

MACMON NAC WHITEPAPER

Anbindung an Matrix42

EgoSecure Data Protection

Inhaltsverzeichnis

Einleitung 3

Anwendungsfälle 4

 Erkennung von Schadsoftware 4

 Erkennung einer unerwünschte Anwendung..... 4

 Überschreitung von Datenzugriffen auf externen Speichermedien 5

 Überschreitung von unverschlüsselten Schreibzugriffen auf externen Speichermedien..... 6

Konfiguration von EgoSecure Data Protection..... 7

 Einstellungen zur Kommunikation mit macmon NAC..... 7

Konfiguration von macmon NAC 8

 Regelwerk 8

Übersicht der Compliance-Verstöße 8

Kontakt bei EgoSecure – a Matrix42 Company 10

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.

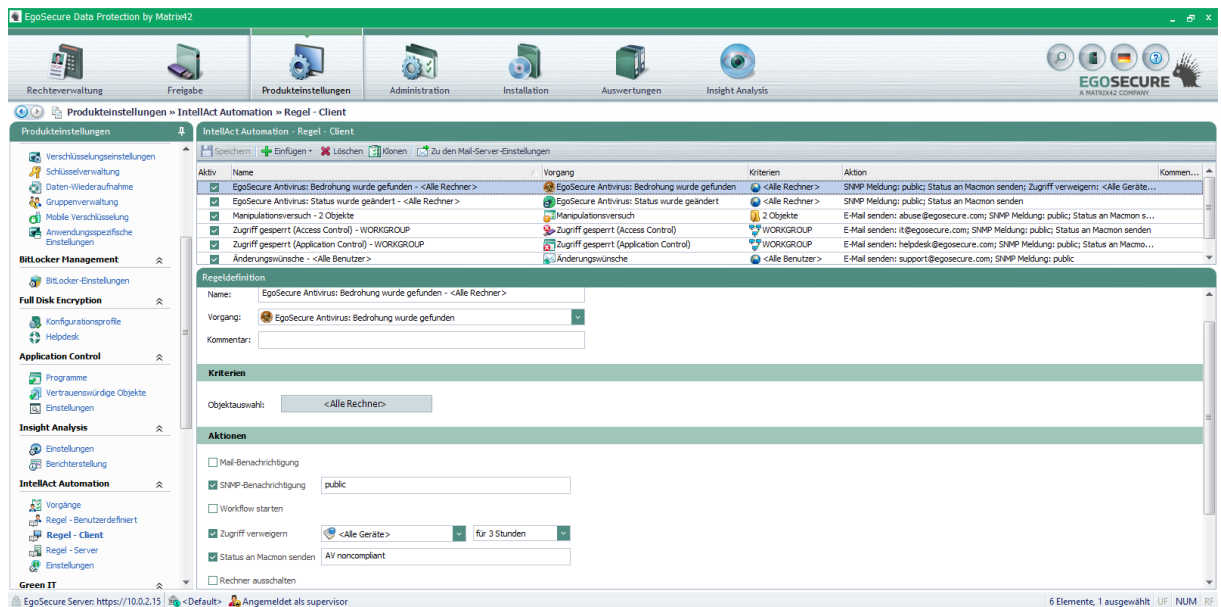
Auf Basis jedes Ereignisses und jedes Richtlinienverstoßes kann macmon NAC über Endgeräte informiert werden, die nicht den Vorgaben entsprechen und daher vom normalen Unternehmensnetzwerk getrennt werden sollen. macmon NAC wiederum kann flexibel auf jede Situation reagieren und die betroffenen Endgeräte 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

