Einfache, umfassende und flexible Datensicherheit für Ihr gesamtes Unternehmen

Dell Encryption

Heutzutage müssen Unternehmen sowohl Endgeräte als auch die darauf befindlichen Daten sichern und zugleich die Mobilität der Mitarbeiter stärken. Herkömmliche Verschlüsselungslösungen bieten nur begrenzte Möglichkeiten und schränken Bereitstellungen, Umfang der Endgeräteabdeckung und Leistung für Benutzer ein. Herkömmliche Verschlüsselungslösungen versuchen zwar, diese Anforderungen zu erfüllen, sind aber oftmals kompliziert in der Bereitstellung und Verwaltung, decken nicht alle Endgeräte ab und bieten Benutzern keine ausreichende Leistung.

Dell Encryption Enterprise bietet mit seiner flexiblen Verschlüsselungstechnologie unterschiedliche Möglichkeiten zum Schutz Ihrer Daten. Dazu gehören ein datenzentrierter und richtlinienbasierter Ansatz und ein Ansatz zur vollständigen Festplattenverschlüsselung. Die Lösung ist konzipiert für:

– Einfache Bereitstellung

– Transparenz für Endbenutzer

– Unkomplizierte Einhaltung von Vorschriften

– Einfache Verwaltung über eine zentrale Konsole

Dell Encryption steht für ein flexibles Angebot an optimierten Sicherheitslösungen, die Folgendes umfassen: dateibasierte Verschlüsselung, vollständige Festplattenverschlüsselung, verbesserte, zentralisierte Verwaltung nativer Verschlüsselungen (Microsoft BitLocker und Mac FireVault) sowie Schutz von Daten auf externen Medien, selbstverschlüsselnden Festplatten und mobilen Geräten.

Dell Encryption Enterprise

Dank Dell Encryption Enterprise können IT-Abteilungen Verschlüsselungsrichtlinien problemlos durchsetzen, ganz unabhängig davon, ob sich die Daten auf dem Systemlaufwerk oder auf externen Medien befinden. Die Endbenutzer selbst müssen nicht eingreifen.

Als perfekte Lösung für heterogene Umgebungen bietet Encryption Enterprise folgende Vorteile:

- Automatische Bereitstellung und Provisionierung bei werkseitiger Installation auf kommerziellen Dell Geräten
- Bereitstellung in VMware Umgebungen in weniger als 30 Minuten durch assistentengestützte Installation sowie vollständig integrierte Datenbank- und Schlüsselverwaltung
- Keine Notwendigkeit für eine Defragmentierung vor der Verschlüsselung
- Verschlüsselung für Systemdatenträger und externe Medien in einer einzigen Lösung
- Wählen Sie die vollständige Festplattenverschlüsselung oder dateibasierte Verschlüsselung, beide softwarebasiert
- Problemlose Compliance-Verwaltung und -Überwachung mit Compliance-Richtlinienvorlagen, die per einfachem Tastendruck aufgerufen werden können, sowie Funktionen für Remote-Verwaltung und schnelle Systemwiederherstellung
- Nahtlose Integration in vorhandene Prozesse für Authentifizierung, Patching und mehr
- Vertrieb und Support für Ihre Hardware und Sicherheitslösungen aus einer Quelle
- Verschlüsselung aller Daten (außer Dateien, die wichtig für den Start des Betriebssystems sind) oder vollständige Festplattenverschlüsselung, je nach Ihren Präferenzen
- Erweitertes Port-Steuerungssystem zur Verhinderung von Datenlecks
- Verschlüsselung basierend auf Endbenutzerprofilen, Daten und Gruppen innerhalb Ihrer Organisation
- Zentrale Verwaltung aller Verschlüsselungsrichtlinien, einschließlich selbstverschlüsselnder Festplatten, vollständiger Festplattenverschlüsselung und Verschlüsselung durch Microsoft BitLocker
- Verbesserte Authentifizierung für OPAL-konforme Geräte, einschließlich einmalige Anmeldung im Betriebssystem per Authentifizierung vor dem Startvorgang mithilfe von Smartcards und Kennwörtern

