

# Helping IT Managers measure user risk

## Importance of measuring risk to your sensitive data from users

In 2020 nearly 75% of all breaches reported in Australia were attributed to user actions either due to human error or malicious activity (OAIC NDB statistics). Knowing what data is critical, where it is stored, how it is being used and accessed is a basic requirement to ensure compliance with NDB, GDPR, PCI DSS and conform to ISO 27001. It also forms the basis for an effective data governance strategy.

The importance of monitoring user actions has been highlighted by the Australian Cyber Security Centre (ACSC) who in their latest iteration of ISM (Information Security Manual) have outlined the need to have a Trusted Insider Program in order to detect and respond to trusted insider threats.

Unfortunately, most organizations are ill-equipped to handle risk to data from user actions. They tend to rely on user awareness and education with no actual way of measuring the effectiveness of these programmes. Their existing network-based security technologies primarily focus on external attacks and don't report on trusted insider (user) actions.

## How does e-Safe's User and Data Security Risk Assessment solves these challenges?

e-Safe's assessment service is a quick and easy way to check on ACSC recommended use cases and highlight potential sources of data breach risk that exist within an organisation. It does this with specific attention to sensitive information as defined by various privacy regulations and standards like NDB (Australia), GDPR, PCI DSS and ISO 27001.

## How does e-Safe's assessment identify sources of data and user risk?

Assessments are run from the e-Safe cloud for ease of implementation. Implementation follows three keys steps:

1. Classification and discovery of sensitive information within an organisation's environment, made easy through predefined lists and specialised automated tools that require no integration.
2. Monitoring of data movement and user habits with respect to only classified sensitive information via a scanning agent on each endpoint.
3. Generation of a comprehensive report, detailing analysis of potential sources of risk and suggestions for risk reduction through process and technology adoption.

## What outcomes can we expect from using e-Safe's assessment service?

1. A detailed assessment report, highlighting sources of risk by analysing:
  - a. User actions and behaviours as per ACSC ISM.
  - b. Storage, usage, and movement of sensitive data on corporate and non-corporate channels, including online and offline media.
2. Detailed reports, with data that enables them to take corrective action for any events that are identified.
3. Clear direction on which areas need further investment in the form of training, process optimisation and technology.

