

# 8MAN

Access Rights Management. **Only much Smarter.**



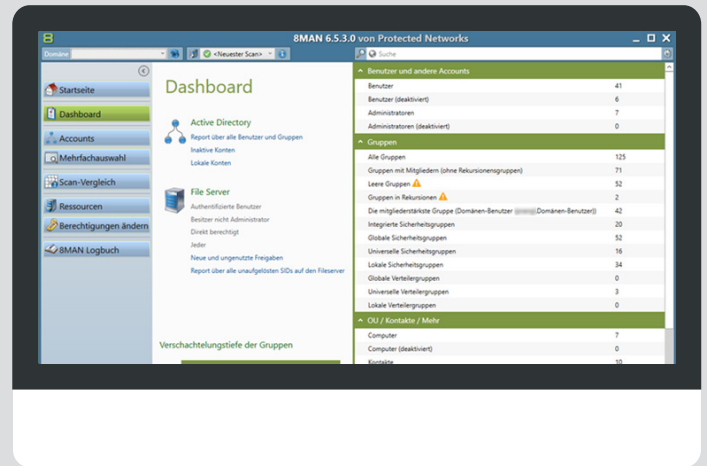
8MATEs IM ÜBERBLICK

# 8MAN Access Rights Management

8MAN ist eine führende Lösung für Access Rights Management (ARM) in Microsoft- und virtuellen Server-Umgebungen und schützt damit Unternehmen vor unberechtigten Zugriffen auf sensible Daten. Die in Deutschland von Protected Networks entwickelte Software-Lösung setzt Maßstäbe für professionelle Netzwerksicherheit und agile IT-Organisation und bündelt modernste Funktionalität mit der Erfüllung gängiger Sicherheits- und Compliance-Richtlinien.

## Die 8MAN Kernfunktionen umfassen:

Permission Analysis | Documentation & Reporting |  
Security Monitoring | Role & Process Optimization |  
User Provisioning.



## 8MATEs im Überblick:



### Security Monitoring

- 8MATE AD Logga
- 8MATE Alerts
- 8MATE FS Logga



### Role & Process Optimization

- 8MATE GrantMA



### Integration

- 8MATE Exchange
- 8MATE vSphere
- 8MATE SharePoint



### Threat & Gap Management

- 8MATE Clean!



### 8MAN Application Integration

- 8MATE Matrix42



## SECURITY MONITORING

Mit unserem 8MATE AD Logga schützen Sie sich vor temporären, selbstvergebenen Zugriffsrechten mit dem Ziel des Datendiebstahls. Der 8MATE Alerts erweitert den 8MATE AD Logga, um ein Meldesystem. Administratoren werden damit über sicherheitskritische Events proaktiv informiert. Der FS Logga überwacht Aktivitäten auf Dateiebene. Datendiebstahl bleibt in den überwachten Verzeichnissen nicht mehr unter dem Radar.



8MATE  
AD Logga



8MATE  
Alerts



8MATE  
FS Logga

### Problem

Auf dem Active Directory (AD) führen Mitarbeiter Änderungen aus – ohne vollumfängliches Monitoring mit folgenden Sicherheitsrisiken:

- Unautorisierte Mitarbeiter erhalten Zugriff durch temporäre Gruppenmitgliedschaften; werden diese anschließend wieder entzogen, bleibt der Vorfall unerkannt.
- Prozesse darüber, wer Mitgliedschaften vergibt und Passwörter zurücksetzt sind unklar. Ohne Fehleranalyse ist eine Klärung z.B. für die Erstellung eines individuellen Gruppenvergabekonzepts nicht möglich.

Im Active Directory finden täglich Änderungen statt. In einigen Bereichen ist das sicherheitskritisch: Dazu zählen insbesondere Benutzerkonten und Gruppenmitgliedschaften.

- Bei Benutzerkonten gibt es eine zentrale Gefahr. Das Kennwort einer Führungskraft wird durch einen Innentäter zurückgesetzt. Mit dem vorläufigen Kennwort lassen sich anschließend vertrauliche Verzeichnisse durchsuchen.
- Gruppenmitgliedschaften ermöglichen den Zugriff auf Verzeichnisse und andere Ressourcen. Sicherheitskritische Gruppen müssen deshalb kontinuierlich auf neue Mitgliedschaften geprüft werden.

Auf den Fileserver erfolgen unzählige Zugriffe mit Änderungen von einer Vielzahl von Mitarbeitern – ohne vollumfängliches Monitoring mit folgenden Sicherheitsrisiken:

- Unautorisierte Mitarbeiter erhalten Zugriff durch temporäre Gruppenmitgliedschaften auf vertrauliche Dokumente und können einsehen, löschen, schreiben, kopieren oder verschieben. Werden Rechte anschließend wieder entzogen, kann der Vorfall nicht mehr nachvollzogen werden.
- Der Prozess über die Vergabe von Rechten, wer wem und warum ist unklar. Ohne eine Fehleranalyse ist eine Klärung z.B. für die Erstellung eines individuellen Berechtigungskonzept nicht möglich.

