EGOSECURE
ENJOY DATA PROTECTION

macmon
nac intelligent einfach

MACMON NAC WHITEPAPER

Anbindung an Matrix42
EgoSecure Data Protection

Inhaltsverzeichnis

Version: 1.2_de

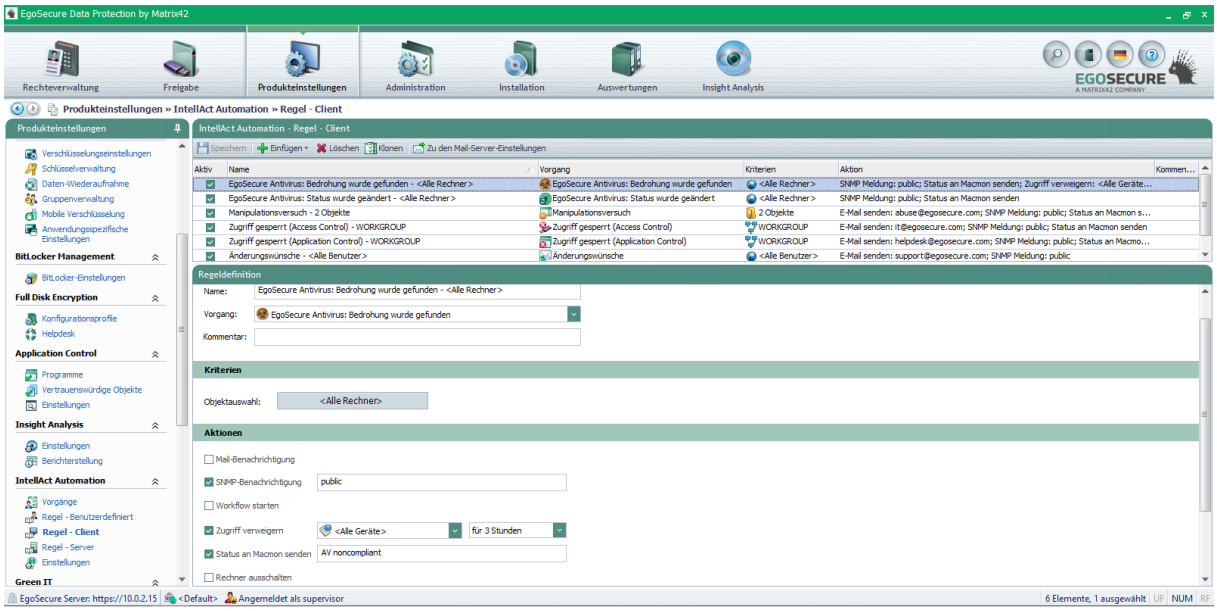
Einleitung

EgoSecure Data Protection bietet eine umfassende Endpoint-Security-Lösung, die Endgeräte mit einem zentralen Management für Sicherheitsfunktionen von Virenschutz über Device Control und Application Control bis zur Verschlüsselung ausstattet. Durch die stets aktuelle Übersicht der Vorkommnisse auf den Endgeräten und die Einhaltung der Sicherheitsrichtlinien bietet EgoSecure Data Protection eine hervorragende Quelle von Informationen über Compliance-Verstößen für macmon NAC.
Auf Basis jedes Ereignisses und jedes Richtlinienverstoßes kann macmon NAC über Endgeräte informiert werden, die nicht den Vorgaben entsprechen und daher vom normalen Unternehmensnetzwerk getrennt werden sollen. macmon NAC wiederum kann flexibel auf jede Situation reagieren und die betroffenen Endgeräte in ein konfiguriertes Isolations-VLAN verschieben und ganz vom Netzwerk trennen.
Die direkte Verbindung der beiden Systeme und die damit verbundene automatisierbare Reaktion auf Verstöße werden in diesem Whitepaper erläutert.

