

Modul	Funktion DW 3.5	Verfügbar für CITRIX & Terminalserver
Basisfunktion	Netzweites Management	✓
	Anzahl der Administrationsinstallationen	nicht relevant
	Alle Replikationmechanismen	✓
	Beliebige Policy-Changes	✓
	Remote Connect	✓
	Properties der Policies	✓
	Off-line Freigabe von Policies	✓
	Echtzeit wechsel der Policy (setpolicy)	✓
	ODBC Interface für Inventar	✓
<i>DeviceWatch</i>	Sperrern / Freigeben aller Schnittstellen	✓ lokal
	Sperrern / Freigeben aller Geräte / -klassen	✓ lokal
	Zeitl. Gültigkeit DeviceFreigabe	✓ lokal
	Drive Mapping: Vergabe der Laufwerksbuchstaben	✓ lokal
	Logging Device Verwendung	✓ lokal
	Gerätedatenbank	✓ lokal
	Datenträger personalisieren	✓ lokal
	EchtzeitAPI zur Gerätefreigabe (ChangeDevState)	✓ lokal
	Content Filter zur Überwachung Devices mit "Vorlage für neue Klassen" inkl:	✓
	Pattern Prüfung	✓
	Audit Dateinamen	✓
	Shadowing	bedingt
	Rechte für personalisierte Devices	✓ lokal
	Content Filter zur Überwachung Devices detailliert inkl:	✓
	Pattern Prüfung	✓
	Audit Dateinamen	✓
	Shadowing	bedingt
Rechte für personalisierte Devices	✓ lokal	
<i>XRayWatch</i>	ContentFilter (CF) editieren: Dateien oder -typen; Lesen / Schreiben freigeben/sperrern	✓
	Pattern Prüfung: Inhaltliche Prüfung von Dateien (Signaturfeld in CF)	✓
	Verwendung der vordefinierten Content Filter	✓
	Verwendung der vordefinierten Pattern	✓
	Eigenständige Erweiterung der Pattern	✓
	Mit Exclude	✓
	Mit logischen Operatoren	✓
	Logging Dateizugriffe	✓
	Shadowing komplette Dateien bei Zugriff	bedingt
	Content Filter zur Überwachung Netzlaufwerke inkl:	✓
	Pattern Prüfung	✓
	Audit Dateinamen	✓
	Shadowing	bedingt
	Content Filter zur Überwachung lokale Drives inkl:	✓
	Pattern Prüfung	✓
	Audit Dateinamen	✓
	Shadowing	bedingt
<i>ApplicationWatch</i>	Anwendungen sperren und Freigeben	✓ von Netzwerk oder Thin Client
	zentrales Logging aller Anwendungen inkl. Portable Apps	✓
	DLLs und Plug-Ins sperren und freigeben für einzelne Anwendungen	
	Vordefinierte Content Filter zur Überwachung der Zugriffe und Rechte von Anwendungen	
	Upload Internet Explorer verbieten	
	Plug-Ins in den Internet Explorer kontrollieren	
	Content Filter zur Überwachung der Zugriffe und Rechte von Anwendungen inkl:	
	Pattern Prüfung	
	Audit Dateinamen	
Shadowing		
<i>PDWatch</i>	Verschlüsselung mobiler Datenträger	✓
	optional	✓
	erzwungen	✓
	Verschlüsselung Netzlaufwerke	✓
	optional	✓
	erzwungen	✓
	Verschlüsselung lokale Daten	
	Unternehmensschlüssel	✓
	optional	✓
	erzwungen	✓
	Persönlicher Schlüssel	✓
	optional	✓
	erzwungen	✓
	Schlüssel hinterlegung	✓
	lokal	✓
	zentral	✓
	PDWatch2Go	✓
	auf PCs mit eigener Lizenz	✓
	zur direkten Weitergabe mit verschlüsselter Datei	✓
portable Lizenz	✓	
<i>Serverkomponente</i>		nicht relevant
	Schlüsselverteilservers für Unternehmensschlüssel	nicht relevant
	Zentrale Schlüssel hinterlegung für persönliche Schlüssel (in DEvCon)	✓
<i>Admin</i>	Administrationskomponente für Unternehmensschlüssel	✓
<i>DEvCon</i>		✓
<i>Clientkomponente</i>		✓
	zentrales Logging aller Ereignisse	✓
	Benutzerdialog mit / ohne Protokollierung	
	Client Plug-Ins (z.B. Skript oder Visual Basic)	✓
	E-Mail notification	✓
	Inventarermittlung (PCs / Policies)	✓
	Netzwerksicherheit	
	Netzwerk Kontakte der Clients tracen	✓
	Friendly Net Detection nach Kundenkriterien	✓
<i>Serverkomponente</i>		✓
	E-Mail notification	
	Zentrale Schlüssel hinterlegung für persönliche Schlüssel	✓
	Server Plug-Ins (z.B. Skripting)	✓
<i>Admin&amp;Infrastruktur</i>		✓
	Echtzeitkonsole (DCView)	✓
	Kaskadierende Konsole: Weiterleitung von Ereignissen	✓
	von Server zu Server	✓
	an Anwendungen von Drittanbietern	✓
	Reportgenerator (DCReport)	✓
	vordefinierte Reports	✓
	selbstdefinierte Reports	✓
	Anzahl Server	nicht relevant
<i>CDWatch</i>	Medienbasierter Schutz	
<i>updates</i>	patches auf lizenzierte Funktionen	
	minor auf lizenzierte Funktionen	
	major auf lizenzierten Funktionen	
	Module bei Auslieferung	
	Alle neuen Plug-ins und weiteren Funktionen	
<i>Sonstige Leistungen</i>		