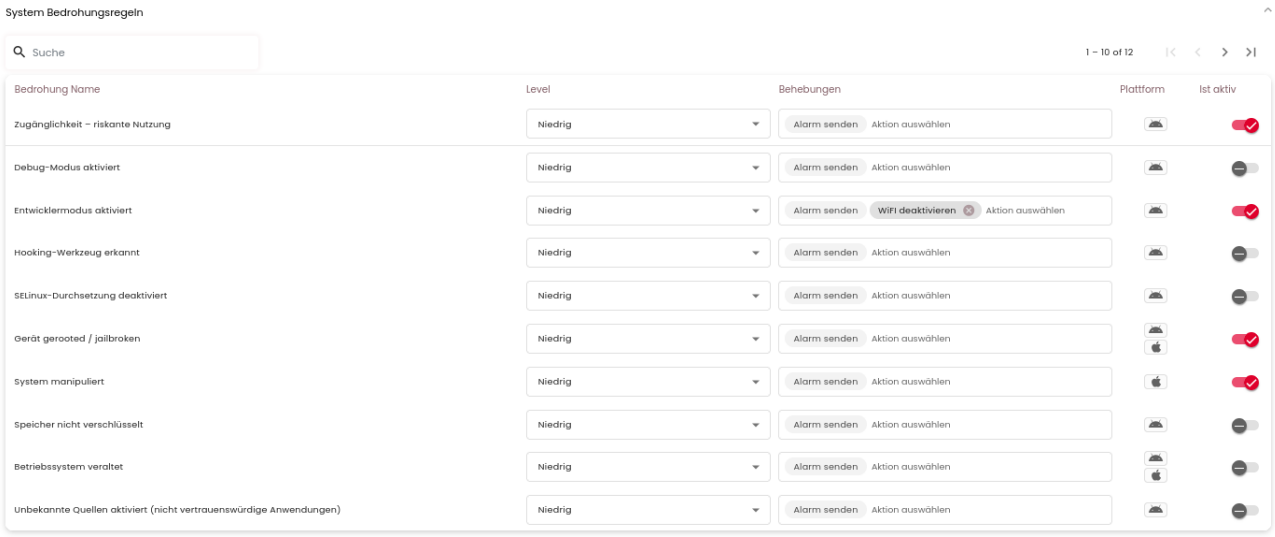
Nicht alle Einstellungen werden auf jeder Plattform unterstützt. Kompatibilitäts-Symbole erscheinen neben dem Abschnittsnamen oder innerhalb von Abschnitten neben spezifischen Schaltern:

Alle Bedrohungen, die auf dem Gerät auftreten können, sind als Regeln definiert, unabhängig davon, welchem Abschnitt sie angehören. Sie werden als Regeln bezeichnet, weil jede Bedrohung mit einer entsprechenden Gegenmaßnahme-Aktion (Behebung) verknüpft ist. Das bedeutet, dass bei Erkennung einer Bedrohung die passende Gegenmaßnahme automatisch auf der mobilen Seite ausgeführt wird, selbst ohne aktive Internetverbindung.

Derzeit werden drei Reaktionen unterstützt: Server-Alarm, Geräte-Benachrichtigung und WLAN-Deaktivierung. Alarm- und Benachrichtigungsmechanismen informieren sowohl den Administrator als auch den Benutzer, während die Option WLAN-Deaktivierung besonders bei Man-in-the-Middle-Angriffen oder Rogue-Access-Point-Bedrohungen nützlich ist. Die Liste verfügbarer Reaktionen wird zukünftig erweitert werden.

3.1 Netzwerk- und Systembedrohungsregeln

Netzwerk- und Systembedrohungen werden auf Geräten gemäß dem Intervall in den Organisationseinstellungen gescannt. Scans erfolgen in Batches, die alle aktivierten Bedrohungen aus der aktiven Richtlinie während jedes geplanten Intervalls abdecken. Bei Erkennung einer Bedrohung werden die entsprechenden Behebungen automatisch ausgelöst, basierend auf der Richtlinieneinstellung und ausgewählten Behebungsstypen. Mehrere Reaktionen können gleichzeitig angewendet werden.



Da Bedrohungstypen unten beschrieben sind und Behebungen bereits definiert wurden, sollte die Spalte Level ebenfalls erwähnt werden. Diese Spalte dient als Informationsindikator für Administratoren und Benutzer. Sie beeinflusst Nachrichten, die während der Berichterstellung an den Server gesendet werden, sowie die Anzeige in Geräteagenten. Im iOS-Agent werden drei Orange- und Rottöne verwendet, um unterschiedliche Bedrohungslevels zu repräsentieren.

Daneben zeigt das Plattformkompatibilitäts-Symbol an, welche Plattform diese Art der Bedrohungserkennung unterstützt. Rechts befindet sich ein Schalter, mit dem die Erkennung von Bedrohungen auf dem Gerät aktiviert oder deaktiviert werden kann.

3.1.1 Status und Mechanismus

Bedrohungen und Behebungen haben explizite Statuswerte, um Erkennungs-, Ausführungs- und Verifizierungsphasen zu reflektieren. Bei Erkennung einer Bedrohung wird der Status auf *Behebung gestartet* gesetzt; nach erfolgreichem Abschluss aller konfigurierten Gegenmaßnahmen ändert sich der Status zu *Behebungen erfolgreich ausgeführt*. Dies impliziert nicht, dass die Bedrohung entfernt wurde – ein zusätzlicher Verifizierungsschritt prüft, ob die Bedrohung noch vorhanden ist. Wenn sie behoben ist, wird der Status auf *Erfolgreich* aktualisiert, andernfalls bleibt er *Behebungen erfolgreich ausgeführt*.

Falls eine Gegenmaßnahme fehlschlägt und die Bedrohung weiterhin besteht, wird der Gesamtszustand der Bedrohung auf *Fehlgeschlagen* gesetzt. Jede Behebung hat drei mögliche Status: *In Ausführung* (Ausführung läuft nach Erkennung), *Erfolgreich* (erfolgreich ausgeführt) oder *Fehlgeschlagen* (nicht erfolgreich abgeschlossen). Wenn ein bestimmter Bedrohungstyp, z. B. veraltetes OS, gelöst ist, wird der Status automatisch aktualisiert und retrospektiv bei bestehenden Operationen dieses Typs geändert.

Status von erkannten Bedrohungen sind in den Geräteeinstellungen auf dem Logs-Tab sowie im Benachrichtigungs-Tab verfügbar, die alle vom mobilen Gerät generierten Alarme bündeln. Eine dedizierte Tabelle mit erkannten Bedrohungen wurde ebenfalls zur Gerätestatus-Ansicht hinzugefügt und ist unter Geräte → Liste → (Gerät auswählen) → Gerätestatus → MTD-Chart „Mobiler Bedrohungsschutz“ zu finden.

3.1.2 Netzwerk- & Systembedrohungstabelle

Fast alle aktuellen Netzwerk- und Systembedrohungs-Erkennungsfunktionen von Pradeo wurden implementiert; zusätzliche Features werden in zukünftigen Versionen ergänzt. Die aktuelle Liste wird unten dargestellt.

Parameter	Beschreibung	Kompatibilität
ARP-Poisoning	Das Gerät ist einem ARP-Poisoning-Angriff ausgesetzt, was bedeutet, dass sein Netzwerkverkehr ohne Wissen abgefangen oder umgeleitet werden kann. Dies birgt das Risiko von Datenabfluss oder Manipulation.	Android
Bluetooth aktiviert	Eine Bluetooth-Verbindung ist aktiv und könnte das Gerät für unbefugten Zugriff oder Datenaustausch mit einem nahegelegenen Gerät öffnen. Dies kann zu Informationsabfluss über den Bluetooth-Kanal führen.	Android
Mit offenem WLAN verbinden	Das Gerät ist mit einem unsicheren (offenen) WLAN-Netzwerk verbunden, was das Risiko von Netzwerk-Level-Angriffen wie Abfangen oder Spoofing erhöht. Die Verwendung solcher Netzwerke kann Schutzmaßnahmen umgehen.	Android
Hosts-Datei geändert	Die System-Hosts-Datei wurde modifiziert, was anzeigen könnte, dass der Netzwerkverkehr zu unautorisierten Servern umgeleitet wird oder	Android

