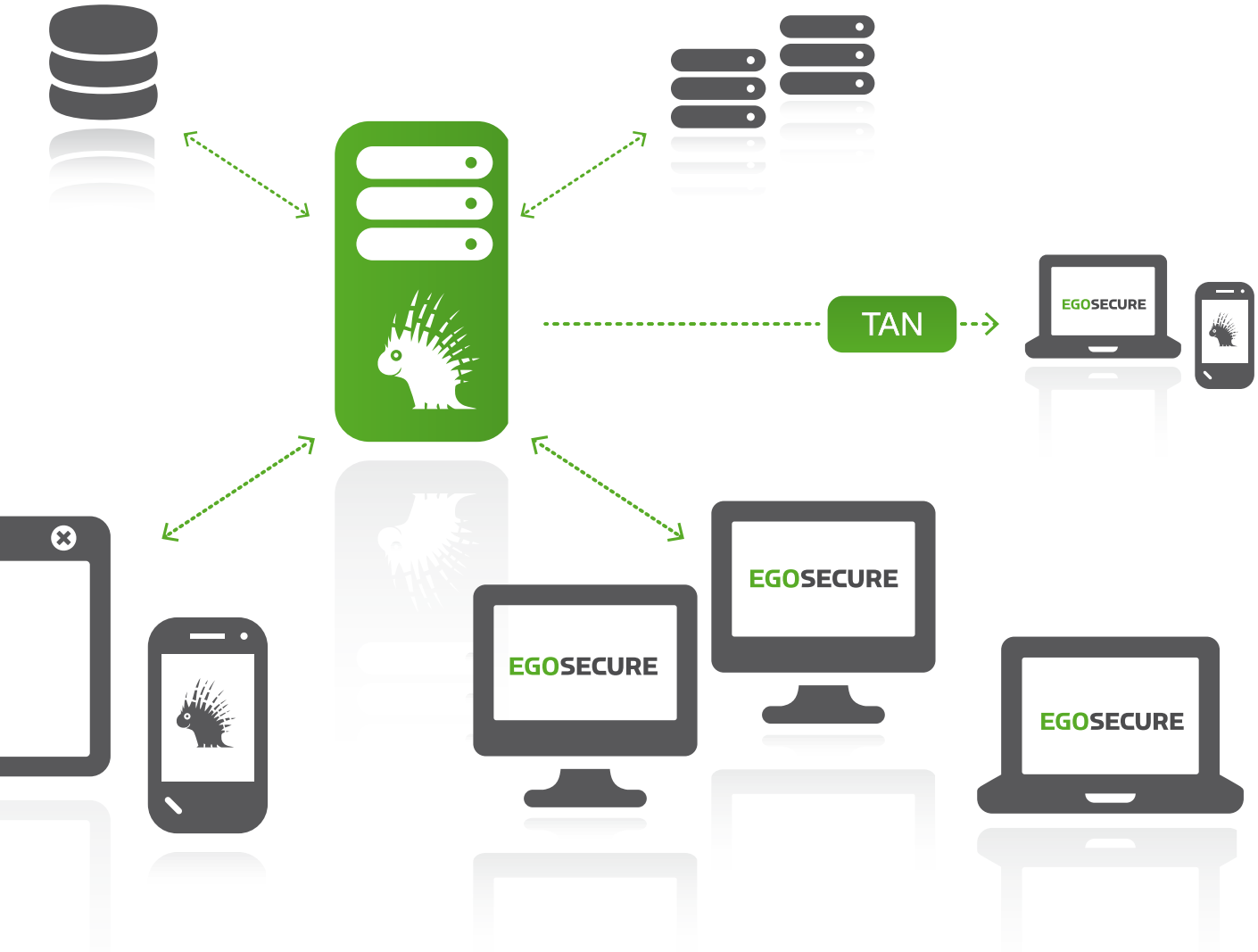
EGOSECURE

WHITEPAPER

EGOSECURE®
ENDPOINT



www.egosecure.com

Die Lösungen der EgoSecure® GmbH ermöglichen höchste IT-Security Standards ohne den Arbeitsfluss des Mitarbeiters zu stören. Sie erfordern keine hohen Verwaltungsaufwände – somit werden Betriebskosten gespart.