Der Dell Encryption Vorteil

Umfassender Schutz, hohes Maß an Sicherheit

- Schützt Daten auf allen Geräten und externen Medien
- Gefährdet keine Master Boot Records oder Schlüssel

Produktivität und Einfachheit für IT und Endbenutzer

- Wählen Sie Security Management Server Virtual für vereinfachte Bereitstellungen oder Security Management Server zum Skalieren zu Tausenden Benutzern
- Nahtlose Integration mit bestehenden Systemverwaltungs- und Authentifizierungsprozessen
- Für Endbenutzer transparente Verschlüsselung zur Aufrechterhaltung der Produktivität

Flexible Verschlüsselung

- Basierend auf Endbenutzerprofilen, der Vertraulichkeit von Daten sowie Leistungs- oder Compliance-Anforderungen
- Verschlüsselung von Daten auf externen Medien oder vollständige Deaktivierung aller Ports, während Geräte ohne Speicherfunktion weiterhin funktionieren
- Verwaltung und Überprüfung von Microsoft BitLocker sowie selbstverschlüsselnden Laufwerken für eine bessere Compliance

Dell Security Management Server Virtual

Dell setzt ganz neue Maßstäbe für die schnelle, unkomplizierte Bereitstellung und Inbetriebnahme der Verschlüsselungslösung Dell Encryption in den meisten mittelgroßen Unternehmensumgebungen mit bis zu 3.500 Endgeräten. Dies gelingt Dell mit einer vereinfachten Bereitstellung mit einem maßgeschneiderten virtuellen Verwaltungsserver und einer Konsolenanwendung für VMware.

Mit Dell Security Management Server Virtual wird Dell Encryption zur idealen Lösung für KMUs, die bereits VMware Lösungen besitzen und nach einer einfachen, schnell bereitstellbaren Verwaltungsplattform für ihre Verschlüsselungs- und Authentifizierungsrichtlinien suchen. Die Lösung vereint sämtliche Funktionen und Vorteile des Standardservers, zu denen auch die vollständige Unterstützung für die umfassenden Verschlüsselungsoptionen gehört, die für Notebooks, Desktop-PCs und externe Medien verfügbar sind.

Verwaltung selbstverschlüsselnder Festplatten mit Dell Encryption Enterprise

Organisationen, die selbstverschlüsselnde Festplatten (Self-Encrypting Drives, SEDs) verwenden, sind zusätzlich auf eine sorgfältige Verwaltung angewiesen, wenn sie das Risiko von Datenverlusten wirksam reduzieren und ihre Audit- und Compliance-Ziele erreichen möchten.

Dell Encryption Enterprise ermöglicht die zentrale und sichere Verwaltung von selbstverschlüsselnden Festplatten in Ihrem gesamten Unternehmen, sowohl lokal als auch remote. Alle Richtlinien-, Authentifizierungs- und Verwaltungsaufgaben sowie das Speichern und Abrufen von Verschlüsselungsschlüsseln können über eine zentrale Konsole ausgeführt werden. So wird der Aufwand für die Sicherung wichtiger Daten ebenso reduziert wie das Risiko, dass Systeme bei Verlust oder nicht autorisierten Zugriffen ungeschützt sind. Was jedoch am wichtigsten ist: Die Verwaltung für OPAL-Standardgeräte ist vollständig in dieselbe Data-Protection-Plattform integriert wie die dateibasierte Verschlüsselung, die Verschlüsselung durch Microsoft BitLocker und die Verschlüsselung von Wechselmedien.

Zu den Remote-Verwaltungsfunktionen gehören:

- Deaktivierung von Anmeldungen und Löschung von Benutzer-Caches zum Schutz von Daten und zur Gewährleistung, dass nur ein autorisierter Administrator den Zugriff auf die geschützten Daten wieder aktivieren kann
- Deaktivierung des Geräts, damit sich Benutzer erst dann beim System anmelden können, wenn ein Befehl zum Entsperren ausgegeben wurde
- Aktivierung des Geräts, damit sich Benutzer für die Nutzung der selbstverschlüsselnden Festplatte anmelden können
- Durchführung einer automatischen Remote-Entsperrung der Festplatte, damit Administratoren wichtige Aufgaben, wie z. B. Patching, ausführen können, ohne dass das entsprechende Gerät über Nacht entsperrt bleiben muss
- Vollständige Authentifizierung vor dem Startvorgang, einschließlich Authentifizierung über Active Directory
- Festlegung von Richtlinien für die automatisierte Reaktion auf Angriffe (einschließlich Brute-Force-Angriffen)