### Lösung

Klarheit über die Berechtigungssituation im AD: 8MATE AD Logga erweitert die Transparenz auf die gesamte Änderungshistorie. Auch außerhalb vom 8MAN vorgenommene Aktivitäten werden durch das Monitoring erfasst. Temporäre Gruppenmitgliedschaften und unkontrollierte Berechtigungsvergaben sind sofort nachvollziehbar. Sicherheitsrelevante Aktivitäten auf Konten, Objekte, Gruppen und Attribute lassen sich anhand konfigurierbarer Reporte lückenlos nachweisen und kontrollieren.

Der 8MATE Alerts nutzt die Überwachungsmethode des AD Loggas und erweitert diesen um eine Alarmfunktion. Sollte jemand sicherheitsrelevante Konten oder Gruppen manipulieren, wird der Administrator sofort informiert.

Klarheit über die Berechtigungssituation auf dem Fileserver: 8MATE FS Logga erweitert die Transparenz auf die gesamte Zugriffs- und Änderungshistorie im System. Auch außerhalb vom 8MAN vorgenommene Aktivitäten werden durch das Monitoring erfasst. Sicherheitsrelevante temporäre Berechtigungen und Veränderungen an überwachten Verzeichnissen lassen sich anhand konfigurierbarer Reporte lückenlos aufdecken und gegensteuern.



## ROLE & PROCESS OPTIMIZATION

Sicherheitsbeauftragte oder Administratoren wissen nicht wo wichtige Daten liegen und wer darauf zugreifen darf. Role & Process Optimization delegiert diese Aufgabe an die Entscheider in Ihrer Firma.

Mit dem 8MATE GrantMA wird dieser Prozess nochmal vereinfacht. In einem frei definierbaren Workflow erteilen Führungskräfte webbasiert die Zugriffsrechte an ihre Mitarbeiter.

Die Vorteile: Der Administrator hat wieder Zeit für seine Kernaufgaben.



8MATE  
GrantMA

### Problem

Administratoren verwenden einen guten Teil Ihrer Zeit mit der Vergabe von Zugriffsrechten. Im klassischen Prozess ist die Entscheidung über die Vergabe von Rechten (Vorgesetzter) und die technische Ausführung (Administrator) voneinander getrennt.

- Der Administrator weiß nicht, wer welche Rechte haben soll und wird zum reinen Ausführer von Vorgaben.

