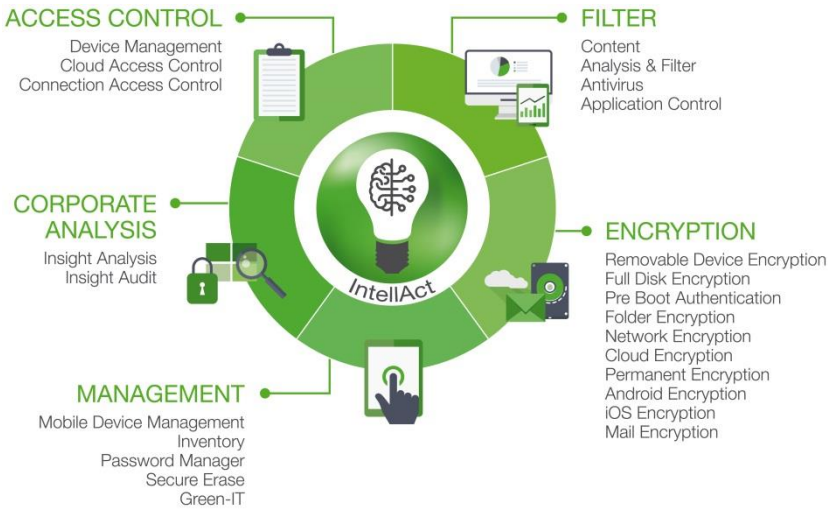
EGOSECURE FUNCTIONS



INTELLACT

The new IntellAct module analyses the facts from Insight and automatically activates protective measures based on pre-defined rules. In addition, it can make comparisons with benchmarks, automatically detecting anomalies and critical situations so that an appropriate response is triggered to protect an organization's data. This automation greatly facilitates the work of administrators and minimizes reaction times considerably..

CORPORATE ANALYSIS

INSIGHT ANALYSIS

To make sure that protective measures are implemented optimally, the INSIGHT module first determines the user's overall safety situation in the corporate network. The results of this analysis are then processed according to management needs and shown in graphs and tables. Thus INSIGHT provides the facts to show an overall picture of the data security for every business and organization. The display is cumulative, so that conclusions about the activities of individual users are not possible. The data shown this way are optimal to specifically establish the protective measures that are really needed.

INSIGHT AUDIT

Audit makes the data flow visible in detail, showing potential weaknesses in the security settings. It therefore allows the determination of forensic information. The ability to generate this information is an important contribution to IT compliance and matches with laws and industry regulations. The Federal Data Protection Act, for example, specifies a logging as mandatory. At the same time EgoSecure INSIGHT Audit makes the violation of the privacy rights of employees impossible, since the access to logging data is protected by a 4 or 6 eye principle..

ACCESS CONTROL

DEVICE MANAGEMENT

Device management allows a clear definition of who can use which devices (e.g. USB sticks, CDs, TV tuner) or interfaces (e.g. WLAN, Firewire, USB) and to what extent. Thus, all of these devices can be used without causing abuse or risking the loss of data. It also prevents malware of getting into the corporate network via these interfaces. Device Management offers effective protection against "attackers from inside".

CLOUD ACCESS CONTROL

The use of the cloud has many advantages in terms of flexibility of labour, because data can be accessed anywhere. Particularly sensitive data, however, should not be saved in the cloud and some data types may not even be allowed by law to be saved. Especially in so-called third countries. Cloud Access Control checks which employee is allowed to use which cloud services to which extent..

CONNECTION ACCESS CONTROL

Data transfers are nowadays, in addition to the official channels via the corporate network, possible through many ways - Bluetooth, WiFi, modem, etc. However, a company should control via which routes data leave the company. Connection Access Control checks which employee has access to which data transmission devices.

CONTENT ANALYSIS & FILTER

Analyzing content and filtering secret information from data that leave the company as well as blocking unacceptable information within incoming data are also components of an integrated, overall security concept. Content Analysis & Filter provides granular and reliable protection for corporate data communications without affecting users‘ workflows and desired data transfers.

ANTIVIRUS

An antivirus solution provides proven protection against anonymous attackers from the Internet. It is important to ensure a high detection rate to be able to respond very quickly to new viruses and Trojans. EGOSECURE DATA PROTECTION provides an integrated antivirus solution which, according to many test reports, is the leading solution in the market and features an acknowledged high detection rate.