Anwendungsfälle

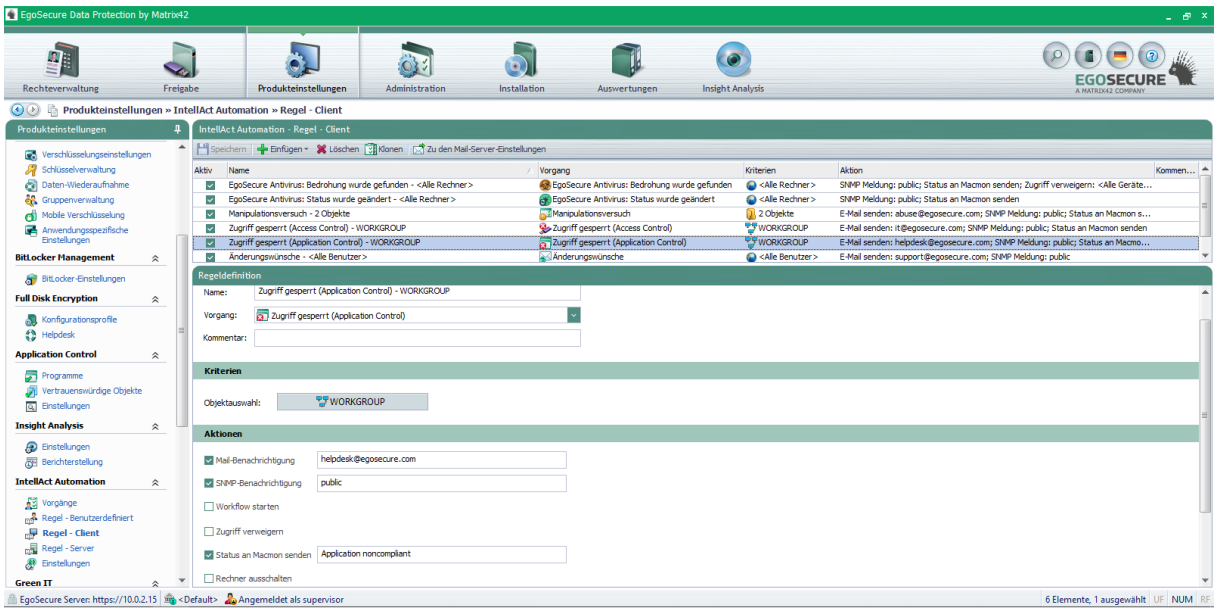
Erkennung von Schadsoftware

Unter *Produkteinstellungen* → *IntellAct Automation* → *Regel* → *Client* kann eine Richtlinie erstellt werden, die macmon NAC bei der Erkennung von Viren, Trojanern und schädlichem Code informiert.



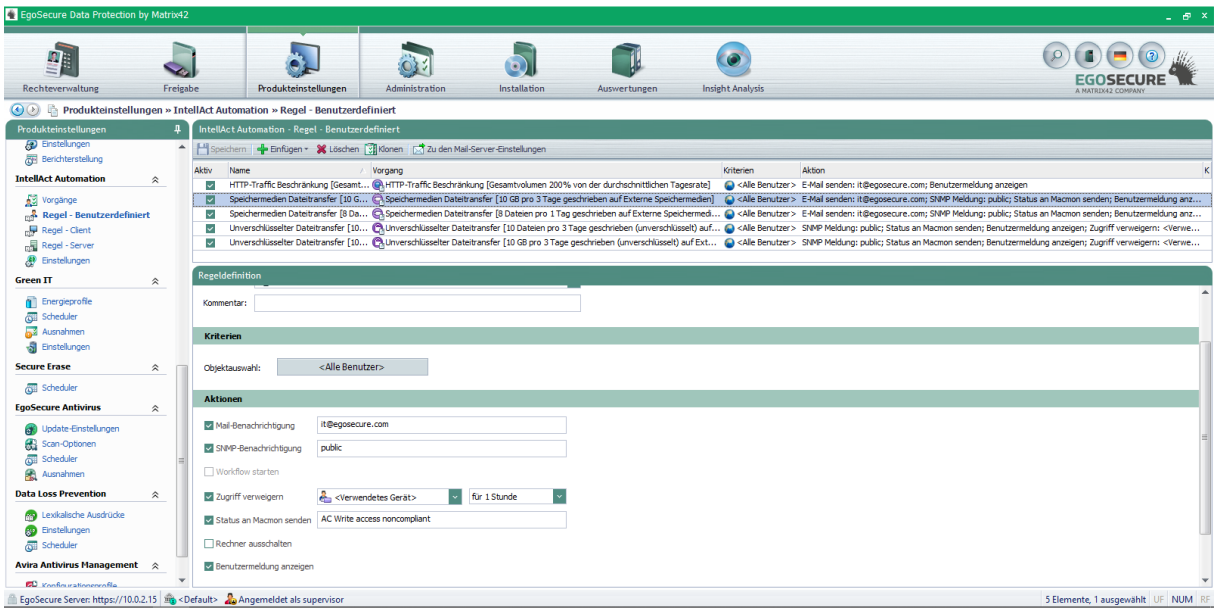
Erkennung einer unerwünschte Anwendung

Erkennt EgoSecure Application Control eine gestartete Anwendung, die nicht auf der Whitelist, bzw. auf der Blacklist steht, erfolgt eine *non-compliant*-Nachricht an macmon NAC.



