CryptoPro Secure Disk for BitLocker inkl. zentraler Managementkonsole

vs

BitLocker Drive Encryption mit Microsoft MBAM sowie BitLocker im Azure AD mit Intune

Gegenüberstellung

Die Komponenten CryptoPro Secure Disk for BitLocker und Microsoft MBAM/Intune bzw. Azure / Intune können Ergänzungen zueinander sein, erfüllen jedoch unterschiedliche Aufgabenstellungen.
Die Hauptaufgabe von Secure Disk ist die Benutzer-Authentisierung (kryptographische Authentisierung/Schlüsselübergabe) und Help Desk Funktionen, mittels einer eigenen BitLocker integrierten PreBoot-Technologie (PBA). In der PBA werden unterschiedliche Authentisierungsmethoden wie Name/Passwort (Windows credentials), Smartcard/Zertifikat, YubiKey und das Smartphone unterstützt.
Zusätzlich stehen dem Anwender umfängliche offline HelpDesk-Mechanismen zur Verfügung, wenn er seine Authentisierung credentials vergessen hat. Mit Hilfe des HelpDesk kann sich der Anwender, im offline Betrieb, jederzeit an seinem Betriebssystem anmelden um an seine Daten zu gelangen. Mit der zentralen Management-Komponente werden Security Policies für die Endgeräte, auf OU und Rechner Ebene, definiert und bereitgestellt.

Microsoft MBAM und Intune, sofern das Azure AD verwendet wird, (**note:** End of Microsoft Support, Juli 2019) konzentriert sich auf die zentrale Administration der BitLocker-Einstellungen, deren Verteilung, Überwachung und der Zuordnung unterschiedlicher Administrations-Rollen. Des Weiteren liegt ein Hauptbestandteil in dem Management des TPM und der Recovery-Key´s in Verbindung mit BitLocker. Die nachfolgende Darstellung gibt einen Überblick über die aktuellen Funktionen beider Technologien.

Release: 2.0 Datum: 30.09. 2020

Anforderungen an eine Festplattenverschlüsselung	Secure Disk for Bitlocker 7.x, inkl. Managementkonsole	Microsoft BitLocker mit MBAM	BitLocker mit Azure AD und Intune
Benutzerbezogene PreBoot-Authentisierung	Ja	Nein (nur Maschinen PIN)	Nein (nur Maschinen PIN)
Multi-User-Betrieb für BitLocker Authentisierung	Ja	Nein	Nein
Anmeldung mit Microsoft credentials (Name/Passwort) in der PBA	Ja	Nein	Nein
Anmeldung mit Smartcard und Zertifikat in der PBA	Ja	Nein	Nein
Anmeldung mit dem Smartphone in der PBA (2FA für BitLocker und Windows)	Ja	Nein	Nein
Passwort Policy gemäß Windows Einstellungen	Ja	Nein	Nein
Fingerprint Support (UPEC) in der PBA	Ja	Nein	Nein
Unterstützung internationaler Keyboard-Layouts/Sprachen in der PBA	Ja	Nein	Nein
Sicherer Bitlocker Betrieb ohne TPM	Ja	Ja	Ja
Gültigkeit des offline HelpDesk Schlüssel ist temporär einschränkbar (Anzahl Bootvorgänge oder Anzahl Tage)	Ja	Nein	Nein
Offline HelpDesk (Challenge/Response) für vergessene Windows-Passworte	Ja	Nein	Nein
Zentrales Enforcement/Policy-Management für Bitlocker Einstellungen	Ja / GPO	Ja	Ja
Zentrale Management-Konsole für Benutzer-Authentisierung und SSO	Ja	Nein	Nein
Absicherung der zentralen Datenbank mit HSM (Encryption Key für Datenbank)	Ja	Nein	Nein
Zentrales Management für TPM Einstellungen	Nein	Nein	Nein
Softwareverteilung mit Neustarts ohne Benutzerinteraktion z.B. via Wake-on-LAN bei aktiver BitLockerverschlüsselung	Ja	Ja	Ja