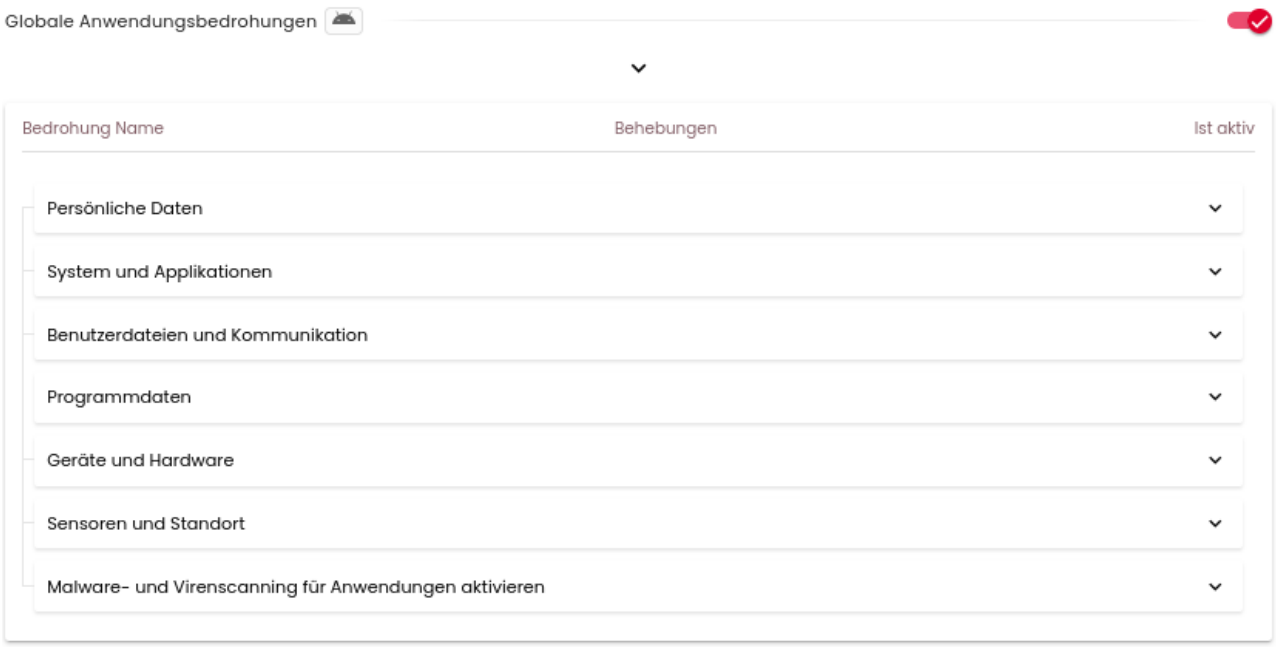
Parameter	Beschreibung	Kompatibilität
	schädliche Konfigurationsänderungen existieren. Dies gefährdet die Integrität der Kommunikation.	
Man-in-the-Middle-Angriff	Das Gerät ist einem MITM-Angriff ausgesetzt, bei dem ein Angreifer Kommunikationskanäle zwischen Gerät und Remote-Server abfängt oder verändert. Dies gefährdet Datenvertraulichkeit und -integrität.	Android, iOS
NFC aktiviert	Die Near-Field-Communication (NFC)-Funktion ist aktiv und könnte das Gerät lokalen Angriffen aussetzen, wie Datenerfassung, Tag-Manipulation oder unbefugter Bereitstellung. Dies gefährdet Daten über NFC.	Android
Betrügerischer WLAN-Zugangspunkt	Das Gerät ist mit einem Wi-Fi-Access-Point verbunden oder erkennt einen, der möglicherweise bösartig ist (Rogue-AP). Solche Access-Points können Netzwerkverkehr abfangen oder manipulieren.	Android, iOS
Betrügerischer Mobilfunkturm	Das Gerät ist einem gefälschten oder Rogue-Mobilfunkmasten ausgesetzt, die Sprach-, SMS- oder Datenverkehr abfangen kann, indem dieser sich als legitimer Mobilfunkmast tarnt. Dies gefährdet Kommunikationsvertraulichkeit.	Android, iOS
Tracking aktiviert (Standort, Telemetrie)	Das Gerät hat Tracking-Funktionen wie Standortdienste aktiviert, was zu übermäßiger Überwachung oder Datensammlung führen kann und die Privatsphäre beeinträchtigt.	Android, iOS
VPN aktiv	Ein Virtual Private Network (VPN) ist auf dem Gerät aktiv, das Netzwerkverkehr maskieren kann, aber auch Interferenzen mit Unternehmens-Monitoring oder Kommunikationskontrolle verursachen kann. Administratoren müssen die Richtlinienkonformität prüfen.	Android, iOS
Zugänglichkeit - Riskante Nutzung	Accessibility-Dienste werden verwendet, sodass Apps Bildschirminhalt oder Daten anderer Apps erfassen können. Dies kann von böswilligen Apps für Datenspionage oder Übernahme genutzt werden.	Android
Debug-Modus aktiv	Das Gerät läuft im Debug-Modus, der erhöhte Zugriffsrechte bietet und es böswilligen Akteuren ermöglicht, das System zu manipulieren oder unberechtigten Zugriff auf Daten zu erlangen. Dies schwächt die Gerätesicherheit.	Android
Entwicklermodus	Der Entwickler-Modus ist aktiviert, wodurch	Android

Parameter	Beschreibung	Kompatibilität
aktiviert	fortgeschrittene Einstellungen und Änderungen zugelassen werden, die Standard-Schutzmaßnahmen umgehen können. Dies kann die Installation riskanter Apps oder Systemänderungen ermöglichen.	
Hooking-Werkzeuge erkannt	Ein Hooking-Framework (z. B. für App-Instrumentierung oder Interception) wurde entdeckt, was anzeigt, dass Apps oder Systemfunktionen auf nicht standardmäßige Weise manipuliert werden können. Dies gefährdet Anwendungs- und Systemintegrität.	Android
SELinux Durchsetzung deaktiviert	Der SELinux-Enforcement-Modus ist deaktiviert oder permissiv, wodurch die Stärke der Sicherheitsrichtlinie des Systems reduziert wird und böswillige Änderungen wahrscheinlicher erfolgreich sind.	Android
Rooted / Jailbroken Gerät	Das Gerät wurde gerootet (Android) oder jailbroken (iOS). Systemschutzmaßnahmen wurden umgangen, was das Risiko von Malware, Datenexfiltration und Kontrollverlust erheblich erhöht.	Android, iOS
System manipuliert	Die Betriebssystemintegrität auf dem Gerät wurde manipuliert (iOS-Variante), was auf unautorisierte Änderungen oder einen kompromittierten Zustand hinweist. Dies kann das Vertrauen in die Gerätes Umgebung beeinträchtigen.	iOS
Speicher nicht verschlüsselt	Der Datenspeicher des Geräts ist nicht verschlüsselt, wodurch gespeicherte Daten leicht zugänglich sind, wenn das Gerät verloren geht oder kompromittiert wird. Dies erhöht das Risiko eines Datenverlusts.	Android
OS veraltet	Das Betriebssystem des Geräts ist veraltet und enthält kritische Sicherheitslücken. Dadurch bleibt es anfällig für bekannte Exploits. Dies reduziert die allgemeine Sicherheitslage des Geräts.	Android, iOS
Ujnbekannte Quellen aktiviert (nicht vertrauenswürdige Anwendungen)	Das Gerät erlaubt die Installation von Anwendungen aus unbekannten oder nicht vertrauenswürdigen Quellen (nur Android). Dadurch steigt das Risiko der Installation von Malware oder unsicheren Apps. Administratoren sollten dies einschränken.	Android
Bildschirmspiegelung	Die Screen-Mirroring-Funktion ist aktiv (iOS), was	iOS

Parameter	Beschreibung	Kompatibilität
aktiv	bedeutet, dass die Anzeige des Geräts extern geteilt wird und damit visuelle sensible Informationen unbeabsichtigt an unbefugte Zuschauer weitergegeben werden können.	
Läuft in Simulator	Das App oder Gerät läuft innerhalb eines Simulators (iOS). Dies kann auf Test- oder Reverse-Engineering-Bedingungen hinweisen und das Vertrauen in die Gerätes Umgebung verringern.	iOS

4 Globale Anwendungsregeln

Nach Aktivierung globaler Anwendungbedrohungen analysiert Pradeo die Binärdateien von auf dem Gerät installierten Anwendungen. Vorinstallierte Apps sind davon ausgeschlossen. Der Abschnitt wird wie unten dargestellt veranschaulicht.



Für jeden Bedrohungstyp sind drei Modi definiert, die die Nutzung sensibler Daten durch Anwendungen beschreiben:

- **At Rest** (Lesezugriff)
- **In Use** (Änderungszugriff)
- **In Transit** (Datenübertragung an Dritte).

Jeder Modus kann unabhängig aktiviert und überwacht werden.

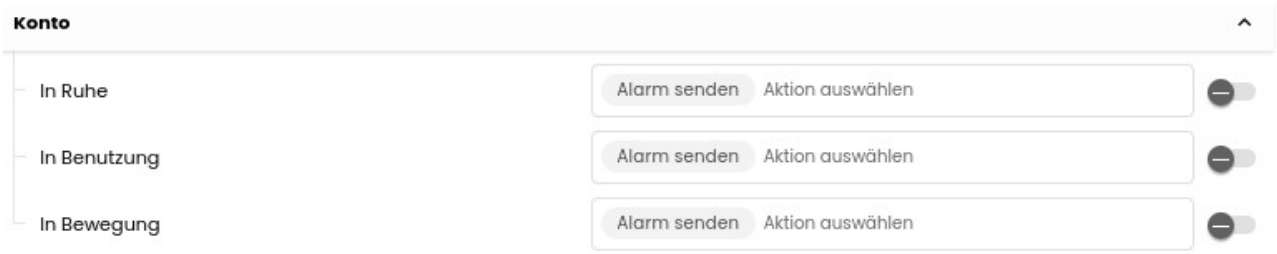
Bei Erkennung einer Bedrohung wird der Status auf *Behebung gestartet* gesetzt. Bei erfolgreichem Abschluss aller konfigurierten Behebungen ändert sich der Status zu *Behebungen erfolgreich ausgeführt*. Dieser Prozess ist konsistent mit dem Handling von System- und

Netzwerkregeln. Zusätzlich wird der Administrator über die spezifische Anwendung informiert (identifiziert durch Paketname), welche die Erkennung ausgelöst hat.

Derzeit unterliegen Anwendungsbedrohungen keinem Verifizierungsschritt. *Behebungen erfolgreich ausgeführt* ist also der Endstatus.

Um Berichtsanfragen von Anwedungen zu optimieren, passt ein Mechanismus dynamisch das Berichts-Intervall an, beginnend mit dem konfigurierten Bedrohungsaktualisierungs-Intervall. Aufgrund der Anzahl von Anwendungen und serverseitigen Scans wird dieses Intervall effizient geplant und kann je nach Berichtverfügbarkeit verlängert werden.