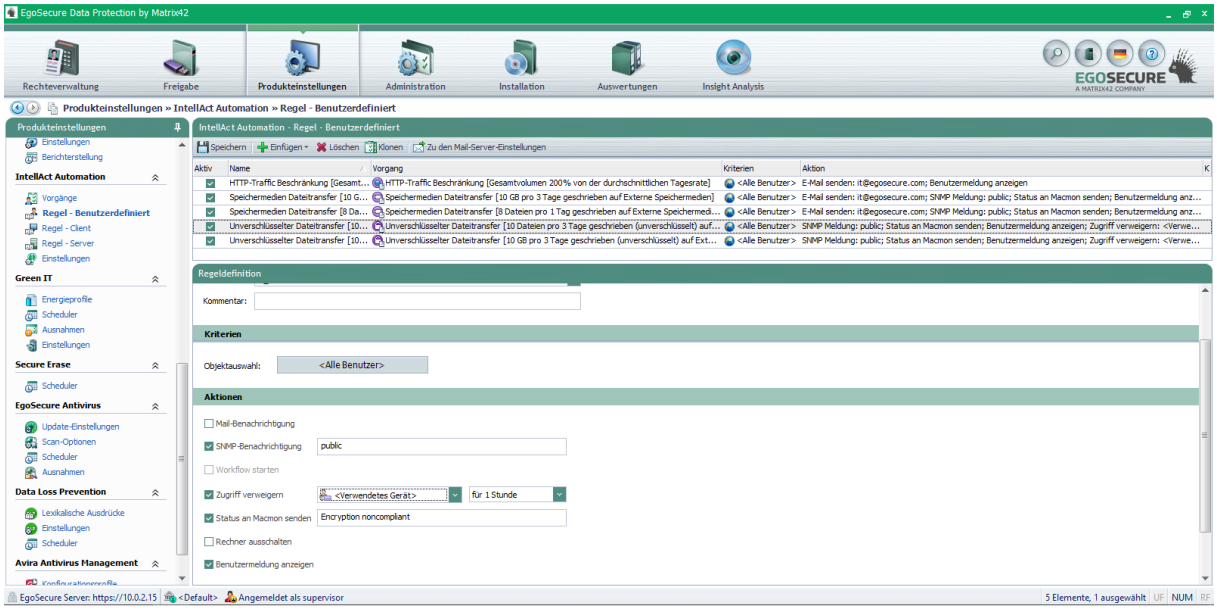
Überschreitung von Datenzugriffen auf externen Speichermedien

Wird eine bestimmte Grenze von Datenzugriffen auf externe Speichermedien überschritten, wird eine Statusmeldung an macmon NAC übergeben.



Überschreitung von unverschlüsselten Schreibzugriffen auf externen Speichermedien

