e-safe Compliance

GOAL GROUP

e-Safe Compliance

Experts in monitoring user behaviour, data movement and its protection

e-safe Systems

Step 1: Know the unknowns – User Behavior Analytics

The Issue

Organisations are struggling to adapt to today's realities. Both the volume and variety of security attacks are escalating at a time when the underlying infrastructure is moving from a physical environment to one that is virtualized and in the cloud. The focus of external threats and addressing information security via traditional measures - firewalls, email security, SIEM, RBAC - means the internal risks are often ignored and yet have the potential to be extremely damaging. Staff, privileged users, contractors and management, all need access to sensitive or confidential information. e-Safe Compliance delivers visibility around how users are interacting with this information especially if it is moved off approved platforms.

e-Safe Compliance

e-Safe Compliance analyzes the information captured and identifies user-based risks.

- Transfer of unprotected sensitive information out of the company using cloud drives, non-corporate emails, social media, chat applications, external media devices, non-corporate websites, etc.
- Suspicious usage of sensitive information based on change in user behaviour inside / outside of working hours and inside / outside of the company network. Suspicious usage of sensitive information based on comparison of user behaviour against peer group.

e-Safe Compliance's User Behaviour Analytics can be deployed quickly and easily.

The system can be immediately populated with user information from Active Directory. Sensitive information within databases and file servers can be discovered and tagged by server-side components. The flow of sensitive information can be tracked with centrally created rules. These rules include:

- Occurrence of sensitive words and phrases within files, emails, and chat conversations.
- Occurrence of regular expressions including specific values, such as bank account numbers of VIPs.
- Tracking usage of documents via file name expressions or by fingerprinting of document contents.
- Tracking usage of source code specified class, function and variable names

e-Safe Compliance monitors sensitive information usage and user behaviour including:

- Usage of applications including breakdown by user and type of application.
- Usage of websites including the nature of the material being accessed.
- Usage of communication channels, such as email, chat and social media.
- File changes and movement of files to cloud, local, external and shared drives.
- Hardware, software and network configuration changes to PCs.

Step 2: Reduce risk – Encryption and Document Rights Management

The Issue

The insider risk cannot be eliminated unless access to sensitive information and its usage its controlled through encryption and Document Rights Management. To be effective, the protection must apply to all file types and allow users to perform their work without interruption.

e-Safe Compliance

e-Safe Compliance protects files using transparent file-based encryption.

Files encrypted by e-Safe Compliance can be opened normally without the need for passwords and remain secure no matter how they are transferred. Furthermore, e-Safe Compliance encryption works with all file types, such as MS Office, Adobe, CAD-CAM and images - even when devices are offline.

e-Safe Compliance ensures files are protected without information classification rules.

e-Safe Compliance encrypts files either automatically, based on information classification, or when a user simply right-clicks on a document and selects the 'protect' option in the pop-up menu. This avoids the disproportionate effort required to create information classification rules where the volume of sensitive data is low or ad-hoc. e-Safe Compliance tracks encrypted documents throughout their lifecycle from creation to deletion and provides reports of their usage to the relevant department manager so that 'unclassified' sensitive data can be monitored.

e-Safe Compliance's access controls and Document Rights Management protect against insiders.

Information classification rules and authorised end-users define which users can access which files. In addition, the ability to extract sensitive information using copy / paste, printing or screen capture can also be restricted based on the user and information content. e-Safe Compliance applies three levels of document usage restriction:

- Green – Office Use. No restriction on extracting information from the file.
- Yellow – Sensitive. User can extract information but needs to give a reason for doing so.
- Red – Highly Sensitive. User is not allowed to extract information from the file.

Step 3: Protect sensitive information – Secured Third Party Access

✓ The Issue

Traditional information security products only protect access to information while it resides within the organisation's network. However, organisations are required to protect information at all times while also allowing users and partners access to the information on their remote devices.

✓ e-Safe Compliance

e-Safe Compliance allows users to work on sensitive information on their home PC.

The BYOD module creates a business account on the user's PC. Access of sensitive information on the user's PC is restricted to the business account and its usage monitored. Further, new information created within the business account is automatically protected. The use of the business account ensures that the user's own personal information is not captured in the process of protecting and monitoring the use of sensitive information.

e-Safe Compliance allows users to access encrypted documents on mobile devices.

The purpose of the e-Safe Compliance's mobile app is to allow end-users to open files protected via encryption on mobile devices. The app enforces the same access and usage rights as on PCs.

e-Safe Compliance's information sharing module ensures partner companies do not leak sensitive information.

e-Safe Compliance provides a light-weight information sharing module. This module allows users in the partner company to access encrypted files and applies the appropriate document rights to protect the information contained within. The module also tracks the usage of the encrypted documents.

e-Safe Compliance applies visible and invisible watermarking to printed documents.

Printed documents are common source of data leaks. Incorporating watermarks into documents at the time of printing not only acts as a deterrent to users leaking information but also allows companies to track their subsequent usage. If the document is leaked then the user who printed the leaked copy can be identified.

Contact Us

Australia
e-Safe Systems Pty Ltd
Lumley House, Level 14,
309 Kent St,
Sydney 2000,
NSW
Australia
Phone: +61 2 9994 8004

Europe
e-Safe Systems Ltd
Salford Innovation Forum,
51 Frederick Road,
Salford,
M6 6FP
United Kingdom
Phone: +44 08443 443001

Asia
e-Safe Systems Sdn Bhd
L2-I-2, Enterprise 4,
Technology Park Malaysia,
Bukit Jalil,
57000 Kuala Lumpur
Malaysia
Phone: +60 3 89966061

Web: www.e-safecompliance.com
Email: sales@e-safesystems.com