Implementierte Anwendungsbedrohungen repräsentieren Fälle, in denen eine Anwendung spezifische Einträge, Daten oder Informationen nutzt. Beispiel: Erkennung einer Bedrohung basierend auf dem Parameter **Konto** bedeutet, dass die Anwendung ein lokales Android-Konto verwendet, was unter bestimmten Szenarien Risiken birgt.



Die Liste implementierter Anwendungsbedrohungen ist als benutzerfreundliche Baumstruktur organisiert (siehe Bild unten).

Diese hierarchische Struktur erweitert sich zu einer detaillierten Liste von Anwendungsbedrohungen und wird in diesem Abschnitt weiter beschrieben.

4.1 Anwendungsbedrohungstabelle

Alle aktivierten Anwendungbedrohungen in Richtlinien werden an den Server gemeldet, und Behebungen werden entsprechend ausgeführt. Die initiale Version von datomo MDM mit Pradeo-Integration unterstützt jedoch keine automatische Entfernung von Anwendungen über Behebungen; dies muss manuell über die Geräteeinstellungen erfolgen. Zukünftige Versionen werden automatische Behebungen zum Deinstallieren gefährlicher Apps enthalten.

Die untenstehende Liste stellt alle derzeit implementierten Anwendungbedrohungen dar.

Parameter	Beschreibung	Kompatibilität
Benutzersprache	Die App liest oder verwendet die vom Gerät konfigurierte Sprache. Dies kann für Lokalisierung genutzt werden, aber auch zum Fingerprinting der Benutzerregion oder -präferenzen.	Android

Parameter	Beschreibung	Kompatibilität
Benutzername	Die App greift auf den Benutzernamen des Gerätes zu. Dies kann einen persönlichen Identifikator offenbaren, der für Profiling oder Verknüpfung mit einer realen Person verwendet werden kann.	Android
Gerätehersteller	Die App liest die Herstellerinformation des Geräts. Diese hilft, Gerätemodelle zu identifizieren und kann auch zur Finger-Prägnanz von Geräten eingesetzt werden.	Android
Gerätedaten	Die App sammelt Details wie Modell, Anzeige, Produkt, Hardware, Seriennummer. Solche Daten können das Gerät eindeutig identifizieren und unterstützen gezielte Angriffe oder Tracking.	Android
Sensor	Die App liest Sensordaten (z. B. Beschleunigungssensor, Gyroskop). Sensorzugriff kann Funktionen der App unterstützen, aber auch die Aktivität oder Umgebung des Benutzers ermitteln.	Android
Geolokalisation	Die App greift auf präzise oder ungefähre GPS/Standortdaten zu. Standortzugriff offenbart Bewegungen und birgt Privatsphären- oder Sicherheitsrisiken, falls ohne Zustimmung geteilt.	Android
Netzwerkinformation	Die App sammelt Informationen zum aktuell verbundenen Netzwerk. Netzwerkinfos können für Verbindungs-Handling verwendet werden, aber auch zur Erkennung unsicherer Netzwerke oder Fingerprinting.	Android
Betriebssystem	Die App liest die OS-Version oder den Namen. Das Wissen um die OS-Version kann hilfreich sein, es legt aber auch Geräte mit bekannten Schwachstellen offen.	Android
Mobilfunknetzbetreiber	Die App liest die GSM-Operator-Kennung. Dies enthüllt den Mobilfunkanbieter und kann für Profiling verwendet werden.	Android
Internetdienstleister	Die App liest die ISP/Netzwerkbetreiberkennung. Nutzbar für Profiling oder Routing.	Android
Kamera	Die App greift auf die Kamera oder Kameradaten zu. Kamerazugriff kann legitim sein, birgt jedoch Risiko sensibler visueller Daten bei Missbrauch.	Android

Parameter	Beschreibung	Kompatibilität
Kontakt	Die App greift auf Kontaktdaten (Namen, Telefonnummern, Thumbnails) zu. Kontaktzugriff offenbart persönliche Verbindungen und birgt hohes Datenschutz-Risiko bei Übertragung.	Android
Anschrift	Die App liest gespeicherte zivile/Adresse-Informationen von Gerät. Das enthüllt genaue persönliche Adressen – sensibler persönlicher Daten.	Android
Lokales Konto	Die App nutzt ein lokales Android-Konto. Dies zeigt, dass die App Kontoinformationen lesen kann und möglicherweise Appdaten mit diesem Konto verknüpfen kann.	Android
Anwendungen im Vordergrund	Die App erkennt, welche Anwendung gerade im Vordergrund ist. Das kann zur Ableitung von Benutzeraktivität oder Verhalten je nach sichtbarer App genutzt werden.	Android
Laufende Applikationen	Die App listet aktuell laufende Apps oder Dienste auf. Das Auflisten ermöglicht Fingerprinting, Kompatibilitätschecks oder Schwachstellenfindung.	Android
Installierte Anwendungen	Die App listet installierte Anwendungen auf dem Gerät auf. Dies ist nützlich für Kompatibilität, kann aber Interessen und Sicherheitswerkzeuge des Benutzers offenbaren.	Android
IMEI	Die App liest die IMEI des Gerätes. IMEI ist ein persistenter Hardware-Identifier und kann zum Tracken oder eindeutigen Identifizieren des Geräts verwendet werden.	Android
IP-Adresse	Die App erfasst die aktuelle IP-Adresse des Gerätes. IPs zeigen Netzwerkposition und können für Geolokalisierung oder netzwerkbasierte Profiling genutzt werden.	Android
MAC-Adresse	Die App liest die MAC-Adresse des Geräts. MAC ist ein Hardware-Netzwerk-Identifikator, der bei Offenlegung zu persistenter Geräteverfolgung führen kann.	Android
Screenshot	Die App greift auf Daten eines Screenshots des aktuellen Bildschirms zu. Screenshots können sensible UI-Inhalte enthalten und sollten als hochsensibel behandelt werden.	Android

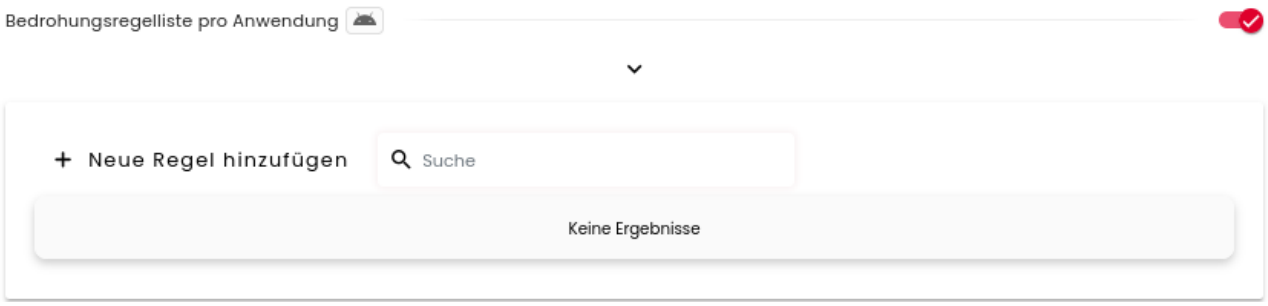
Parameter	Beschreibung	Kompatibilität
SIM-Telefonnummer	Die App liest die Telefonnummer der SIM-Karte. Telefonzugriff verbindet das Gerät mit einer kontaktierbaren Identität, verursacht Datenschutzprobleme.	Android
Nachrichteninhalt	Die App liest Nachrichteninhalte von SMS/MMS (Inhalt, Telefonnummer,...). Nachrichtenzugriff offenbart private Kommunikation und ist hochsensibel.	Android
Laufzeit-Information	Die App greift auf aktuelle Prozess-Infos zu (pid, tid, uid). Laufzeit-Infos können für Debugging, Ausnutzung oder zur Erkennung von Sandbox/Analyse-Umgebungen verwendet werden.	Android
Kalender	Die App liest Kalenderdaten (Ereignisse, Teilnehmer). Kalenderzugriff enthüllt Zeitpläne und Kontakte, kann persönliche oder geschäftliche Informationen offenbaren.	Android
Persönliche Dateien	Die App liest oder manipuliert Benutzerdaten (Home, Download, SD). Zugriff auf persönliche Dateien kann Dokumente, Fotos oder andere sensible Daten preisgeben.	Android
Inoffizielle Anwendungen	Die App erkennt das Vorhandensein von inoffiziellen oder nicht vertrauenswürdigen Apps. Diese Erkennung bestimmt, ob eine Anwendung aus einem offiziellen Store (z. B. Google Play) installiert wurde oder auf dem Gerät "sideloaded" ist. Dies kann ein riskantes Umfeld anzeigen, wo ungeprüfte Apps die Angriffsfläche erhöhen.	Android
Anrufprotokolle	Die App liest oder ändert Anrufprotokolle. Anrufprotokoll-Zugriff offenbart Kommunikationsmuster und Kontaktdaten – Datenschutzsensibel.	Android
Hardware-Informationen	Die App liest oder verändert Telefon-Hardware-Infos. Zugriff auf Hardware-Info kann Gerätee-Fingerprinting oder Manipulation von Hardwarefunktionen ermöglichen.	Android
Anwendungsdaten	Die App greift auf Dateien oder Daten zu, die von der Anwendung selbst gehandhabt werden (Dateien, Shared Prefences...). Diese beschreiben lokale Datenverarbeitung und eventuelle sensible Inhalte, die gespeichert sind.	Android

Parameter	Beschreibung	Kompatibilität
Anwendungs-nachrichten	Die App liest oder behandelt Nachrichten, die von der eigenen Anwendung verwaltet werden. Dies kann In-App-Kommunikationen beinhalten, die private Inhalte enthalten können.	Android
Anwendungs-ressourcen	Die App untersucht Daten im Ressourcenordner (Strings, Assets). Resource-Info kann eingebettete Konfigurationen, Schlüssel oder sensible Texte offenbaren.	Android
Anwendungsdatei-Inhalt	Die App liest in der lokalen Speicherung gespeicherte Dateien. Lokale Dateiinhalte können gecachte Zugangsdaten, Tokens oder persönliche Daten enthalten, die geschützt werden müssen.	Android

