DELL
DISTRIBUTED DEVICE MANAGEMENT

PRODUCT AND ARCHITECTURAL OVERVIEW
Dell™ ProManage Services

www.dell.com/services
# Table of Contents

Key Challenges for Managing Distributed Client PCs ................................................................. 3  
Introduction ........................................................................................................................................ 3  
The Need for an Internet Based Platform .......................................................................................... 4  
Dell Distributed Device Management Platform ................................................................................. 5  
  Platform Specifics .............................................................................................................................. 5  
  Integration Framework ...................................................................................................................... 6  
  Device Agents ................................................................................................................................... 7  
  DDM Control Center ......................................................................................................................... 9  
  Customer and Partner APIs ............................................................................................................. 10  
  Multi-tenancy Infrastructure ........................................................................................................... 10  
Dell Distributed Device Management Services Overview .............................................................. 11  
  Service Features ............................................................................................................................... 11  
  Service Details - FAQs ..................................................................................................................... 13  
    FAQ Dell Distributed Device Management (DDM) – General Service Information: ......................... 13  
    FAQ - Asset Management – Service Details: ................................................................................ 20  
    FAQ - Software Distribution (and Removal) – Service Details: ..................................................... 24  
    FAQ : Anti-Malware & Virus Management – Service Details .......................................................... 31  
    FAQ - Dell Online Backup & Restore – Service Details: ............................................................... 35  
    Laptop Data Encryption – Service Details: .................................................................................... 42  
Summary ............................................................................................................................................. 47
Key Challenges for Managing Distributed Client PCs

Global workforces, multi-facility operations and the proliferation of mobile employees are making it increasingly difficult for organizations to track, manage and protect end user systems, especially those outside the corporate headquarters and the corporate network. For IT, this can lead to poor visibility into remote assets, less protection from security threats, compliance issues and difficulty in delivering a consistent level of service to end users. Key challenges for IT include:

An increasingly mobile and distributed workforce – Users commonly work in multiple locations and do not regularly connect to the company’s network (WAN/ LAN or VPN), making PC management difficult.

The need to maintain an accurate inventory of PC assets – It is nearly impossible to securely manage PCs without knowing their location, what software is installed, patch history, remaining lease life, current user, and other critical data.

Security and virus threats – The inability to adequately manage remote desktop protection and security exposes a company to viruses, hackers and data loss.

Compliance – Burdensome regulations such as Sarbanes-Oxley, HIPAA and GLBA require companies to maintain 24 x 7 visibility and control over their client PCs.

As the number and complexity of distributed PCs has grown - along with their value to the enterprise, it has become more imperative that these devices are operating correctly and in compliance with legal, regulatory, and contractual requirements. Maximizing the uptime and overall usability of companies’ desktop and laptop assets through effective management and improved security can have a significant and positive impact to employee productivity – and the bottom line.

Introduction

This paper provides an in-depth look at Dell’s Distributed Device Management Platform and service solutions for PC and desktop management. These solutions leverage the Internet to provide efficient, cost effective services to simplify and automate IT tasks such as patch management, software distribution, asset management, performing backups and more for remote and distributed environments. This paper also provides a detailed FAQ section which provides answers to specific questions about each of Dell’s services:

- Asset Management
- Patch Management
- Software Distribution
- Anti-Malware & Virus Management
- Online Backup & Restore
- Laptop Data Encryption
The Need for an Internet Based Platform

According to Gartner, properly managing their PC’s can save companies up to $1,900 per year on desktop PCs and up to $2,700 per year on laptop PCs.\(^1\)

The Internet has paved the way for a mobile, distributed workforce. The interconnectivity of distributed client PCs with the rest of corporate IT has been an essential element in the overall growth in productivity in the last decade. With that connectivity, however, comes a vulnerability that poses two serious management problems for CIOs and IT management.

The first challenge involves security for distributed PCs. The Internet is rife with viruses and other malware that can be a major source of downtime and potential data loss. Connectivity via the Internet, though providing mobility and flexibility for the workforce, can also be a great source of vulnerability.

Secondly, the Internet’s role as the common network for corporate devices complicates their management significantly. Traditionally, IT departments’ choices for solving IT problems involving the Internet have been limited; IT could use the tool included with a given device as part of their existing management suite, or deploy a new point solution for each of the myriad of IT problems faced (e.g. viruses, poor patch management, lack of effective backup), increasing their management challenge by adding yet another console to monitor.

A centralized Internet-based management platform is ideal for helping solve both of these problems. Typical solutions for managing individual, remote devices – particularly those deployed in the field – to a LAN or VPN-based solution within the corporate network can be very complex, as well as costly to deploy and manage. In addition, a true Internet-based management platform integrates the best point solutions from multiple providers, freeing IT from the choice of “good enough” versus “too complex.”

Dell’s Distributed Device Management (DDM) service is a centralized desktop management tool that is built using an Internet-based platform that delivers scalability for client PC management to organizations of all sizes – whether they have 100 PCs or 100,000. Hosted by Dell and delivered through the Internet, DDM services provide an integrated, hosted management solution for local and remote PCs. IT administrators can centrally track dispersed client assets, distribute software, manage patches and anti-malware definitions, and enforce IT policies, such as online backup and data encryption, for PCs located almost anywhere. Policy-based, automated management helps eliminate the administrative burdens of manual management systems and provides bandwidth-gated, granular control of your distributed devices. The

\(^1\) Gartner, “How to Reduce Your PC TCO 30% in 2011”, By Federica Troni, Brian Gammage, Michael A. Silver, March 2009 (Table 3 – Estimated savings by moving from unmanaged desktops and travelling worker notebooks to well managed ones).
services can be deployed under multiple options – PCs can be managed solely by an organization’s own IT department using the DDM platform, remotely by Dell or managed using a combination of services and options that best fits the your organization’s IT resources.

**Dell Distributed Device Management Platform**

**Platform Specifics**

Dell’s Distributed Device Management Platform provides three common functions that can be used by any application on the DDM Platform or that is part of a partner offering. These functions are exposed through the DDM Control Center, a single window into the environment of all managed devices. The three functions are as follows:

- **Analytics** – This function supports standard reporting and analysis across device data, financial data, and application data gathered from applications integrated into the integration framework.

- **User Management** – This function allows administrators to maintain user roles, permissions, and the list of services that users are allowed to access.

- **Security** – This function supports security for sign on, user access, and encryption of communications between the device being managed and the DDM data centers.

Each of the above functions can be applied to any of the data or operations of applications running on the DDM Platform and all these functions further support DDM’s plug-and-play requirement. In addition, the analytics capability allows the DDM platform to function as a business intelligence platform for the delivery of reports and other analytics.

Dell Distributed Device Management Platform has five main components:

- Integration Framework
- Device Agents
- DDM Control Center
- Customer and Partner APIs
- Multi-tenancy Infrastructure
Integration Framework

The Integration Framework is a combination of web-services and device-resident command line APIs that supports the integration of software applications and other functional components that deliver management services or provide functionality to the devices supported by DDM. These applications also make use of DDM Device Agents (see below).

Applications running in the Integration Framework can be delivered via an on-demand model as part of Dell’s DDM services or as part of a third-party service provider offering. Dell DDM Platform currently supports services including Dell Asset Management, Dell Software Distribution, Dell Patch Management, Dell Anti-Malware & Virus Management, Dell Online Backup & Restore, Dell Laptop Data Encryption, as well as provides remote support. Dell is in the process of opening the Integration Framework to allow virtually any application to be integrated into the DDM Platform in a plug-and-play manner.

*Note: Client PC data for the DDM Online Backup & Restore service is backed up to and restored from data centers of Dell Partner Iron Mountain.
The platform also supports Permissions Management as well as Service Entitlement Management functions, both of which can be used by Dell partners and independent service vendors. Permissions Management allows user access to applications running on the platform to be managed according to users’ specific roles and the permissions associated with those roles. Similarly, Service Entitlement Management allows applications running on the platform to deliver functionality based on varying levels of service. This allows Dell and Dell’s services partners to control service delivery and costs based on the actual services contracted by an individual customer or user organization.

The Integration Framework allows Dell to deliver a plug-and-play environment that is extensible to the greatest possible range of devices and management solutions.

**Device Agents**

Device agents must be deployed on every device DDM manages and provide the direct connection – via the Internet – between the device and DDM Platform. Agents are also designed as open platforms that can run either the basic asset management service DDM provides or additional desktop management services powered by applications from Dell or Dell’s partners.

The device agents provide extensible mechanisms for software download, inventory gathering, logging, and diagnostics. The information collected from the device agents integrates through the Integration Framework and is made accessible to applications running on the platform.

