

# DEFENDER COLLECTION™ CONTROL SERVER



## PRODUCT DESCRIPTION

### MAXIMIZE SECURITY. MINIMIZE RISK.

Take control of ALL the removable data storage devices and media in your organization.

Imation Defender Collection Control Server allows security and compliance leaders and network administrators to control, manage and audit the removable data storage devices used by their organizations.

This powerful web-based software application is designed for use with Defender Collection Control Client software on client PCs, and Defender Collection Device Control on devices, to manage policies for removable media. Administrators can set policies for users, removable device types (e.g. USB flash drives, external hard drives, iPods, or individual devices, based on brand, model or serial number), passwords, off-network usage, encryption, or device usage—all tied to robust reporting and forensic auditing capabilities. Administrators can also block files by name or type that represent risks of data leaks or virus/malware propagation.

## FEATURES AND BENEFITS

- Provides robust policy definition enforcement and tracking of removable data storage devices
- Offers policy management controls for administrators and security and compliance officers—such as password creation and enforcement, length, special characters, re-authorization interval settings, and automatic drive authorization and encryption
- Retains audit trail of what files are stored and used on removable drives and media, plus details on where files are copied to from the removable device; audit trail contains metadata about drive and media contents, easily searched for reporting purposes
- Tracks and manages recordable optical discs used throughout your organization; gain more control with unique features tied to management of Imation Defender Optical discs
- Provides administrators with the ability to pre-establish offline usage policies that disable devices from being used off the network after a predefined period
- Allows administrators to remotely revoke devices exposed through theft or loss
- Helps administrators assist users remotely recover lost or forgotten passwords, without exposing the passwords to the help desk administrators
- Master key enablement allows highest level administrators (typically Chief Security Officer) to access protected devices
- Supports multiple browsers including Internet Explorer, Google Chrome, and Firefox

## CONTROL AND SIMPLICITY

**Control access privileges**—A remote command allows an administrator to revoke access to lost or stolen drives and media

**Delete device content**—When used with the Defender Collection Control Client or Device Control, device contents can be deleted remotely by an administrator

**Authenticate by domain**—Username and password are not required to access protected devices when the user is logged on to the corporate network

**Apply and enforce rules**—Set policies by device type, brand, model or serial number—Use with Defender Collection Control Client to set unique policies by device type, brand, model, VID, PID or serial number

## SYSTEM REQUIREMENTS

Operating System: Microsoft Windows Server 2000, 2003, 2005 and/or 2008

Database: Microsoft SQL Server 2000 SP3 or higher

Hardware: Intel or AMD 2.6 GHZ CPU or higher, 2 GB RAM, 100GB HDD

Apache Tomcat 6.0