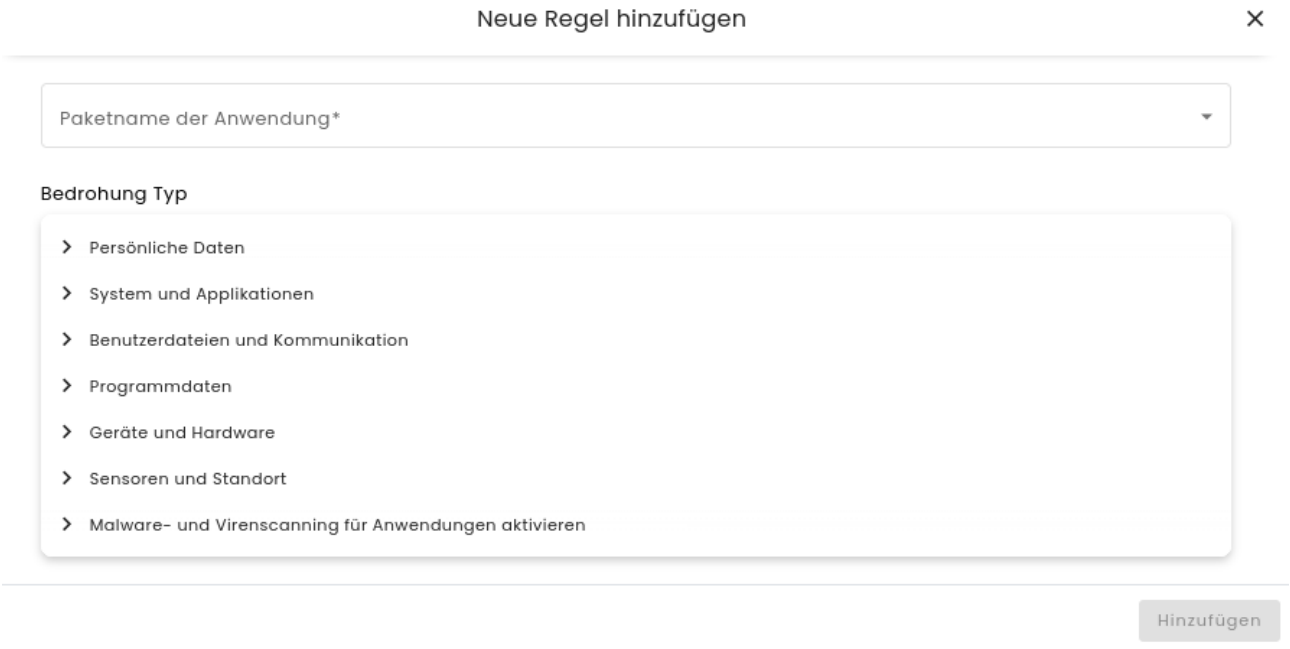
5 Bedrohungsliste pro Anwendung

Der pro-Anwendungsbereich erlaubt das Erstellen einer Regel für einen bestimmten Paketnamen kombiniert mit einer Anwendungbedrohung aus der globalen Liste. So kann eine globale Einstellung für dieses spezifische Paket überschrieben werden. Diese Funktion ist ausschließlich auf Android verfügbar, ähnlich wie die globalen Anwendungsregeln.

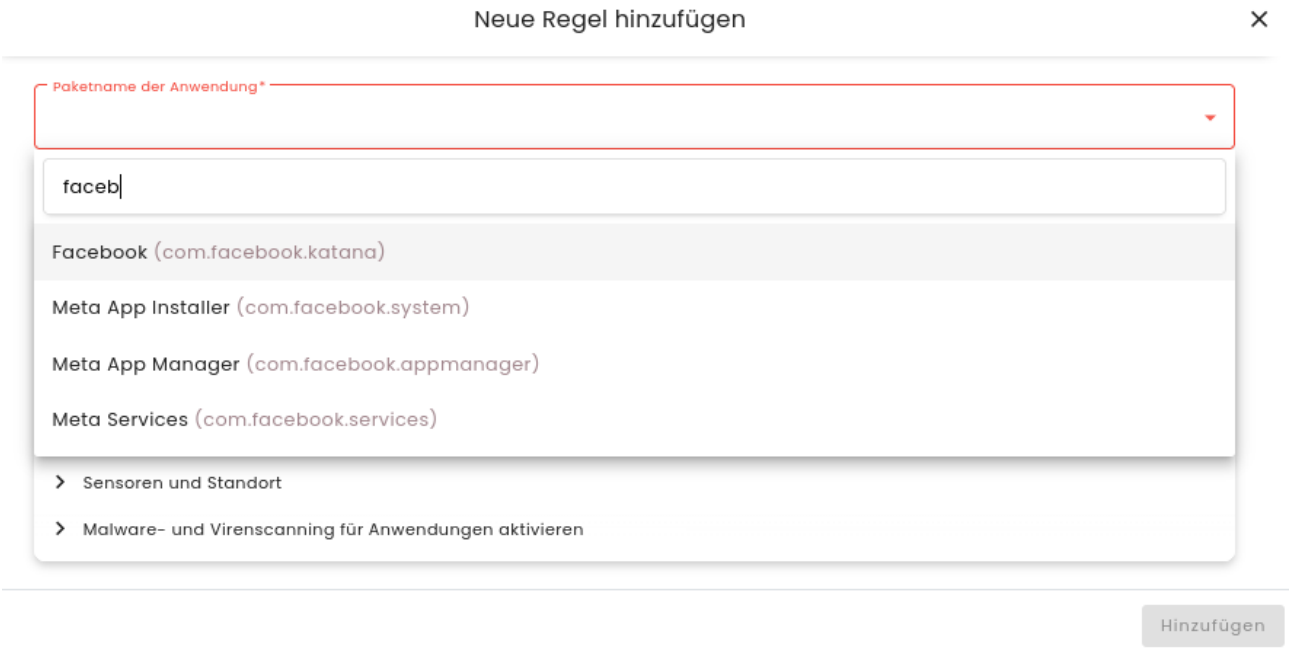
Um neue Regeln hinzuzufügen, muss der Schalter des Abschnitts aktiviert sein. Danach klicken Sie auf **Neue Regel hinzufügen**.



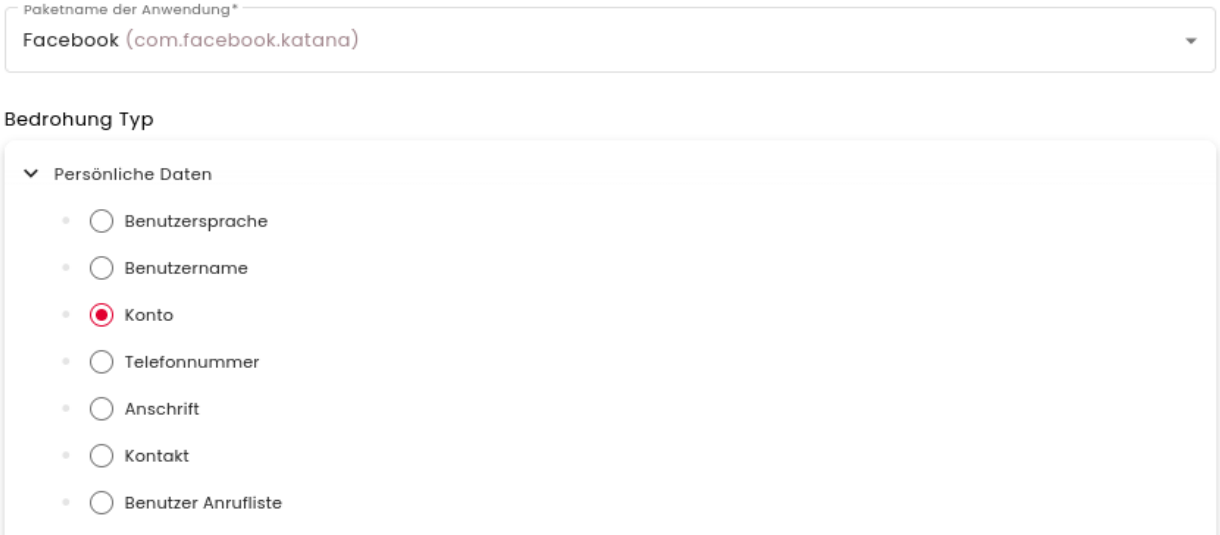
Es erscheint dann eine Ansicht mit zwei Abschnitten: **Paketname der Anwendung** und **Bedrohung Typ**.



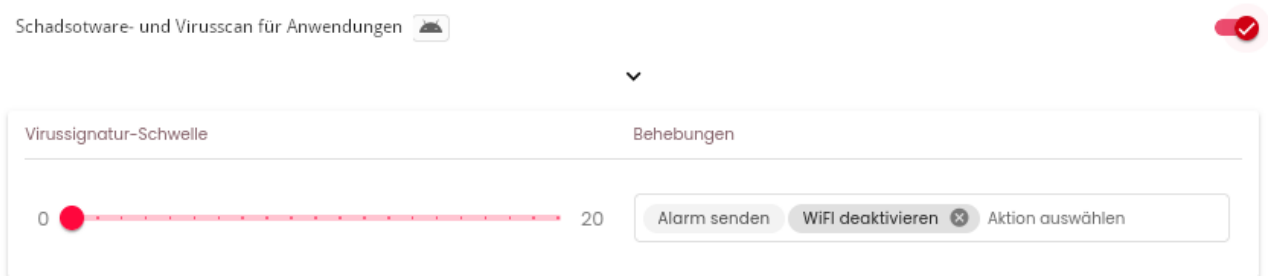
Zuerst geben Sie den Paketnamen der Anwendung ein, für welche die Regel erstellt werden soll. Die Suchfunktion erleichtert das Auffinden des gewünschten Pakets.