The Device Agents extend the openness, extensibility, and scalability of the Integration Framework directly to the client PCs to be managed. This further supports Dell’s goal to make DDM Platform plug-and-play and makes it possible for the DDM Platform to support virtually any Internet-connected device. The ability to deploy these Device Agents to any Internet-aware device enables Dell to provide network-neutral deployment architecture for the DDM Platform.
### Table 1: Communications Between the Managed Device and the DDM Data Center

<table>
<thead>
<tr>
<th>DDM Service</th>
<th>Data Being Transferred</th>
<th>From - To</th>
<th>Transfer Interval</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>All DDM Services</td>
<td>Agent heartbeat</td>
<td>Device to DDM Data Center</td>
<td>Every 15 minutes for each device</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Asset Management</td>
<td>Device hardware and basic software</td>
<td>Device to DDM Data Center</td>
<td>Once a day for each device</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Software Distribution</td>
<td>Application being distributed</td>
<td>DDM Data Center or Relay Server to Device</td>
<td>Based on distribution policy set by IT</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Patch Distribution</td>
<td>Patch being distributed</td>
<td>DDM Data Center or Relay Server to Device</td>
<td>Based on distribution policy set by IT</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Anti-Malware &amp; Virus Management</td>
<td>Virus definition check/update</td>
<td>DDM Data Center to Device</td>
<td>Every hour for each device</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Anti-Malware &amp; Virus Management</td>
<td>Firewall policy setup</td>
<td>DDM Data Center to Device</td>
<td>Based on policy setup and/or change by IT</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Anti-Malware &amp; Virus Management</td>
<td>Firewall policy check/reset</td>
<td>DDM Data Center to Device</td>
<td>Every three hours for each device</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Online Backup &amp; Restore</td>
<td>Hard drive backup</td>
<td>Device to DDM/Iron Mountain Data Center</td>
<td>Every 24 hours and/or manually at any time initiated by end user or IT</td>
<td>https / 128-bit Advanced Encryption Standard (AES)</td>
<td>16384</td>
</tr>
<tr>
<td>DDM – Online Backup &amp; Restore</td>
<td>Data restore</td>
<td>DDM/Iron Mountain Data Center to Device</td>
<td>Manually at any time initiated by end user or IT</td>
<td>https / 128-bit Advanced Encryption Standard (AES)</td>
<td>16384</td>
</tr>
<tr>
<td>DDM – Laptop Data Encryption</td>
<td>Instruction to delete encryption key</td>
<td>DDM Data Center to Device</td>
<td>Automatically based on policy or manually if device is reported lost to Dell</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
<tr>
<td>DDM – Laptop Data Encryption</td>
<td>Instruction to restore encryption key</td>
<td>DDM Data Center to Device</td>
<td>Manually by Dell if device is found</td>
<td>https / SSL Encrypted</td>
<td>443</td>
</tr>
</tbody>
</table>
**DDM Control Center**

The DDM Control Center provides a single Web-based window into the environment of all devices that are by a given company. Administrators can access the DDM Control Center over the Internet and can get an up to date view of all managed devices and perform any authorized tasks – from distributing software upgrades or the latest security patches to updating antivirus definition files to running a report on device that have not connected to the Internet for a specific period of time. The DDM Control Center has a number of features that makes it easy for IT to administer all devices under management:

- **Web 2.0 User Interface (AJAX based)** – Customizable dashboard driven user interface with drag and drop capabilities, customizable grids, multi-select rows, right click, clipboard, and client like interactions

- **Widgets** – Multiple actionable widgets – can click on widget to directly go to data – enable personalized home pages

- **Reporting** – Nearly 60 reports and charts

- **Query and Search** – Advanced query tool with both Boolean and full text search

**Figure 2: Monitoring Devices with the DDM Control Center**
**Customer and Partner APIs**

The DDM platform can provide external-facing data retrieval APIs that enables Dell’s partners and third parties to extract data from the DDM Platform and its applications. This data can be used in internal reporting, application integration and other functions, enabling DDM to provide extensibility and plug-and-play support based on an open Web Services model. Document APIs will be provided by Dell in late 2009.

Virtually any programming environment can be used to access these interfaces, including Java, C#, Perl, or C++. Dell will continue to extend the nature and quantity of API’s available in upcoming releases of DDM.

The customer-facing APIs will enable Dell to integrate existing data regarding users, applications and other information that may be needed by an application running in the Integration Framework. This allows Dell to not only make use of existing directory data for device management, but it also enables DDM customers to run internal applications alongside the DDM platform, allowing deployment of hybrid systems that mix cloud-delivered and on-premise functionality – for example, integrating DDM data with an on-premise service desk ticketing solution.

The partner-facing APIs will perform a similar role. Partner service providers can link their existing on-premise or managed solutions, such as customer relationship management and server management, directly to the DDM platform. This enables them to deliver solutions on top of the DDM services provided by Dell.

**Multi-tenancy Infrastructure**

Finally, the Dell DDM Platform is based on a multi-tenancy architecture that vastly simplifies implementation and services costs. This allows Dell and Dell’s partners to deliver device management services that are highly functional while remaining very cost effective. The redundancy and failover capabilities built into the DDM platform enable Dell to meet its criteria for built-in failover.
Dell Distributed Device Management Services Overview

Service Features

Dell Distributed Device Management Platform
- Provides a single “window” into PCs located anywhere on the Internet.
- Provides an intuitive, easy-to-use web interface. Allows for customized branding for partners, VARS, or customers.

Dell Asset Management Service – automatically discover, inventory and track distributed desktops and notebooks.
- Track warranty information, cost, and lease information.
- Help enforce enterprise, standard use policies.
- Evaluate assets for hardware refresh or upgrades.

Dell Software Distribution Service – distribute and control software and versioning.
- Enable policy-based management to maintain PCs by type or use, not one-by-one
- Help enforce software compliance; track and report on all software distributions
- Automate complex deployments using intelligent software-installer compatibility capabilities

Dell Patch Management Service – automate and centralize patch management processes for major vendors including Microsoft® (Windows, Vista and Office) Adobe®, VMware® and Apple® and over 500 applications.
- Customer-defined policies to automate deployment and patch management analysis
- Policy-based bandwidth management and historical reporting.
- Dell Does IT For You option available

Dell Anti-Malware & Virus Management Service – remotely install and control virus and malware updates for Symantec® and McAfee® software for distributed PCs.
- Centrally install files and upgrades without user involvement – whenever the user connects to the Internet
- Identify and monitor virus and malware infections
- Relieves IT from the complex tasks of configuring and maintaining on premise server and management console from anti-malware vendors
- Dell Does IT For You option available
Dell Online Backup & Restore Service – automatically back up data from desktops and laptops to an off-site top-tier datacenter providing an accurate, secure and worry-free data store.

- Eliminates dependence on end users – Backups are run automatically without end-user action
- Does not require corporate network connectivity – Only an Internet connection is required to back up or retrieve data (no WAN/ LAN or VPN required).
- Centralized management and reporting console (integrated with Dell Distributed Device Management service) enables identifying non-compliant PCs and initiating backups.
- Minimize network and end-user impact – Data compression, backup of only incremental changes, check-point restart and other policies minimize impact.

Dell Laptop Data Encryption Service – protects all data on an organization’s laptops/PCs by encrypting all data to ensure that only authorized users have access.

- Designed to protect all data – All end-user data on a protected PC is encrypted and remains secure even when a laptop is lost or stolen.
- Fully managed, hosted service – Dell hosts and manages the service – no infrastructure or management costs. Centrally manage security policy – Deploy encryption on remote PCs. Encryption keys are automatically destroyed by predefined policies and can be centrally restored as needed.
- Intelligent data encryption – Locates and encrypts all data files residing on a hard drive, without encrypting the OS or application files, providing the same benefits of full disk encryptions solutions without the negative impact on PC performance generally seen with the full disk encryption solutions.
- Automated encryption – All data files on a PC are encrypted without any input or involvement by end users, effectively eliminating any security issues due to user errors.
- Pre-set protection policies – Encryption key is eliminated and data is made inaccessible under policy driven, specific pre-set conditions including password hack, hard drive removal, reported theft or failure to connect over a pre-set period.
- Remote data restoration – Data on a lost or stolen PC can be remotely restored by Dell if the PC is ultimately recovered
- Help with recovery of stolen PCs – Dell can provide information on lost devices using network traces, network configuration data, and user activity.

Fully Managed Desktop Services – You also have the option of having Dell remotely manage your entire desktop environment for you using the Distributed Device Management Platform, providing Service Desk, onsite Field Service, Asset, Patch and Anti-Malware & Virus Management, along with additional services of your choosing.
Service Details - FAQs

FAQ Dell Distributed Device Management (DDM) – General Service Information:

1. **How does the DDM Service work?**
   An agent, running as a service, is installed upon devices that are to be managed. This agent then orchestrates a number of silent operations including hardware inventorying and coordinating upload/download of configurations and information.

2. **Can DDM Services be sold a la carte?**
   Yes. DDM Services can be purchased a la carte or part of a bundle of services. Dell highly recommends a customer purchase the Asset Management service along with any other a la carte service.

3. **If I purchase a DDM Service a la carte, can I purchase and install additional services at a later date?**
   Each DDM Service provides the administrator with ability to easily layer services at a later date. Once the Dell DDM Agent has been installed on a device and a customer has purchased the additional service, the DDM Control Center will dynamically provide the additional functionality and make available all necessary installation media to the customer via the console.

4. **How are DDM Services priced?**
   Each DDM Service is priced on a per-seat, per-month model and can be billed monthly or annually.

5. **What is the annual maintenance fee for DDM Services?**
   There are no annual maintenance fees for DDM Services. DDM is delivered using the SaaS (Software as a Service) model; it is delivered remotely and paid for monthly on a subscription-like basis. Updates are automatically applied to the DDM Control Center and underlying services with no end user or IT administrator interactions.