Das in allen Branchen bewährte C.A.F.E. (Control, Audit, Filter, Encryption) Management Prinzip sichert alle Schnittstellen an Ihren Endgeräten. Die zentrale Verwaltung ermöglicht somit, dass Datenflüsse der Mitarbeiter gezielt am Arbeitsplatz automatisch im Hintergrund kontrolliert, protokolliert, gefiltert und verschlüsselt werden können.

Dies sind jedoch nicht die einzigen Vorteile der EgoSecure® Lösungen. Weitere Vorteile ergeben sich aus folgenden Aspekten:

Flexible Rechteverwaltung des C.A.F.E. Management Prinzips

Alle Rechte können sowohl benutzer- oder maschinenspezifisch, als auch kombiniert vergeben werden. Vererbungsstrukturen ermöglichen die Übertragung von Gruppenrechten auf Untergruppen und Benutzer, wobei einzelne Benutzer oder Geräte ausgenommen werden können. Berechtigungen können den automatisch synchronisierten Active Directory/ eDirectory bzw. LDAP Organisationseinheiten und Gruppen oder individuell erzeugten Gruppen zugewiesen werden. Das reduziert den Verwaltungsaufwand auf ein Minimum. Darüber hinaus ist es möglich Berechtigungen in Abhängigkeit von Benutzerszenarien zu definieren , so können Benutzer beispielsweise unterschiedliche Online- und Offline-Rechte haben.

Real-Time Management stört nicht den Arbeitsfluss

Die EgoSecure® Client-Server-Architektur basiert auf einer Echtzeit-Lösung. Zur Rechteaktualisierung benötigen Sie keine Gruppenrichtlinien und Schemaerweiterungen, die in der Regel einen Neustart, eine Neuanmeldung oder ‚Group Policy Updates' erfordern. Organisationen, welche auf unterbrechungsfreie Prozesse, in Produktionsstraßen oder ähnlichem angewiesen sind, haben beispielsweise nicht die Möglichkeit einer Neuanmeldung oder gar eines Neustarts. Die Arbeitsplätze bleiben somit von den Änderungen der Gruppenrichtlinien ausgenommen und stellen damit ein Sicherheitsrisiko dar. Zudem ist es der IT-Administration nicht möglich die Richtlinien des IT-Managements produktiv umzusetzen.

Minimale Netzwerklast

Sämtliche Änderungen, die der Administrator in der zentralen Managementkonsole vornimmt, werden in Echtzeit über Push und Pull realisiert. Andere Lösungen, welche ‚Polling Intervalle' (zyklische Abfragen der Clients an den Server) zur Basis haben, verursachen unnötige Netzwerklast, aus welcher Datenkollisionen resultieren, die den Arbeitsalltag deutlich beeinträchtigen können.

Minimale Systemvoraussetzungen

Abgesehen von der SQL Server Datenbank (die kostenlose Express Version ist ausreichend) wird keine weitere Software (wie z.B. IIS-Server oder .Net-Client) benötigt. Es werden somit keine neuen Sicherheitslücken, durch die Installation zusätzlicher Backendsoftware geschaffen und Arbeitsspeicher-, sowie CPU-Last werden nicht unnötig verschwendet.

Support für Rechner außerhalb vom Netzwerk

Rechner außerhalb des Firmennetzwerkes können auch ohne VPN Anbindung verwaltet werden. Mit Freischaltcodes (sicheres TAN-Verfahren) sind Benutzerrechte temporär oder permanent änderbar. Mit CryptionMobile können Daten auf mobilen Geräten überall und jederzeit ver- und entschlüsselt werden, ohne dass der EgoSecure® Agent installiert sein muss und ohne eine Spur auf dem Client-System zu hinterlassen.