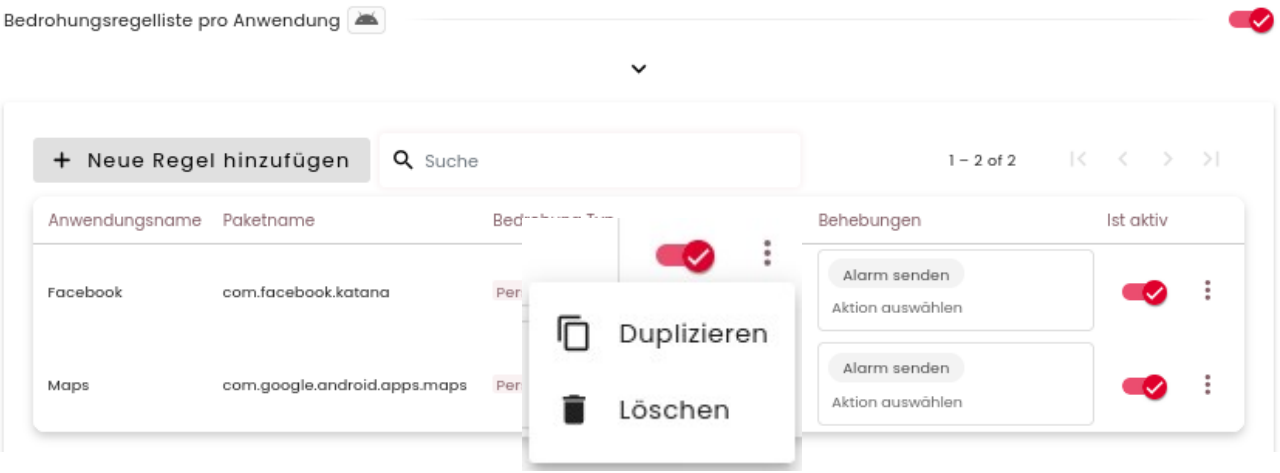
Die gleiche hierarchische Baumstruktur von Anwendungsbedrohungen wie in den globalen Anwendungsregeln ist auch in diesem Abschnitt verfügbar und erleichtert ein konsistentes Bedrohungsmanagement. Aus dem Kategorienbaum wählen Sie einen Bedrohungstyp aus, um ihn in dieser Anwendungsregel zu konfigurieren.



Nach Auswahl einer Anwendungsbedrohung aus dem Baum werden alle drei Datennutzungstypen (At Rest, In Use, In Transit) automatisch gemeldet, sobald die Regel erstellt und aktiviert ist. Klicken Sie dann unten auf **Hinzufügen**.



Wenn zwei Regeln hinzugefügt wurden, wird die Liste der pro-Anwendung-Regeln angezeigt, wie unten gezeigt.



Sie können sofort Gegenmaßnahmen festlegen sowie Regeln hinzufügen, duplizieren oder löschen über das 3-Punkte Symbol:

Hinweis: Diese Einstellung überschreibt die globalen Anwendungsregeln für die angegebene Applikation.

6 Schadsoftware- und Virusscan für Anwendungen

Dieser Abschnitt bietet die Möglichkeit, installierte Anwendungen (ausgenommen vorinstallierte Apps) zu scannen. Die Funktion kann über einen Schalter aktiviert werden. Sobald sie aktiv ist, werden alle installierten Anwendungen automatisch gescannt und an die Administratorkonsole gemeldet, da die **Alarm-Senden** Gegenmaßnahme-Einstellung verwendet wird. Abhängig von den ausgewählten Gegenmaßnahmen können weitere Aktionen ausgelöst werden.

Es gibt zwei Konfigurationsfelder:

- **Gegenmaßnahmen**, welche die Aktion definiert, die bei Viruserkennung ausgeführt werden soll, und
- **Virussignatur-Schwelle**, welche angibt, wie viele aufeinanderfolgende Virus-Erkennungen erforderlich sind, bevor eine Anwendung gemeldet wird.

Zum Beispiel bedeutet ein Schwellenwert von 5, dass die App nach fünfmaliger Malware-/Virus-Kennzeichnung in Folge gemeldet wird. Scans werden auf Pradeo-Servern ausgeführt, die proprietäre Datenbanken, Algorithmen und weitere Mechanismen zur Erkennung nutzen.

Der gleiche Mechanismus wie im Anwendungsbedrohungsmodul wird hier verwendet, um Anwendungsbericht-Anfragen zu optimieren. Das Bericht-Intervall passt sich dynamisch an, beginnend mit dem konfigurierten Bedrohungserneurungs-Intervall. Aufgrund der Anzahl gescannter Anwendungen und serverseitiger Verarbeitung wird dieses Intervall effizient geplant und kann je nach Berichtverfügbarkeit verlängert werden.

Diese Funktion ist ausschließlich für Android-Geräte verfügbar.

7 Kategorisierte URL-Überwachung

Kategorisiertes URL-Monitoring lässt sich in den Organisationseinstellungen (Abschnitt 2) aktivieren und ist nur bei Betreuten (supervised) iOS- und iPadOS-Geräten verfügbar.

Diese Funktion aktiviert das Web-Content-Filtering-Feature. Dieses Feature fängt Browserverkehr auf Systemebene ab und entscheidet, welche URLs erlaubt oder blockiert werden sollen. Apple hat diesen Mechanismus entwickelt, um maximale Privatsphäre und Sicherheit zu gewährleisten – weder Pradeo noch datomo MDM können den Netzwerkverkehr sehen, jedoch kann der Zugriff auf von Pradeo als riskant identifizierte URLs (z. B. Phishing-Sites) verweigert werden.

Die Funktion arbeitet automatisch, es ist keine zusätzliche Konfiguration ist erforderlich. Um zu verifizieren, dass der Web-Content-Filter aktiv ist, gehen Sie auf dem Gerät auf **Einstellungen**, dann **Allgemein → VPN und Geräteverwaltung Management**. Die Filter-Statusbestätigung wird dort sichtbar sein.

8 Administrationskonsole

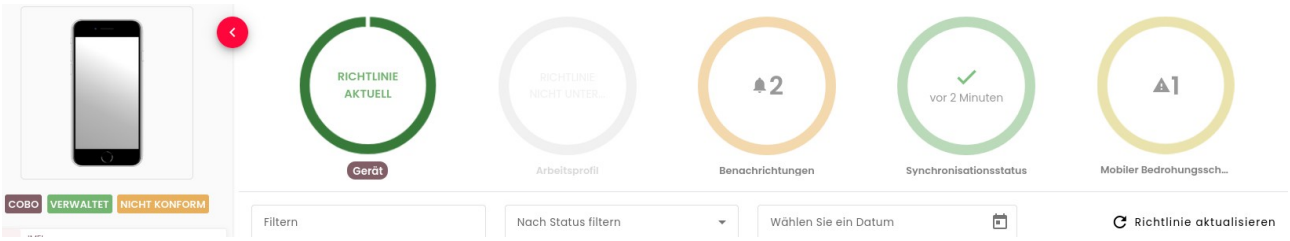
Administratoren können den Status erkannter Bedrohungen auf Geräten an drei Orten prüfen:

- im Gerätestatus unter dem Mobilen Bedrohungsschutz-Chart,
- im Benachrichtigungs-Tab und
- in der Log-Liste in den Geräteeinstellungen.

8.1 Mobiler Bedrohungsschutz-Tab

Der erste Abschnitt, der sich ausschließlich auf die auf dem Gerät erkannten Bedrohungen bezieht, ist ein neuer Bestandteil der Konsole unter **Gerätedetails**.

Wählen Sie den **Gerätestatus- Tab** links und klicken den letzten Chart oben mit Titel **Mobiler Bedrohungsschutz**.



Das Diagramm zeigt eine Verteilung erkannter Bedrohungstypen und bietet einen schnellen Überblick:

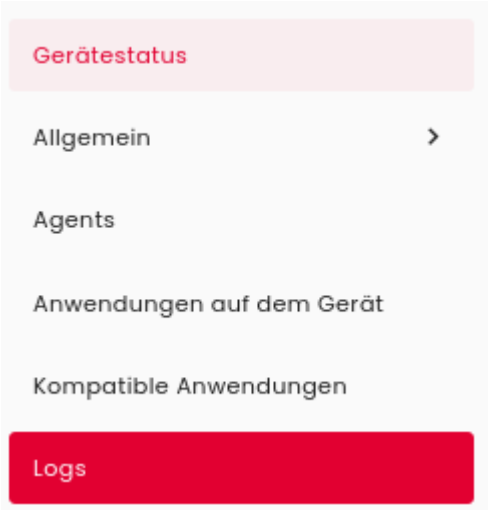
Die Zahl vor jedem Bedrohungstyp gibt die genaue Anzahl erkannter Bedrohungen für diese Kategorie an. Die Zahl im Kreis neben dem Dreieck repräsentiert die Gesamtzahl aller erkannten Bedrohungen.

Unterhalb des Diagramms listet eine Tabelle alle auf dem Gerät erkannten Bedrohungen auf. Diese Tabelle enthält folgende Spalten:

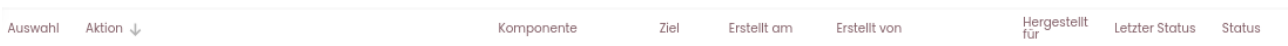
- Bedrohungsname
- Berichtet am – Zeit, wann das Problem erkannt wurde
- Behebung – Alle zugewiesenen Korrekturmaßnahmen
- Bedrohungsstatus – Aktueller Status (wie in Abschnitt 3 beschrieben).