6. **How will service updates to the DDM client be made?**
   Enhancements and fixes are applied automatically by the Dell team. No IT administrator or end user involvement is necessary.
**DDM – Deployment:**

7. **How long does it take to provision a DDM Service?**
   Once purchased, the process of configuring the DDM Control Center and creating an installer takes no more than thirty minutes.

8. **How do I retrieve the DDM Service installer?**
   The Agent Installer is hosted within the DDM Control Center and is easily downloaded from a unique URL.

9. **How is a DDM Service deployed?**
   There are several methods for deploying a service. The simplest way is to double click on the Agent Installer. In larger deployments, login scripts can be used or Dell’s Asset Discovery from the DDM Control Center can be utilized to identify and target computers for installation.

10. **Where do DDM Services install?**
    The services install to: <specified drive>/svctools.

11. **How does DDM uniquely identify a computer?**
    When the Agent Installer is executed, it communicates with the DDM Control Center and requests a subscription id (Asset Number) from the Control Center. It is this value that is used to uniquely identify a computer and ensure proper communication.

12. **Can I install DDM on a drive other than “c:”?**
    Yes.

13. **How does a DDM Service get installed if the end user is not a local administrator?**
    If the end user does not have the local permission to add software, Dell has a solution called Domain Administrator Impersonation that can help. A user has the ability to utilize a “run-as” function that will execute the installer automatically utilizing credentials that allow for software installation. This means that the end user’s permissions never need to be adjusted and deployment can continue silently and without interference.

14. **Can I integrate DDM Services with Active Directory?**
    Not at this time. DDM does have the ability to query Active Directory servers and retrieve user information and sync the data to managed devices. Dell understands that integration with Active Directory is a key request and is working towards a solution in a future release.
15. What is necessary to deploy a DDM Service?

The essential requirements necessary to deploy DDM are Internet connectivity and a Windows® operating system on the device(s) that will be managed by DDM.

16. How long does installation execution take? Is a reboot required during installation?

The installation of the Agent typically takes no more than 15 minutes. The installation can be configured to occur silently with no end user interaction whatsoever or to include a Registration page that asks the user to enter in their contact information. In both cases, no reboot is required when installing the Dell Agent.

17. Can I change the polling frequency of the DDM Agent?

No. Currently the Dell Agent is configured to make an outbound heartbeat on 15 minute intervals.

18. What are the installation requirements for DDM Agent on a client device?

The device must have a Windows® Operating System, Internet connectivity at the time of install, and the individual executing the installer must have sufficient permissions to install software on the device (if Domain Administrator Impersonation was configured, the last requirement is met). Different DDM services have different minimum Windows Systems requirements. The following table provides minimum system requirements for each DDM service:
Table 2: Operating Systems Supported by DDM Agent and DDM Services:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core DDM Agent</td>
<td>Windows® 2000® SP3, SP4 Workstation, Windows® 2000 Server® SP4, Windows XP® SP1, SP2, SP3, Windows 2003 OEM, SP1, SP2, Windows Vista® SP1, SP2</td>
</tr>
<tr>
<td>Antivirus – McAfee® Security 8.5</td>
<td>Windows 2000 SP3, SP4 Workstation, Windows 2000 Server SP4, Windows XP SP1, SP2, SP3, Windows 2003 OEM, SP1, SP2, Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>Antivirus – Symantec™ 10.1</td>
<td>Windows 2000 SP4 Workstation, Windows 2000 Server SP4, Windows XP SP1, SP2, SP3, Windows 2003 OEM, SP1, SP2, Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>Antivirus - Symantec 10.2</td>
<td>Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>Antivirus - Symantec 11</td>
<td>Windows 2000 SP4 Workstation, Windows 2000 Server SP4, Windows XP SP1, SP2, SP3, Windows 2003 OEM, SP1, SP2, Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>Laptop Data Encryption</td>
<td>Windows 2000 SP4 Workstation, Windows XP SP2, SP3, Windows VISTA SP1</td>
</tr>
<tr>
<td>Device Discovery (Host)</td>
<td>Windows 2000 SP3, SP4 Workstation, Windows 2000 Server SP4, Windows XP SP1,SP2 ,SP3, Windows 2003 OEM, SP1, SP2, Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>LAN-Based remote control</td>
<td>Windows 2000 SP3, SP4 Workstation, Windows 2000 Server SP4, Windows XP SP2, SP3, Windows 2003 OEM, SP1,SP2</td>
</tr>
<tr>
<td>Online Backup and Reset</td>
<td>Windows 2000 SP4 Workstation, Windows XP SP1, SP2, SP3, Windows Vista SP1, SP2</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Windows 2000 SP3, SP4 Workstation, Windows 2000 Server SP4, Windows XP SP1, SP2, SP3, Windows 2003 SP1, SP2, Windows Vista SP1, SP2</td>
</tr>
</tbody>
</table>

19. How much hard drive space is required to install the DDM client service?
   It is recommended to that the device has at least 50 MB of free space.

20. What operating systems are supported by the DDM client service?
   At this time, operating systems for Windows 2000® through Vista® are supported. Please see the chart above for more details. Support for Windows 7 OS is expected in late 2009.

21. Is the service available for non-Windows OS’s like RedHat linux?
   Only Windows operating systems are supported at this time. Dell plans to have support for devices running on Mac OS X 10.5 and higher in early 2010.

22. How do I export data out of the DDM Control Center and into productivity software (Microsoft Excel®, Microsoft Access®, SQL Server®)?
   Nearly every page within the Control Center has an “Export to Excel” option that places the displayed data into an Excel spreadsheet on the user’s computer. Additionally, with the planned release of documented API’s in October 2009, DDM will enable transfer of data from DDM to other applications.

23. How much RAM is required to install the DDM client service?
   At least 32 MB of RAM is required to install DDM Services.

24. How large is the installer/package?
   The basic Agent Installer is only 4.3 MB in size. This size increases as additional services such as Dell Online Backup & Restore or Dell Laptop Data Encryption are added.

25. What is the footprint size of the application?
   Less than 50 MB

26. What is the memory usage?
   If all processes are running concurrently, memory usage could be up to 40 MB.

27. Does the end user see the DDM Services installed when viewing Add/ Remove Programs?
   No, Dell does not register its Agent in the Add/ Remove programs. This is done purposely in order to help keep the end users from tampering with the installation.

28. How can I uninstall the DDM client service?
   The Agent can be uninstalled either by distributing a package from the DDM Control Center or by executing an Dell utility called “Agentrem” locally on the device.
DDM – Networking and Servers:

29. Will DDM Services work without a domain?
Yes. The underlying service is based on Internet connectivity and not based on the existence of a network or a domain.

30. How much network traffic is generated by the DDM Agent?
If a managed device was left turned on 24 hours a day, 7 days a week, the normal traffic generated by the device would up to 600 KB per day. This does not include any network traffic required for distribution of patches, software or backup of data.

31. Do all managed devices connect to the Data Center at the same time?
No. A managed device will send out its heartbeat when the device first connects to the Internet. Since all computers are not turned on simultaneously and, thus, not all computers connect to the Internet simultaneously, a staggering of connections is achieved.

32. How does the data center communicate with the managed devices?
All communication between the managed device and the data center is initiated by the device. This means that the data center never makes an inbound connection to the device. This has been purposely configured in order to ensure proper security protocols are followed.

33. How secure is my data?
Dell is committed to providing a high level of security for Distributed Device Management services customers and their data. Dell’s data centers use a number of industry-standard security solutions to secure their internal network environment and associated assets. Such solutions include, but are not limited to: virus detection, email attachment scanning, system and application patch compliance, intrusion prevention and detection systems, and firewalls. Dell also provides industry standard physical controls in its data centers, such as fire prevention systems, access controls, and exit routes. Technical controls act as countermeasures to mitigate risk, such as firewalls, encryption and alternate systems. Dell also has administrative controls in place for Distributed Device Management services that involves policy and procedures, such as security policies and testing.
34. **What type of encryption is used to transport data from the device to the data center?**
   All data transmitted from the managed device to the Control Center is encrypted with SSL and transported via port 443.

35. **Do DDM Services work behind an authenticated proxy?**
   Yes, upon configuration of the Agent Installer, the credentials necessary to allow outbound communication to the Internet can be specified.
FAQ - Asset Management – Service Details:

1. What are the components of Asset Management?
   Asset Management is comprised of comprehensive hardware and basic software inventory, hardware change tracking, LAN-based remote control, ability to enter financial/purchase information about the device, asset discovery, Active Directory import, and end user contact management.

2. How does Dell Asset Management work?
   The Asset Management service incorporates a two-step process that first includes the discovery and inventory of Windows devices and then enables an IT department to actively manage all discovered Windows-based PCs. Once deployed, Dell Asset Management enables IT administrators to scan their network to discover, identify and inventory all IP-based computers (desktops, laptops and servers).

3. What devices can be managed using Dell Asset Management?
   Dell Asset Management can discover IP-based devices on your network and provide detailed up to date information (over 100 hardware characteristics) devices based on Microsoft Windows® (Windows 2000, Windows 2003, Windows XP® SP1 – 3, Vista®) The service can also help you obtain up-to-date information on off-network devices that are only connected to the Internet (no requirement for a device to be on the WAN/LAN or connected to a VPN). Only 32-bit systems are supported at this time.