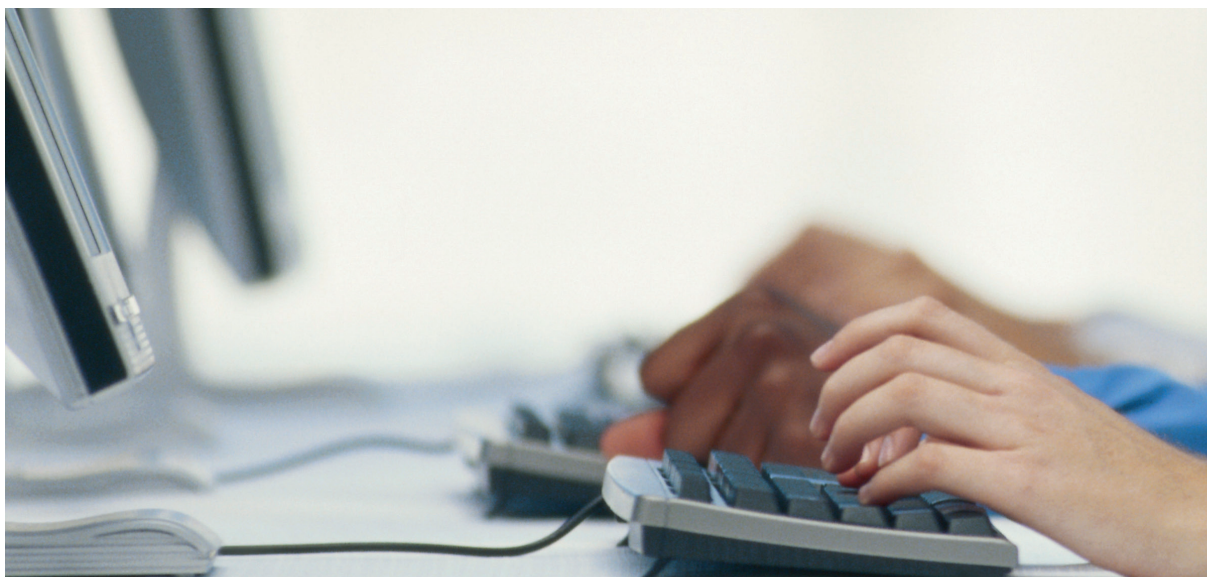
### Lösung

Es ist effizienter die Bewilligung und tatsächliche Aktivierung von Rechten in einem Schritt zu gestalten. Damit sind nur die Akteure in den Prozess involviert, die wirklich nötig sind. Der 8MATE GrantMA nutzt einen Workflow, an dem nur der Mitarbeiter und sein Vorgesetzter (Data Owner) beteiligt sind:

- Der Mitarbeiter bestellt über ein Webportal seine Berechtigungen.
- Der Data Owner entscheidet über die Zugriffsrechte in seiner Abteilung.

#### **Der 8MATE GrantMA Workflow hat folgende Vorteile:**

- Die Führungskraft, die am besten die Informationsstruktur der Abteilung kennt, entscheidet über die Freigabe von Daten und vergibt die Rechte in einem Schritt.
- Durchgeführte Änderungen werden revisionssicher im 8MAN Logbuch protokolliert.
- Der Administrator ist nicht mehr Teil des Prozesses und kann sich auf seine Kernaufgaben konzentrieren.





## THREAT & GAP MANAGEMENT

Threat & Gap Management entfernt sicherheitskritische Berechtigungsfehler automatisch und standardisiert das Rechtesystem nach Ihren Vorgaben.

### Problem

Die Korrektur von Berechtigungsfehlern und Inkonsistenzen ist auf Fileservern nur schwer möglich. Die Umsetzung von Best Practices scheitern an zwei zentralen Hürden: Wissen und Zeit. Darüber hinaus liegt der Fokus im klassischen Access Rights Management (ARM) auf der Verzeichnisebene. Sie ist die zentrale Analyseebene, blendet aber die Dateiebene aus.

### Lösung

8MATE "Clean!" startet einen Prozess, der in einen sicheren und standardisierten Fileserver mündet. Durch eine Reihe klarer Entscheidungen definieren Sie, wie mit Sicherheits- und Strukturproblemen umgegangen werden soll. Ihre Anforderungen und die in 8MAN hinterlegten Best Practices werden automatisch umgesetzt. Darüber hinaus ist die Archivierung veralteter Daten möglich. Denn: Je geringer die Dateimasse, desto einfacher die Verwaltung.

#### Der 8MATE Clean!

- Archiviert alte Fileserver-Dateien
- Entfernt kritische Berechtigungen automatisch
- Entfernt oder ersetzt Direktberechtigungen
- Standardisiert vorhandene Berechtigungsarten auf Ihren Fileservern



8MATE  
Clean!



## INTEGRATION

Mit den 8MATEs folgen wir unserer Vision, immer mehr berechtigungsabhängige Software in die 8MAN Lösung zu integrieren. Unser Zielbild ist eine Oberfläche, mit der Sie alle Anwendungen analysieren und administrieren können.

Neben den Basistechnologien Active Directory und Fileserver haben wir MS Exchange, MS SharePoint und vSphere erfolgreich eingebunden.



8MATE for  
Exchange

### Problem

Die Verwaltung von Berechtigungen mit Microsoft Exchange ist komplex. Die Microsoft Bordmittel erlauben keine ganzheitliche Sicht auf Zugriffsrechte von öffentlichen Ordnern und Postfächern. Auch die Administration der Zugriffsrechte ist umständlich und zeitintensiv.

### Lösung

Mit dem 8MATE for Exchange erweitern Sie den 8MAN für E-Mail-Ressourcen. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. In der gewohnten 8MAN Übersicht sehen Sie auf einen Blick, wer auf öffentliche Ordner, Postfächer, Postfachordner und z.B. Kalender zugreifen kann.

Die Administration von Microsoft Exchange ist eng an den Mitarbeiter-Onboarding-Prozess angelegt: Die Anlage von Postfächern und Vergabe von Zugriffsrechten erfolgt direkt im 8MAN. Änderungen werden revisionssicher im 8MAN dokumentiert.

Neben der Analyse und Administration von Berechtigungen im Microsoft Exchange verfügt der 8MATE for Exchange über weitere Features:

Erstellung von Abwesenheitsnotizen ohne Zugriff auf das E-Mail-Konto  
Auflistung von Stellvertretern für Postfächer und Send-as-Berechtigungen  
Administration von Postfachgrößen, Gruppen und Attribute lückenlos aufdecken

- Administratoren erhalten ein vollständiges Bild über die Aktivitäten im AD, Prozesse können so optimiert werden.
- Auditoren erkennen Sicherheitsvorfälle und die involvierten Akteure, Maßnahmen können so ergriffen werden.
- Die Geschäftsführung hat die Gewissheit: Der 8MATE AD Logga stellt mit dem Monitoring die Daten für interne Sicherheit und Prozessverbesserungen bereit.