8.2 Log-Tab

Jede auf dem Gerät erkannte Bedrohung wird zusätzlich zum Mobilen Bedrohungsschutz-Bereich als Operation protokolliert.



Das Tabellenlayout hängt von den ausgewählten Spalten ab, aber die wichtigsten Details befinden sich in der **Aktion**-Spalte, welche angibt, ob es sich um eine erkannten Bedrohung oder eine zugehörige Behebung handelt.



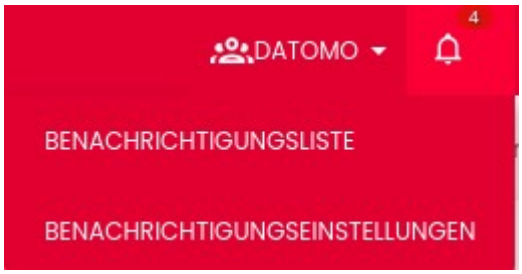
Die **Komponent**-Spalte liefert Informationen über den Bedrohungstyp und die Status entsprechen denen im Mobilen Bedrohungsschutz-Tab. Das letzte nützliche Detail ist die vom Gerät generierte Nachricht gemäß Schema: „Bedrohung gefunden in Applikation: [Bedrohungsname] mit [Level aus Level-Feld].“

Innerhalb der Operations-Ansicht können sowohl Behebungs-Status als auch einzelne Bedrohungsstatus überprüft werden.

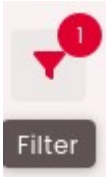
8.3 Benachrichtigungs-Tab

Der letzte Abschnitt zeigt erkannte und an den Server gemeldete Bedrohungen, die über die persistente Behebungsaktion **Alarm senden** gesendet wurden. Wenn ein Gerät Alarme an den Server sendet, werden alle im Benachrichtigungs-Tab angezeigt.

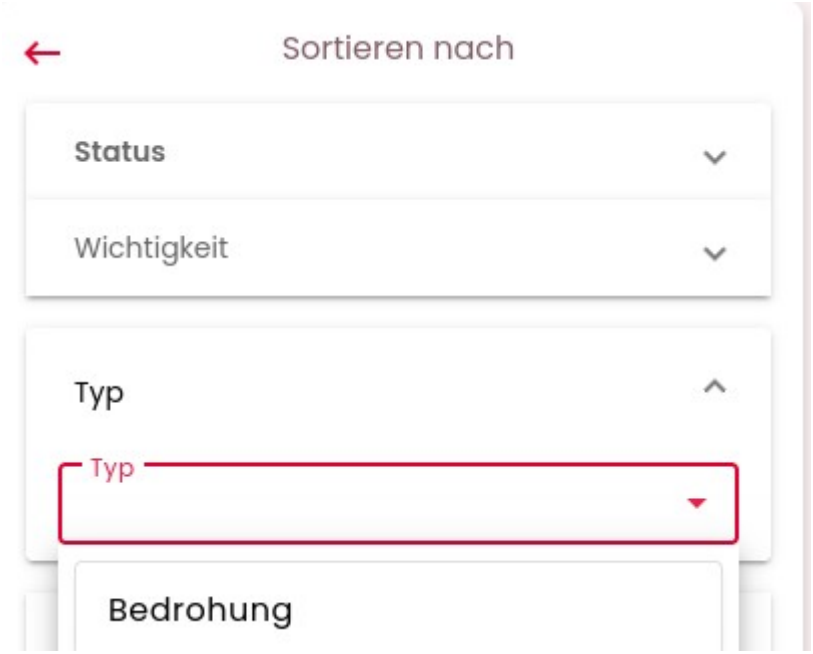
Um zum Benachrichtigungs-Tab zu gelangen, klicken Sie auf das Glocken-Szmbol oben im Hauptmenü und wählen **Benachrichtigungsliste**.

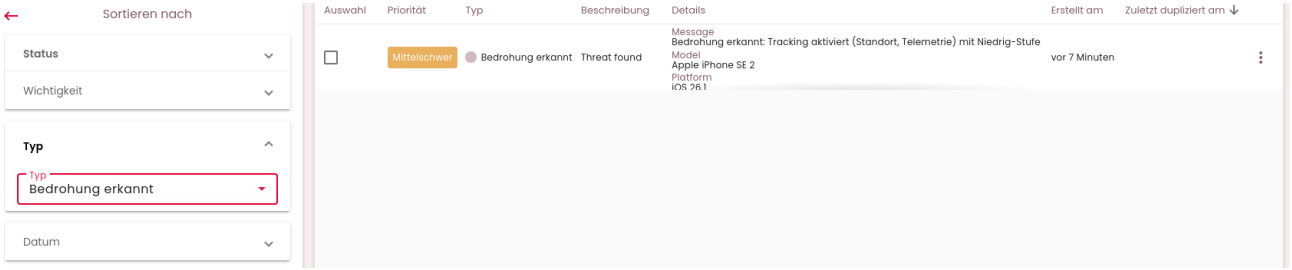


Der Benachrichtigungs-Tab öffnet sich und zeigt sämtliche vorhandenen Alarme an. Um nur solche im Zusammenhang mit erkannten Bedrohungen anzuzeigen, klicken Sie das Filter-Symbol.



Im der am linken Bildrand angezeigten Filter-Liste wählen Sie **Typ** und dann **Bedrohung erkannt**.





Eine Liste aller erkannten Bedrohungen auf allen Geräten wird angezeigt. In dieser Ansicht können Sie Alarme filtern und gruppieren. Alarme können als gelesen markiert werden, sodass sie nicht mehr im ungelesenen Zähler erscheinen. Nutzen Sie dafür die Aktions-Schaltfläche am Ende der Alarmzeile.

Weitere Details zur Funktionalität der Benachrichtigungen finden Sie in der zugehörigen Dokumentation.

9 Auf den Geräten

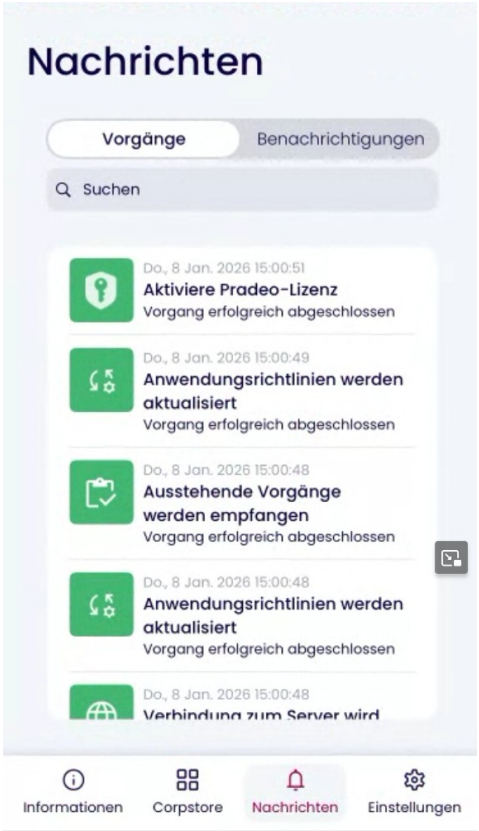
Dieser Abschnitt gibt einen Überblick über die Mobilen Bedrohungsschutz-Status-Ansicht, welche auf verwalteten Geräten verfügbar ist. Die Ansicht ist sowohl bei iOS- als auch bei Android-Plattformen ähnlich; die Logik für Behebungen und Bedrohungsstatus bleibt konsistent.

9.1 iOS & iPadOS Geräte

Beide mobilen Plattformen werden unterstützt. Die Ansicht ist an das jeweilige System angepasst und umfasst zwei zusammenhängende Abschnitte: den **Nachrichten**-Tab und den **Informationen**-Tab mit einem dedizierten Chart.

9.1.1 Lizenzaktivierung

Um Pradeo auf verwalteten Geräten zu nutzen, muss die Lizenz aktiviert werden. Der Aktivierungsprozess wird in Abschnitt 2 dieses Dokumentes beschrieben. Sobald die Lizenz in der Administrator-Konsole konfiguriert ist und ein Schalter unter Mobiler Bedrohungsschutz in den Richtlinien aktiviert ist, wird die Operation **Aktivierung der Lizenz** an das Gerät gesendet.



Diese Operation speichert die erforderliche Lizenz lokal und ermöglicht Zugriff auf Pradeo-Funktionalität.

Eine ähnliche Operation zur Deaktivierung der Pradeo-Lizenz wird gesendet, falls alle Schalter in der Richtlinie deaktiviert sind oder die Integration ausgeschaltet ist.

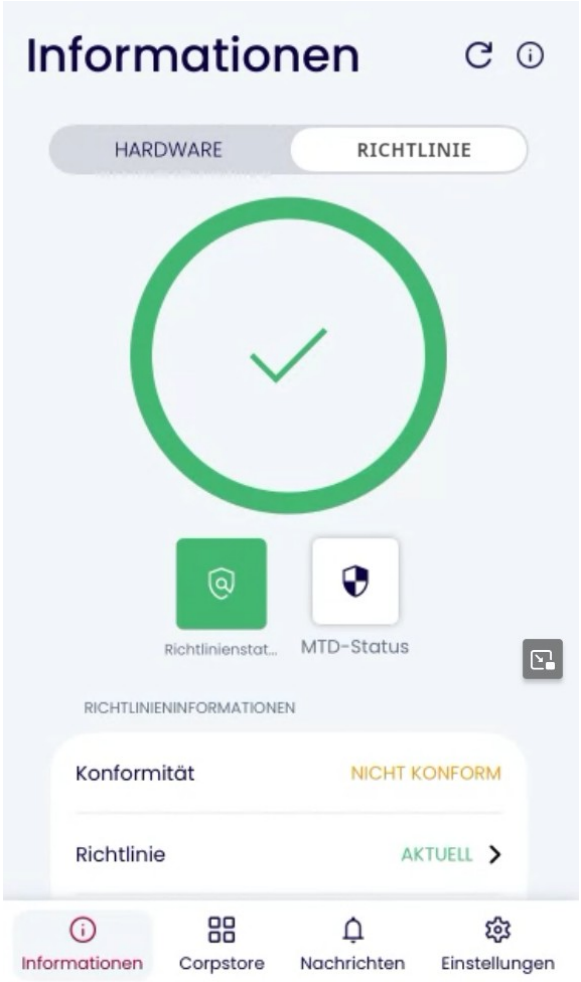
9.1.2 Chart-Ansicht im Informations-Tab

In der **Informationen**-Ansicht befindet sich der **Richtlinien-Chart**.

