



Classified Data Protection

Case Study

Using Data Privacy Manager to protect sensitive data in laptops and Windows servers with encryption, access control and auditing.

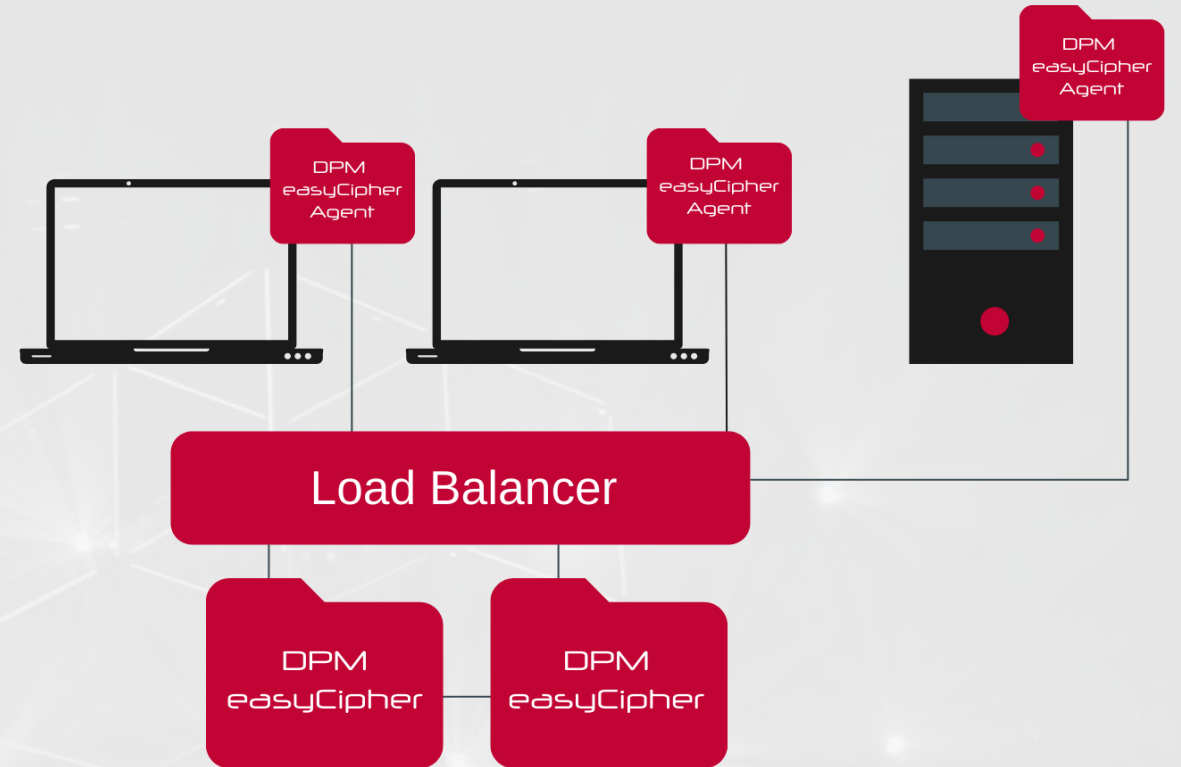
The Challenge

The client needed to protect highly sensitive data shared between governments used in the protection of people and infrastructure from terrorist. Data were stored and shared in laptops and Windows servers with no encryption, access control or auditing. Files needed to be protected so that only authorized users with the right access levels could access the files.

The Solution

DPM was used to encrypt the files and provide granular access control based on roles:

- DPM easyCipher Agent was installed on each laptop and server
- DPM easyCipher Manager was installed on a new virtual machine in HA



The Benefits

1. Different user groups and users were granted different access levels – depending on roles, users have different read, modify and delete permissions
2. Roles and users in DPM and Windows AD sync automatically when changed in AD
3. DPM HA using load balancing
4. Files securely stored on shared laptops and individual user folders were protected from each other and systems users
5. Laptop files were protected even when in offline mode
6. Full auditing on all users' operations on protected files
7. High performance – application impact was negligible

Randtronics LLC

Redwood City CA 94065 United States
+1 (650) 241 2671
enquiry@randtronics.com

Randtronics Pty Limited

S1.1, Level 1, Building A 64 Talavera Road
North Ryde, NSW 2113 Australia
+61 418 226 234



randtronics