Fact Sheet

MATRIX42

EgoSecure Data Protection

Functions

Access Control

- Control and governance of access to external devices and client environment interfaces
- Access permission to cloud services
- Control of all data transmission paths
- Control of network connections (e.g. WLAN, anti-bridging, USB network adapters)
- BadUSB protective measures
- File filter for blocking certain data formats
- Whitelisting of external devices
- Revision security according to Basel II, Sarbanes-Oxley, PCI conformity

Application Control

- Black- and whitelisting of applications, Java applets and DLL files
- End-user invisible control over which programs can be started
- Protection against execution of unwanted applications, e.g. insufficiently licensed applications, key generators and pirated copies
- Supports the prevention of malware outbreaks through blocking
- Simulation mode (demo mode)

Secure Audit

- Verification of all traffic to and from each endpoint in real time
- Traceability of the data flow according to EU-DSGVO article 30, 33
- Protection against misuse and anonymization of audit data (according to personnel/works council conformity)

Insight Analysis

- Monitoring of all data movements in the corporate network
- Collects facts about the data protection situation in the network
- Visualization of all data protection-relevant processes in a clear dashboard
- Cumulative display of results (user data is anonymized)
- Automated reporting and email delivery

IntellAct Automation

- Evaluates data from Insight Analysis and Secure Audit and triggers pre-defined protection measures based on a set of rules
- Possibility of comparison with normal values to automatically detect anomalies or critical situations and trigger protective reaction
- Integration with Matrix42 Workflow Studio

Encryption

- Transparent on-the-fly encryption (without loss of productivity)
- Encryption types: general, group encryption, individual encryption, unencrypted
- Encryption algorithms: AES-256 or Triple DES-192 (again encrypted with up to RSA-4096)
- Protection of personal data according to EU-DSGVO article 32
- Decryption and encryption via agent, depending on defined company policies e.g. decryption only possible if the file is located on the company device
- Extensive policy model

Cloud and Network-Share

- Encryption of folders and files in cloud storage (e.g. OneDrive, GoogleDrive, Dropbox) or on any network share
- Encryption keys are never stored in the cloud or on the network share at any time

Local Folder

- Protection of dedicated files and folder structures
- Targeted authorization for individual persons, even when sharing devices
- Reliable protection of sensitive data also towards employees with admin rights - e.g. IT employees

Removable Device

- File-level encryption
- Encrypts data on mobile data carriers, such as USB sticks, external hard disks, etc.
- Unlimited data size, e.g. also encryption of terabyte large disks

Full Disk Encryption (FDE)

- Encryption of the entire hard disk
- Encryption algorithms: AES-256, Triple DES-192 or BlowFish-448
- Windows 10 build upgrade support
- Password protected emergency recovery file for recovery of inaccessible hard disks

Preboot Authentication (PBA)

- Operating systems can only be started after executing the Preboot Authentication (PBA).
- Support of EgoSecure Full Disk Encryption; as well as Microsoft BitLocker
- Multi-User/Multi-Smartcard support
- challenge response
- Linux-based, BIOS-based and UE-FI-based

Permanent Encryption

- Persistent encryption of files on any data carrier
- Access to files is only possible for authorized users. Decryption at the target device via password entry, PKI token or EgoSecure agent.
- Encryption status remains independent of the target disk
- Generates an encrypted data package that can be sent as an e-mail attachment or made available via a web upload

Modules and add-ons available for purchase

Data Loss & Leakage Prevention

- Protect against theft and unauthorized disclosure of highly sensitive data with pre-defined search patterns, whether on the endpoint, external devices, in the cloud or on the file server
- Predefined, common search patterns for national & international number codes like insurance numbers, password IDs, IBAN & Swift, credit card numbers etc.
- Blocks the use of data or performs actions such as moving files to a secure location/ quarantine or deleting them
- Detailed logging of finds
- Global, group-specific or individual rule assignment

Automated Endpoint Detection & Response with Post-Infection Protection

- Blocks malware outbreaks at kernel level in real time
- Reduces the time from infestation to neutralization through automation (dwell-time)
- Generates a single alert for each incident, reducing the number of alerts to a minimum
- Detects any non legitimate communicating application and blocks real-time data communication
- Analysis function which uses collected data to proactively detect and prevent attacks as well as root cause analysis (threat hunting)

NextGen Antivirus

- Virus protection against known and unknown threats
- Proven high detection rate
- Detects even advanced malware through certified Next Generation Antivirus (NGAV) and Application Communication Control