GANEC
Kundenzentrierte IT-Lösungen

Übersicht über die von der GANEC GmbH angebotenen Verwaltungslösungen

	IronKey Enterprise Managed Service	*IronKey Enterprise Server*	*Kanguru KRMC Cloud*	*Kanguru KRMC Enterprise Edition*	*Blockmaster SafeConsole Enforce*	*Blockmaster SafeConsole Enforce&Enable*	*MXI Access Enterprise*
Betreiber der Lösung (H = Hersteller; K = Kunde)	H (Cloud-Lösung)	K	H (Cloud-Lösung)	K	K	K	folgt
Definition von Rollen (z.B. Administrator / Nutzer)	v	v	v	v	v #1	v #1	folgt
Definition von Benutzergruppen	v	x	v	v	v #1	v #1	folgt
zentrale Verteilung von Richtlinien (z.B. bezüglich des Passworts)	v	v	v	v	v	v	folgt
Active-Directory Unterstützung	x	x	x	v	v	v	folgt
zentrale Verteilung von Updates (z.B. Firmware)	v	v	x	v	x	v	folgt
zentrale Verteilung von Software	v #2	v #2	x	x	x	v	folgt
Einschränkung der Nutzbarkeit auf bestimmte vertrauenswürdige Netzwerke über "IP- Whitelist"	v	v	v	v	v #3	v #3	folgt
zentral verwalteter Anti-Virenschutz	v #4	v #4	v #4	v #4	x	x #5	folgt
zentrale Verteilung von Kontaktinformationen auf User-Sticks („Findertext“)	v	v	v	v	v	v	folgt
Unterstützung von Nutzern bei vergessenem Passwort	v	v	v	v	v	v	folgt
USB-Sticks können aus der Ferne vorübergehend deaktiviert werden	v	v	v	v	v	v	folgt
permanente Deaktivierung (= Zerstörung) von User-Sticks aus der Ferne	v	v	x	x	x	x	folgt
Nachrichtenversand an Sticks	x	x	v	v	x	x	folgt
Zurücksetzen von User-Sticks in den Grundzustand	v	v	v	v	v	v	folgt
zentrale Vorgabe, nach welcher Dauer der Inaktivität der Nutzer automatisch abgemeldet wird	x	x	v	v	v	v	folgt
Statistikfunktionen	v	v	v	v	v	v	folgt
integrierte Backuplösung	v #6	v #6	x	x	v	v	folgt
Besonderheiten (Auswahl)	der Administrator benötigt neben einem Passwort auch einen Admin-Stick zur Administration; neue Features werden zunächst in die Cloud-Lösung integriert, ca. 6-12 Monate später in die Server-Lösung	der Administrator benötigt neben einem Passwort auch einen Admin-Stick zur Administration; neue Features werden zunächst in die Cloud-Lösung integriert, ca. 6-12 Monate später in die Server-Lösung	weniger Funktionen als die Enterprise - Edition	verfügt gegenüber der Cloud-Lösung über weitere, zum Teil hier nicht aufgeführte Funktionen; optional: integrierte Endpoint-Security Lösung	optional können andere USB-Speichermedien blockiert werden	verfügt gegenüber der Enforce-Variante über weitere, z.T. hier nicht gelistete Funktionen; z.B. Single-Sign-on für geschützte Webseiten; Blockieren von bestimmten Dateitypen	die Details zur MXI Access Enterprise folgen in Kürze, vielen Dank für Ihr Verständnis

Diese Übersicht wurde von uns nach bestem Wissen und Gewissen erstellt. Die meisten Informationen basieren auf den Herstellerangaben. Es handelt sich aus Gründen der Übersichtlichkeit um eine vereinfachte Darstellung. Wir übernehmen für eventuelle Fehler und Irrtümer keine Haftung. Weitere Informationen finden Sie auf unserer Webseite www.ganec.de. Informieren Sie sich in unserem Online-Shop www.ganec-shop.de, welche Kosten entstehen, wenn Sie alle Features des jeweiligen Produkts nutzen möchten. Diese Übersicht darf ohne unsere Zustimmung weder kopiert, verändert noch weitergegeben werden. Stand: 14.09.2011 GANEC GmbH | Technologiepark 24 | 22946 Trittau | Tel: 04154/6025-14 | service@ganec.de