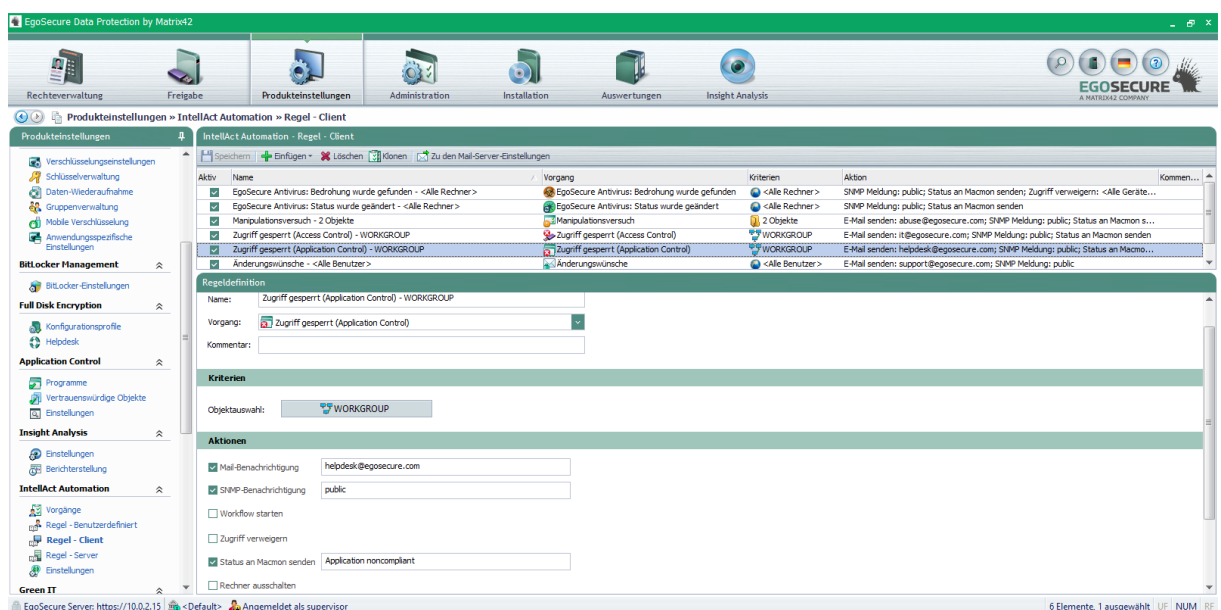
Erkennung von Schadsoftware

Unter *Produkteinstellungen* → *IntelAct 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.

The screenshot shows the 'EgoSecure Data Protection by Matrix42' interface. The left sidebar contains various modules: Rechteverwaltung, Freigabe, Produkteinstellungen, Administration, Installation, Auswertungen, and Insight Analysis. The main window is titled 'Produkteinstellungen » IntelliAct Automation » Regel - Benutzerdefiniert'. It displays a list of rules and a detailed view of a selected rule.

Regeldefinition	Kriterien	Aktionen
Objektauswahl: <Alle Benutzer> ☒ Mail-Benachrichtigung: it@egosecure.com ☒ SNMP-Benachrichtigung: public ☐ Workflow starten ☒ Zugriff verweigern: <Verwendetes Gerät> für 1 Stunde ☒ Status an Macmon senden: AC Write access noncompliant ☐ Rechner ausschalten ☒ Benutzermeldung anzeigen	<Alle Benutzer>	☒ E-Mail senden: it@egosecure.com; Benutzermeldung anzeigen ☒ E-Mail senden: it@egosecure.com; SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen ☒ E-Mail senden: it@egosecure.com; SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen ☒ SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen; Zugriff verweigern: <Verwendetes Gerät>

Überschreitung von unverschlüsselten Schreibzugriffen auf externen Speichermedien

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

The screenshot shows the 'EgoSecure Data Protection by Matrix42' interface. The left sidebar contains various modules: Rechteverwaltung, Freigabe, Produkteinstellungen, Administration, Installation, Auswertungen, and Insight Analysis. The main window is titled 'Produkteinstellungen » IntelliAct Automation » Regel - Benutzerdefiniert'. It displays a list of rules and a detailed view of a selected rule.

Regeldefinition	Kriterien	Aktionen
Objektauswahl: <Alle Benutzer> ☐ Mail-Benachrichtigung ☒ SNMP-Benachrichtigung: public ☐ Workflow starten ☒ Zugriff verweigern: <Verwendetes Gerät> für 1 Stunde ☒ Status an Macmon senden: Encryption noncompliant ☐ Rechner ausschalten ☒ Benutzermeldung anzeigen	<Alle Benutzer>	☐ E-Mail senden: it@egosecure.com; Benutzermeldung anzeigen ☒ E-Mail senden: it@egosecure.com; SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen ☒ E-Mail senden: it@egosecure.com; SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen ☒ SNMP Meldung: public; Status an Macmon senden; Benutzermeldung anzeigen; Zugriff verweigern: <Verwendetes Gerät>

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.