4. What type of information is captured by Asset Management?
   Over 100 comprehensive hardware and software characteristics are automatically captured and reported to the Control Center. Items such as installed software, CPU, memory, and hard drive information including drive location, user information, processor speed, memory, Bios, OS, video card, system enclosure, memory slots, disk drives, battery, printers, baseboard, and more.

5. Does Asset Management track changes to the hardware profiles of managed devices?
   Yes. The DDM Control Center provides delta analysis and reporting to users, identifying configuration changes across the enterprise.

6. Can Asset Management help me with computer life cycle management?
   Yes. By utilizing the flexible querying and reporting capabilities, a user can easily identify devices that should be retired. A comprehensive tech-refresh plan can easily be developed by reviewing the data that the Control Center provides.
7. Can you manage software licenses with DDM Asset Management?
DDM Asset Management provides for basic software inventory, but does not currently have extensive software license management capabilities. Dell has a separate Internet-based service, Dell Software Inventory & Usage Management that provides extensive software license management and software usage metering capabilities.

8. Am I able to track non-Windows OS devices in Asset Management?
Not at this time. Dell plans to add this function in a future release.

9. What kind of reporting is available?
There are comprehensive querying capabilities within the DDM Control Center. In addition, there are several pre-configured reports and dashboard graphics that can be used to analyze the environment. Build in report include Assets by Operating System, Assets by Location, Assets by Processor Speed, or List of Defective Devices. All of the report results (built in or custom created) can be exported to Microsoft Excel®.

10. What events trigger an Asset Management client computer to check in with the Asset Management server (i.e., what is the frequency of the agent’s heartbeat)?
The Agent on a managed device attempts to connect to the DDM Control Center on a 15 minute interval.

11. What is the desktop interface for the Asset Management client application?
The Asset Management client does not have a desktop interface. The Asset Management agent runs in the background, transparent to the end user.

12. What are the associated computer services that are used by Asset Management?
There are a number of processes that could be running on a managed device. Not all run concurrently and in fact, only lnchr.exe (two instances, one in user context and the other in system) runs continuously. The others are: hbeat.exe, curl.exe, curlcfg.exe, download.exe, upload.exe, inventory.exe, lrotate.exe, xmldiff.exe, and swmeter.exe.

13. Does Asset Management require hardware to be deployed to my local network?
No. One of the greatest values achieved by using a cloud-based architecture delivered via a SaaS –based model is the reduced time to deploy and utilizing the multi-tenancy provided via a shared infrastructure.
14. Where are the Asset Management console and associated servers hosted?
The DDM Control Center infrastructure for the latest version of DDM resides in redundant
data centers in Austin, TX at this time. Dell plans to utilize data centers in Frankfurt,
Germany and Amsterdam, Netherlands for EMEA-based clients beginning in late 2009. Dell
also plans to utilize data centers in Latin America and Asia-Pacific regions in the near feature
for clients based in those areas.

15. How does Asset Management deliver LAN-Based Remote Control?
LAN-Based Remote Control is based on a modified version of Tight-VNC.

16. Does LAN-Based Remote Control utilize “wake-on-LAN” techniques?
No, LAN-based Remote Control requires both the initiating and targeted computer to be
“awake” at the time of the requested session.

17. How do I identify managed devices that may have been stolen, lost, or had the service
manually uninstalled?
By referencing the “Last Modified Date”, DDM Control Center users can identify managed
devices that have not been properly communicating back to the Control Center. This field
captures the date of the last time a device was modified and can be used to identifying
problematic or lost devices.

18. Can I force a managed device to upload its hardware/ software inventory?
Yes.

19. Can I track company specific information that may not be common to all companies?
No. Dell plans to add this functionality in a future release.

20. What is the update frequency of a device’s inventory information?
All hardware / basic software information is uploaded to DDM data centers on a daily basis.

21. Can end users update their own contact information for devices they are using?
Yes. There are two avenues for accomplishing this: end user is prompted at the time of
Agent installation to enter in their contact information. Alternately, a DDM Control Center
administrator sends a command to the managed device to prompt the end user for their
contact information.
22. Is there an ability to batch upload and sync data?
   Yes. Batch uploads and synchronizations can be conducted on behalf of customers by Dell. In addition, DDM can also query Active Directory servers and retrieve user information and sync the data to managed devices.

23. Does the service upload inventory information even when the device is not on the local network?
   Yes. Because the Dell solution is Internet based and not LAN or network based, information is automatically uploaded to the Control Center as long as the device has connected to the Internet.
FAQ - Software Distribution (and Removal) – Service Details:

1. **What type of software can be distributed by Software Distribution?**
   The service is flexible enough to accept .msi, .msp, and .exe files.

2. **To what devices can Dell Software Distribution distribute software?**
   Dell Software Distribution can distribute software to devices running Microsoft® Windows® (Windows® 2000, Windows 2003, Windows XP® SP1 – 3, Windows Vista®) through the Internet virtually regardless of the device’s location. Only 32-bit systems are supported at this time.

3. **What other uses are there for Software Distribution?**
   Because Software Distribution accepts .exe files, many new uses have been exposed. A skilled script writer can build a package that could change nearly any configuration on the managed device or execute any Windows command locally. For example, a command can be scripted to execute “defrag” on a targeted device. Many customers have taken advantage of this extension.

4. **How much hard drive space is required to install the Software Distribution client service?**
   It is recommended to that the device has at least 50 MB of free space. In addition, there should be ample space available for downloading and de-compressing packages in order to properly install the distributed software.

5. **How much network traffic is generated by the Software Distribution agent?**
   If a managed device was left turned on 24 hours a day, 7 days a week, the normal traffic generated by the device (for all DDM services total) would up to 600 KB per day. Additional traffic is generated, during the distribution of a software package to a managed device.

6. **What kind of reporting is available?**
   There are comprehensive querying capabilities within the DDM Control Center. In addition, there are several pre-configured reports and dashboard graphics that can be used to analyze the environment.

7. **What is the desktop interface for the Software Distribution client application?**
   The Software Distribution client does not have a desktop interface. The Software Distribution Agent runs in the background, transparent to the end user.
8. What are the associated computer services that are used by Software Distribution?
   There are a number of processes that could be running on a managed device. Not all run concurrently and in fact, only lnchr.exe (two instances, one in user context and the other in system) runs continuously. The others are: hbeat.exe, curl.exe, curlcfg.exe, download.exe, upload.exe, inventory.exe, lrotate.exe, xmldiff.exe, and swmeter.exe.

9. How does the service handle download interruptions?
   Dell Software Distribution utilizes checkpoint restart, ensuring that interrupted downloads resume at the last bit downloaded.

10. Can end users request download to their computer?
    Not in this release. Dell plans to add this functionality in a future release.

11. How can I manage the distributions?
    All distributions are available for review in the DDM Control Center. Users also have the ability to view an individual device to see its distribution history. Distributions can be scheduled for the future or advertised immediately. Additionally, distributions can be cancelled at any time up to a successful download of the software package. Administrations can also pause a distribution and resume it at a later time to minimize impact of a distribution on network performance.

12. What occurs if a managed device is not on the Internet at the time of distribution?
    When a software package is distributed, the DDM Control Center advertises the package for download. It will continue to advertise the package until the targeted machine connects to the Internet and sends its heartbeat to the Control Center. At that time, the download will initiate.

13. Can I (IT administrator) upload my own software packages?
    Yes. There the DDM Platform has an intuitive interface that allows for software upload by DDM Administrators. Users can also specify minimum requirements from this screen to ensure compatibility. Characteristics like Operating System can be checked before allowing distribution.
14. How do distributions occur?
When a software package is distributed, the DDM Control Center advertises the package for download. At 15 minute intervals, managed devices transmit a heartbeat to the Control Center. The heartbeat will be given a command to begin download a package from a specified point and the download will initiate. The Control Center will report on the progress of the distribution, the status of the execution, and whether or not the execution was successful.

15. How can I make sure the right software is distributed to the right device?
Dell Software Distribution comes with Intelligent Package Distribution which allows you to send a single distribution package with multiple installers (i.e., multiple installers for an application upgrade due to the fact that different versions of the upgrade are necessary based on operating system). The service compares the device specifications with the installer requirements and determines the correct installer to distribute to particular devices.

16. How do I control the flow of distributions?
There are several techniques that can be used. First, bandwidth policies can be established that can limit the number of concurrent downloads and the maximum amount of bandwidth to be used by a device during download. Dell Software Distribution is designed to have the minimum amount of impact on your network bandwidth. Distribution of software is policy driven and gives you the ability to minimize the utilization on your network while making sure that critical updates get to the devices that need them as soon as possible. You can limit the amount of bandwidth per device and per location based on the time of day, days of the week and criticality of the distribution, so that the majority of software distributions occur at off-work hours and the impact on the performance of each device and the bandwidth consumed for each network node is minimized for most distributions.

