Technical Specifications for DLP product

I. Introduction

The purpose of this document is to establish technical specifications for a DLP product that offers control over USB Devices and peripheral ports, control of company's data sent outside the network over the internet and offers a detailed report with registered events.

II. Objective

The product must offer control over computer network, detect threats of data loss, data leakage or theft of data generated by controlled devices, portable storage, peripheral ports. Moreover, the product must offer control of data in motion, filter company's confidential information that can be sent out of the network through various exit points like browsers, Emails, cloud storage, social media.
The product enables IT administrators to manage all networked computers (Windows, Mac OS X and Linux) from a centralized management console, a Cloud Server or a virtual machine (virtual appliance). Local agent is required to be installed on each computer.

III. General description and details

General description of the product: Management and control of portable storage devices and peripheral ports, monitoring file transfers and changing user rights, depending on the specific circumstances.

1. General Description:

1.1. The product has a server-client architecture and it is available as a Virtual Appliance in different formats (.VMX, .OVF, .OVA, .XVA, .VHD, .PVM) preconfigured and preset by the manufacturer and Cloud. The Virtual Appliance is available also on AWS (Amazon Web Services).

1.2. For a better adapt, the solution is available also as Hardware Appliance which comes with the solution and licenses preinstalled, mountable in a rack (19 inch) and with with all accessories.

1.3. The client is available for various operating systems Windows, Mac OS X, Linux and the option to be marked as Terminal Server.

Windows (32/64 bit)	Mac	Linux
Windows 10	macOS 10.12	Ubuntu 10.04
Windows 8	Mac OS X 10.11	Ubuntu 12.04
Windows 7	Mac OS X 10.10	Ubuntu 14.04
Windows Vista	Mac OS X 10.9	Ubuntu 16.04
Windows XP	Mac OS X 10.8	Ubuntu 18.04
Windows Server 2016	Mac OS X 10.7	OpenSUSE / SUSE 12.1
Windows Server 2012	Mac OS X 10.6	OpenSUSE / SUSE 11.04

Windows Server 2008	Mac OS X 10.5	CentOS / RedHat 7.0+
Windows Server 2000 / 2003		CentOS / RedHat 6.0+

1.4. The communication between server and client is performed via a secure connection (https:)

1.5. The product provides integration with Active Directory, meaning that AD entities (Organizational Units, Groups, Computers, Users) can be imported onto the server. Additionally an AD Sync can be set up to synchronize the newly added AD entities with the solution. The installing of the agent on all computer in the network can be done automatically, without user intervention.

1.6. The product has a web interface accessible from the internal network or external, through IP address. The administrator has the possibility to connect with the username and the password from any computer in the network or over the internet, if the appliance has an external IP.

1.7. The product interface is available in multiple languages .

1.8. The product has a system with permanent licenses, meaning that the licenses do not expire.

1.9. The manufacturer offers the possibility of annual renewal contract for technical support and updates.

2. Technical Details:

2.1. The product has a few levels for admin. Super Administrator with full privileges at product and normal administrators with fewer privileges. Normal Administrators can be restricted even further by taking advantage of various roles. For a more restrictive access, the Normal Administrators would have to be included into Administrators Groups, each having a specific role attached to them (e.g.: Administrators can be added into a Helpdesk group, having the Offline Temporary Password and Enforced Encryption roles). The product is able to provide management services, each department can have its own administrator who will manage only entity or his department (groups, computers, users, devices).

2.2. The network administrator has the ability to block / allow / read only for portable storage devices used internally by the users (employees). In addition to the Standard device control rights, the administrator has the ability to provide fallback policies for Outside Network and Outside Hours circumstances. Rights are assigned at several levels:

- Globally (settings apply to all computers on the network);
- Group level (settings apply to computers and users in a group);
- Computer level (valid for one computer settings);
- User Level (available settings for a single user);
- Device Level (available settings for a certain portable device);

The administrator is able to choose between computer or user, as highest priority on the server.

