

Bereich	Bereichsgewichtung (0-10)	Thema	Themengewichtung (0-10)	Hersteller	Gewichtung (0-10)	KO-Kriterium
				Produkt		
				Ziel: DLP und Endpoint Security		
Technik	ung: 10 von 10 Punkten	Architektur	10 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Datenhaltung im Betrieb	9	
				Skalierbarkeit für verteilte Umgebungen und schwierige Netztopologien	8	
				Unterstütze Betriebssysteme für Schutzsoftware: Windows 2000	5	
				Unterstütze Betriebssysteme für Schutzsoftware: Windows XP	10	ja
				Unterstütze Betriebssysteme für Schutzsoftware: Windows Vista	10	ja
				Unterstütze Betriebssysteme für Schutzsoftware: Windows 7	10	ja
				Unterstütze Betriebssysteme für Schutzsoftware: Terminalserver	7	ja
				Unterstütze Betriebssysteme für Schutzsoftware: CITRIX	7	ja
				Unterstütze Betriebssysteme für Schutzsoftware: Linux	2	
				Unterstütze Betriebssysteme für Datenhaltung	10	
				Integritätsschutz der Konfiguration	8	
				Integration mit Frameworks z.B. Tivoli, OpenView, SNMP	5	
				Aufbau des Sicherheitssystems	5	
				Art der Einbindung ins System - evtl mit Anhängigkeiten	10	
				Architekturelle Defizite	10	
				Sicherheit auch im off-line Betrieb	10	ja
		Protokollierung/Audit/Logging	8 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Logging folgender Ereignisse: - muss zentral sein	10	ja
				Logging ist konfigurierbar	10	
				Devices und Ports: Nutzung, Verbot, Aktivierung, Fehlermeldungen	10	
				Datei Bewegungen: Netzwerkshares, lokale Platte, mobile Datenträger, inhaltsabhängig	7	
				Bestimmte Dateien müssen vollständig oder deren sensible Inhalte protokolliert werden, um den Inhalt beweisen zu können	7	
				Quota: belegter und freier Speicherplatz, Datenträgergröße	3	
				Ausgeführte und blockierte Anwendungen inklusive Herkunft	5	
				Protokollierung von Druckvorgängen	4	
				Echtzeitmonitoring nach Themen / Standorten etc. gruppiert an den Nutzungspunkt senden	4	
				Kundenseitige Erweiterung der Ereignisse, Daten und Formate	6	
				automatisierte Weiterleitung von Events an Dritte Anwendungen (IDS) oder managed service	5	
				Ereignisse per E-Mail, syslog etc. an selbst definierte Ziele senden (z.B. Handy oder Pager)	8	
				Nachvollziehbarkeit der Admin-Aktionen (Historisierung)	9	
				Berichtsauswertung von Logging für Revision (auch vordefinierte Reports)	5	
		Unterstützte Schnittstellen	10 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				USB	5	
				FireWire	5	
				Bluetooth	4	
				SATA	4	
				Seriell / Parallel	4	
				alle weiteren oder noch unbekannte ohne Produktupdate	10	ja

Bereich	Bereichsgewichtung (0-10)	Thema	Themengewichtung (0-10)	Hersteller	Gewichtung (0-10)	KO-Kriterium
				Produkt		
				Ziel: DLP und Endpoint Security		
Bereichsgewichtung	Bereichsgewichtung	Unterstützte Geräte- (klassen)	10 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				CD/DVD - auch virtuelle Laufwerke	4	
				WiFi	4	
				Diskettenlaufwerke	4	
				PDA, MDA	4	
				Externe Datenträger / removable Media	6	
				Compact Flash	5	
				Kamera	5	
				Authentisierungsgeräte	5	
				Multifunktionsgeräte automatisiert zerlegen in die einzelnen logischen Geräte	8	ja
				Schutz auf einzeltem Gerät möglich Personalisierung von Datenträgern ohne Seriennummern	9	
				Personalisierung von Datenträgern ohne Seriennummern	4	
				alle weiteren oder noch unbekannte ohne Produktupdate	10	
		Inhaltsbezogener Schutz (Content-Security)	10 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Zusammenfassung Dateitypen zu Gruppen	3	
				Prüfung auf Dateinamen / mit Wildcards	5	
				Prüfung auf Dateiendung	7	
				Syntaktische und Semantische Inhaltsprüfung der Dateien	8	ja
				White und Black List bei Content Prüfung	10	ja
				Read-Only-Access	2	
				Write-Only-Access z.B. für Backup	2	
				Definition von eigenen Pattern für inhaltliche Prüfung	3	
				Inhaltliche Prüfung identisch für Terminalserver / CITRIX - für Netzwerkshares und mobile Datenträger	4	
				Content Prüfung für alle Datenträger leistbar und identisch steuerbar (auch brennbare CD / DVD)	6	
				Integration mit Verschlüsselung, so dass Verschlüsselung inhaltsbezogen erzwungen werden kann	7	
				Inhaltliche Prüfung muss "embedded Objects" z.B. embedded executables erkennen und sicher verhindern	10	ja
				Inhaltliche Prüfung auch ausserhalb der Benutzeranmeldung	6	
				Gerätespezifische Content-Filter (z.B. CD und Kameras verschiedene Einstellungen)	5	
				Medienbezogener Schutz	5	
				Content-Security bei CD-Writern	6	
				Individualisierte Installationsroutinen authentisierter CD / DVD	3	
				Integrationsmöglichkeit von Drittprodukten bei der inhaltlichen Rechteentscheidung z.B. für DLP	10	
				Berücksichtigung von Labels und Attributen bei der Rechteprüfung	7	