Second, the service allows you designate a local device as a relay point that will act as a proxy between the managed devices and the Internet. As the managed devices request files from the service, the proxy machine will download the necessary files and will serve them to the managed devices through the local area network, minimizing the impact on network bandwidth. Finally, you always have the ability to over-ride any policies and distribute software out immediately.
17. **How do I track the success of a distribution?**

The Control Center provides two methods by which a user can track software distributions. The first method is to view the target itself via Basic or Advanced search. Once you have displayed the Asset Details screen, select Other Options at the top of the window and click on View Package History. The second method is to navigate to Monitor Distributions. From this interface, users have the ability to query based on a number of characteristics: date distributed, package status, device location, etc.

18. **Are there logging capabilities to help troubleshoot distributions?**

Yes. The DDM Control Center will accept logging events from software packages.

19. **Can I queue distributions to a device?**

Yes. A current distribution does not need to complete in order to distribute additional packages. Each distribution will be queued, downloaded, and executed serially.

20. **Are there methods to help reduce WAN usage during distributions?**

The bandwidth throttling techniques as well as the ability to utilize Relay Points, both of which are described in detail in response to Question 15 above, help minimize WAN usage and impact on network performance during a software distribution.

21. **What events trigger a Software Distribution client computer to check in with the Software Distribution server (i.e., what is the frequency of the agent’s heartbeat)?**

The Agent on a managed device will attempt to connect to the Control Center on a fifteen minute interval.

22. **Where are the Software Distribution console and associated servers hosted?**

The DDM Control Center infrastructure for the latest version of DDM resides in redundant data centers in Austin, Texas, at this time. Dell plans to utilize for Americas-based clients and data centers in Frankfurt, Germany and Amsterdam, Netherlands for EMEA-based clients beginning in September/October 2009 timeframe. Dell also plans to utilize data centers in Latin America and Asia-Pacific regions in the near feature for clients based in those areas.

23. **Is it possible to target software distributions based on the types of software installed on target machines?**

Yes, with the purchase of the Dell DDM Software Inventory and Usage Management service in addition to software distribution, customers have the ability to run complex queries on the software inventory of their installed base. The results of these searches can be used to
distribute software to targeted machines, for example, only deploying Microsoft Publisher to PCs that already have Microsoft Office installed.

**Patch Management – Service Details:**

1. **What is the Dell Patch Management software service?**
   The Dell Patch Management software service enables the distribution of patches from major vendors including Microsoft® (Windows, Vista and Office) Adobe®, VMware® and Apple® (over 500 applications). Dell's on-demand Patch Management service utilizes the Dell DDM Control Center --- our centralized, easy-to-use management platform --- to enhance the ability of IT to respond to software vulnerabilities in a timely manner by controlling when patches are applied.

   Patch Management enables you to:
   - Automatically deploy patches or target deployment of patches to specific systems depending on business or technical considerations.
   - Perform multi-patch management to support Q-chaining, bandwidth throttling and Binary Delta Compression of patches.
   - Manage deployment schedules, utilize sign-posting messages for the end-user, permit checkpoint restart, and ensure delivery of all packages using 128-bit SSL encryption.

2. **What are the benefits of using Dell Patch Management?**
   The Patch Management service enables the distribution of patches from Microsoft and other leading vendors consistent with IT and business policies. Ideally suited to deliver patch management services to both corporate and remote systems, Dell Patch Management provides IT organizations greater control over and visibility into the patching process. This service provides the following benefits:
   - Rapid deployment
   - Extensive Policy Management (Flexible patching options – vendor criticality, automated, targeted, multi-patch, etc.)
   - Centralized management and reporting
   - Reduced burden on IT
   - Transparent to end users
   - Bandwidth policies and option Relay Points to minimize WAN usage and impact on network performance
3. **How does the Patch Management service work?**

Dell’s lightweight, unobtrusive software agent, running as a service, is installed on all devices that are to be managed. This agent orchestrates a number of silent operations including compiling hardware and software inventory, and coordinating upload/download of configurations and information – depending on the services purchased by the customer. The agent uploads patch compliance information on a daily basis to the DDM Control Center, allowing users to assess their environment in near-real time. The Control Center also provides the ability to distribute the necessary patches to those devices in need. Via Dell’s Software Distribution capabilities or by using inherent Microsoft patch distribution, Dell is able to transmit the desired patches to the target machines and monitor their success.

4. **What types of patches can be distributed by Dell Patch Management Service?**

Dell Patch Management supports the patching of Microsoft operating systems and the Microsoft Office® key business productivity suite of products along with patches from other major vendors including Adobe®, VMware® and Apple® (over 500 applications).

5. **What devices can Dell Patch Management distribute patches to?**

Dell Patch Management can distribute application patches to devices running Microsoft® Windows (Microsoft® Windows 2000®, Windows 2003, Windows XP® SP1 – 3, Vista®) through the Internet no matter where they are located. Only 32-bit systems are supported at this time.

6. **Does Patch Management track patch distributions?**

Patches distributed manually are tracked via Dell’s Software Distribution module. Users can query and monitor distributions based on date, patch, office, and status. This function allows for complete visibility of the patching process and ensures users can identify problem devices proactively.

7. **How do I control the flow of patch distributions (minimize impact on network)?**

Dell Patch Management is designed to have the minimum amount of impact on your network bandwidth. Distribution of patches are policy driven and you can set multiple policies based on bandwidth and patch status to minimize the impact on your network while making sure that critical patches get to the devices that need them as soon as possible.

You can set when (and if) a patch is distributed based on application vendor and patch criticality. You can also set additional parameters around the distribution of the patch based on bandwidth policies (i.e., limit the amount of bandwidth per device and per location based on the time of the day and/or the day of the week). This two-tier patch policy
approach enables you to help ensure that the majority of patch distributions occur at off-work hours and that the impact on the performance of each device and the bandwidth consumed for each network node is minimized for most distributions.

The service also allows you designate a local device as a relay point that will act as a proxy between the managed devices and the Internet. As the managed devices request patches from the Dell Patch Management, the proxy machine will download the necessary patches and will serve them to the managed devices through the local area network, minimizing the impact on WAN bandwidth.

8. **What happens if a device is turned off or loses its Internet connection in the middle of a patch distribution?**
   Dell Patch Management comes with checkpoint restart; if a patch distribution is interrupted for any reason, the next time that device connects to the Internet, the distribution will continue from the point of interruption and not start over, which also helps minimize the bandwidth impact on each device and on your network.

9. **How can I make sure that a particular patch has been installed?**
   Dell Patch Management provides real time reporting and charting on the status of each patch distribution so that you can have up-to-the-minute data on the status of a distribution.

10. **What if a patch causes unforeseen problems and needs to be uninstalled?**
    Dell Patch Management allows you to uninstall most patches and bring the device back to the state it was in before the installation of the trouble-causing patch.

11. **What if I want to test a patch before I distribute it?**
    Dell Patch Management allows you to set a number of hierarchy-based policies to make sure that the patches are distributed exactly to your specifications with minimum work. You can distribute patches manually, automatically or at a set time after they are released by the application vendor (giving you a chance to test the patch and/or make sure that there is no industry-wide problem with the patch). You can also set patch distribution policy by patch criticality and vendor. The patch policy setting tool is easy to use and designed to provide you with maximum flexibility in your patch distribution process.
FAQ: Anti-Malware & Virus Management – Service Details

1. What is the Dell Anti-Malware & Virus Management Service?
   The Dell Anti-Malware & Virus Management service helps enable the management, configuration, and reporting on multiple antivirus and anti-spyware engines, all from a single management interface. IT administrators can identify virus infections across multiple vendors, configure administrative scans, and force virus/spyware definition file updates remotely. To complement the antivirus and anti-spyware capabilities, customers who purchase this service has the ability to manage the Operating System firewalls on systems with Windows XP.

2. What customer challenges does Anti-Malware & Virus Management address?
   • Loss of end-user productivity due to virus and spyware outbreaks
   • Inability to protect networks and desktops from virus outbreaks
   • Negative impact resulting from business downtime
   • IT resources are diverted to deal with virus outbreaks
   • Inability to rapidly detect infected machines during a virus outbreak
   • Difficulty in managing multiple antivirus and anti-spyware products
   • Difficulty in centrally managing the Microsoft Client Firewall
   • Visibility of anti-virus state before device re-enters domain/corporate network

3. What are the key benefits of Dell Anti-Malware & Virus Management?
   • Helps reduce IT support costs
   • Creates a predictable cost structure for IT services
   • Helps reduce end-user downtime
   • Minimizes onsite visits by support personnel
   • Helps conserve critical IT resources
   • Can improve IT responsiveness to virus outbreaks
   • Helps lower administration costs
   • Helps increase productivity
   • Helps reduce security risks
   • Allows AV enforcement on the perimeter (protect and manage laptops before they come back on the corporate network)
4. Which vendors and products are supported for the different categories of antivirus, antisyware and firewall within the Anti-Malware & Virus Management service?
   • Supported Antivirus Vendors: Symantec 10 & 11, McAfee 8.5
   • Supported Anti-Spyware Vendors: Symantec 10 & 11, McAfee 8.5
   • Supported Firewall Vendor: Microsoft

5. What devices can Dell Anti-Malware & Virus Management support?
   Dell Anti-Malware & Virus Management supports Microsoft Windows based devices (Windows 2000, Windows 2003, Windows XP SP1 – 3, Vista). Note: Setting/enforcing Windows firewall policies is only available for PCs running on Microsoft Windows XP. Only 32-bit systems are supported at this time.