2.3. The product identifies and manages the following portable devices and peripheral ports, with the following rights:

Device Type	Rights
USB Storage Devices	Deny Access / Allow Access / Read Only Access / Allow Access if TD level 1,2,3,4 /Allow Access if TD 1+ / Allow Access if TD Level 1+ Otherwise Read-Only
Internal CD or DVD RW	Deny Access / Allow Access / Read Only Access
Internal Card Reader	Deny Access / Allow Access / Read Only Access
Internal Floppy Drive	Deny Access / Allow Access / Read Only Access
Local Printers	Deny Access / Allow Access
Windows Portable Devices	Deny Access / Allow Access
Digital Camera	Deny Access / Allow Access
BlackBerry	Deny Access / Allow Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access / Allow Access
SmartPhone (USB Sync)	Deny Access / Allow Access
SmartPhone (Windows CE)	Deny Access / Allow Access
SmartPhone (Symbian)	Deny Access / Allow Access
Webcam	Deny Access / Allow Access
iPhone	Deny Access / Allow Access
iPad	Deny Access / Allow Access
iPod	Deny Access / Allow Access
Serial ATA Controller	Deny Access / Allow Access
WiFi	Deny Access / Allow Access / Block WiFi if wired network is present
Bluetooth	Deny Access / Allow Access
FireWire Bus	Deny Access / Allow Access / Read Only Access
Serial Port	Deny Access / Allow Access
PCMCIA	Deny Access / Allow Access / Read Only Access
Card Reader Device (MTD)	Deny Access / Allow Access / Read Only Access
Card Reader Device (SCSI)	Deny Access / Allow Access / Read Only Access
ZIP Drive	Deny Access / Allow Access / Read Only Access
Teensy Board	Deny Access / Allow Access
Thunderbolt	Deny Access / Allow Access / Read Only Access

Network Share	Deny Access / Allow Access
Infrared Doungle	Deny Access / Allow Access
Parallel Port (LPT)	Deny Access / Allow Access
Thin Client Storage (RDP Storage)	Deny Access / Allow Access / Read Only Access
Additional Keyboard	Deny Access / Allow Access
USB Modem	Deny Access / Allow Access / Block if wired network is present
Android Smartphone (Media Transfer Protocol)	Deny Access / Allow Access
Unknown Device	Deny Access / Allow Access

2.4. The administrator can monitor which files have been copied by users (employees) and what devices were used (authorized in advance by the administrator). The product can generate logs reports which include: what file was transferred, the type and size, transferring user, computer name and IP address from which the transfer was made, portable device name, date and time of the transfer, hash of the file. The created Reports can be exported as CSV files to a location specified by the administrator.

2.5. The product gives the possibility of the administrator to control the transfer of files via online applications: web browser, email, cloud storage solutions, file sharing and more. The most important are:

Web Browser	E-mail	Instant Messaging	Cloud Services / File Sharing	Social Media / Others
Internet Explorer	Outlook	ICQ	Google Drive Client	Windows Apps
Chrome	Outlook (Body)	AIM	iCloud Client	EasyLock
Mozilla Firefox	Mozilla Thunderbird	Skype	uTorrent	Team Viewer
Opera	Mozilla Thunderbird (Body)	Windows Live Messenger	BitComet	Windows DVD Maker
Safari	IBM Lotus Notes v.6.5 - v 9.0	Yahoo Messenger	Daum Cloud	Total Commander
AOL Desktop 9.6	IBM Lotus Notes v.8.5 - v 9.0 (Body)	Gaim	KT Olleh uCloud	ALFTP
Aurora Firefox	Geary	Pidgin	Azureus	LogMeIn Pro

Adobe Flash Player	Evolution	Trillian	Box Sync	iTunes
Tor	Claws Mail	NateOn Messenger	Sugar Sync	FileZilla
Camino	Sylpheed	Spark	Picasa	SCP
iCab	Balsa Mail Client	Telegram Desktop	Amazon Drive	Total Commander 64 bit
OmniWeb	Windows Live Mail	Messages	iBooks Author	Sony Ericsson PC Companion
Sleipnir	GroupWise Client	Audium	MediaFire Client	InfraRecorder CD-DVD
K-Meleon	Foxmail	Line	Novell Filr Client	HTC Sync for Android
SeaMonkey	SeaMonkey Mail	Hall	AirDrop	GoToMeeting
Maxthon	Zimbra Desktop Mail	OpenTalk	Transmission	Nokia PC Suite 2011 Video Transfer
	Endora	TurboIRC	Morpheus	Nokia PC Suite 2011 Image Store
	eM Client	WinSent Messenger	FileCloud Sync Client	Nokia PC Suite 2011
	Sparrow	xChat	OneDrive (Skydrive) Client	Nokia PC Suite 2008 Main
	GyazMail	TweetDeck	Lime Wire	Nokia PC Suite 2008
	PowerMail	Pink Notes Plus	FTP Command	
	AirMail Beta	Google Talk	BitTorrent	
	Sparrow Lite	Twhirl	ownCloud Client	
	Postbox	QQ International	Pogoplug Backup	
	Mail	mIRC	Shareaza	
	Outlook Express	MySpace IM	Pruna P2P	
	Windows Mail	Duam MyPeople	SendSpace	
	AOL Mail	Kakao Talk	DC ++	
	Courier	Chit Chat for Facebook	Dropbox	
	Opera Mail	eBuddy	eMule	
		Facebook Messenger	Evernote	