Verwalten der vollständigen Festplatten-verschlüsselung mit Dell Encryption Enterprise

Unternehmen, die die vollständige Festplattenverschlüsselung nutzen, können rund um die Uhr sensible Daten schützen, die sich auf dem PC und weiteren Endgeräten befinden. Mit der neuesten Funktion von Dell Enterprise Encryption, der vollständigen Festplattenverschlüsselung, können Sie die herausfordernden Anforderungen der Datensicherung effektiv erfüllen. Vorteile der vollständigen Festplattenverschlüsselung:

- Ergänzt unser aktuelles Angebot an Verschlüsselungsoptionen und macht unsere Verschlüsselungslösung zu einer der solidesten in der Branche
- Bietet für Enterprise-Bereitstellungen die Authentifizierung vor dem Startvorgang der Enterprise-Klasse

- Verwendet TPM zum Schutz von Schlüsseln; Angreifer können so keine Festplatten aus der Plattform entfernen oder Offline-Angriffe auf verschleierte Schlüssel, die sich auf dem Laufwerk befinden, durchführen
- Verschlüsselt alle lokalen Festplatten in einem vereinfachten Bereitstellungs- und Remote-Verwaltungs-Framework
- Bietet eine einfach zu verwaltende Verschlüsselungstechnologie, die mit minimalem Aufwand aktiviert und verwaltet werden kann
- Ein herausragendes, transparentes Benutzererlebnis
- Mit der unternehmenstauglichen Authentifizierung vor dem Startvorgang bietet die vollständige Festplattenverschlüsselung folgende Vorteile:
  - o Einmalige Anmeldung im Betriebssystem und Netzwerk
  - o Support für einen Client/mehrere Benutzer
  - o Einfache Wiederherstellung von Verschlüsselungsschlüsseln und Datenzugriff durch den Administrator

Hinweis: Die vollständige Festplattenverschlüsselung von Dell wird derzeit auf kommerziellen Dell PCs (ab X7) im UEFI-Startmodus mit dem Authentifizierungsfaktor Kennwort unterstützt. Nicht von Dell stammende PCs und der Legacy-Startmodus mit Smartcard-Authentifizierung werden in nachfolgenden Versionen unterstützt.

Dell Encryption – Funktionen und Vorteile

Vereinfachung von Bereitstellung und Verwaltung

Da Sie eine Lösung benötigen, die sich einfach bereitstellen und verwalten lässt, ohne Ihre vorhandenen IT-Prozesse zu beeinträchtigen, bietet Ihnen Dell Encryption folgende Vorteile:

- Automatische Einrichtung und Bereitstellung für Benutzer, wenn Dell Encryption auf ausgewählten kommerziellen Dell Geräten werkseitig vorinstalliert ist
- Bereitstellung der Lösung in VMware Umgebungen in weniger als 30 Minuten[1] mit vollständig integrierter Datenbank- und Schlüsselverwaltung im Vergleich zu typischen Mitbewerberlösungen, die mehrere Server, eine separate Datenbank und mehrere Lizenzen erfordern
- Schnelle Bereitstellung ohne eine zeitaufwendige vollständige Defragmentierung aller betroffenen Festplatten
- Implementierung einer sofort einsatzbereiten Lösung, die keinerlei Neukonfiguration erfordert und sich problemlos in Ihre bestehenden IT-Prozesse integrieren lässt
- Integration der Lösung in vorhandene Authentifizierungsprozesse wie Windows-Kennwörter, RSA, Fingerabdrücke und Smartcards
- Fehlerbehebung, Schutz und Governance dank schneller Geräteerkennung sowie Durchsetzung und Überwachung der Verschlüsselung
- Verschlüsselung vertraulicher Benutzerdateien oder -daten, sogar wenn die IT Zugriff auf Ihr Endgerät benötigt
- Vollständige Integration der Verwaltung von OPAL-konformen Geräten in eine zentrale Konsole für alle Endgeräte
- Endgeräteschutz in heterogenen Umgebungen unabhängig von Benutzer, Gerät oder Ort