Bereich	Bereichsgewichtung (0-10)	Thema	Themengewichtung (0-10)	Hersteller	Gewichtung (0-10)	KO-Kriterium
				Produkt		
				Ziel: DLP und Endpoint Security		
		System Management	7 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				automatisches Drive Mapping nach zentralen Vorgaben	7	ja
				Device-Driver Management on-demand	5	
				Automatische Synchronisation von PDAs nach zentralen Vorgaben	5	
				Echtzeitmonitor über alle oder ausgewählte Geräteereignisse	10	
				Prüfung der Devices auf Unternehmenseigentum	4	
				Definierbare Reaktionen auf Ereignisse:	6	
				Device, Datenträger, (neu, zulässig, unzulässig)	9	
				Netzwerk (neu verbunden / disconnected)	7	
				Wechsel der gültigen Policy in Echtzeit abhängig vom Systemzustand	8	ja
				Vollständiger Überblick über alle gestarteten Anwen-dungen inkl. portable Apps, Herkunft (PC) und Attribute	9	
				Automatische Historisierung und Revisionssicherheit der Policies	9	
				Automatisierte vordefinierte Reports	7	
				Vollständiges Geräteinventar in beliebiger kundenseitig definierbarer Datenbank	5	
				APIs zur Steuerung von aussen	2	
				Life Cycle Management der Devices, Applikationen und Contents	5	
				Alerting bei versuchten Verstößen oder besonderen Systemsituationen	9	ja
				Eine Policy für alle Client Betriebssysteme (W2K, XP, Vista...)	9	
				Permanenter Überblick über die eingesetzten Geräte mit Inventarisierungsschnittstelle	8	
		Verschlüsselung	8 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Zentrales Durchsetzen von Verschlüsselungsrichtlinien	7	ja
				Einsatz von zentral definierten Firmenschlüsseln	8	
				Keymanagement deckt alle erforderlichen use cases ab? Transport, firmenvertraulich, öffentliche Daten etc.	8	
				Einsatz von benutzerdefinierten Schlüsseln	6	
				Zentral verwaltete Unternehmensschlüssel mit Gruppenberechtigung (optimal an AD Gruppen)	10	
				Usability / Endbenutzerunterstützung	10	
				Unternehmensindividuelle Komplexitätsprüfung der benutzerdefinierten Schlüssel	5	
				Einsatz ausserhalb des Firmennetzes	9	
				Verschlüsselungsalgorithmen	8	
				Verschlüsselungsstärke	9	
				Datei, Container und Partitionsverschlüsselung	10	ja
				Zwangsverschlüsselung von Netzwerkshares, lokalen Verzeichnissen und mobilen Datenträgern	9	
				Zwangsverschlüsselung inhaltsabhängig (z.B. vertraulich)	4	
				Zwangsverschlüsselung je User / Gruppe unterscheidbar nach "bleibt in der Firma" - "darf weitergegeben werden"	6	
				Unverschlüsselte Daten neben verschlüsselten auf einem Datenträger	9	
				Regel "firmenvertraulich muss verschlüsselt werden" muss abbildbar sein	6	
				Schlüsselhinterlegung lokal für den Anwender, um den Helpdesk zu entlasten	4	
				Schlüsselhinterlegung zentral für den Notfall	6	
				nur verschlüsselter Import von Daten nach zentralen Vorgaben	5	
				nur verschlüsselter Export von Daten nach zentralen Vorgaben	7	ja
				MS-Suchfunktionen bleiben in verschlüsselten Containeren erhalten	6	

