

Becrypt Connect Protect

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

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

Protecting your organization’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 – organizations run the risk of their data being left vulnerable to theft, loss or even the ‘toxic’ liability of data or viruses being imported into the network.

The unmanaged use of such external devices exposes organizations to high risk. Flash memory sticks are now commonplace and provide a convenient way to store and transport data. However, they can be easily lost or stolen. To protect against vulnerability, organizations require a centrally managed policy to ensure the controlled use of such devices.

Connect Protect Overview

Connect Protect is an end point control solution that helps stop data leakage by preventing unauthorized access to external devices.

It controls the use of all “plug and play” devices, USB sticks and other removable media, enabling an organization to enforce a usage policy. It can prevent unauthorized

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

Connect Protect features digital signing for approved devices, allowing an organization to strictly control the number and type of removable storage devices that are in use within the company. This control also prevents authorized 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.

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 organization.

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 centralized 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 device 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 authorized 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, providing varying levels of detail	Administrators are able to choose level of detail required for each task or investigation
Integration of Becrypt Enterprise Manager provides centralized audit capability from the same console for both Becrypt DISK Protect and Becrypt Connect Protect	Centralized 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 customizable 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

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



For more information please call (877) 221-7775, email info@becrypt.com or visit www.becrypt.com

Becrypt Inc. 225 Franklin Street, 26th Floor Boston, MA 02110

Becrypt is a global leading supplier of innovative Information Assurance solutions and services, providing secure, feature rich, out of the box products that are government-certified and suitable for all industry sectors. Through technology and OEM partnerships Becrypt enables third-party solutions with encryption and other data security capabilities. Becrypt has offices in Boston, USA and London, UK and Sydney, Australia serving clients worldwide.

© 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.