The screenshot shows the 'Macmon Einstellungen' window. At the top, there is a header bar with the title 'Macmon Einstellungen'. Below it, a message says 'Hier können Sie die Verbindung zu einem Macmon Server konfigurieren.' with a 'Speichern' button. A checkbox labeled 'Macmon aktivieren' is checked. Below this, there is a section titled 'Macmon Einstellungen' containing three input fields: 'Server:' with the value 'servername_macmon', 'Benutzername:' with the value 'root', and 'Passwort:' with a masked password represented by dots.

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

The screenshot shows the 'NAC Einstellungen' window. At the top, there is a header bar with the title 'NAC Einstellungen'. Below it, a message says 'Hier können Sie definieren, unter welchen Umständen der Rechner als nicht mehr vertrauenswürdig eingestuft wird.' with a 'Speichern' button. A status bar indicates 'Netzwerkkontrolle ist aktiviert -' with a green checkmark icon. Below this, there are four sections: 'EgoSecure Antivirus' with settings for 'Inaktiv', 'Kein Update seit 7 Tagen', and 'Mehr als 3 Schadprogramm(e) innerhalb von 24 Stunden gefunden'; 'Encryption' with settings for 'Removable Device Encryption inaktiv', 'Full Disk Encryption inaktiv', 'Pre-Boot Authentifizierung inaktiv', and 'Local Folder Encryption inaktiv'; 'Access Control' with a setting for 'Inaktiv'; and 'Application Control' with a setting for 'Inaktiv'.

Konfiguration von macmon NAC

Regelwerk

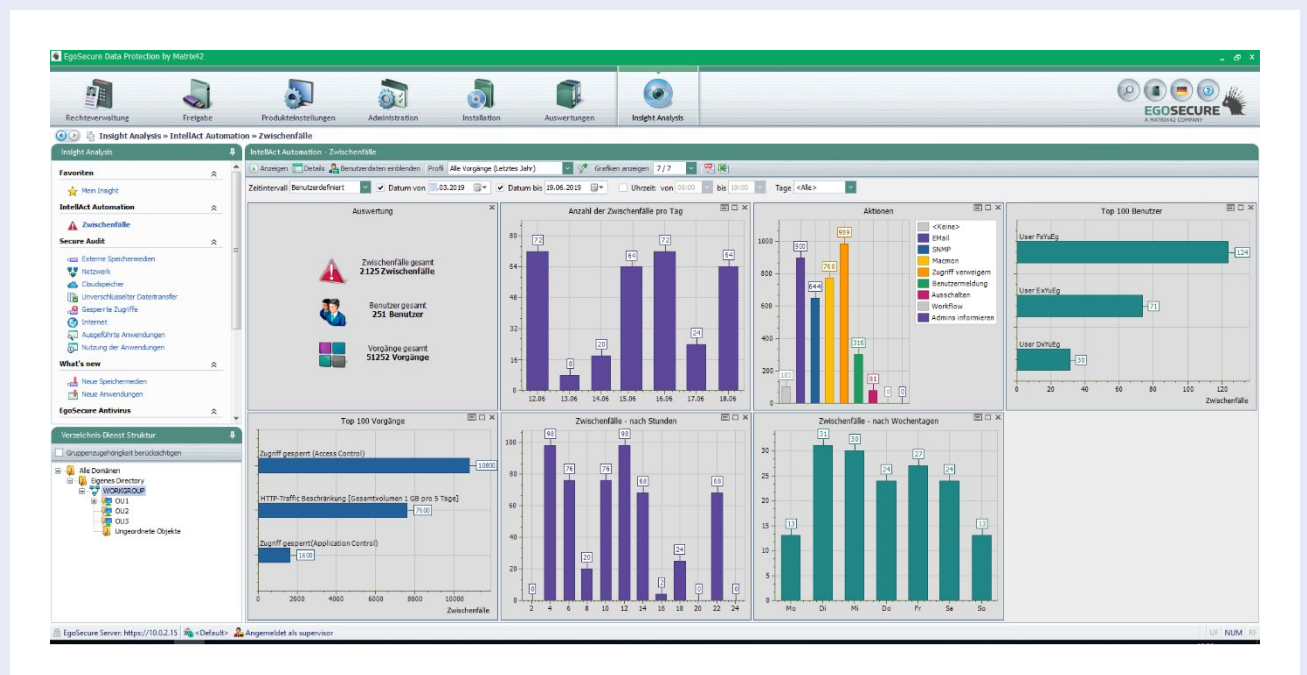
Endgeräte werden automatisch in das sogenannte Remediation-VLAN verschoben, sobald sie von EgoSecure Data Protection als *non-compliant* markiert werden. Dieses VLAN wird unter *Einstellungen* → *Scan-Engine* → *remediation_vlans* konfiguriert. Eine weitere Konfiguration wird nicht benötigt.