6. Are any anti-virus solutions available for purchase from Dell?
   Yes. anti-virus solutions from Symantec and McAfee are available for purchase from Dell.

7. How can I make sure that all of my devices are free of viruses?
   Dell Anti-Malware & Virus Management provides you information on the virus definition status of all devices under management so that you can see which devices are fully protected and which ones are potentially under threat. You can then update the definition of all devices with a single click. You can also run a system scan on all managed devices (no matter what version of a supported application is running on a device) with a single click to find out if any of your devices are infected and can take appropriate remedial action.

8. How often are virus, malware and spyware definitions updated on Dell’s Anti-Malware & Virus Administration service?
   Anti-virus definitions on managed devices are updated hourly and the data is reported to the Distributed Device Management Services Control Center daily.

9. How can I make sure that a definition update has been installed?
   Dell Anti-Malware & Virus Management provides you with information on the virus definition status of all devices under management so that you can see which devices are fully protected and which ones are under threat.

10. How are Microsoft Windows firewall policies enforced?
    Dell Anti-Malware & Virus Management service enables you to remotely set Windows Firewall policies on devices running on Microsoft Windows XP and checks the status of the policy on each managed device every three hours. If a user manually changes the policy set, the changes made by the user will be overridden and the policy set by your Dell Anti-Malware & Virus Management administrator will be reset within three hours.
11. Why would IT departments choose to use Dell’s Anti-Malware & Virus Management service to manage their firewalls?

There are three main reasons for IT departments to choose Dell Anti-Malware & Virus Management to manage their firewalls:

- Anti-Malware & Virus Management centrally manages the Microsoft Windows Firewall which is included with the Windows operating system. This makes it a natural choice for IT departments to standardize on.
- The Microsoft Windows Firewall is fully supported by Dell’s integration layer.
- Many companies have a distributed environment in which the IT department needs to have remote control over distributed assets. The Anti-Malware & Virus Management service enables you to centrally manage their firewall policies across all assets.

12. What is the benefit of using Dell’s anti-virus service vs. a management console provided by Symantec or McAfee?

A properly architected and managed on-premise antivirus management console is a powerful IT tool that can help ensure that devices have the latest virus definitions and configurations. Its alerting capabilities ensure near real-time virus events are sent to the appropriate IT personnel via pages or email and the ability of the console to act as a cache for virus definitions allows low bandwidth environments to receive the most recent virus definitions without overburdening the network.

However, using on-premise solutions comes at a price. The cost of purchasing server hardware and the server operating system as well as configuring and maintaining the server itself can be an issue for small and medium size businesses. In addition, since the console is LAN-based, its reach is limited to those devices that reside on the network.

Dell’s DDM Anti-Malware & Virus Management service relies on simplicity. Installation occurs either during the initial installation of the Dell agent or by simply distributing the necessary components from the DDM Control Center. Because the Dell solution is software-as-a-service, speed of deployment is greatly accelerated, occurring in hours or days rather than weeks or months. Finally, Dell is able to manage multiple antivirus solutions from different vendors seamlessly whereas individual vendors such as Symantec and McAfee have designed their management consoles to only work with their products. The Dell Anti-Malware & Virus Management service can either be used in tandem with an existing on-premise management console or it can replace those consoles depending on your business requirements:
Coexistence

The Dell DDM Anti-Malware & Virus Management service compliments environments where an antivirus manufacturer’s management console may already exist. IT managers can be assured that they have the ability to monitor, manage, and detect infections with end users that travel, locations not tied via a logical LAN, or where a company may not wish to install multiple console servers in disparate locations. The key distinction of using the Internet to manage devices helps Dell’s customers ensure that the device is managed and protected before it comes back onto the network.

Displacement

Some organizations may have deployed an antivirus manufacturer’s console, but are not using its full scope of functionality. Common reasons are:

- Complexity of configuring and maintaining the server
- It was used only to deploy the antivirus software
- It does not effectively manage antivirus software on remote devices

Dell’s Anti-Malware & Virus Management service allows customers to leverage the Internet to eliminate onsite maintenance of servers and ensures that the antivirus software on the device, regardless of physical location, can be managed.
FAQ - Dell Online Backup & Restore – Service Details:

1. **What is Dell Online Backup & Restore?**
   Dell Online Backup & Restore is a fully automated, hosted service that automatically backs up data from desktops and laptops to a highly secure off site datacenter, saving companies time and money while providing an accurate, secure, and worry free data backup. This service eliminates the uncertainty of traditional PC backup methods – generally relying on users to perform backups to a CD or the network.

2. **What data security challenges does Dell Online Backup & Restore service address?**
   The Dell Online Backup and Restore service helps your IT organization meet the following data security challenges:

   - Loss of data by end users due to hard disk failures and laptop loss
   - End-user failure to backup critical data at regular intervals
   - Difficulty protecting against unwanted intrusion
   - Compliance challenges - backup and recovery are key requirements of regulatory compliance – HIPAA, Sarbanes-Oxley, the Gramm-Leach-Bliley Act, etc.
   - Enforcing backup policies on remote, off-the-network, users
   - Avoiding negative impacts resulting from business downtime
   - IT workload due to hard drive failure and user migration to new PCs
   - Increased cost of supporting mobile users
   - Limited network resources – storage, bandwidth, etc.
3. What are the key features and advantages of Dell Online Backup & Restore Service?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iron Mountain automatic and Internet-based backup software, deployed</td>
<td>Protects corporate users – especially remote users from data loss.</td>
</tr>
<tr>
<td>automatically over the Internet.</td>
<td>Does not require a VPN Connection.</td>
</tr>
<tr>
<td>Provides 3 deployment options:</td>
<td>Provides multiple deployment options to best meet the needs of the organization.</td>
</tr>
<tr>
<td>• Select data backup</td>
<td>Requires no end-user interaction and can run in the background while users work, without interrupting them.</td>
</tr>
<tr>
<td>• Flexible select data backup</td>
<td></td>
</tr>
<tr>
<td>• Complete data backup</td>
<td></td>
</tr>
<tr>
<td>Automated scheduling and execution of backups.</td>
<td></td>
</tr>
<tr>
<td>• Nightly or configurable</td>
<td></td>
</tr>
<tr>
<td>• After hours or during power sequence</td>
<td></td>
</tr>
<tr>
<td>• ‘not to exceed’ rules provided</td>
<td></td>
</tr>
<tr>
<td>User-initiated file restore enables end users to retrieve up to ten</td>
<td>Enables users to restore their own files without assistance from IT administration.</td>
</tr>
<tr>
<td>versions of each file.</td>
<td></td>
</tr>
<tr>
<td>Secure data transmission and storage via 128-bit Advanced Encryption</td>
<td>Safeguards critical data from being compromised or lost.</td>
</tr>
<tr>
<td>Standard. Data is stored off-site</td>
<td></td>
</tr>
<tr>
<td>• Co-location for redundancy and failover</td>
<td></td>
</tr>
<tr>
<td>• Mirrored server pairs</td>
<td></td>
</tr>
<tr>
<td>Data compression and file transfer optimization</td>
<td>Minimizes bandwidth usage and network traffic.</td>
</tr>
<tr>
<td></td>
<td>Eliminates sending duplicate files</td>
</tr>
<tr>
<td>Incremental backups and backup resumptions</td>
<td>Resumes partially completed backups for intermittent connections</td>
</tr>
<tr>
<td>Advanced data retention</td>
<td>Ensures critical data is protected through secure and extensive file retention policy</td>
</tr>
<tr>
<td>• Ten versions of each backed up file stored at the data center.</td>
<td></td>
</tr>
<tr>
<td>• Files deleted by end users are stored for 90 days at the data center</td>
<td></td>
</tr>
<tr>
<td>• Files re-selected by end users from their backup list are stored</td>
<td></td>
</tr>
<tr>
<td>for another 7 days at the data center.</td>
<td></td>
</tr>
<tr>
<td>Jumpstarts failed online backup agents</td>
<td>Ensure that online backups occur for maximum data protection.</td>
</tr>
<tr>
<td>Intuitive, dashboard driven UI with centralized management reporting</td>
<td>Streamlines and centralizes backup reporting to ensure that all users are compliant and up to date with their backups</td>
</tr>
<tr>
<td>• By date of last backup and size of backup</td>
<td></td>
</tr>
<tr>
<td>• By account number</td>
<td></td>
</tr>
</tbody>
</table>
4. **Why is the service unique?**

The service is fully integrated with Dell Distributed Device Management’s web-based management console, which enables administration and reporting anywhere, anytime, over the Internet.

- Designed for distributed environments – Each file is sent and stored only once, even if stored in multiple locations. When changes occur, only incremental or changed data blocks are sent and stored.
- Hosted SaaS service – Easy to purchase without up-front capital investment (per month, per PC), and quick and easy to deploy (in days, not months).

5. **Why Should I Buy Online Backup and Restore?**

According to leading industry research, 20% of end users lose data annually due to hardware failure, theft, user error or viruses. For many companies, growth in the number of mobile workers and distributed locations create an increasing challenge for IT to safeguard critical company data. Although loss of critical data can be devastating to a company’s finances and productivity, companies routinely rely on end users to back up their systems, which can be time consuming and complex for the end users, and difficult for IT to control. Online Backup & Restore service is a fully automated online backup solution for desktops and laptops. It eliminates the uncertainty of traditional data backup methods through an automated process that sends critical data from end users’ PCs via a secure Internet connection to an offsite datacenter.

