"Enterprise Endpoint Security - Prevention" Feature Overview

Endpoint Security
powered by
EGOSECURE

This document provides an overview about the "Enterprise Endpoint Security - Prevention" powered by EgoSecure
Malware Protection & Prevention | Analysis & Analytics

According to "Standard Endpoint Security - Protection"

Access Control	✓*
Secure Audit	✓*
Application Control	✓*
Removable Device Encryption	✓*
Local Folder Encryption	✓*
Cloud Encryption	✓*
Network Share Encryption	✓*
Permanent Encryption	✓*
Full Disk Encryption (FDE)	✓*
PreBoot Authentication (PBA)	✓*

Insight Analysis

Determines the status quo of the data security	✓
Automatically visualized in meaningful dashboards	✓
Conclusions on the activities of individual users anonymized possible	✓
Monitors access to:	
Removable Disk/ CD/DVD, Mobile Devices	✓
Unauthorized access	✓
Network directories	✓
Unencrypted file access	✓
Data traffic on http / https	✓
Execution and usage of applications	✓
Antivirus activities and results	✓
Protected access to user / computer informationby the 4-6-eye principle	✓
Automated customizable reporting and emailing	✓
Drill-In functionaltiy and customizable view profiles	✓
Connectors to other modules and solutions	✓

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	✓

IntellAct Automation

Automatically protective measures based on predefined rules	✓
Statistics of incidents (on each ruleset)	✓
Global summaries in Insight Analysis	✓
Evaluates the data of Insight Audit and/ or Insight Analysis	✓
Anonymously detection of user behavior default values (machine-based learning)	✓
Custom analysis rules for:	
Usage of Removable Disk/ CD/DVD, Mobile Devices	✓
Unauthorized access	✓
File Traffic on Network Shares	✓
Unencrypted file access	✓
Data traffic on http / https	✓
Execution and usage of blocked applications	✓
Antivirus activities and results	✓
Automate protective measures:	
E-Mail notification	✓
SNMP notification	✓
Time locking of devices and interfaces	✓
Non-Compliant Notification to NAC Solutions	✓
Turn off the computer	✓
Show user message	✓

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

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

Matrix42 AG | Elbinger Str. 7 | 60487 Frankfurt | Germany | www.matrix42.com