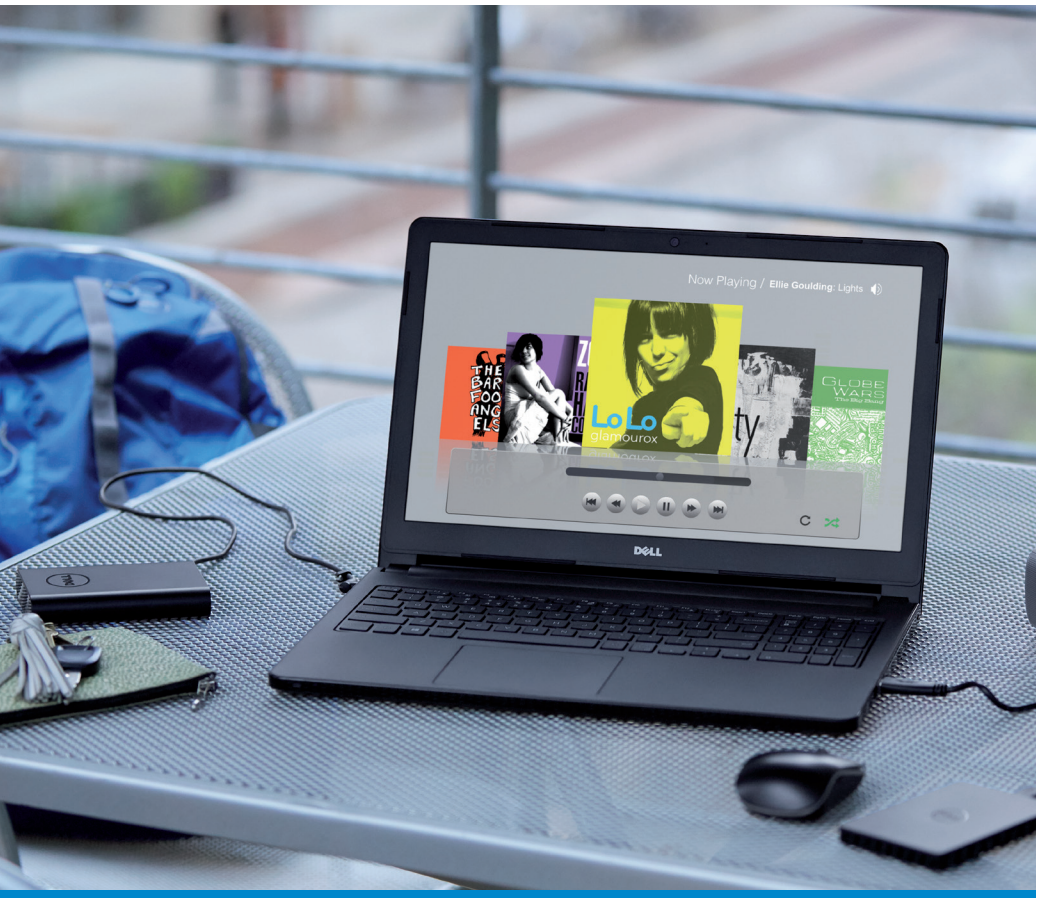
Encrypting global devices quickly and transparently

Dell protects data on 100,000 laptops with a flexible encryption solution that keeps business and IT employees around the world mobile and productive



"We never told our users we were encrypting their devices with DDP | E, and they didn't even realize that their system had been encrypted unless they checked the toolbar. That's when we knew we had real success."

Alan Daines, Chief Information Security Officer and Executive Director, Dell

Customer profile

Company	Dell
Industry	Technology
Country	United States
Employees	100,000
Website	www.dell.com

Business need

To comply with regulations, increase staff efficiency and allow employees to work anywhere, Dell needed to encrypt data on a global scale without disrupting IT or business workflows.

Solution

Dell deployed its endpoint data security solution that runs transparently on devices, provides FIPS 140-2 Level 3 encryption and gives IT staff a centralized console to manage all encryption policies.

Benefits

- Protects data on 100,000 laptops with consistent and granular policies
- Keeps employees productive with nondisruptive encryption
- IT tasks that used to take days now take minutes
- Easy deployment and instant insight into devices' encryption status
- Simplifies regulatory compliance

Solutions at a glance

- Data Protection & Encryption

Data is the lifeblood of business. To realize their full potential, organizations must protect data from increasing security threats without slowing productivity. When encryption solutions restrict data flow or are difficult to use, a well-intentioned employee may stop a critical process from running, possibly creating risk and compliance issues. Companies also need encryption tools that support greater control and customization so that they can meet changing requirements.