**Eliminates dependence on end users** – Backups are run automatically without end-user action ensuring data is consistently backed up.

**Minimize network and end-user impact** – Mass upgrades are compressed and sent only once regardless of the number of copies stored on various user’s PCs. Only incremental data is sent and all backups are automatically “check-pointed” so that interrupted backups restart where they left off.

**Maximum data security** – All data is transmitted using 128-bit AES encryption and is stored in fully redundant off site data storage facilities that feature mirrored servers.

**Centralized management and reporting** – Centralized management and reporting console (integrated with Dell Distributed Device Management) enables remote deployment of the service to PCs, identifying non-compliant PCs and initiating backups.

**Does not require corporate network connectivity** – Only an Internet connection is required to back up or retrieve data (no need to be connected to the corporate network via WAN/LAN or VPN).
Robust file retention policy – Up to ten versions of any backed up file are retained, and deleted files are retained for 90 days, enabling easy restoration of an older version of a file or of files that were unintentionally deleted.

6. What devices can Dell Online Backup & Restore work with?
Dell Online Backup & Restore can automatically back up data files from and restores data files to devices running Microsoft® Windows® (Windows 2000, Windows 2003, Windows XP SP1 – 3, Vista® ) no matter where they are located on the Internet. Devices do not have to be at the office or connected to the company network (locally or via VPN). As long as a device is connected to the Internet, data files are automatically backed up at scheduled times without any user intervention and can be restored by the user. Only 32-bit systems are supported at this time.

7. What type of backup does Dell Online Backup & Restore provide?
Dell Online Backup & Restore provides ‘Data Only’ backup; your critical data files are backed up and protected, but software applications that are installed from a disk or CD are not backed up. This methodology not only can save you time and money (shorter backup times and less GBs stored and paid for), but would also help in recovery of a system crash by re-installing your software so that essential information can be written back into the Windows registry database that is part of your operating system.

8. Does Dell provide different backup plans / options?
Yes. Dell Online Backup & Restore can be configured to back up data in a number of different options. You can back up all data files, all business files (exclude video, audio and graphic files), or give end users flexibility in the files they chose to backup based on company presets. The plan you choose determines the amount of data being backed up for each device, and you are charged a monthly fee per device based on that amount of data.

9. How long will the first backup on a device take?
This depends on a number of factors including the device’s Internet connection speed, the level of service that a company signs up for (e.g. backup all data files vs. business files only) and the number and size of the files to be backed up. Based on Dell’s experience with its customers, the first backup typically can take several hours. Each successive backup thereafter will generally take approximately ten to fifteen minutes because only the changed portions of the files need to be compressed, encrypted and backed up. During a backup, user productivity is not impacted, and users can check email or perform other computing activities while the backup takes place.

10. What is the retention policy for files?
Once a file is backed up, any changes between different versions of that file are also backed up for up to ten versions. The policy is that the most recent ten versions within a 30-day period are retained on the data center servers. This policy enables you to easily find and revert to an older version of a file. In addition, deleted files are retained in the data center servers for 90 days and deselected files (i.e., a file that was initially selected to be backed up and later removed from the list) are retained in the data center servers for 30 days. This policy enables you to easily get back files that were unintentionally deleted or deselected.

11. **How do I access files that have been backed up?**
Accessing your data is easy using the intuitive interface of the Dell Online Backup & Restore agent. Just click on the Retrieve View tab and select the files you wish to restore. Then click ‘Retrieve Now’ to download the files to your machine.

12. **How do I retrieve data in case of a catastrophic failure (i.e., the data has to be put on a different or re-imaged device)?**
Once the new or the re-imaged device is up and running, you will have to reinstall the Dell Online Backup & Restore Agent on that device. This can be done by simply e-mailing the agent to the new device or, if your company is using Dell Software Distribution, by sending the agent to the new or re-imaged device using that service. Once the agent is installed on the new or re-imaged machine, contact Dell Services team and they will assign the data backed up from the old device to the new one. Once that is done, simply access the Dell Online Backup & Restore Interface and click on ‘Retrieve Now’ to download all the files back to the new or re-imaged machine.

13. **At what time does the backup run?**
You may back up your data as often as you like, as long as your computer is turned on and connected to the Internet. In fact, the more often you backup, the faster your backups will be, since less data will need to be sent each time. This service also provides the capability to preset times/dates for backups to occur in the future, that will kick off automatically at the given time.

14. **How often can I perform a backup?**
You may back up your data as often as you like, as long as your computer is turned on and connected to the Internet. In fact, the more often you backup, the faster your backups will be, since less data will need to be sent each time. The easy-to-use Dell Online Backup & Restore Agent Schedule Settings are located in the Options / Backup Schedule menu and from there you can set days and times for your backup to automatically happen.

15. **How does Dell help ensure that Online Backup & Restore is secure?**
16. Can I use Online Backup & Restore service with a firewall?
Yes. Online Backup & Restore service uses TCP connections on port 16384 so it is compliant with all firewalls that conform to the TCP/IP protocol standard, including SOCKS Proxy firewalls.

17. Regarding Macs (Moves, Adds, And Changes), does the online back-up data remain with the device or the user?
Each device, and not the user, is associated with a Dell Online Backup & Restore account. However, since the data for each account resides in a secure datacenter facility, the data from the original account can be easily shared to a new account on a new machine so that data can follow the end user if he or she gets a new PC.

18. How will Dell Online Backup & Restore impact the performance of my network?
Dell Online Backup & Restore is designed to minimize the impact on your network bandwidth. Backups are scheduled during off-work evening hours and you can set policies to minimize the bandwidth impact of multiple devices backing up at the same time. In addition, data compression and file transfer optimization eliminates sending duplicate files and minimizes bandwidth usage and network traffic.

19. What happens if a device is turned off or loses its Internet connection in the middle of a backup?
Dell Online Backup & Restore comes with checkpoint restart. This means that if a backup is interrupted for any reason, the next time data is backed up from that device, the backup resumes from previous point of interruption and does not start over. This is another way that Dell Online Backup & Restore minimizes the bandwidth impact on each device and on your network.

20. How can I make sure that a particular device has been backing up its data?
Dell Online Backup & Restore provides real time reporting and charting on the backup status of each device.

21. Is Dell Online Backup & Restore difficult to deploy?
No. If you already are using Dell Distributed Device Management service, Dell Online Backup & Restore can be deployed in a matter of minutes. If you are purchasing Dell Online Backup & Restore as a standalone service solution, depending on the size of your

The data is compressed and encrypted using 128-bit AES encryption on the user’s machine by the Dell Online Backup & Restore agent before ever being sent out over the Internet to a secure off-site facility, where it is stored in its encrypted and compressed state.
organization, this service can be deployed in a matter of days to weeks – much faster than typical on-premise solutions which can take months to get up and running. Since Dell Online Backup & Restore is a hosted SaaS solution, it works over the Internet and does not require you to purchase any hardware or software, and does not require any staff to administer or support.

22. What hardware do I need?
None. Dell Online Backup & Restore does not require any hardware on a customer site or network. The Dell Desktop Manager is a hosted SaaS-enabled solution that runs on Dell’s datacenters and is administered by the customer or Dell Services (if the customer chooses) through a web-based console.

23. Can Online Backup be purchased a la carte?
Yes

24. Who is using Dell Online Backup & Restore?
Over 45,000 PCs globally are currently protected by Dell Online Backup and Restore services. Clients include: Bowe, Bell & Howell, Brocade Communications, CB Richard Ellis, salesforce.com, Sealed Air and WebEx.

25. Is there any activity reporting available?
In the Dell Distributed Device Management Control Center, there is dashboard-driven, centralized management reporting:

- By date of last backup & size of backup
- By account number

26. Where are the Online Backup &Restore console and associated servers hosted?
The Control Center infrastructure for the latest version of DDM resides in redundant data centers in Austin, TX at this time. Dell plans to utilize datacenters in Frankfurt, Germany and Amsterdam, Netherlands for EMEA-based clients beginning in late 2009. Dell also plans to utilize data centers in Latin America and Asia-Pacific regions in the near feature for clients based in those areas.

The actual data is backed up to data centers of Dell partner Iron Mountain. Iron Mountain has data centers in the United States, Canada, and the United Kingdom, and data is generally backed up to the closest geographic location to a customer’s headquarters, unless the customer requests otherwise.
Laptop Data Encryption – Service Details:

1. What is the Dell Laptop Data Encryption service?

Dell Laptop Data Encryption service helps ensure that sensitive data stored on desktops, laptops and tablet PCs will not fall into the wrong hands - even if the computer itself is lost, stolen or compromised. Laptop Data Encryption helps secure access to all data on your computer by detecting user behaviors which are inconsistent with expected norms and providing an indicator that unauthorized persons may be attempting to access the device. More specifically, all data on the disk is protected by encryption against all major threats and the encryption key is deleted, barring access to the data, if specific indicators for unauthorized access are present.