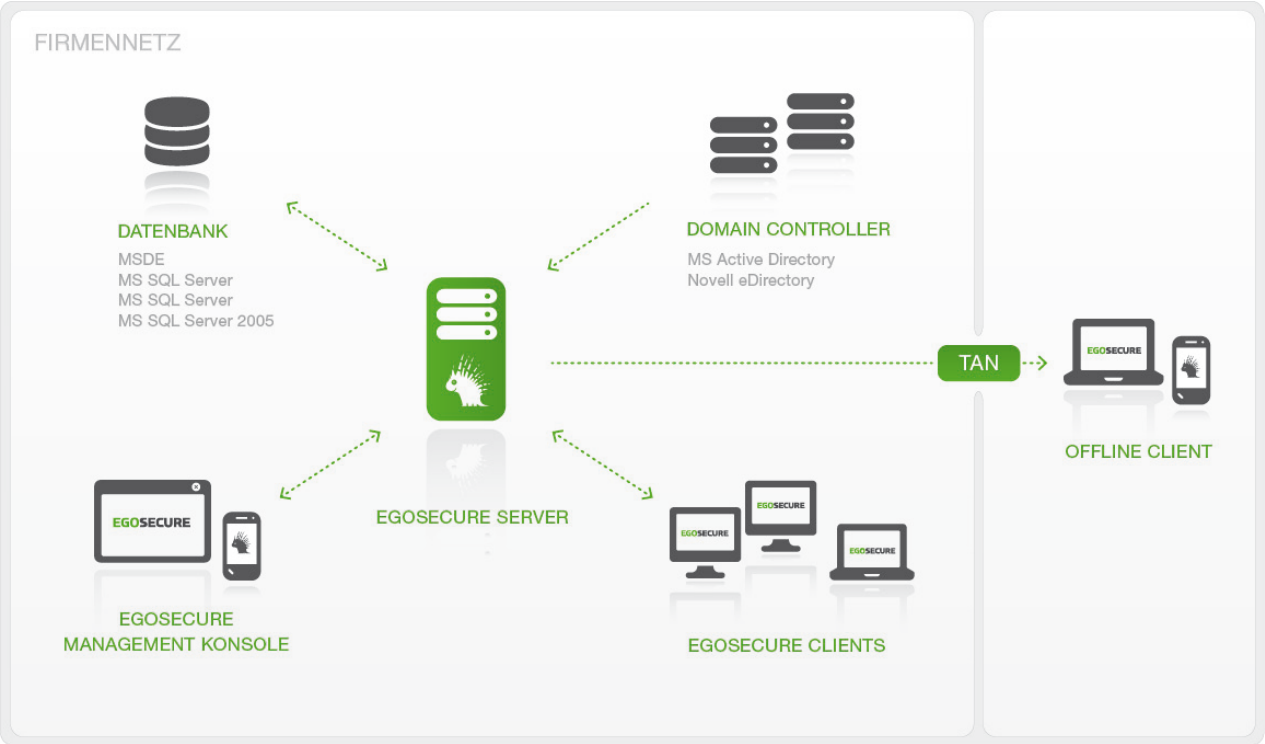
Kerneltreibertechnologie ermöglicht hohe Manipulationssicherheit

Die ‚EgoSecure® Kerneltreibertechnologie', welche sich während der Bootphase ins Betriebssystem lädt, ist ein zusätzlicher Garant, dass der Agentendienst auf dem Client immer aktiv ist. Des Weiteren können nur autorisierte Administratoren den Clientdienst deinstallieren oder stoppen.

Flexibilität durch Integrationsmöglichkeit in Drittanwendungen

Die XML-Schnittstelle ermöglicht eine automatische Rechteverwaltung direkt aus vorhandenen Drittanwendungen wie z.B. Helpdesk-Lösungen heraus, so dass existierende Prozesse, Genehmigungsverfahren, Benachrichtigungen und Berichte verwendet werden können, ohne dass die Support-Mitarbeiter eine zweite Konsole öffnen müssen.

EGOSECURE® ARCHITEKTUR



Zentraler Server und sichere Datenablage

Der EgoSecure® Server ist für die zentrale Verwaltung Ihrer Clients verantwortlich. Sie können diesen auf einem beliebigen Rechner in Ihrem Netzwerk installieren. In großen Umgebungen, oder um eine Ausfallsicherung zu haben, kann die Software auf zwei oder mehreren sich gegenseitig replizierenden Servern installiert werden.

Alle Datensätze und wichtigen Konfigurationen werden in einer SQL Datenbank (MSDE, alle Microsoft SQL Server Versionen, sowie MySQL ab Version 5) vom EgoSecure® Server verwaltet. Somit können Sie durch Sicherung der Datenbank eine hohe Ausfallsicherheit mit minimalem Backupaufwand erreichen.

Einfache Installation und Aktualisierung des EgoSecure® Agenten

In der EgoSecure® Managementkonsole können Sie ein MSI-Paket erstellen und mit den üblichen Softwareverteilungsmechanismen oder über AD Gruppenrichtlinien verteilen. Bereits installierte Agenten werden je nach Einstellung automatisch vom EgoSecure® Server oder manuell über die Managementkonsole aktualisiert.