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

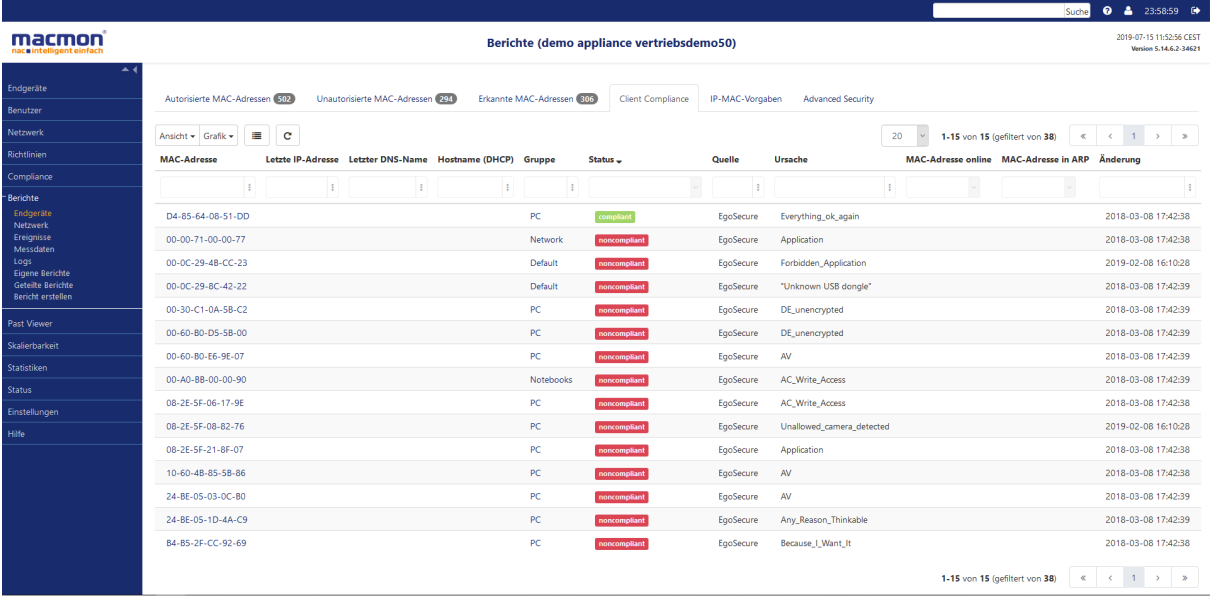
- Klick auf *Regel hinzufügen*
- *Name* und *Beschreibung* sind frei wählbar
- Ereignis *now_noncompliant*
- Bedingung:
 - Erkennung von Schadsoftware:
`mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AV noncompliant")`
 - Erkennung einer unerwünschte Anwendung:
`mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Application 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:

