cryptware
secure your way

CryptoPro
Unlock Anywhere for BitLocker

Die meisten Unternehmen und Behörden/Verwaltungen wünschen sich einen nachweisbar sicheren BitLocker-Betrieb ohne die Nachteile einer zusätzlichen PreBoot-Authentifizierung (TPM+PIN) sowie die zentrale Administration in einer Cloud-Umgebung.

Mit der cloudbasierten Netzwerkentsperrung können BitLocker-fähige Computer ohne Benutzereingriff, sprich ohne Benutzer-Authentisierung, direkt in Windows booten und sich dort mit ihrer gewünschten Authentisierungsmethode anmelden. Diese passwortlose Authentifizierung bietet nicht nur einen hohen Benutzerkomfort und hohe Sicherheit, sondern vereinfacht auch die internen IT-Prozesse und senkt die Kosten im HelpDesk.

Bis heute führte die Abschaltung der BitLocker-PreBoot-Authentisierung (TPM+PIN) immer dazu, dass die Computer unsicher sind! Die neue cloud basierte BitLocker-Unlock-Technologie verbindet nun diese Kundenanforderung mit hoher Sicherheit. Ein weiterer Vorzug der Technologie ist, dass Computer zentral in der Cloud gesperrt werden können. Dadurch steht dem Computer kein Schlüsselmaterial mehr zur Verfügung, um das Windows-Betriebssystem zu starten (Remote Lock). Eine ideale Lösung im Fall eines Computerdiebstahls, Verlustes oder temporärer Nichtnutzung des Endgerätes (Urlaub, Krankheit, etc.)

Systemanforderung Server:

- Windows 10 (64 Bit)
- Windows 11 (64 Bit)

Systemanforderungen Cloud Service:

- Docker (Linux Container)
- Microsoft Kestrel Webserver
- Microsoft Azure SQL Datenbank

Übersicht der Funktionen:

- Cloudbasierte passwortlose Entsperrung eines BitLocker verschlüsselten Computers
- Sicherheit: Anerkannte OTP-Technologie mit TPM und TSL
- Zentrale Administration und Konfiguration in der Cloud (Zero Admin)
- Backupfunktion der Recovery-Daten aus der Cloud in das Netzwerk des Endkunden
- Offline HelpDesk
- Client-Kommunikation: Netzwerkkabel, WLAN, 802.1X
- Endgeräte benötigen keine hardwareabhängige Konfiguration
- Mandantenfähiges Konzept, ideal für Managed-Cloud-Anbieter
- Zentrale Sperrfunktion "Remote-Lock", Endgerät kann Windows nicht mehr starten

Vorteile der Lösung:

- Wegfall der Pre-Boot-Authentifizierung für den Anwender
- Wegfall der TPM+PIN Authentifizierung
- Passwortlose Authentifizierung, erhöht die Benutzerakzeptanz und Sicherheit
- Zentrale Verwaltung in der Cloud bietet Kosteneffizienz, Skalierbarkeit und Flexibilität (Mandantenfähigkeit wird gewährleistet)
- Keine Änderung von bestehenden IT-Prozessen (Softwareverteilung, Patchmanagement, etc.)
- Backup der Recovery-Keys sichert die Wiederherstellung im Falle eines Ausfalls
- Remote-Lock (Sperrfunktion) stellt sicher, dass verlorene oder gestohlene Endgeräte nicht mehr verwendet werden können. Die Fernsperrfunktion wird ohne Internetzugang ermöglicht.

cryptware
secure your way

CryptWare IT Security GmbH
Frankfurter Str. 2
65549 Limburg

Phone: +49 (0) 6431 977790 - 0
Fax: +49 (0) 6431 977790 - 22
info@cryptware.eu

www.cryptware.eu