Einfachere Compliance

Dell Encryption verfügt über vordefinierte Richtlinienvorlagen, mit denen Sie den Compliance-Anforderungen der verschiedensten gesetzlichen Bestimmungen problemlos gerecht werden:

- Branchenvorschriften: PCI DSS, Sarbanes Oxley (SOX)
- Bestimmungen der US-Regierung und -Bundesstaaten HIPAA und HITECH Act, Gramm-Leach-Bliley Act; Kalifornien, SB1386; Massachusetts, 201 CMR 17; Nevada, NRS 603A (setzt PCI DSS voraus) und über 45 weitere US-Gesetze auf bundesstaatlicher und staatlicher Ebene
- Internationale Vorschriften: Die US-europäische Safe Harbor-Vereinbarung, die EU-Richtlinie zum Schutz personenbezogener Daten 95/46/EC, das britische Datenschutzgesetz, das deutsche Bundesdatenschutzgesetz (BDSG) und ähnliche Gesetze, die in den EU-Mitgliedsstaaten gelten, Kanada (PIPEDA)

Technische Daten

Dell Encryption Enterprise kann in Umgebungen mit Komponenten verschiedener Anbieter eingesetzt werden, die die unten aufgeführten Anforderungen erfüllen.

Unterstützte Client-Betriebssysteme:

- Microsoft Windows 7 Ultimate, Enterprise und Professional Edition
- Microsoft Windows 8 und 8.1 Enterprise und Professional Edition
- Microsoft Windows 10 Education, Enterprise und Pro Edition
- Mac OS X El Capitan, Sierra

Dell Security Management Server ist in folgenden Betriebssystemumgebungen validiert worden:

- Windows Server 2008 R2 SP0-SP1, 64 Bit (Standard und Enterprise Edition)
- Windows Server 2012 R2 (Standard und Datacenter Edition)
- Windows Server 2016 (Standard und Datacenter Edition)
- VMware ESXi 5.5, 6.0 und 6.5
- VMware Workstation 11 und 12.5

Die folgenden Internetbrowser bieten Unterstützung für die Remote-Verwaltungskonsole und Compliance Reporter:

- Internet Explorer 11.x oder nachfolgende Versionen
- Mozilla Firefox 41.x oder nachfolgende Versionen
- Google Chrome 46.x oder nachfolgende Versionen

Endbenutzerproduktivität

Dell weiß, dass ein Betrieb mit Maximalkapazität, ohne Unterbrechungen oder Verzögerungen, unerlässlich für Ihren Erfolg ist. Aus diesem Grund sind alle unsere Lösungen vollkommen transparent. Unterbrechungen während der Geräteverschlüsselung werden nahezu gänzlich vermieden. Da die Verschlüsselung der Geräte äußerst unauffällig im Hintergrund ausgeführt wird, wird sie von den Benutzern häufig nicht einmal bemerkt.

Bereitstellungsservices

Lassen Sie uns Ihre Lösung bereitstellen. Wir verfügen über ein vollumfängliches Portfolio an Services zur Bereitstellung von Sicherheitslösungen in Ihrer Umgebung. Unser Team an Cybersicherheitsexperten bewertet zuerst Ihre Umgebung, um Bereiche zu ermitteln, in denen Verbesserungen bei Datensicherheit auf Endgeräten, Servern, Cloud-Daten und mobilen Geräten notwendig sind. Anschließend implementieren, optimieren und verwalten wir Ihre Lösung.

Umfangreicher Verschlüsselungsschutz

Vertrauen Sie auf Dell Encryption und schützen Sie Ihre wertvollen Daten auf allen Geräten, externen Medien und in öffentlichen Cloud-Speichern ohne Produktivitätseinbußen. Die Lösung ist ein weiteres leistungsstarkes Dell Produkt, mit dem Sie effizienter arbeiten und Prozesse optimieren können. Weitere Informationen zu Dell Data Security finden Sie unter Dell.com/DataSecurity.