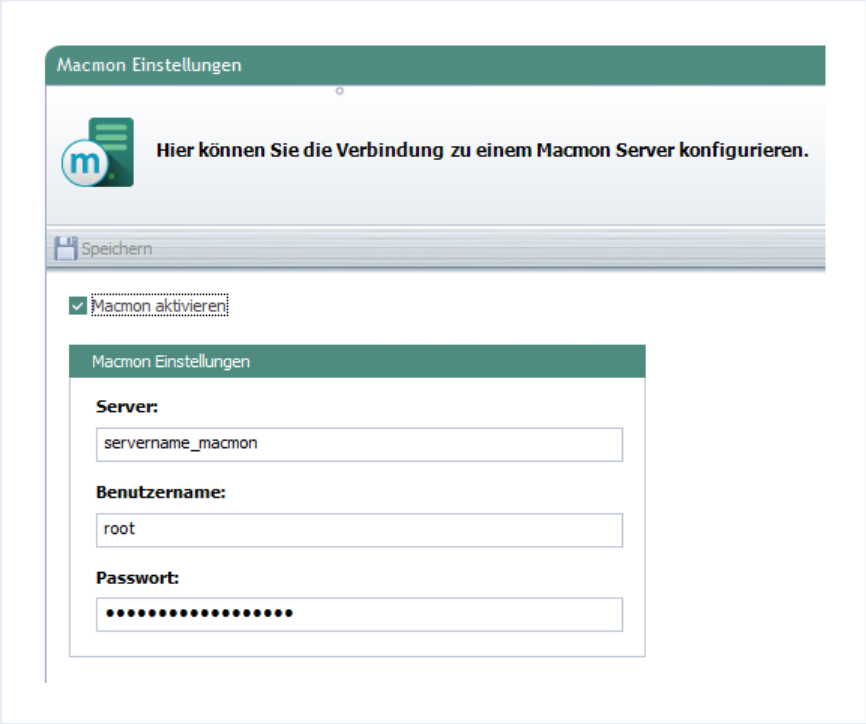
Wird eine Menge von unverschlüsselten Schreibzugriffen auf externe Speichermedien überschritten, wird eine Statusmeldung an macmon NAC übergeben.



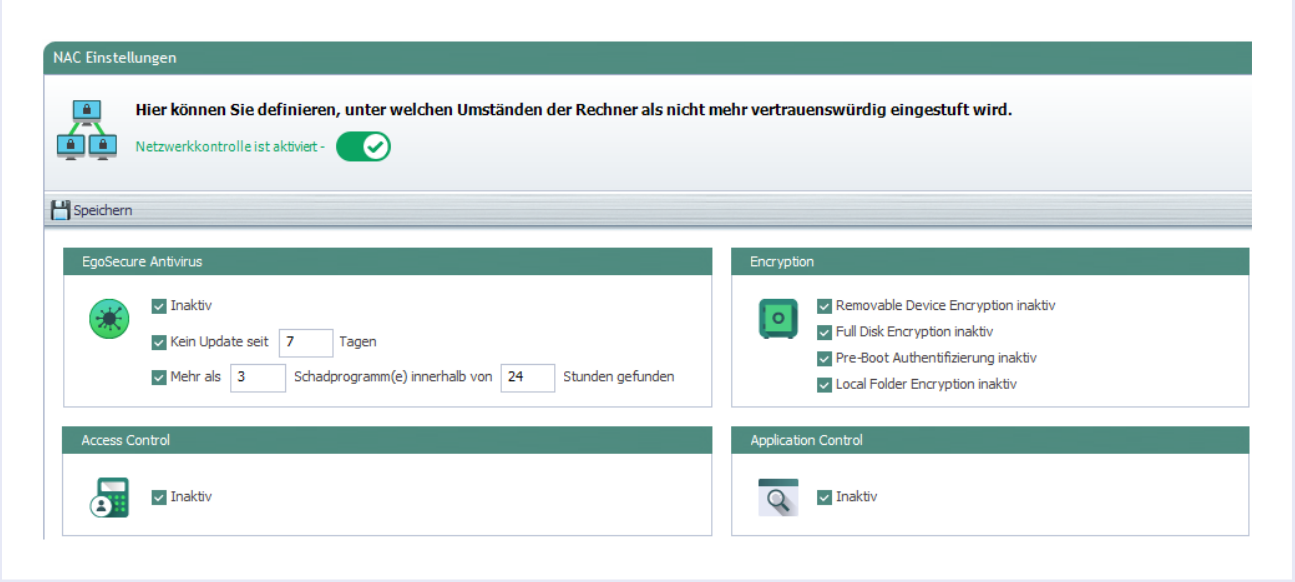
Konfiguration von EgoSecure Data Protection

Einstellungen zur Kommunikation mit macmon NAC

Unter *Administration* → *NAC* → *macmon Einstellungen* muss lediglich die Anbindung an macmon NAC aktiviert werden und der Servername im Feld *Server* zusammen mit *Benutzername* und *Passwort* für die Authentifizierung hinterlegt werden.



Unter *Administration* → *NAC* → *NAC Einstellungen* kann eine generelle Vorgabe erstellt werden, in welchen Situationen ein Endgerät als *non-compliant* gilt.