"We can instantly see how many devices are encrypted and how often they check in with the server from the single, centralized DDP | E console. We can sort views based on device type, users and encryption levels — and generate reports in minutes."

Ralph Miller, Security Engineer, Dell

To give staff the freedom to work outside of the office, Dell encrypts every one of its employee laptops using multiple levels of FIPS 140-2 encryption. As a manufacturer, Dell must also keep its supply chain information confidential so it can compete. Other security requirements come from the U.S. Securities Exchange Commission (SEC), whose regulations call for companies to protect sensitive information about products, employees and clients.

Over the past decade, Dell has deployed three different third-party encryption solutions. Each proved unreliable and time-consuming to use. IT personnel often sent messages to employees describing what encryption popup messages looked like and how to handle them. When updates occurred, IT staff had to remind employees to plug in laptops and reboot in the evening, because encryption processes would render them unusable for at least four hours. In addition, there was no easy way to apply encryption settings consistently across all sites or to see whether devices were still encrypted. Generating audit reports was also a slow, manual process. Alan Daines, chief information security officer and executive director at Dell, says, "Encrypting 100,000 devices is a daunting task, but proving that they all remain encrypted is the bigger challenge, especially from an audit perspective."

Creating an enterprise-grade solution

When Dell acquired Credant Technologies, it also acquired an encryption solution. Dell engineers modified it to meet enterprise-grade requirements, branded it as Dell Data Protection | Encryption and implemented it globally. To ensure a smooth rollout, engineers deployed DDP | E on Dell Latitude laptops, notebooks and Ultrabooks™ one region at a time. After verifying that encryption processes were successful, they confirmed that devices were communicating with the DDP | E server at preconfigured intervals. This communication is critical to ensure that devices can regularly confirm whether they're still encrypted and to receive software updates if required.

Today, encryption processes no longer disrupt employee productivity. Daines says, "We never told our users we were encrypting their devices with DDP | E, and they didn't even realize that their system had been encrypted unless they checked the toolbar." Ralph Miller, security engineer at Dell, says, "That's when we knew we had real success. There's less friction to users and devices

Products & Services

Hardware

Dell Latitude Laptops, Tablets and Ultrabooks

Software

Dell Data Protection | Encryption (DDP | E)

with DDP | E because it only encrypts files, folders or the entire PC as needed."

Increasing control and insight

Engineers now create and enforce enterprisewide encryption policies using profile information from Active Directory. For example, the laptops of financial executives and development engineers may be encrypted with FIPS 140-2 Level 3, the highest level commercially available. One group of devices might check in with the server once each day while another group might check in every few hours. "We can apply encryption parameters to specific types of users, machines and user groups quickly and consistently across all sites, because DDP | E works with our existing user profiles," says Miller. "We can also make sure that if encryption settings are changed at the device level for users, the encryption settings for their other devices will automatically be updated, too. Having that level of granularity within a hierarchical framework is really powerful."

Automating processes save time and minimize risk

To make sure that employees can immediately use a new laptop, engineers configured DDP | E so that it detects and encrypts new devices as soon as they connect to the Dell network. Processes are reliable because DDP | E identifies which operating system and applications run on the device so it uses the appropriate installation files. "The encryption process is now automatic without any intervention by human hands," Miller explains. "And people can work while it's happening."

Eliminating days of work and simplifying SEC compliance

Day-to-day management is also easier. "We can instantly see how many devices are encrypted and how often they check in with the server from the single, centralized DDP | E console," Miller explains. "We can sort views based on device type, users and encryption levels — and generate reports in minutes rather than the sometimes four days it used to take us." Daines continues, "If a device is lost or stolen, we can see when it last verified that it was encrypted, and we can also remotely unlock, wipe and disable a device. We can have a high degree of confidence that the data cannot be accessed."

Evolving the product to meet changing global needs

By using its own encryption product, Dell can continually update it to support emerging security and business requirements. "Our development team has the benefit of a 100,000-device sandbox with DDP | E," explains Daines. "We see every possible scenario including devices, operating systems and software versions. Our latest version of DDP | E reflects a huge amount of feedback and lessons learned. We've gone through all of the teething pain of deploying a global encryption solution so that our customers don't have to. If we can scale the product to meet our enterprise needs, then it's safe to say our customers can."

"Our development team has the benefit of a 100,000-device sandbox with DDP | E. ... If we can scale the product to meet our enterprise needs, then it's safe to say our customers can."

Alan Daines, Chief Information Security Officer and Executive Director, Dell

View all Dell case studies at Dell.com/CustomerStories