Unter dem Chart zeigen drei Statuszeilen folgende Informationen an:

- Der erste Eintrag **Konformität** repräsentiert das kombinierte Ergebnis des MTD-Status und des Richtlinienstatus und zeigt an, ob das Gerät konform ist oder nicht.
- Der zweite Eintrag **Richtlinien-Status** gibt den aktuellen Richtlinienstatus sowie etwaige ausstehende Operationen wieder.

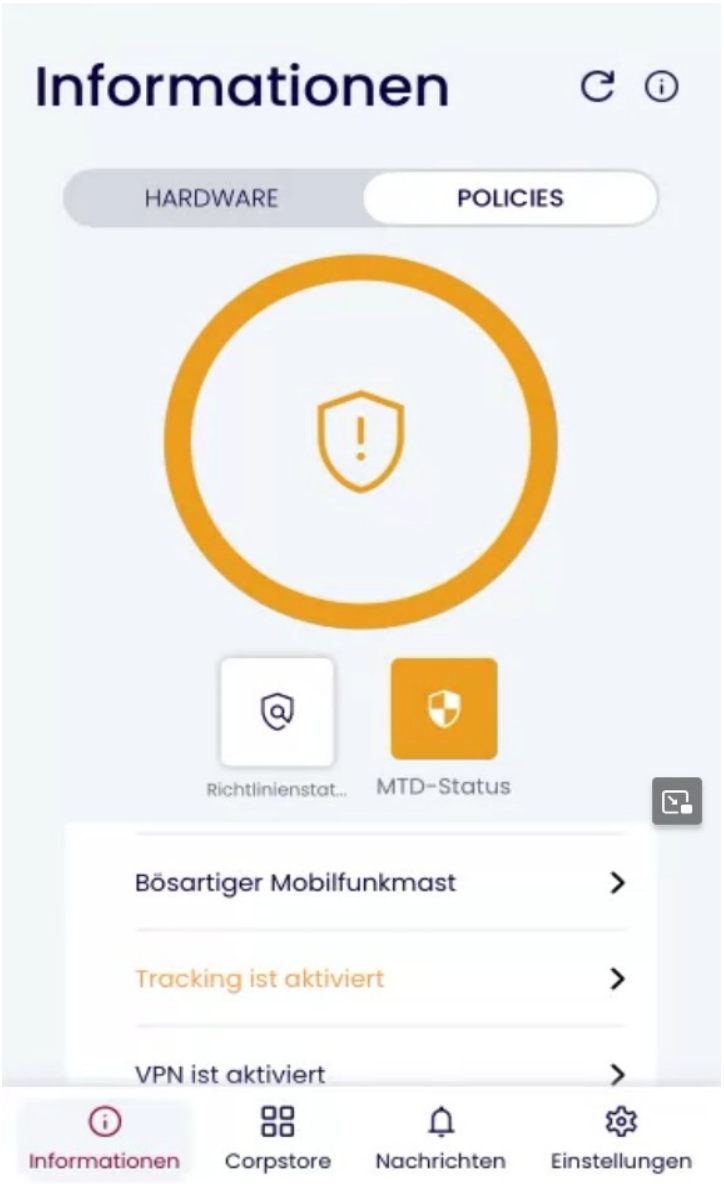
- Der dritte Knoten **MTD Status** zeigt die aktive Mobile Bedrohungsschutz-Richtlinie und deren aktuellen Zustand an. Die gleiche Information wird ebenfalls als kreisförmiger Statusindikator dargestellt. Er füllt sich und wird grün mit einem Häkchen, wenn die Richtlinie erfolgreich angewendet wurde. Bei fehlgeschlagener Behebung nach Bedrohungserkennung wechselt er zu rot. Wenn eine Bedrohung noch vorhanden ist, erscheint er orange mit einem pulsierenden Schild-Symbol.



9.1.3 Mobiler Bedrohungsschutz Tab

Im MTD-Tab werden alle in der Richtlinie definierten Netzwerk- und Systembedrohungen angezeigt, die mit dem Gerät kompatibel sind. Jede aufgeführte Bedrohung kann erweitert werden, um die zugewiesenen Behebungen einzusehen.

Bedrohungen können in drei Farben dargestellt werden, je nach Prioritätslevel, das von Administratoren in den Richtlinien festgelegt wurde: niedrige Priorität ist hellorange, es folgen orange und rot.



Gegenmaßnahmen zeigen ein Status-Symbol auf der rechten Seite an, wenn eine Aktion als Reaktion auf die erkannte Bedrohung ausgeführt wurde. Ein grünes Häkchen bedeutet erfolgreiche Ausführung; ein rotes Kreuz zeigt fehlgeschlagene Behebung an. Kein Symbol bedeutet, dass keine Bedrohung erkannt wurde und die Zeile nur Informationen über den beobachteten Bedrohungstyp und zugewiesene Behebung enthält.

9.1.4 Gegenmaßnahmen

Apple-Plattformen unterstützen nur zwei Arten von Gegenmaßnahmen: **Alarm Senden** und **Benachrichtigung Anzeigen**. Die *Alarm-Aktion* wird auf der Administrationskonsole ausgelöst, die *Benachrichtigung Anzeigen* Aktion wird direkt dem Benutzer angezeigt.

Die Darstellung der Benachrichtigung hängt vom App-Status ab. Wenn der Agent im Vordergrund ist, erscheint ein System-Pop-Up mit Informationen über die erkannte Bedrohung.
Wenn die App im Hintergrund läuft, wird die Information als Standard-Systembenachrichtigung angezeigt.

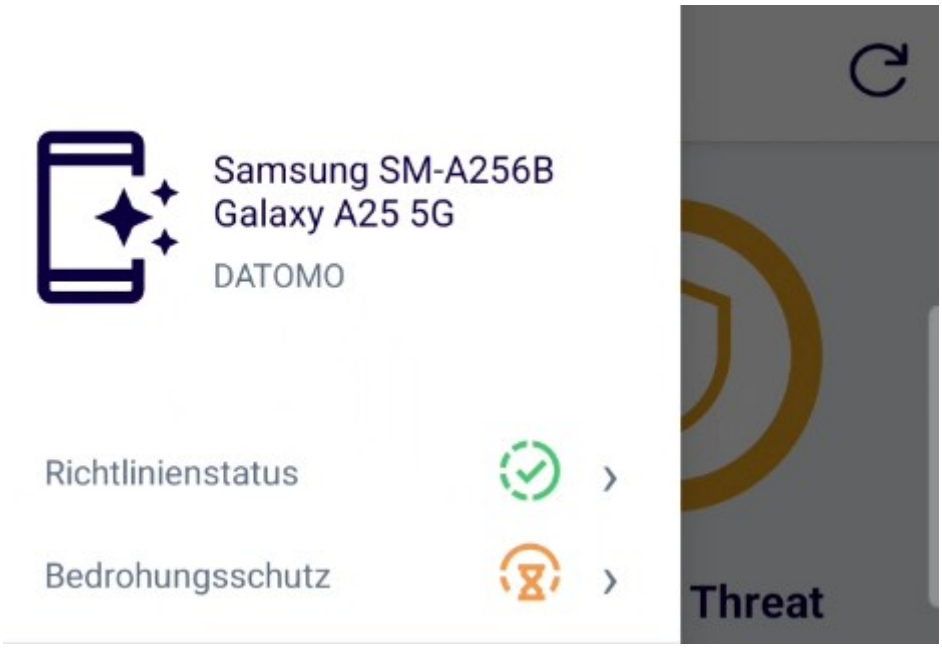
9.1.5 Kategorisierte URLs

Apple-Plattformen unterstützen nativ Web-Content-Filtering auf Systemebene. Dieses Verfahren überwacht Netzwerkverkehr sicher und bestimmt, welche URLs erlaubt sind oder blockiert werden sollen, basierend auf von Pradeo als bedrohlich eingestuften URLs (z. B. Phishing-Sites).

Die Funktion ist mit dem Betriebssystem integriert, um Benutzerprivatsphäre zu wahren und arbeitet automatisch, sobald sie in den Organisationseinstellungen aktiviert ist. Für Details zur Filterstatus-Überprüfung auf dem Gerät siehe Abschnitt 7.

9.2 Android Geräte

Auf Android-Geräten gibt es eine neue Option im linken Menü des Agenten, mit der Nutzer den aktuellen Status von Netzwerk- und Systembedrohungen anzeigen können – ähnlich wie bei iOS.