Sichere und effiziente Kommunikation

Die Kommunikation zwischen Server und Clients erfolgt über XML – RPS (optional auch verschlüsselt). Sämtliche Passwörter und Verschlüsselungs-Keys werden ausnahmslos verschlüsselt übertragen (RSA 1024 Bit).

Die EgoSecure® Agenten kommunizieren über ein Push & Pull Verfahren mit dem Server und holen sich bei Bedarf sofort alle Änderungen ab. Es findet keinerlei Polling statt, was die Auslastung Ihres Netzes deutlich reduziert. Nur die Rechner der Benutzer, deren Rechte geändert werden und online sind werden angesprochen und holen die Veränderungen ab. Ist ein Rechner nicht im Netzwerk, so können Rechteänderungen über eine TAN mitgeteilt werden. Diese Kommunikation innerhalb des Netzwerks läuft über frei definierbare Ports.

Verwaltung von Gruppen, Benutzer und Rechner

Die Verzeichnisdienststruktur Ihrer bereits vorhandenen MS Active Directory, Novell eDirectory oder LDAP Infrastruktur wird vom EgoSecure® Server ausgelesen und in der SQL Datenbank gespeichert. Es finden weder Schemaerweiterungen Ihres Directorys statt, noch werden Informationen in dieses geschrieben. EgoSecure® erstellt lediglich eine Kopie der Struktur, die danach bei Bedarf regelmäßig aktualisiert wird. Dafür wird ein Benutzer benötigt, der lediglich Leserechte besitzt – nicht mehr.

Sichere Rechteverwaltung

Zugriffsrechte auf externe Geräte und Anwendungen werden über den Kerneltreiber kontrolliert. Rechteänderungen für Benutzer oder Systeme, die nicht mit dem Netzwerk verbunden sind können über ein TAN-Verfahren zugewiesen werden.

FUNKTIONSÜBERSICHT

Architektur

- Sichere Kerneltreibertechnologie
- MS AD, NDS, LDAP, Workgroup Synchronisation
- Bidirektionale Kommunikation (Push & Pull)

Rechteverwaltung

- Gruppen-/ Benutzer-/ Rechnerspezifische Rechtevergabe
- Automatische, temporäre und zeitgesteuerte Rechtevergabe

Management Konsole & Agent

- Multilinguale, intuitive Oberfläche
- Rollen- und zuständigkeitsabhängige Oberfläche
- Offline Unterstützung (intelligentCache und TAN)
- Revisionssichere Protokolle (SOX, Basel II)
- Reports und Analysen
- Anmelden als (u.a. Vorteil für Produktionsstraßen)
- Ticketsystem für Änderungswünsche
- MSI-Packager für x32 und x64

Control

- Geräte Whitelist (Zertifizierung)
- Spezifische Freigabe einzelner Geräte nach Seriennummer, HardwareID, VolumeID oder Name
- Automatische Geräteerkennung
- Individuelle Freigabe von Medien (CD/DVD) nach Hashwert
- Geräte in Read-only-Modus versetzen
- WiFi bzw. HotSpot Kontrollen

Filtering

- Content Header Filter für Dateitypen
- Filterung nach unterschiedlichen Kriterien wie Dateiname und Dateigröße

Auditing

- Passwort-geschützte Protokollierung des Datentransfers (betriebsratskonform)
- Protokollierung von Datentransfer auf externe Datenträger, CD/DVD, Netzwerkverzeichnisse
- Protokollierung von Benutzeraktivitäten wie gesperrte Zugriffe, Zugriffstatistiken oder unverschlüsselter Datentransfer

Encryption

- Dateibasierte, transparente Verschlüsselung
- Automatisierte On-The-Fly-Verschlüsselung
- U.a. AES256 und TripleDES192 Verschlüsselung
- Zentrale Schlüsselverwaltung und Wiederherstellung
- Blacklist/Whitelist für Geräte
- Mobiler Client zur Ver-/Entschlüsselung an Fremdrechnern (ohne Installation)
- Zentrale Vergabe von Passwortrichtlinien für mobile Clients an Fremdrechnern

