

MANAGEMENT SYSTEM COMPARISON



SERVER DEPLOYMENT OPTIONS

US based datacenter	•	•
Hi Availability Option		•
Cloud multi-tenant SaaS	•	
Cloud single tenant SaaS		•
Global hosting options		•
Available as an On-Prem installation	Yes, VMware image	Yes, Windows installable, automigrate from 4.7/4.9

DEVICES TO MANAGE

Compatible Devices	Sentry ONE, IronKey D, S Series flash drives, DataLocker / Ironkey H300 / H350 hard drives	DataLocker Sentry ONE, SafeStick, Sentry K300, DL3 & DL3 FE, H300 / H350 hard drives, Origin SC100, Kingston DTVP30DM, DT4000DM, D300-M, D300-SM, S1000 (Require latest client software for D300-M and S1000)
Supported OS's	Windows (All devices), Mac and Linux (Select Devices)	Windows (All devices), Mac and Linux (Select Devices)

Forced management available?



GENERAL FEATURES

Active directory integration		•
Browser based service interface	•	•
Automatic inventory directory of all users and devices	•	•
Self-service plug-and-play device deployment	•	•
Centrally enforce security policies of devices	•	•
Accessible from mobile device		•
Filter and sort data tables		•
Search for devices and users	•	•
Two-factor authentication to management system	•	Mobile text message or token
Deployment Wizard	•	•
Information Dashboard	•	•
Optimized for large enterprises	•	•
Admin and role management	•	•
Multiple administrator roles	•	•
Dynamic licensing	•	•
Integrated help text in the user interface	•	•
Export data in CSV format	•	•
Group users without need of directory service	•	
Automated server updates		•
Device Software updates from console	•	•
Server/device locked to organization with a certificate		•



MANAGEMENT SYSTEM COMPARISON



SECURITY FEATURES AND CONFIGURATIONS

Custom device password policy	●	●
Device remote password reset over phone or Internet (Challenge/Response - PKI).	●	●
Device self-service remote reset	●	
Local device self-service password reset (PKI) using ZoneBuilder.		●
ZoneBuilder (automatic unlock on trusted user accounts)		●
Remotely reassign device to new user		●
Manage the device states. Automate with rules.		●
Self-service mark a device as "found" on successful unlock.		●
Offline restrictions for device usage	●	●
Custom return-to-owner message displayed on device if lost.	●	●
File Restrictions (white-list accepted file-types)		●
Inactivity Lock management	●	●
Device/User audit (Excel, XML)	●	●
File audit (Excel, XML, Syslog)		●
Audit reports	●	●
Device Backup	●	Integration available
Publisher file distribution		●
ZoneBuilder (restrict devices to work on select machines)		●
Autorun applications	●	●
Set offline devices to read-only	●	
Enable users to unlock drives in write protected mode	●	●
Collect and use device user information. Sort and search based on collected information in the Device Overview.		●
Customize device "about" screen		●
Manage portable antivirus on the devices	McAfee	McAfee
Audit trail for threat detections with McAfee AV	●	
Geo location of devices	●	●
Single Sign-On (SAML2, OKTA)		●
SIEM Integration		●
Customize Email Templates		●

Remote Device Management

Remotely reset device. (Can be scheduled)	●	●
Remotely kill devices	Zeroizes encryption keys and firmware	Zeroizes encryption keys
Remotely set device as disabled (Can be Scheduled)	●	●
Remotely set device as lost or to deny access to the device (Can be scheduled)	●	●