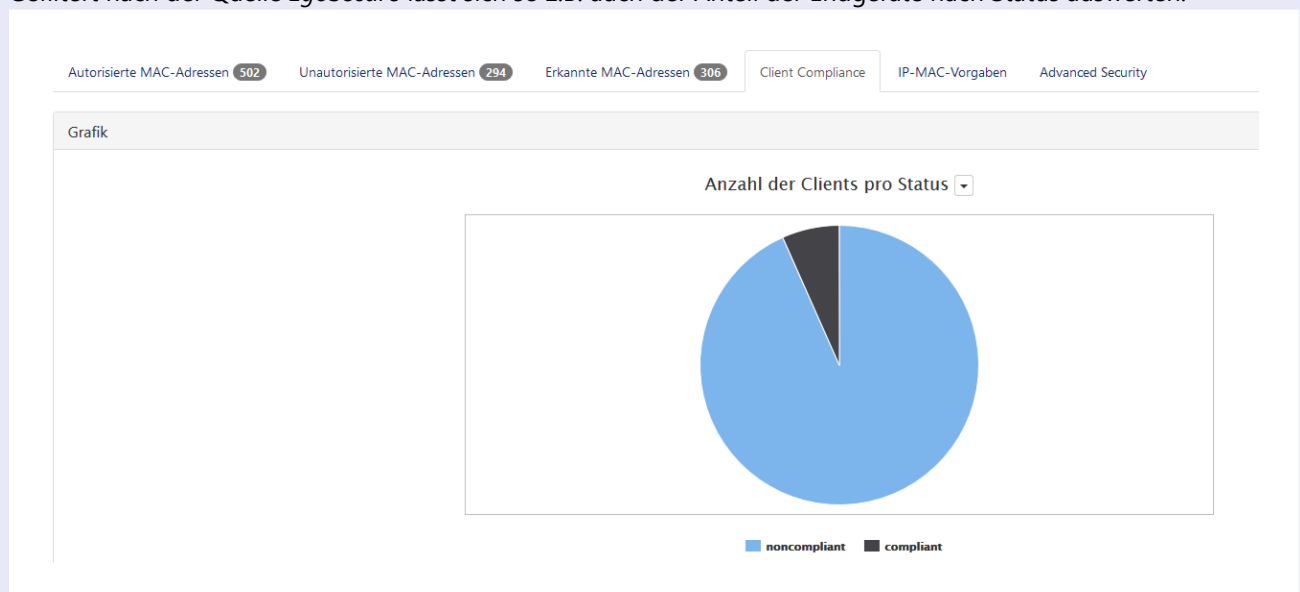


Im Report „Client Compliance“ werden in der macmon-GUI die Status der Endgeräte dargestellt – dabei sind die Quelle und die Gründe mit aufgeführt.



MAC-Adresse	Letzte IP-Adresse	Letzter DNS-Name	Hostname (DHCP)	Gruppe	Status	Quelle	Ursache	MAC-Adresse online	MAC-Adresse in ARP	Änderung
D4-85-64-08-51-DD				PC	compliant	EgoSecure	Everything_ok_again			2018-03-08 17:42:38
00-00-71-00-00-77				Network	noncompliant	EgoSecure	Application			2018-03-08 17:42:38
00-0C-29-48-CC-23				Default	noncompliant	EgoSecure	Forbidden_Application			2019-02-08 16:10:28
00-0C-29-8C-42-22				Default	noncompliant	EgoSecure	"Unknown USB dongle"			2018-03-08 17:42:39
00-30-C1-0A-58-C2				PC	noncompliant	EgoSecure	DE_unencrypted			2018-03-08 17:42:39
00-60-80-D5-58-00				PC	noncompliant	EgoSecure	DE_unencrypted			2018-03-08 17:42:39
00-60-80-E6-9E-07				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:39
00-A0-88-00-00-90				Notebooks	noncompliant	EgoSecure	AC_Write_Access			2018-03-08 17:42:39
08-2E-5F-06-17-9E				PC	noncompliant	EgoSecure	AC_Write_Access			2018-03-08 17:42:38
08-2E-5F-08-B2-76				PC	noncompliant	EgoSecure	Unallowed_camera_detected			2019-02-08 16:10:28
08-2E-5F-21-8F-07				PC	noncompliant	EgoSecure	Application			2018-03-08 17:42:38
10-60-48-85-58-86				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:38
24-8E-05-03-0C-80				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:39
24-8E-05-1D-4A-C9				PC	noncompliant	EgoSecure	Any_Reason_Thinkable			2018-03-08 17:42:39
B4-85-2F-CC-92-69				PC	noncompliant	EgoSecure	Because_I_Want_It			2018-03-08 17:42:38

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