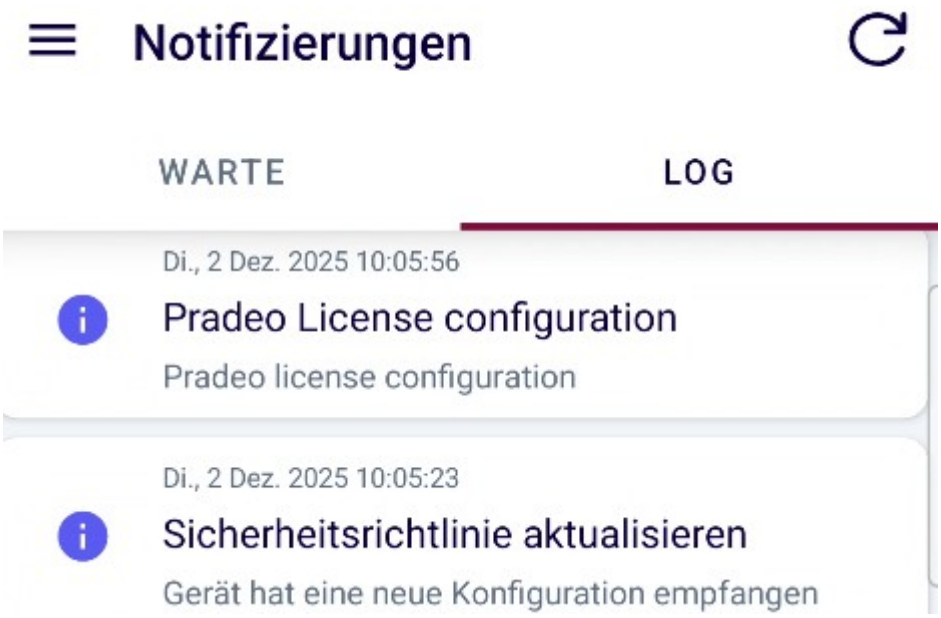


Statusindikatoren werden ebenfalls in einem Kreissymbol angezeigt, die sowohl den aktiven Richtlinienstatus als auch den neuen Mobilen Bedrohungsschutz-Status darstellen. Dafür muss zunächst die MTD-Lizenz aktiviert sein.

9.2.1 Lizenzaktivierung

Zur Nutzung von Pradeo auf verwalteten Geräten ist eine Lizenzaktivierung erforderlich (siehe Abschnitt 2). Sobald die Lizenz in der Administrationskonsole konfiguriert und ein Schalter unter *Mobiler Bedrohungsschutz* in den Richtlinien aktiviert ist, wird eine Operation namens **Pradeo Lizenz Konfiguration** an das Gerät gesendet.

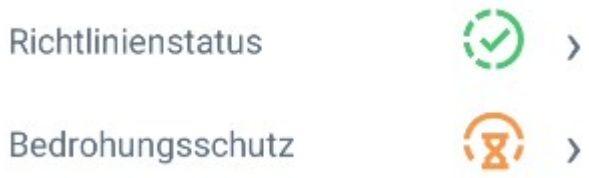
Diese Operation wird im Benachrichtigungs-Tab, Abschnitt Log angezeigt. Hierdurch wird die erforderliche Lizenz lokal auf dem Gerät gespeichert und ermöglicht Zugriff auf Pradeo-Funktionalität.



Eine ähnliche Operation zur Deaktivierung der Pradeo-Lizenz wird gesendet, falls alle Schalter in der Richtlinie deaktiviert sind oder die Integration ausgeschaltet ist.

9.2.2 Status-Tab

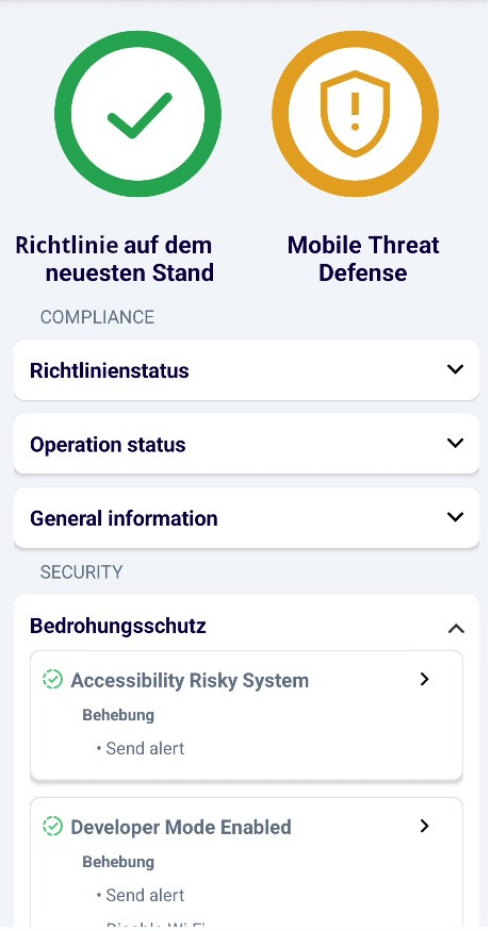
Im **Status**-Tab stehen zwei Richtlinieneinträge bereit: **Richtlinienstatus** und **Bedrohungsschutz**.



Sie ermöglichen dem Benutzer Zugriff auf die **Compliance**- und **Sicherheits**-Abschnitte. Die Auswahl öffnet eine neue Ansicht.

Diese Charts geben Einblick in den Politikstatus und MTD-Status, um Administratoren effektive Überwachung und Management zu ermöglichen.

Unter dem Chart steht der erste Abschnitt namens **Compliance**, der den Richtlinienstatus sowie die Operations-Status mit allen ausstehenden Operationen darstellt. Zusätzlich werden allgemeine Informationen über das Gerät und den Benutzer bereitgestellt.



Der zweite Abschnitt **Sicherheit** gibt an, welchen aktuellen Mobile Threat Defense-Zustand das Gerät hat. Er zeigt die aktive MTD-Richtlinie und deren Status an. Die Zusammenfassung der Bedrohungsstatus aus beobachteten Regeln wird ebenfalls als kreisförmiger Statusindikator angezeigt. Der Indikator wird grün mit einem Häkchen, wenn die Richtlinie erfolgreich angewendet wurde, bei fehlgeschlagener Gegenmaßnahme nach Bedrohungserkennung rot und orange mit Schild-Symbol, wenn eine Bedrohung noch vorhanden oder noch nicht geprüft ist. Um beobachtete Regeln anzuzeigen, erweitern Sie das Feld **Mobile Threat Defense**.

9.2.3 Mobile Threat Defense Tab

Im Mobile Threat Defense-Tab werden alle in der Richtlinie definierten Netzwerk- und Systembedrohungen angezeigt, die mit dem Gerät kompatibel sind. Jede aufgeführte Bedrohung kann ausgeklappt werden, um die zugewiesenen Gegenmaßnahmen einzusehen.

Wenn eine Bedrohung erkannt wurde, erscheint ein rotes Dreieck vor dem Namen der Bedrohung. Ist die Bedrohung nicht vorhanden, wird ein grünes Häkchen angezeigt. Wenn noch kein Scan durchgeführt wurde, ist ein orangefarbiges „nicht Aktuell“-Symbol sichtbar.

Gegenmaßnahmen zeigen einen Status-Symbol rechts an, wenn eine Aktion als Reaktion auf die erkannte Bedrohung ausgeführt wurde. Ein grünes Häkchen bedeutet erfolgreiche Ausführung; ein rotes Kreuz zeigt fehlgeschlagene Gegenmaßnahmen an. Kein Symbol bedeutet, dass keine Bedrohung erkannt wurde und die Zeile nur Informationen über den beobachteten Bedrohungstyp sowie zugewiesene Behebungen enthält.

9.2.4 Gegemaßnahmen

Android-Plattformen unterstützen drei Arten von Behebungen: **Alarm Senden**, **Benachrichtigung Anzeigen** und **WLAN Deaktivieren**. Die Alarm-Senden-Aktion wird auf der Administrationskonsole ausgelöst, während Benachrichtiung-Anzeigen- und WLAN-Deaktivieren-Gegenmaßnahme direkt mit dem Gerät interagieren.

Wenn der Agent eine Bedrohung erkennt, zeigt er die Information über die erkannte Bedrohung in einer Benachrichtigung an.

9.2.5 Globale & pro-Anwendungsregeln

Auf der Geräteseite werden Anwendungen im Hintergrund bei jeder Richtlinien-Aktualisierung gescannt. Der Scan umfasst alle installierten Apps (ohne vorinstallierte). Das Scannen jeder App kann bis zu 12 Minuten dauern; wenn eine Bedrohung erkannt wird, werden Gegenmaßnahmen automatisch ausgeführt.

Scans erfolgen im Auftrag des Mobile Threat Defense-Anbieters; falls der Dienstleister keinen Bericht zurückliefert, kann der Prozess ohne Benachrichtigung ablaufen.

In Zukunft wird die gesamte Anwendungsbericht-Funktionalität in eine Backend-zu-Backend-Lösung verlagert werden, um Leistung und Sicherheit zu verbessern. Informationen darüber, wie globale Anwendungbedrohungen funktionieren, finden Sie in den Abschnitten **Globale Anwendungsbedrohung** und **Pro-Applikationbedrohung**. Die einzige Information, die der Benutzer über den auf dem Gerät durchgeführten Scan sieht, ist eine Gegenmaßnahme-Benachrichtigung, ähnlich wie bei anderen Bedrohungen.

9.2.6 Malware & Virus-Scannen für Anwendungen

Der Scannungsmechanismus läuft mit einem Timeout von 12 Minuten während des Malware-Scans, der bei Richtlinienaktualisierung ausgeführt wird. Nach dem Scan versucht das Gerät, innerhalb desselben 12-minütigen Timeouts einen Bericht über gefundene Viren oder Malware zu senden. Wenn eine Zeitüberschreitung aufritt, wird kein Bericht an den Server gesendet.

Wenn ein Virus erkannt wird, werden die vom Administrator in den Richtlinien konfigurierten Gegenmaßnahmen automatisch initiiert.