Hinweise:

#1 Da die Blockmaster SafeConsole nicht nur eine Unterstützung des Active Directorys mitbringt, sondern sehr auf dessen organisatorische Struktur zugeschnitten ist, sind auch die administrative Rollenverteilung sowie die Definition von Benutzergruppen von der bestehenden Struktur im Active Directory abhängig. Die Rollen „Administrator“, „Manager“ und „Support“ werden schon beim Einrichten der SafeConsole je einer Nutzergruppe im AD zugewiesen, so dass die innerhalb einer Rolle vorgesehenen Rechte automatisch auf alle Nutzer innerhalb der definierten Benutzergruppe übergehen. Auch Login-Informationen werden direkt aus dem AD für die administrative Nutzung der SafeConsole wiederverwendet. Die Verwaltung nach „Benutzergruppen“ innerhalb der SafeConsole funktioniert auf ähnlichem Wege, so dass gesonderte Richtlinien über die SafeConsole für gesamte organisatorische Gruppen des Active Directorys festgelegt werden können.
Für weitere Informationen (auch bezüglich einer Verwendung der SafeConsole ohne AD-Anbindung) kontaktieren Sie uns bitte.

#2 Die Verteilung von Software über die IronKey Enterprise Dienste ist auf die im Lieferumfang inbegriffene Software der IronKeys in der Enterprise Variante beschränkt – eigene Anwendungen lassen sich nicht zentral verwalten bzw. verbreiten.

#3 In der Blockmaster SafeConsole lassen sich sowohl der Zugriff auf die SafeConsole selbst, als auch die Nutzbarkeit von ausgewählten Funktionen auf dem SafeStick auf einen „vertrauenswürdigen Bereich“ beschränken – eine Black- bzw. Whitelist, die die gesamte Funktionalität des SafeSticks in „fremden“ Netzwerken unterbindet, bietet die SafeConsole aber nicht.

#4 Die Anti-Virus Lösungen des IronKeys und der Kanguru Defender sind bereits integriert und vorkonfiguriert - beim IronKey kommt McAfee zum Einsatz, die Kanguru Defender greifen auf BitDefender zurück. Durch die Verwendung des integrierten Anti-Virenschutzes entstehen gesonderte Nutzungsgebühren.

#5 Eine integrierte Anti-Virus Lösung gibt es in der SafeConsole nicht - auch für die SafeSticks selber ist in keiner Version ein Virenschutz vorgesehen, allerdings bietet die SafeConsole Enforce & Enable über den „Publisher“ die Möglichkeit, beliebige Programme, oder Dateien mit allen Nutzern der SafeConsole zu teilen und über die „Autostart Application“ Funktion mit bestimmten Parametern automatisch auszuführen, sobald ein SafeStick aufgeschlossen wird.
Auf diesem Wege ließe sich auch eine beliebige Anti-Virus Lösung auf dem SafeStick realisieren.

#6 Ein Backup der Dateien auf dem sicheren Laufwerk eines IronKeys ist über den Enterprise Dienst nicht vorgesehen – hier können lediglich das IronKey-Passwort, sowie die im Identity Manager hinterlegten Login-Informationen synchronisiert und gesichert werden. Zum reinen Datenbackup lässt sich allerdings die bereits im Stick hinterlegte „Secure Backup“ Funktion des IronKeys nutzen, mit der lokal (beispielsweise am Arbeitsplatz) verschlüsselte Backups erstellt, oder bereits gesicherte Daten wiederhergestellt werden können.
Der Zugriff auf die „Secure Backup“ Funktion kann über den Enterprise Dienst gesteuert werden.