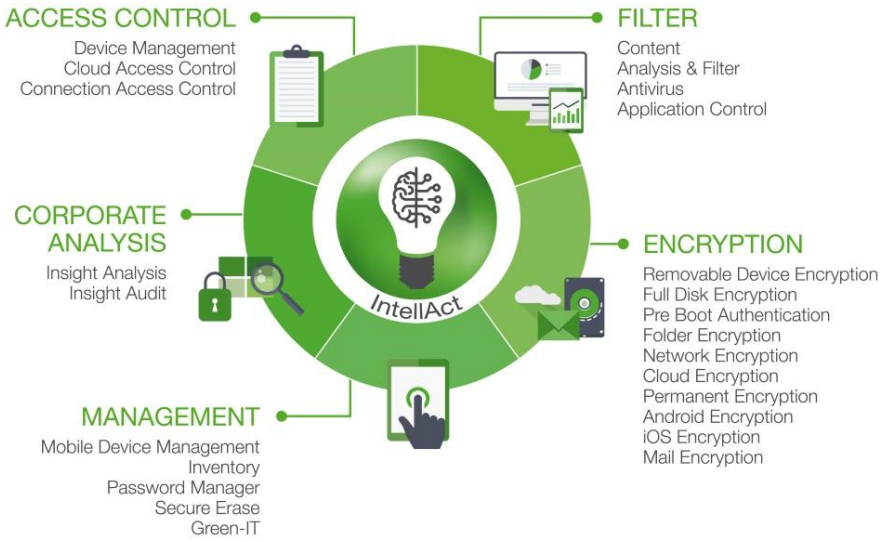
EGOSECURE - Module and Product Overview



INTELLACT

The new IntellAct module analyses the data 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 organisation's data. This automation greatly facilitates the work of administrators and minimises reaction times considerably.

CORPORATE ANALYSIS

INSIGHT ANALYSIS

INSIGHT Analysis provides factual data showing the overall picture of the data security situation for any organisation.
The Analysis module first determines the user's overall safety situation in the corporate network. The results of this analysis are processed according to management needs, then displayed in graphs and tables. Displaying the data in this simplified way means that management can easily see what protective measures need to be taken.

INSIGHT AUDIT

Audit gives a detailed view of the data flow that identifies potential weaknesses in the current security settings, thus enabling forensic examination. The ability to generate this information is an important contribution to IT compliance and adherence to laws and industry regulations.
As an example, **GDPR** specifies logging as being mandatory. EgoSecure INSIGHT Audit makes the violation of the privacy rights of employees impossible, since the access to logging data is protected by a default 4, or 6 eye principle - which can be fine-tuned for individual nation states' data privacy laws.

ACCESS CONTROL

DEVICE MANAGEMENT

Device management allows a clear definition of who can use which devices (e.g. USB sticks, CDs, etc), or interfaces (e.g. WLAN, Firewire, USB, etc.) and to what extent. Therefore, all these devices and interfaces can be used without risking data loss. It also prevents malware infiltrating the corporate network via these routes.
Device Management therefore offers effective protection against 'insider attacks.'

CLOUD ACCESS CONTROL

The Cloud has many advantages for flexible working because data can be accessed anywhere. However, caution has to be exercised when sensitive data is saved in the cloud - some data types may not even be allowed by law to be saved in the cloud. Cloud Access Control checks which employee is allowed to use which cloud services and to what extent, employing protective controls to ensure compliance.

CONNECTION ACCESS CONTROL

In addition to 'official' communication channels (e.g. the corporate network), data transfer is possible via many other routes - Bluetooth, WiFi, etc.. Any organisation must ALWAYS be in control of which routes data leaves the company perimeter. Connection Access Control checks which employee has access to which data transmission paths and via which devices.

FILTER

CONTENT ANALYSIS & FILTER

Analysing content, filtering secret information from data that leaves the company and blocking unacceptable information within incoming files, are components of an integrated security posture. Content Analysis & Filter provides granular and reliable protection for corporate data communications without affecting user workflows and normal data transfer in the course of their duties.

ANTIVIRUS

An antivirus solution provides proven protection against malware attacks. To ensure a high detection rate, it is important to respond very quickly to new viruses and Trojans and other attack vectors. EGOSECURE DATA PROTECTION provides an integrated antivirus solution, with an acknowledged high detection rate. According to many test reports, it is the leading antivirus solution in the market.

APPLICATION CONTROL

Application Control regulates which user is allowed to start which programs. For example, the use of games or unlicensed software products can be prevented, avoiding liability risks, financial loss and fines resulting from data breach. It also helps to block malware contained therein, even before antivirus solutions have detected them, e.g. stopping outbreaks of Ransomware.

ENCRYPTION

REMOVABLE DEVICE ENCRYPTION

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

FULL DISK ENCRYPTION

Full Disk Encryption provides comprehensive protection of all devices and encrypts the complete hard disk or partitions at the sector level. The solution also provides on-demand pre-boot authentication of users before the operating system is started as well as 2 factor authentication using tokens and/or biometrics. Lightning-fast initial encryption and centralised management ensure seamless integration with existing IT infrastructure and meets FIPS 140-2, the global security standard expected by all users. Support and integration for Bitlocker is also provided.

PRE-BOOT AUTHENTICATION

Pre Boot Authentication ensures that registration at Windows and related encryption 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 of the correct terminal takes place immediately after the BIOS loading process (before the start of the operating system). As well as passwords, smart cards are supported as login security. Enterprise features such as help desk, self-initialisation and more, are also available. Login screens can be customised for each customer.

FOLDER ENCRYPTION

Folder Encryption protects data segments of data. We can encrypt data on notebooks, hard drives and individually defined sensitive data on systems that can be accessed by several users. For instance, highly sensitive management data can be protected against access by employees with high 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, irrespective of data carriers/pathways. These encrypted data packets remain encrypted during the transfer to other data carriers. So, 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. The file is encrypted for life!

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 users familiar environment. It is also easy to encrypt and transport very large e-mails.

MANAGEMENT

MOBILE DEVICE MANAGEMENT

The increasing 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

Inventory identifies which hardware and software products are installed on the computers in the corporate network. The most important benefit is that Inventory allows users and management to be alerted if something changes. The condition of the hardware is clearly displayed, reliably indicating any problems.

PASSWORD MANAGER

Deploying Password Manager means that employees no longer have to write down their passwords and logins in vulnerable formats. Password Manager can support the most complex of passwords. 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, whether 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 can also ensures that there are no accidental data breaches from discarded IT equipment.

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 and the company’s environmental impact.

EGOSECURE UK
Abbey House, 1650 Arlington Business Park
Theale, Reading. Berkshire RG7 4SA

Tel.: +44 (0) 203 876 8310
Web: www.egosecure.co.uk
E-Mail: sales@egosecure.co.uk