opentext™

Datenblatt

ZENworks Full Disk Encryption

Implementieren Sie Richtlinien, um sicherzustellen, dass alle Festplatten mit sensiblen Daten verschlüsselt werden und die Daten selbst bei Diebstahl oder Verlust des jeweiligen Geräts geschützt sind. Setzen Sie auf eine Verschlüsselung, die den Handlungsspielraum Ihrer IT-Abteilung bei der Ausübung ihrer Verwaltungsaufgaben nicht beschneidet.

Produktübersicht

Mit OpenText ZENworks Full Disk Encryption lassen sich Richtlinien zur Verschlüsselung ganzer Festplatten unter Windows 7, Windows 8 und Windows 10 zentral implementieren. Die Verwaltung erfolgt über dieselbe Webkonsole und denselben Adaptive Agent, die bzw. den Sie bereits von anderen OpenText ZENworks Produkten kennen.

Hauptvorteile

ZENworks Full Disk Encryption erfüllt sowohl die Datenschutzanforderungen Ihres Unternehmens als auch alle wichtigen gesetzlichen Vorschriften, ohne dabei die Verwaltung Ihrer Assets zu erschweren:

- Zuverlässiger Schutz Ihrer Unternehmensdaten durch die bewährte Verschlüsselung der gesamten Festplatte.
- Einfache Verwaltung verschlüsselter Geräte innerhalb des gesamten Unternehmens. Geräte, die mit Full Disk Encryption verschlüsselt wurden, können remote entsperrt werden, sodass die Produktivität mobiler Mitarbeiter nicht durch gesperrte Geräte beeinträchtigt wird.
- Einhaltung branchenspezifischer Bestimmungen und gesetzlicher Auflagen zum Schutz von Kunden- und Patientendaten.
- Nutzung Ihrer Erfahrung mit ZENworks zur Senkung der Kosten für die Implementierung von Full Disk Encryption.

Hauptfunktionen

ZENworks Full Disk Encryption ist Teil der ZENworks Plattform, die eine einheitliche, webbasierte Konsole, einen zentralen ZENworks Adaptive Agent und ZENworks-Serversoftware enthält. Das Produkt bietet die folgenden integrierten Funktionen zur Festplattenverschlüsselung:

Datenschutz

- Federal Information Processing Standards (FIPS) 140-2 Level-2-Verschlüsselungsmodul für OPAL-Hardwareverschlüsselung
- FIPS 140-2 Level-1-Verschlüsselungsmodul für softwarebasierte Verschlüsselung
- Fordert den Benutzer vor dem Start des Systems (Pre-Boot) auf, sich durch Eingabe von Benutzername und Passwort zu authentifizieren. Alternativ dazu kann die Authentifizierung auch über eine Smartcard mit PIN erfolgen.
- Ermöglicht die sofortige Deaktivierung jedes beliebigen Geräts, das sich innerhalb der Reichweite des ZENworks Servers befindet.
- Umfasst ein eigenständiges Tool zum Testen selbstverschlüsselnder OPAL-Laufwerke, um festzustellen, ob sie mit ZENworks Full Disk Encryption kompatibel sind

Auswahl der zu verschlüsselnden Geräte von einem zentralen Ort aus

- Über eine zentralisierte, browserbasierte Benutzeroberfläche können Sie im Handumdrehen Verschlüsselungsrichtlinien für Ihre Geräte erstellen.
- Dank eines Firewall-freundlichen Agent lassen sich die Richtlinien ganz einfach auf jedes Gerät anwenden, das sich über eine standardmäßige HTTP-Verbindung mit dem ZENworks Server verbinden kann.
- Umfassende Richtlinien ermöglichen die zentrale Verwaltung von OPAL-Hardwareverschlüsselung und Festplattenverschlüsselung via ZENworks Software.

Systemanforderungen

Genaue Angaben zum Produkt und zu den Systemanforderungen erhalten Sie unter: **www.microfocus.com/de-de/products/zenworks-suite/overview**

Stets das Neueste erfahren

- Darüber hinaus bietet das Produkt die Option, anstelle der Pre-Boot-Authentifizierung die Windows-Authentifizierung zu nutzen. Auf diese Weise wird der Schutz der Festplatte gewährleistet, ohne die Benutzerfreundlichkeit zu beeinträchtigen.
- Eine entsprechende Einstellung verhindert, dass das Laufwerk ohne Administratoreingriff entschlüsselt wird, wenn eine Full Disk Encryption-Richtlinie von einem Gerät entfernt wird.

Aufrechterhaltung der Benutzerproduktivität

- Benutzer müssen ihre Geräte nicht mehr mit ins Büro bringen, um sie verschlüsseln zu lassen.
- Dank zentralisiertem Schlüsselmanagement haben Ihre IT-Mitarbeiter bei einem Hardwareausfall stets Zugriff auf die Verschlüsselungsschlüssel.
- Die Pre-Boot-Authentifizierung lässt sich von zentraler Stelle aus deaktivieren, sodass IT-Mitarbeiter Benutzern, die ihr Passwort vergessen haben, ganz einfach Zugriff gewähren können.
- Die Verschlüsselung ist für den Benutzer vollkommen transparent, d. h., die Benutzererfahrung bleibt – abgesehen von der Pre-Boot-Authentifizierung – dieselbe.
- Die Ver- und Entschlüsselung findet im Hintergrund statt.

Erfahren Sie mehr unter
www.opentext.com

opentext™