Konfiguration von macmon NAC

Regelwerk

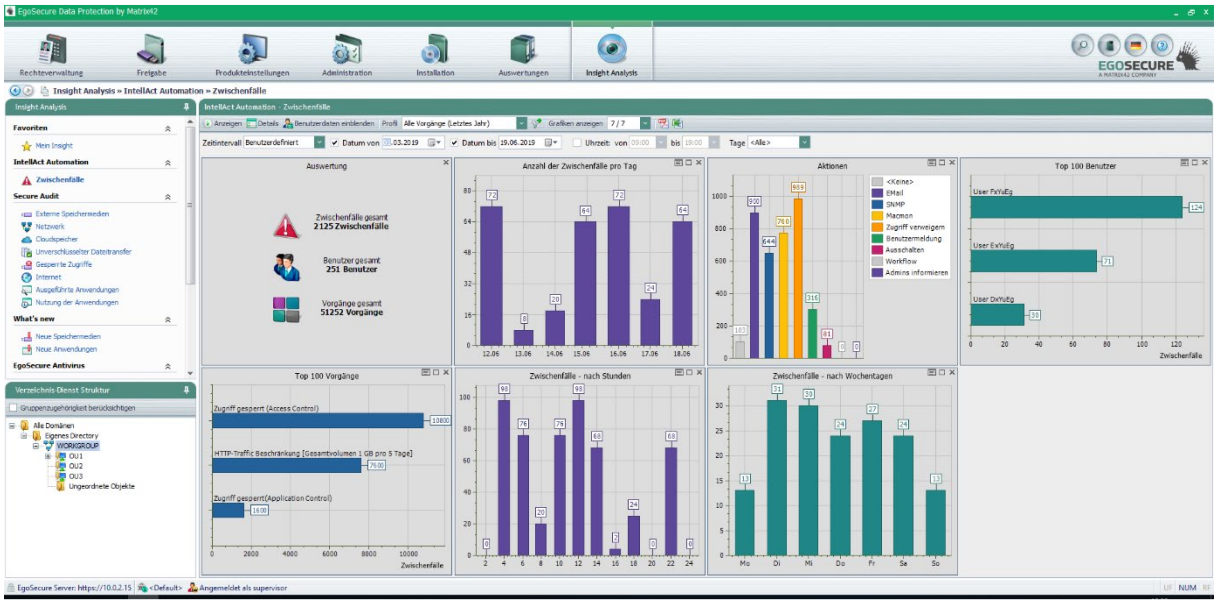
Endgeräte werden automatisch in das sogenannte Remediation-VLAN verschoben, sobald sie von EgoSecure Data Protection als *non-compliant* markiert werden. Dieses VLAN wird unter *Einstellungen* → *Scan-Engine* → *remediation_vlans* konfiguriert. Eine weitere Konfiguration wird nicht benötigt.

Um differenziert auf bestimmte Gründe (reason) für den non-compliant-Status zu reagieren, können verschiedene Regeln unter Richtlinien → Ereignisse angelegt werden.

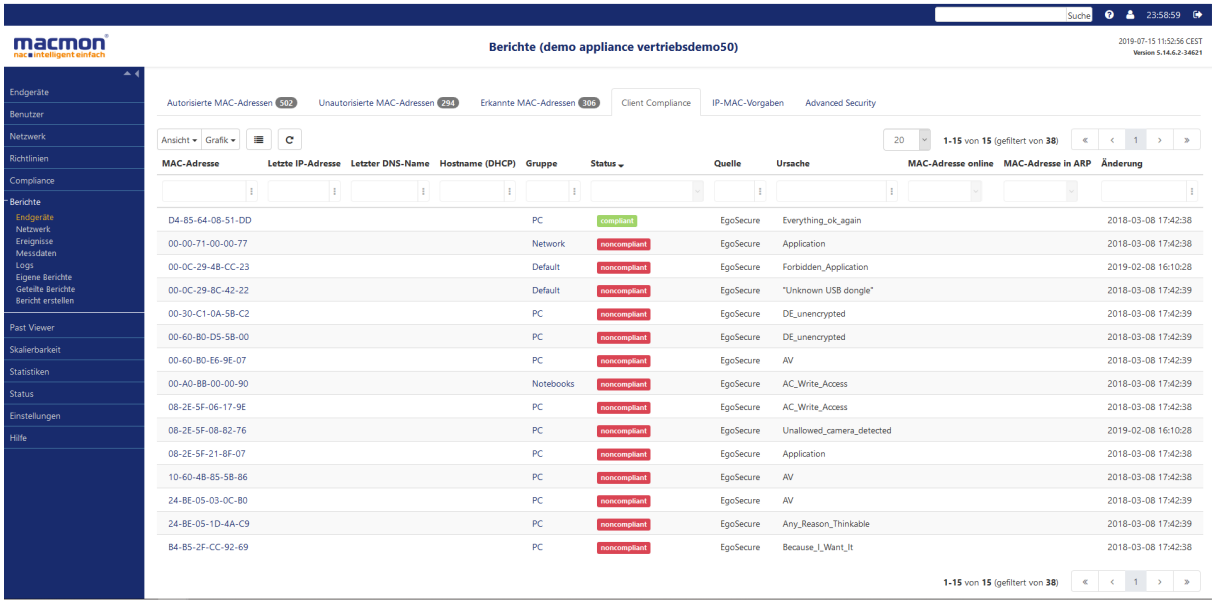
- Klick auf *Regel hinzufügen*
- *Name* und *Beschreibung* sind frei wählbar
- Ereignis *now_noncompliant*
- Bedingung:
  - Erkennung von Schadsoftware:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AV noncompliant")
  - Erkennung einer unerwünschte Anwendung:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Application noncompliant")
  - Überschreitung von Datenzugriffen auf externen Speichermedien:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AC Write access noncompliant")
  - Überschreitung von unverschlüsselten Schreibzugriffen auf externen Speichermedien:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Encryption noncompliant")
- Reaktion beispielsweise *Mailbenachrichtigung*