APPLICATION CONTROL

Application Control controls which user is allowed to start which programs. This prevents, for instance, that games or unlicensed software products are used to avoid liability risks and economic damage. It is also possible to block most viruses, even before antivirus solutions have detected them.

ENCRYPTION

REMOVABLE DEVICE ENCRYPTION

Mobile data media such as USB sticks get increasingly smaller and powerful; however, this also means that they can get lost or stolen much more easily. Removable Device Encryption ensures that the data cannot be used by unauthorized parties. Password-based encryption and decryption can be done on any Windows computer, with full transparency for authorized users. Encryption is file-based and multiple kinds of encryption are available and can be used simultaneously on one medium.

FULL DISK ENCRYPTION

Full Disk Encryption provides comprehensive protection of all devices and encrypts the complete hard disk or partitions on the sector level. The solution also provides on-demand pre-boot authentication to authenticate users before the operating system is started. Automatic detection of new hard disks in the integrated encryption chip, lightning-fast initial encryption and the centralized management ensure the seamless integration with existing IT infrastructures.

PRE BOOT AUTHENTICATION

Pre Boot Authentication ensures that registration at Windows and related encryptions, such as the disk encryption, cannot be manipulated and circumvented by converting the hard drives, starting of USB / CD or the replacement of the operating system. The registration to the corresponding terminal will thereby take place immediately after the BIOS loading process, but before the start of the operating system. Besides passwords also many smart cards are supported as login security. Enterprise features such as help desk, self-initialization and more, are also available. Login screens can be customized to each customer.

FOLDER ENCRYPTION

Folder Encryption protects data on lost notebooks or hard drives and also individually defined sensitive data on systems that can be accessed by several users. For instance, highly sensitive management data can be protected against access through employees with many privileges, such as IT staff.

CLOUD/NETWORK ENCRYPTION

Cloud and Network Encryption can be used to encrypt folders in the cloud or on any network. Encryption keys remain within the company and are never stored in the cloud – a clear advantage over encryption solutions provided by cloud storage providers themselves.

PERMANENT ENCRYPTION

Permanent Encryption encrypts files, no matter on which data carriers they are stored. These encrypted data packets also remain encrypted during the transfer to other data carriers. Thus, an encrypted file can be copied into an e-mail attachment or uploaded to a web-based cloud while being permanently encrypted. On external computers and mobile devices, the file can be opened by entering a password or by using a PKI token.

ANDROID/IOS ENCRYPTION

The transparent “on-the-fly“ encryption for iOS and Android devices offers file-based protection on internal storages and memory cards and cloud accounts of mobile devices via app. Files are decrypted by entering a password.

MAIL ENCRYPTION

Mail Encryption ensures the safe exchange of e-mails; no software needs to be installed for this purpose on the receiving or transmitting system. Encrypted e-mails with an electronic signature can be sent and read within the user‘s familiar environment. It is also easy to encrypt and transport very large e-mails.

MANAGEMENT

MOBILE DEVICE MANAGMENT

The increasing degree of adoption of mobile devices such as tablets or smartphones must also be reflected in corporate security architectures. Mobile Device Management ensures the intelligent integration of mobile devices, including support of the Android and iOS operating systems.

INVENTORY

With INVENTORY can be seen which hardware and software products are installed on the computers in the corporate network. However, the functions in INVENTORY that allow to see changes and to analyze those and also to be alerted if something changes, are much more important. The condition of the hardware can be displayed and reliably indicate any problems.

PASSWORT MANAGER

Employees no longer have to write down their passwords and logins on Post-It's or in files - this task is now taken over by the secure Password Manager. Even when creating complex passwords, the password manager can support through an intelligent process. It is also possible to exchange logon information with colleagues by storing the protected Password Manager files in the network..

SECURE ERASE

Secure Erase ensures that deleted files cannot be restored, no matter if they are located on the internal hard disk or on an external storage medium. Users can choose among multiple deletion methods. They have the option to securely delete documents immediately or to destroy all deleted files irrevocably, based on a specific schedule. Secure Erase also ensures that you discard hardware only when you sell or withdraw respective hardware.

GREEN-IT

Intelligent power management ensures efficient device operations by only consuming energy when the computer is actually used. Green-IT helps reduce IT operational costs while also contributing to the company’s environmental balance and ensuring a fast ROI for the EGOSECURE DATA PROTECTION implementation.