Anforderungen an eine Festplattenverschlüsselung	Secure Disk for Bitlocker 7.x, inkl. Managementkonsole	Microsoft BitLocker mit MBAM	BitLocker mit Azure AD und Intune
Single SignOn ans Betriebssystem (Verhinderung einer zweiten Benutzer-Anmeldung)	Ja	Nein	Nein
Verschlüsselung von virtuellen Festplatten mit BitLocker (VMware, ESX, Hyper-V, o.ä.)	Ja	Ja	Ja
Zentrale Policy auf pro Maschine via zentralem Management	Ja	Ja	Ja
Zentrale Verwaltung der BitLocker Recovery Keys in zentraler Datenbank	Ja	Ja	Ja
Verschlüsselte Ablage der BitLocker Recovery Keys in der Datenbank	Ja	Ja	Nein
Zentrales Protokollverzeichnis für Bitlocker Vorfälle	Ja	Ja	Ja
Trennung von AD-Administratoren und BitLocker Administratoren	Ja	Ja	sehr eingeschränkt
Network Unlock Betrieb: (Kabel) Client Authentisierung im sicheren LAN gegen einen Server anstatt lokale PBA-Anmeldung	Ja	Ja	Ja
Network Unlock Betrieb: (WLAN) Client Authentisierung im sicheren WLAN gegen einen Server anstatt PBA-Anmeldung	Ja	Nein	Nein
Network Unlock Betrieb bei eingeschalteter 802.1x Sicherheit	Ja	Nein	Nein
Compliance-Reports: Status je Rechner	Ja	Ja	Ja
Offline Challenge/Response: HelpDesk für vergessene Passworte	Ja	Nein	Nein
Online User-Self-Service Portal um den BitLocker Recovery Key zu erhalten	Nein (API vorhanden)	Ja nur online verfügbar	Ja (nur online/Internet)
Offline User-Self-Service für vergessene Anmelde Credentials in der PBA	Ja	Nein	Nein
BitLocker Enterprise Compliance Dashboard (zeigt grafisch Verschlüsselungs-Status etc.)	Ja	Ja	Ja

Anforderungen an eine Festplattenverschlüsselung	Secure Disk for Bitlocker 7.x, inkl. Managementkonsole	Microsoft BitLocker mit MBAM	BitLocker mit Azure AD und Intune
Virtuelle Tastatur für Tablets	Ja	Hardware-Abhängig, 3	Hardware-Abhängig, 3
Mandantenfähigkeit: Zuordnung von Administratoren zu bestimmten OUs (Organisations-Units))	Ja	Nein	Nein
Detaillierte HelpDesk Protokollierung	Ja	Ja	Ja
HelpDesk Calls können Benutzer zugewiesen werden	Ja	Nein	Nein
Hintergrundbild in der PBA wählbar	Ja	Nein	Nein
Barrierefreiheit: Sprachausgabe in der PBA für sehbehinderte Anwender	Ja	Nein	Nein
Eigener Mechanismus zum Shutdown in der PBA, wenn längere Zeit keine Eingabe erfolgt	Ja	Nein	Nein
Zentrales Löschen (Wiping) des Schlüsselmaterials auf dem Client	Ja	Nein	Nein
Überwachung der Client-Verschlüsselung, z.B. beim Anhalten von Bitlocker durch einen lokalen Admin. Ein Service führt zur automatischen Aktivierung der Verschlüsselung, gemäß Policy	Ja	Nein	Ja, über Konformitätsrichtlinien
Support von Secure Boot, Credential Guard	Ja	Ja	Ja
Option: Virencheck aus der PBA heraus bei nicht gestartetem Windows (On Demand Scan von BitLocker verschlüsselten Festplatten)	Ja	Nein	Nein
Steuerung des Zugriffs auf die Bitlocker Recovery Keys?	Ja, über User/Gruppen	Ja, über User/Gruppen	Alle Global Admins und Intune Admins haben Zugriff
Erneuerung des Schlüsselmaterials nach Herausgabe bzw. Verwenung des BitLocker Key´s	Ja	Ja	Ja
Anmeldung vor BitLocker mit Azure AD Credentials (Azure AD Native, kein Legacy AD vorhanden)	Ja (mit Workaround)	Nein	Nein

CryptWare IT Security GmbH
Frankfurter Str.2 ♦ D-65549 Limburg/Lahn
E-Mail: info@cryptware.eu ♦ Tel: +49 (0) 6431 97 77 90-0