		fTalk	Kazaa	
		Microsoft Communicator 2007	Android File Transfer	
		LingoWare	GitHub Client	
		Lan Chat Enterprise	MEGA	
		My Chat	Yandex Desk	
		Nimbuzz	KRDC	
		ooVoo	qBittorrent	
		Microsoft Link	Linux DC++	
		Mail.Ru Agent		
		Slack		
		Psi+		

2.6. The product allows administrators to control file transfers by creating filters based on file extension, predefined content, personalized content and regular expressions. Administrator should be also able to set Transfer Limit, within a specific time interval (hours).

a. Filters by file extension gives administrators the ability to manage the transfer of file types. Among these:

Graphic Files	Office Files	Archive Files	Programming Files	Media Files	Other Files
JPEG	Word	ZIP	C, pp, java	Mov	AutoCAD
PNG	Excel	ZIP / password	Py	Mp3	Text files
GIF	PowerPoint	7z	Sh, csh	M4a, mp4	DRM Files
ICO	PDF	RAR	Bat, cmd	Wav	Exe, sys, dll
BMP	Infopath	ACE	Pas	Wma	Fasoo Files
TIFF	Outlook	TAR	Xml, dtd	Avi	Journal files
CGM	Publisher	XZ	Tex	Aif	so
Corel Photo - Paint	iWork files	.xar	F	M3u	Unidentified
CorelDraw	Office 2007+/password	ACE / password	Asm		.accdb
DJV		RAR / password	Makefile		DTA

EPS		bz2	Fdl		I-DEAS 3D CAD
Adobe Illustrator		GZ	Perl		NASCA DRM
Adobe InDesign			Php		Pro-E CAD
PSD			Ruby		SgWgc
			Matlab		SID
			VBS		SolidWorks
					Xia
					CATIA

If the additional extensions are needed, the manufacturer has the possibility to complete the list of extensions.

b. The Policy Status can be set to Report only or to Block and Report al transfers of data that includes sensitive content.

c. Predefined content filters gives administrators the ability to manage transfer files with sensitive content: credit cards(Visa, MasterCard, American Express, JCB, Discover Card, Dinners Club, MIR ,China UnionPay bank etc.), IBAN, social security numbers, ID's, email addresses, phone numbers, etc.

d. Custom filters based on content gives administrators the ability to manage transfer files based on keywords (dictionaries) which are confidential.

e. Filters created based on regular expressions gives administrators the ability to manage transfer files containing data recursively. As these filters are created by the Administrator, it must have knowledge about regex syntax.

f. Predefined policies should be available for Windows, Mac and Linux. Predefined policies for different compliance regulations: (GDPR, PCI DSS and others)

2.7. In case of copied file, there is the possibility of creating a duplicate (File Shadow) that administrator can examine.

2.8. The product enables integration with a solution of automatic encryption of portable storage devices.

2.9. The product has the ability to send real time alerts via e-mail to the administrators, when a predefined event (ex. possible data leakage) occurs in the network.

2.10. The product is able to provide statistics and graphs on the use of portable devices and transfer files within the network.

2.11. The product has functionalities such as, File Shadowing and File Tracing in order to prove the transfer of all files of any user connected to a protected computer.

2.12. The product provides continuous protection of a computer, even if it is disconnected or removed from the internal network. The Administrator settings remain valid even if the computer has no connection to the server. During this time, the generated Logs and Reports will be stored locally and at first reconnection, the reports will be sent to the server.

2.13. To avoid uninstalling client software by users (employees), even if they have administrator rights on the computer, the product is protected by an uninstalling password.

2.14. If the users (employees) use laptops, the Administrator may authorize the connection of an USB storage device for a limited period of time, even when the computer is disconnected from the network.

2.15. The product allows administrators to adjust the interval of communication between client and server (the time at which the client sends the logs and reports to the server).

