"Standard Endpoint Security - Protection" Feature Overview

Endpoint Security powered by **EGOSECURE**

This document provides an overview about the "Standard Endpoint Security - Protection" powered by EgoSecure
Data Loss Protection, Encryption

According to "Basic Endpoint Security - Compliance"	
Access Control	✓*
Secure Audit	✓*
Application Control	✓*
Removable Device Encryption	✓*

Local Folder Encryption	
Automatic (and transparent to the user) encryption of file transfer in encrypted folder	✓
Automatic decryption of data during read operations of encryted folder	✓
Centralized report view of encrypted folders	✓
Decryption by Master Key	✓
Different encryption types: Company Key, Group Key, Private Key	✓
Distinction between enforced encryption and selectable user-level encryption.	✓
No external CA or PKI needed	✓
Support of TripleDES 192 and AES 256 bit encryption	✓
The folder does not need to be prepared before the first initial encryption	✓
Users can receive notifications of access by processes and applications to encrypted folders	✓
User-based approval of access by processes and applications to encrypted files	✓
Client side logging of access to files in encrypted folders	✓
Optional: Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓

Cloud Encryption	
Support of OneDrive, GoogleDrive, Dropbox, MagentaCloud, NextCloud, OwnCloud, etc.	✓
Decryption by Master Key	✓
Encryption/Decryption on Android devices	✓
Encryption/Decryption on iOS devices	✓
Encryption/Decryption on MacOS	✓
Different encryption types: Company Key, Group Key, Private Key	✓
Distinction between enforced encryption and selectable user-level encryption.	✓
No external CA or PKI needed	✓
Portable application for decryption by password or PKI	✓
Possibility to store differently encrypted and unencrypted files on the same cloud storage	✓
Support of TripleDES 192 and AES 256 bit encryption	✓
The cloud storage does not need to be prepared before the first encryption	✓
No cloud-API's needed	✓
Optional: Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓

Network Share Encryption	
Automatic (and transparent to the user) encryption of file transfer in network folders	✓
Automatic decryption of data during read operations of encryted network folders	✓
Centralized report view of encrypted folders	✓
Client-based en- and decryption of files in encrypted folders	✓
Decryption by Master Key	✓
Different encryption types: Company Key, Group Key, Private Key	✓
Distinction between enforced encryption and selectable user-level encryption.	✓
Network Share does not need to be prepared before the first initial encryption	✓
No external CA or PKI needed	✓
No file-server restrictions	✓
Optional: Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓
Support of TripleDES 192 and AES 256 bit encryption	✓

ADMINISTRATOR UI	
Multi-Language support for console and client component	✓
Multi-level predefined granular administrator roles and access permissions	✓
Customizable Client Messages	✓
Console layout editor	✓
Detailed reports	✓

Permanent Encryption	
Different encryption types: Company Key, Group Key, Private Key	✓
Distinction between enforced encryption and selectable user-level encryption.	✓
Encrypted files remain encrypted during the transfer to other data carriers	✓
Encrypted files can be copied into an e-mail attachment or web-based upload	✓
Encrypts files, no matter on which data carriers they are stored	✓
No external CA or PKI needed	✓
Portable application for decryption by password or PKI	✓
Support of TripleDES 192 and AES 256 bit encryption	✓
The disk does not need to be prepared before the first initial encryption	✓
Decryption by Master Key	✓
Encryption/Decryption on Android devices	✓
Encryption/Decryption on iOS devices	✓
Encryption/Decryption on MacOS	✓
Optional: Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓

Full Disk Encryption (FDE)	
FIPS-140-2 certified cryptographic Module	✓
Algorithms like DESX, AES 256 and Blowfish 448	✓
Hard- or software based encryption	✓
TPM support	✓
UEFI support	✓
Password protected Emergency-Recovery-Information file	✓
Centralized, script-based and wizzard based installation, initialization and uninstallation	✓
HDD, SSD, nvme supported	✓
Hardware-independent Full Disk Encryption	✓
WinPE disaster recovery application	✓

PreBoot Authentication (PBA)	
Multi User Support	✓
Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓
PBA is available as a Linux kernel (BIOS) or UEFI PBA (Simple PBA)	✓
HelpDesk Function for unlocking locked systems by challenge-response method	✓
Automated user-capturing mode	✓
Friendly-Network-Support	✓
Single-Sign-On for windows authentication	✓
Timeout or complete blocking after wrong authentications	✓
Customizable screen background	✓
Multi-language support	✓
Touch-screen support	✓
Virtual keyboard support	✓

Infrastructure, further information and system requirements	
Audit security according to Basel II, Sarbanes Oxley, PCI	✓
Export/ Import of encryption key's	✓
Fast user change to client component (no Windows logout needed)	✓
Intelligent push & pull or polling method for client-server communication	✓
Multi-Domain, Multi-tenancy and Managed-Services-Provider model supported	✓
Master Password	✓
Only one management interface, one sql database, one client component needed	✓
Synchronisation of existing AD, NDS, oLDAP (read-only) and own directory	✓
Mail notifications	✓

REMARKS

Contact Matrix42 to get more information for your specific project requirements.

✓* = Further details can be found in "Basic Endpoint Security - Compliance Product Fact Sheet"

** = Further Add-On's can be licensed via request to Matrix42 sales department

COMPATIBLE TO FOLLOWING OPTIONS OF MANAGEMENT SERVER CONFIGURATION

Windows 2008 R2 SP1 and higher

Separate, existing Microsoft SQL 2008 R2 /2012 and higher, Standard Edition and higher/ MySQL 5 and higher

Management Server: 64 Bit Quad Core CPU, 2.66 GHz Xeon or faster, 8 GB RAM, 80 GB disk space, 1 GB network interface card

Virtual Machine Support: VMware ESXi, Microsoft Hyper V

Customer specific design will be finalized during project implementation phase