Managament

- Application Management
  - Anwendungskontrolle nach Black-/Whitelistverfahren
  - Lernmodus (manuell oder zeitgesteuert)
  - Freie Programmpaketdefinition
  - Rechtevergabe über Anwenderrollen
  - Temporärer Non-Blocking-Mode
  - Anwendungsprotokollierung
  - Zentrale Versionskontrolle
  - Automatisierte Hashwertermittlung von Anwendungen

- Power Management
  - Intelligente Verwaltung des Rechnerzustands Hibernate , StandBy usw.
  - Zustandsabhängiges Abschalten und Steuern von Monitoren, USB Geräten, Festplatten, Lüfter, CPU, etc.
  - Alarmfunktion bei verdächtigen Aktivitäten
  - Flexible, individuelle Leerlaufdefinition nach unterschiedlichen Kriterien
  - Intelligente Ausnahmenregelung – nach Zustand des Rechners, ausgeführten Programmen oder Netzwerkaktivitäten
  - Scheduler mit mehreren einstellbaren Aktionen
  - Zentrales Management und Reporting - Ersparnisrechner in Euro, KWh und CO2 Ausstoß für die Gesamtfirma, OU, Gruppe oder Benutzer

- Data Destruction Management
  - Vielfältige Löschmethoden wie einfaches Überschreiben, zufällige Reihenfolge oder Peter Gutmann Methode
  - Optimierung der Löschgeschwindigkeit
  - Unterstützung von internen und externen Speichermedien
  - Sicheres Löschen von Dateien, Schattenkopien, Verzeichnissen und Laufwerken
  - Zeitplangesteuertes Löschen von bestimmten Verzeichnissen wie TEMP, Papierkorb usw.
  - Reporting Analyse sowie revisionssichere Protokolle
  - End of Life Management

FEATURE HIGHLIGHTS

Intuitive Management Konsole

Die zentrale, benutzerfreundliche Verwaltungsoberfläche ist selbsterklärend und der Schulungsaufwand dadurch minimal. Die klare und durchdachte Struktur ermöglicht es, mit wenigen Mausklicks komplexe Einstellungen vorzunehmen. Die Managementkonsole und der auf dem Client installierte Agent stehen in verschiedenen Sprachen zur Verfügung.

Helpdesk Unterstützung

Änderungswünsche der Benutzer werden über ein Ticketsystem erfasst und können aus dem Ticket heraus umgesetzt werden. Alternativ können Tickets per Email an Helpdesk-Lösungen anderer Hersteller weitergeleitet werden.

Übersichtliche Auswertungen, Protokolle und Berichte

Informationen über Rechtevergabe, Zugriffskontrolle, gesperrte Zugriffe u.v.m. können ausgewertet, analysiert und exportiert werden.

Flexible Gerätefreigabe

Sowohl die Freigabe von Gerätearten, Gerätetypen oder individuellen Geräten mit Seriennummer ist möglich. So können Sie die Verwendung firmeninterner Geräte erlauben ohne Kompromisse bei der Sicherheit einzugehen.

Content Header Filter

Zusätzlich zu Geräten, können Sie die Datenübertragung abhängig von Dateitypen freischalten oder ausschließen. So verhindern Sie das Kopieren betriebsinterner Daten bzw. Datenmengen auf externe Massenspeicher und damit deren möglichen Missbrauch oder Verlust.

Vollständige Protokollierung

Passwortgeschützte, detaillierte Zugriffsprotokollierung mit Filter- und Sortierfunktionen. Bei Verdacht auf Datenmissbrauch können Sie einsehen, wer auf welche Dateien zugegriffen hat, wobei das betriebsratskonforme Vier-Augen-Prinzip umgesetzt wurde. Auch alle Aktionen des Administrators werden vollständig protokolliert.

LDAP Integration

Bereits vorhandene Benutzer- und Gruppendefinitionen im Microsoft Active Directory, LDAP oder Novell eDirectory werden in die Managementkonsole synchronisiert. So vermeiden Sie doppelten Arbeitsaufwand bei der Definition von Benutzern und Gruppen für die Zugriffskontrolllisten und reduzieren den Konfigurations- und Pflegeaufwand.

Verteilte Umgebungen

Mehrere sich gegenseitig replizierende Server, für das Load Balancing in Enterprise Umgebungen.

EGOSECURE

Pforzheimer Str. 134
76275 Ettlingen/Germany

Phone +49(0)7243.354.95-0
Mail contact@egosecure.com

www.egosecure.com