Trend Micro™

Data Loss Assessment

The Trend Micro™ Data Loss Assessment service, offered by Trend Micro™ certified DLP consultants, will provide you with a detailed, written analysis of your data loss vulnerabilities and information risks. The assessment includes a pilot installation[1] of the Trend Micro™ Data Loss Prevention solution, configured to identify and document your data loss risks.

Approach. Conceptually, implementing a DLP solution requires the following three steps:

1. **Identify Sensitive Data**
    First, determine which data needs protection from unauthorized users

2. **Determine Authorized Access**
    Next, determine which users are authorized to access this sensitive information

3. **Configure the Solution**
    Then, configure the data loss prevention solution using the information to be protected as the basis for the configuration

Methodology. Each Trend Micro Data Loss Assessment follows the process outlined below to help organizations understand their risks as well as the possible solutions.

1. **Audit and Data Loss Prevention Configuration (on site, up to 2 days)**

    • Identify Sensitive Data[2]
      - Where is the data stored?
      - What does the sensitive data look like?
      - What vulnerabilities do these nodes have (print, email, USB, writeable disk, etc.)?

    • Determine Authorized Access
      - Which users, groups and nodes are authorized to access the data?
      - What can authorized users and groups do with the data?

    • Install and configure Trend Micro Data Loss Prevention
      - Define and implement policies
      - Administrative review

2. **Document Creation (off-site)**

3. **Presentation of Findings Document (on-site)**

Schedule Assessment. To schedule your Trend Micro Data Loss Assessment, register **here** or contact your Trend Micro or Partner representative today.

Trend Micro™ Data Loss Prevention (DLP)

Most data loss happens from within, either by accident or on purpose by end users who have access to the data within a corporate network. Trend Micro DLP protects customer and employee privacy, and intellectual property. It prevents data loss with a unique approach that combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology. Trend Micro DLP provides the broadest protection of any endpoint client including USB, webmail, encrypted webmail, IM, and HTTPS–whether on or offline.

[1] Software license is limited to the Trend Micro Data Loss Assessment only, unless license is purchased separately

[2] The standard Trend Micro Data Loss Assessment is limited to one data set, up to five profiles, and up to 30 workstations. Larger scope assessments also may be available.

www.trendmicro.com