Bereich	Bereichsgewichtung (0-10)	Thema	Themengewichtung (0-10)	Hersteller	Gewichtung (0-10)	KO-Kriterium
				Produkt		
				Ziel: DLP und Endpoint Security		
Technik	Bereichsgewichtung: 10 von 10 Punkten	weitere Feartures	6 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Zusammenfassung von Geräten zu Klassen	8	
				Definition eines Nutzungszeitfensters	3	
				Temporärer Zugriff (mit Countdown)	2	
				offline Freigabe per Challenge Response	2	
				Zugriff nur auf Teilfunktionen von Multifunktionsgeräten	10	
				Einsatz Benutzer-transparent / nicht transparant steuerbar	4	
				Gerätedefinition auf Benutzer-Basis	10	
				Rollenbasierte Administation des Systems	8	
				Gerätedefinition auf PC-Basis (statisch / dynamisch)	4	
				Gerätefreigabe algorithmisch in Echtzeit (z.B. abhängig vom Netzwerkkontakt oder installierten Anwendungen)	7	
				Freigabe von Datenträgern abhängig von deren Kapazität	3	
				Freigabe anhand einer Seriennummer und eigenen Inventories	3	
				Automatisches Wechseln von Policies in Abhängigkeit vom benutzten Netzwerk des Clients	6	
				Konfigurierbare Dateiauszüge im Log	8	
				Quota-Regelung nach Standort, User, Datenträgertyp, Dateiert etc.	6	
				Ab hier Application Control		
				Erkennen und blockieren aller lokalen und aus dem Netzwerk ausgeführten Anwendungen anwendungsspezifisch	10	
				Erkennen und blockieren von portable Apps anwendungsspezifisch	10	
				Erkennen und blockieren von U3 Anwendungen - anwendungsspezifisch	10	
				Erkennung der Anwendung auf sicherer Basis (z.B. Hashbasis) nicht nach Namen	10	
				Erkennen und Alerting mehrerer Anwendungen mit gleichem Hash	4	
				Benutzer / Gruppen berechtigungen	9	
				Verwalten nach Black List - je nach PC Gruppe	8	
				Verwalten nach White List - je nach PC Gruppe	6	
				Zeitberechtigungen (z.B WebEx für ein geplantes Meeting)	4	
				Situationsbedingte Berechtigung voll automatisiert (z.B. Skype nur im Hotel über WLAN)	6	
				Blockade von bestimmten benennbaren Plug-Ins (z.B. WebEx als Plug-In in den Internet Explorer)	8	
				Protokollierung von bestimmten Dateizugriffen einer speziellen Anwendung	7	
				Bblockade von bestimmten Dateizugriffen einer speziellen Anwendung (z.B. ftp Client darf keine vertraulichen Dokumente lesen)	6	
				Reporting der Nutzungszeit einer Anwendung	4	
				Multiple Selektion und Gruppierung von Anwendungen bei der Freigabe	10	
		Verteilung	8 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				MSI-Installer, Setup.exe, Eigeninstallation	10	ja
				Softwareverteilung über proprietäre Verteilungsmechanismen	1	
				Weicher Roll-Out einer Security Policy	10	ja
				Initial und FallBack Policies mit in der Verteilung	7	
				Unattended Installation - parametrisiert	10	

Bereich	Bereichsgewichtung (0-10)	Thema	Themengewichtung (0-10)	Hersteller	Gewichtung (0-10)	KO-Kriterium
				Produkt		
				Ziel: DLP und Endpoint Security		
		Administration	7 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Zentrale Verwaltung	10	
				Echtzeit-Zuweisung von Berechtigungen ohne Neuanmeldung	9	
				Veränderbare Meldungen an die Benutzer bei Verweigerung	8	
				kundenseitig definierbare Texte und Dialoge an Benutzer in Echtzeit VOR Freigabe von Devices, Applikationen oder anderen Rechten	9	
				Sprachversionen	8	
				Rollenbasierte Administration des Systems	8	
				Mandantenfähige Administration des Systems in allen Facetten	10	
				geringer Regeldienstaufwand	8	
				Import des Hashwertes und Namens von zu kontrollierenden Applikationen aus Drittsystemen	7	
				Privilegierte Anwender sollten die Möglichkeit zur Selbstfreigabe haben	10	ja
				Import und Export von Teilen einer Sicherheitsrichtlinie und Austausch in Standardformaten	10	
				Import von Plug&Play-Device-Kennungen zentral und am Client	9	
Betriebswirtschaft / Organisation	Bereichsgewichtung: 10 von 10 Punkten	Investitionsschutz	6 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Installierte Basis	10	
				Hotline telefonisch, Email, Support Vorort	10	
				Markteintritt	7	
				Produktqualität	10	
				Roadmap, Marktverlauf	10	
				Sicherheit der Lösung im Betrieb	10	
				Referenzen	10	
				Anbindung von "Home Made Systemen"	10	
				Integration von Drittprodukten	10	
		Prozessintegration	6 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Hardware- und Device-Beschaffung mit fertigen Formularen	9	
				Antragswesen mit fertigen Formularen	7	
				Freigabe der Policy im Rundschreiben-Verfahren und anderen	7	
				Inventarisierungsschnittstelle	9	
				Statistische Daten zur Nutzung und Optimierungsmöglichkeiten	4	
				Revisions-Sicherheit und -Freudigkeit	10	
				Life Cycle Management der Security Policy	10	
		Betriebskosten	9 von 10 Punkten	Falls Eintrag vorhanden, bezieht sich die Bewertung auf das genannte Zusatzprodukt		
				Konw How (Kosten für 7/24)	8	
				Implementierungs-Aufwand inkl. Roll-Out und Erstkonfiguration	6	
				"Schnellstart" möglich	2	
				Infrastrukturbedarf	6	
				Abhängigkeiten im Betrieb von Drittprodukten	10	
				Administrationskomponente (Übersichtlichkeit, Help Desk Unterstützung, Multidomain etc.)	10	
				Aufwand für die Administration des Systems im Betrieb	10	
				Summe		