

Becrypt Connect Protect

An end point security solution that enables organisations to control the use of “plug and play” devices and safeguard data

Connect Protect is Becrypt’s end point control solution that protects organisations against data leakage, by preventing unauthorised access to, and use of, external devices and providing centrally managed audit trails for all connection events.

Protecting your organisation’s data

Managing and protecting data is now top of the agenda for many senior personnel, but with an increasing number of external devices being used – Flash Memory sticks, cameras, iPods and mobile phones, organisations run the risk of their data being vulnerable to theft, accidental or malicious loss or even the ‘toxic’ liability of data or viruses being imported into the network.

The unmanaged use of such external devices exposes organisations to high risk. Flash Memory sticks are now commonplace and provide a convenient way of storing and transporting data. However, they can be easily lost or stolen.

To protect themselves from being vulnerable, organisations require a centrally managed policy to ensure that the usage of such devices is controlled.

Connect Protect Overview

Connect Protect is an end point control solution that helps prevent data leakage by ensuring there is no unauthorised access to external devices.

It controls the use of all “plug and play” devices, USB sticks and other removable media, enabling an organisation to enforce

a usage policy. It prevents unauthorised devices from connecting to the network, or it can restrict their use to approved devices only. In addition, Connect Protect provides a full audit trail to track device usage and highlight denied and authorised connections.

Connect Protect features digital signing for approved devices allowing an organisation to strictly control what type, and how many, removable storage devices are in use inside the organisation. This also prevents unauthorised devices from being cloned.

How it works

Connect Protect works by using filter drivers to allow/deny access to devices. Depending on policy, any external device may be connected but not accessible unless the machine or user has permission to do so.

Connect Protect also allows the signing of removable media, allowing an administrator to sign any removable media device, and prevent access to media that has not been signed. The product can also make use of Active Directory group policies, allowing simple and familiar management of the product and the policies across an organisation.

All user and machine events can be logged (even if the device has not been blocked) allowing an administrator to closely monitor the external devices that are being attached to machines on the network.

Fast Facts

- Controls or prevents the use of plug and play devices
- Audit trail tracks device usage
- Blocked attempts highlighted
- Centrally managed with Enterprise Manager

Becrypt Connect Protect

At a glance

Features	Benefits
Removable media access is based upon a white list of vendor make/model, unique identifier or pre-approved digitally signed devices	Straightforward and fast to deploy as only centrally issued, approved devices may be used. Enforces Information Assurance policy
Integrates with Active Directory to permit centralised management and the use of group policies	Easy to manage – no additional training is required for the administrator
Allows full auditing of device usage, including blocked attempts and passive monitoring and reporting of all devices usage	Usage easily tracked with full auditing reports
Clear Copy. Allows the monitoring of device usage with regards to file copying to and from an authorised device. File names and content copied to and from removable media can be viewed	Copying histories are easy to track and trace for forensic investigations
Integrated Auditing. Flexible auditing of device usage allows for fine grain control, giving varying levels of detail	Administrators are able to choose level of detail required for each task or investigation
Integration of Becrypt Enterprise Manager gives a centralised audit capability from the same console for both Becrypt DISK Protect and Becrypt Connect Protect	Centralised management of all Becrypt products saves time and makes compliance more efficient and effective
Email Alerting. Emails the Administrator with an alert based upon a customisable device event such as a denied device	Administrator is freed from the task of regularly manually checking on systems and devices used
Challenge Response. Allows temporary access to devices to reset passwords	Provides mechanism for resetting lost or forgotten passwords without exposing the original password, maintaining security

Standards and Protocols

Password hashing: SHA-256 is industry standard

Certification

FIPS 140-2 Level 1 – Connect Protect uses Becrypt's Cryptographic Library which is FIPS 140-2 Level 1 certified

For more information please call 0845 838 2050 or +44 (0) 20 3145 1050, or visit www.becrypt.com

Becrypt Limited, 130 Shaftesbury Avenue, London W1D 5EU. www.becrypt.com info@becrypt.com

Becrypt is a leading supplier of innovative Information Assurance solutions and services with operations in the UK and US. Becrypt provides secure, feature rich, out of the box products suitable for all industry sectors, and is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.

© Copyright 2009 by Becrypt Limited. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.