2.16. The product allows administrators to define a "white list" of files that can be copied to authorized devices.

2.17. The product allows administrators to define a "white list" of URLs and domains, making it possible to transfer files to websites and email addresses authorized to receive such information for current activities.

2.18. The product has updates mechanism, where the administrators can apply the latest available versions.

2.19. If the administrator wants to stop or restart the product, the process can be made fast and easy from the user interface.

2.20. The product is capable of receiving a single file that contains all licenses for all computers in the network, the server automatically assigns the client license.

2.21. The product has a technical support section that allows administrators to send messages directly to the manufacturer's Technical Support Department. The Support is offered at least in two international languages.

2.22. The product supports optical character recognition (OCR). Scanning text, through Predefined Content Filter and Custom Content Filter.

2.23. The product should have available filters like Employee ID, Computer ID, Team, etc. in order to give the Administrator a better overview on the users. This details should be filled in either directly by each user through the Client or by the Administrator, from the UI.

2.24. The product should have the option to enable or disable metadata scanning during content inspection for ZIPs, PDFs and Office Files (docx, xlsx, pptx, doc, xls, ppt).

2.25. The notifications for the users can be edited or hidden.

IV. Technical Details

1. Supported Virtual Environments

VMware Workstation	VMware Player	WMware vSphere (ESXi)	VMware Fusion
Oracle VirtualBox	Parallels Desktop Mac	Microsoft Hyper-V Server 2008/2012	Citrix XenServer

The Virtual Appliance should be also available as Amazon EC2 Instance. (AWS)

2. Offline Temporary Password

This feature offers temporarily file transfers to computers disconnected from the network. Once the computer reconnects, the administrator has access to logs and reports. The Universal Offline Temporary Password feature can also be turned on. If enabled, it can be used by any user, on any computer, for any device or file transfers – it eliminates security restrictions for one hour. It can be used multiple times, by any users that knows it.

OTP Timeframe is from 30 minutes and up to 30 days, or this can also be customised.

3. File Tracing / File Shadowing

File Tracing records all data that was copied to / from previously authorized devices.

File Shadowing saves a copy of all files, even deleted ones, that were used in connection with controlled devices.

4. eDiscovery

This module allows the Administrator to create policies that inspect data residing on protected Mac, Windows and Linux computers. The company's data protection strategy can be enforced and risks posed by accidental or intentional data leaks can be managed. The Administrator can mitigate problems posed by data at rest by discovering sensitive data.

a) Scanning is done using all options available for scanning in Content Aware Protection. Scan Location Blacklist has to be available, allowing for scanning data at rest to be performed only on targeted locations.

c) eDiscovery Automatic Scanning has to be available, allowing the administrator to set an Incremental Scan: One time – a scan will run once, at the specific date and time; Weekly – a scan will run every 7 days, from the set date and time; Monthly – a scan will run every 30 days, from the set date and time

b) eDiscovery scans are sets of rules for Policies, defining when the data discovery to start. There are several type of scans:

- Clean scan: starts a new discovery (from scratch)
- Incremental scan: continues the discovery (skipping the previously scanned files)

c) eDiscovery Scan can be stopped at any time as results can also be automatically cleared. This can be done by using:

- Stop Scan: stops the scan (but does not affect the logs)
- Stop scan and cler scan: stops the scan and clears the logs

d) The Administrator can manage the scan results. A list with all the computers that were scanned can be viewed and actions such as deleting, encrypting or decrypting files can be taken. The Administrator can apply the desired action to each item individually or, can select multiple items and apply the desired action simultaneously.

5. Enforced Encryption

Authorize only encrypted USB devices and ensure all data copied on removable storage devices is automatically secured. Creating a master password will provide continuity in various circumstances like resetting the user's password.

6. SIEM Integration

Third-party security information and event management (SIEM) tools allow the logging and analysis of logs generated by network devices and software. Integration with SIEM technology allows the product to transfer activity events to a SIEM server for analysis and reporting.

7. Modes

The agent installed on the computers can be set on Normal, Transparent, Stealth, Panic, Hidden Icon and Silent, meaning:

Normal - default setting

Transparent - blocking all devices without user seeing and knowing anything about the software activity.

Stealth - allows the administrator to monitor all of the users and computers activities and actions with all devices allowed.

Panic - under special circumstances, this mode can be set manually by the administrator in order to block all access to devices.

Hidden Icon - similar to Normal mode, the difference consisting in the fact that the Agent is not visible to the user.

Silent - similar to the Normal mode, the difference consisting in the fact that notifications do not pop-up to the user.