Übersicht der Compliance-Verstöße

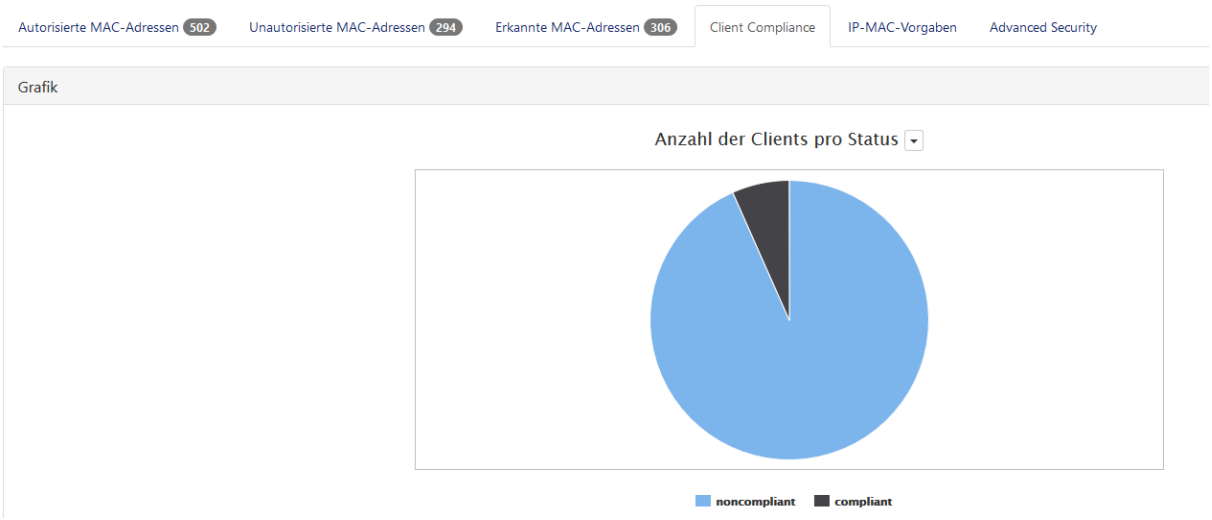
Nach Eintritt der Ereignisse und Ausführen der Aktionen von EgoSecure Data Protection sind die vorgenommenen Aktionen im Reporting wie folgt dargestellt:



Im Report „Client Compliance“ werden in der macmon-GUI die Status der Endgeräte dargestellt – dabei sind die Quelle und die Gründe mit aufgeführt.



Gefiltert nach der Quelle *EgoSecure* lässt sich so z.B. auch der Anteil der Endgeräte nach Status auswerten:



Kontakt bei EgoSecure – a Matrix42 Company

Daniel Döring, Technical Director, Security and Strategic Alliances
Pforzheimer Str. 128b | 76275 Ettlingen
Tel.: +49 724335495-0 | support@egosecure.com | www.egosecure.com

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu