

...better safe  
than sorry!



## Ziele – Nutzen

- Zugangsschutz im Netzwerk vor unbekanntem oder nicht zugelassenen Endgeräten
- Übersicht über die im Netzwerk angeschlossenen Systeme und deren örtliche Verteilung
- Erkennen des Einbringens fremder Systeme im gesamten Netzwerk, auch über mehrere Standorte hinweg
- Erkennen von Standortveränderungen der angeschlossenen Systeme
- Regelbasierte, variable Reaktion auf erkannte Veränderungen im Netzwerk
- Skalierbarkeit nach den Erfordernissen des Unternehmens
- Einsatz von Standardkomponenten
- Geringer administrativer Aufwand
- Erhöhung der Sicherheit im Netzwerk insgesamt

## Funktionsumfang

- Automatische Ermittlung der im Netz aktiven MAC-Adressen durch Abfrage der Switche über das SNMP-Protokoll
- Vergleich der aktiven MAC-Adressen mit den Einträgen in einer Referenzliste auf der Basis einer Datenbank
- Automatisierte Ermittlung aller aktiven MAC-Adressen als Vorschlag für die Datenbank bei der Erstinstallation
- Automatische Übernahme neuer registrierter MAC-Adressen aus vertrauten Bereichen

- Flexible Festlegung von Reaktionen bei Ereignissen, von der Benachrichtigung per E-Mail, Telefon oder SMS, bis zur Portdeaktivierung (permanent oder temporär)
- Ausführen von Reaktionen in Abhängigkeit von Uhrzeit und Tag
- Ereignisgesteuerte Ausführung frei definierbarer Kommandos
- Erkennen von Sicherheitsangriffen auf Switches
- Verwaltung der Stammdaten, Konfiguration und Erfassung des Regelwerkes sowie Bearbeitung von Vorfällen mit Hilfe einer webbasierenden grafischen Benutzeroberfläche
- Datenschnittstelle für den Import zugelassener Endgeräte und der Netzwerkkomponenten
- Kerndaten können mit zusätzlichen Informationen, wie Inventarangaben zugelassener Geräte und Raumidentifizierungen bei den Switchports, ergänzt werden
- Programmschnittstelle zur Kopplung der Referenzdaten an andere Informationssysteme
- Zugangsberechtigung durch passwortgeschützte Benutzererkennung
- SSL-Verschlüsselung der Administrationsverbindung (Web-GUI)

## Komponenten

- **macmon** Web-GUI zur Administration
- **macmon** Monitoring Engine
- **macmon** Ereignisverarbeitung
- **macmon** Reporting

...better safe  
than sorry!



## Voraussetzungen

### Hardware:

- Server mit IA32 Architektur, CPU ab 1 GHz, 1 GB RAM, 20 GB HD

### Software:

- Betriebssystem Microsoft **Windows** Server 2000 und höher oder **Linux** \*
- Apache Webserver ab v1.3
- Net-SNMP ab v5.2 (Linux)
- Datenbanksystem: Microsoft SQL Server ab Version 2000 oder MySQL ab v4.1
- PHP v4.3 oder v5.0
- PEAR DB ab v1.7

### Switches:

Unterstützung der Standards SNMP v1, v2c, v3 und RFC1493 Bridge MIB. MACmon benötigt:

- SNMP-lesenden Zugang zu den Switches
- SNMP-schreibenden Zugang zu den Switches, wenn die Sperrung von Ports gewünscht ist

### Festlegungen zum Betrieb der Lösung:

- Bestimmen des zu überwachenden Bereichs
- Aufbau und Pflege der Datenbasis (Referenzliste der zugelassenen Geräte)
- Reaktionsregeln zur Benachrichtigung
- Automatische Deaktivierung von Ports

Die bestehende Netzwerk- und Client-Architektur wird bei der Implementierung unverändert beibehalten

## Installation

Die Konfiguration und Installation von **macmon** erfolgt durch die mikado ag oder einen qualifizierten Partner:

- Installation der Basiskomponenten
- Installation der MACmon Web-GUI
- Festlegung des zu sichernden Netzwerk-Bereichs
- Abbilden der Netzwerktopologie und Erfassen der Switches sowie anderer Netzkomponenten
- Übernahme der erkannten MAC-Adressen (Clients, Server, Drucker etc.) in die Referenzliste
- Erstellung bzw. Anpassung der Reaktionsregeln im Event-Management entsprechend der Unternehmensforderung
- Import von verifizierten MAC-Adressen aus vom Kunden bereitgestellten Quellen
- Einweisung in Funktionen und Administration von **macmon**

## Nutzungslizenz

**macmon** wird nach Anzahl der **macmon**-Server und Anzahl der zu überwachenden Nodes lizenziert

© Alle erwähnten Firmen-, Waren- oder Dienstleistungsnamen können Warenzeichen oder Dienstleistungsmarken der entsprechenden Eigentümer sein.

\* Das bereitgestellte Linux-System sollte die beschriebenen Softwarekomponenten oder eine aktuelle XAMPP-Version unterstützen.