8MATE for  
SharePoint

## Problem

Die Analyse und Verwaltung von Berechtigungen auf SharePoint ist komplex.

Die Microsoft Bordmittel erlauben keine ganzheitliche Sicht auf die Zugriffsrechte einzelner SharePoint Ressourcen. Auch die Administration von Berechtigungen ist umständlich und zeitintensiv. Vorgenommene Änderungen in der Berechtigungsstruktur sind nicht nachvollziehbar.

## Lösung

Der 8MATE for SharePoint integriert sämtliche SharePoint Ressourcen in Ihren 8MAN. Damit erfolgt die Analyse und Administration von Berechtigungen zentral und im Einklang mit dem Access Management für andere Anwendungen. Sie profitieren von der Analyse- und Darstellungskompetenz von 8MAN und können Zugriffsrechte schnell verändern.

8MAN zeigt die Berechtigungen in einer Baumstruktur an. Damit sehen Sie schnell, wer auf welche SharePoint Ressource zugreifen kann. Über den Scanvergleich-Report erfahren Sie, wer welche Änderungen an Berechtigungen durchgeführt hat und Sie erhalten ein revisionsssicheres Protokoll vorgenommener Aktivitäten.

Mit dem 8MATE for SharePoint können Sie in der 8MAN Oberfläche alle Berechtigungen vergeben. Mit dem Group Wizard und der Vergabe von Namenskonventionen standardisieren Sie Ihren Berechtigungsvergabeprozess.



8MATE for  
vSphere

## Problem

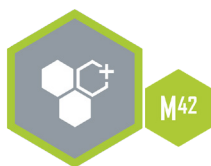
Administratoren müssen zum Überprüfen der Berechtigungslage im vSphere Client jede Ressource einzeln betrachten. Erschwerend kommt die Komplexität an möglichen Privilegien (Nutzerrechten) hinzu.

Die Rechte in vSphere Umgebung können weitreichend sein. Beispielsweise ermöglicht die „Create Snapshot“- Funktion, eine virtuelle Maschine in wenigen Schritten zu kopieren. Rechte wie diese öffnen Datendiebstahl Tür und Tor. Deshalb ist Transparenz bei den Berechtigungen auf virtuellen Servern von höchster Bedeutung.

## Lösung

Der 8MATE for vSphere durchsucht Berechtigungen aller vSphere Ressourcen. Er zeigt auch, über welche Gruppenzugehörigkeit ein User seine Rechte bezieht. Damit schafft der 8MATE for vSphere die Voraussetzungen, gefährliche Sicherheitslücken frühzeitig zu erkennen. Für Standardprozesse sind im 8MATE for vSphere vorgefertigte Berechtigungskonzepte hinterlegt. Mit einem Ist-Soll-Abgleich wird für jede Rolle das passende Berechtigungskonzept ermittelt. Unnötige Rechte lassen sich im vSphere Client anschließend entfernen.

Der 8MATE for vSphere hat eine funktionale Besonderheit. Brisante Rechte, wie z.B. „Create Snapshot“ können im 8MATE vSphere direkt angewählt werden. In einer Übersicht sehen Sie sofort, wer über dieses Recht auf welcher virtuellen Maschine verfügt.



## 8MAN APPLICATION INTEGRATION

Ermöglicht die automatisierte Zusammenarbeit mit anderen Applikationen in Ihrer Softwarelandschaft.



8MATE  
Matrix42

Der 8MATE Matrix42 verknüpft 8MAN mit der IT Service Management Lösung Matrix42. In der von der Futuredata GmbH entwickelten Lösung bestellen Mitarbeiter im Self Service Portal von Matrix42 Fileserver-Berechtigungen.

Data Owners bzw. Administratoren prüfen die Bestellung in einem standardisierten Prozess. Bei Bewilligung wird 8MAN automatisch aktiv und erstellt die Berechtigung auf dem Fileserver. Dies erfolgt nach Microsoft Best Practice über Active Directory Gruppen. Der Prozess wird sowohl in Matrix42 als auch vom 8MAN Logbuch automatisch dokumentiert.

**8MAN | Protected Networks GmbH**

Alt-Moabit 73  
10555 Berlin  
Germany

T: +49 30 390 63 45 - 0  
E: [info@8man.com](mailto:info@8man.com)  
W: [www.8man.com](http://www.8man.com)

Distribution by:

 **ectacom**

**PRIANTO**