2. How does the Laptop Data Encryption service work?

Laptop Data Encryption is an easy-to-deploy service that can be up and running in a matter of hours protecting your company’s most valuable data. This is how it works:

- The Laptop Data Encryption agent is deployed on the device by Dell.
- Pre-set rules are downloaded by the agent and all data is encrypted on the device.
- These policy settings inform the device to eliminate the encryption key under specified conditions. Thus, the device is prepared to protect itself when an unauthorized access attempt occurs such as a password hack, a removal of the hard disk, or a theft of the device.
- If a device is reported lost and if the lost device ever communicates with the server again, the agent will be instructed by Dell’s Managed Services team to immediately eliminate the encryption key.
- If a lost or stolen device does not connect back to the Internet within a specified time, then the pre-set rules trigger the deletion of the encryption key. No manual intervention is needed and the process is transparent to the end user.
- The Dell Managed Services team can also retrieve location-based information for a missing laptop using network traces, network configuration data, and user activity. This information can be provided to law enforcement to help in locating the laptop and prosecuting the perpetrator.
- In the event that the device is found, data recovery is possible by contacting Dell, whose Managed Services team will validate the user and restore the key so that access to data on the device is restored.

3. What are the benefits of using Laptop Data Encryption?

- Helps protect mission critical data with a complete multi-layered security solution that helps prevent unauthorized data use.
- Helps avoid costs and risks associated with negative publicity, legal liability, and regulatory noncompliance by being in control of the data even if not in control of the PC.
- Can maximize end user transparency with a solution that requires virtually no end user acceptance, compliance or training.
• Helps simplify key management and reduce overhead administration costs through a managed service offering.
• Helps prevent identity theft and recover stolen PCs through proactive monitoring of the missing PC.

4. How is Dell Laptop Data Encryption installed on a device?
To deploy Dell Laptop Data Encryption a light-weight client agent is installed on each managed PC. This can be quickly accomplished by using the Dell Software Distribution service, log on scripts, or IT emailing an executable file to end users. The installation of the agent takes approximately 10-15 minutes and most of the data on a device is encrypted at that time. A system reboot is required during the installation.

5. Can Laptop Data Encryption be purchased a la carte?
The Laptop Data Encryption managed service can be purchased a la carte or it can be purchased along with other Dell services.

6. Does the service protect information even when the device is not on the Internet?
Yes. The service will apply the last policy it received from the Laptop Data Encryption server even if the device is not on the Internet. As a result, timer-based policy triggers will cause the encryption key to be deleted, regardless of Internet connectivity.

7. How do we mark the information, documents, etc., which are to be encrypted?
Dell Laptop Data Encryption is pre-configured to automatically identify the most common file types and locations to ensure that all important data on all local drives is encrypted.

8. Does Laptop Data Encryption have the ability to destroy data?
The current version does not destroy data. It intelligently encrypts data which secures the data and prevents it from being misused through elimination of the encryption key when a threat is detected.

9. What devices can Dell Laptop Data Encryption work with?
Dell Laptop Data Encryption can secure access to all data on devices running on Microsoft Windows® 2000 SP4 and Windows XP® SP2 – SP3, and Vista® (BitLocker®) by encrypting all data on a device and detecting user behaviors which are inconsistent with expected norms, providing an indicator that unauthorized persons may be attempting to access the device. Only 32-bit systems are supported at this time. **How can I help ensure that an unauthorized user does not uninstall the Dell Laptop Data Encryption Agent?**

While the Dell Laptop Data Encryption service comes with an uninstaller to uninstall the service/agent from a device, the uninstaller will not work until the Laptop Data Encryption service for that device is deactivated by Dell Services. An authorized person from your
company must first contact Dell Services and deactivate the Laptop Data Encryption service for a particular device before the application/agent can be uninstalled from that device.

10. **What type of encryption is used by Dell Laptop Data Encryption?**

Dell Laptop Data Encryption uses Encryption File System (EFS) algorithms that come with: Microsoft Windows 2000 uses the expanded Data Encryption Standard (DESX) algorithm for EFS encryption and decryption.

- Microsoft Windows XP SP2-SP3 can encrypt/decrypt files using DESX, 3DES, or AES.
- Vista (BitLocker)

11. **What is EFS?**

EFS stands for Encrypting File System which is part of the Microsoft NTFS file system. EFS is a transparent public key encryption technology that works in conjunction with NTFS permissions to grant and deny users access to files and folders in Windows NT (excluding NT4), 2000 and XP (excluding XP Home Edition) operating systems. EFS uses a public key and a private key for encryption. If the user does not have one, EFS generates the key pair automatically. Files can be encrypted individually or a folder can be designated as encrypted, so that any file written to that folder is automatically encrypted. Because EFS’s encryption technology integrates into the file system, users can’t access the hard disk without going through the file system.

12. **What government specifications does Dell Laptop Data Encryption adhere to?**

Dell Laptop Data Encryption adheres to FIPS 140 and DoD 5220.22-M standards. Federal Information Processing Standard (FIPS) 140 is a US Government standard that provides a benchmark for implementing cryptographic software. It specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. DoD5220.22-M is the National Industrial Security Program (NISP) Operating Manual. It references methods to be used to sanitize data from magnetic media such as hard disk drives.

13. **Under what circumstances can the encryption key be deleted?**

Dell Laptop Data Encryption comes with pre-configured policy settings for the following five rules: Invalid Login, Out of Contact, Unrecoverable, Device Reported Lost/Stolen, and Optional, Configurable Date & Time Rule.
There are four actions taken when thresholds are reached for each policy based upon escalating risk. These are 1) Warning Message (optional), 2) Device Shutdown, 3) Persistent Device Shutdown, and 4) Encryption Key Destruction. You can obtain additional details on policy rules and actions taken from Dell Services.

14. How does Dell restore the encryption key once the user is locked out of the device?

The authorized company contact calls Dell and is validated by the Dell Managed Services team. The Dell Managed Services team utilizes the Data Encryption Administrative Console to select the restore key for the locked device. Once the device establishes an Internet connection, the key is automatically downloaded by the Data Encryption agent and installed thereby enabling the end user to access their encrypted data. Throughout this process, no end user involvement is necessary.

15. What are processes undertaken by Dell for encryption key retrieval and destruction?

**Deletion of Encryption Key**

If a system protected by Laptop Data Encryption is reported lost or stolen, within 4 hours of receipt of a client’s notification that a PC with the Laptop Data Encryption service is lost or stolen, Dell will mark the system as lost/stolen and automatically delete the encryption key the next time it connects to the Internet. The request to initiate this service on a lost or stolen PC must originate from an authorized client contact.

Upon request and for a fee, Dell will attempt to identify the location of the PC based on IP address.

**Restoration of Encryption Key**

If a system protected by Laptop Data Encryption needs restoration of the encryption key, within four hours of receipt of a client’s notification that a PC with Data Encryption is found and needs an encryption key to be restored, Dell will mark the system as found and automatically restore the encryption key the next time it connects to the Internet. The request to initiate this service on a system must originate only from an authorized contact.

16. Can I change my default security policy settings as often as I like?

Laptop Data Encryption comes with default policy settings which should meet the needs of the majority of customers. For those customers who would like to modify the policy settings, Laptop Data Encryption enables them to change policies once per year for free. If additional changes are required throughout the year, these will be billed on a time and materials (T&M) basis at the then current rates.

17. Will there be a limited list of customer contacts who can call the Dell Managed Services team reporting a lost/stolen PC?

Yes, two contacts per company.
18. Will the Dell Managed Services team provide 24x7 coverage for lost or stolen assets?
   Yes.

19. Is there an extra charge for key restoration for failed logons?
   Dell recommends using the default policy setting which is set to allow for 8 failed logons before eliminating the encryption key to minimize the number of false alarms. Five key restorations due to failed logons per year per company are free. Additional key restorations due to failed logons will be billed on a time and materials (T&M) basis at the then current rates.

20. Is there any reporting of activity available?
   The Dell Managed Services team has access to screen-based reports in the Laptop Data Encryption administrative console and can use these to monitor all security and administrative actions for the customer. The current release does not come with standard out-of-the-box reports for our customers.

21. What is the load on the network when using the data encryption service?
   Each device checks in with the Laptop Data Encryption server approximately once per hour. This transaction is very light (approximately 1KB) and occurs at different times for each client. Network load scales geometrically as more machines are added. During installation and when new rules are downloaded, the network payload is larger. However, these events occur infrequently and should not significantly impact network traffic.

22. What hardware do I need?
   None. Dell Laptop Data Encryption is a managed service that is administered by Dell Services and does not require any hardware on a customer site or network.

23. Can a customer have access to the Laptop Data Encryption administrative console?
   Laptop Data Encryption is currently only being offered as a managed service in which the Dell Managed Services team provides the service on behalf of the customer.

24. Is this service integrated with the Dell Distributed Management Control Center?
   Not at this time. Integration with the DDM Control Center is planned for a future release.

25. How does the Laptop Data Encryption service differ from other security products available?
   Many security products concentrate on preventing the loss or theft of your computer. Laptop Data Encryption service provides data security by encrypting all data upon installation which secures the data even when you are no longer in possession of the device.
26. How does Laptop Data Encryption differ from a Full Disk Encryption (FDE) solution?

Unlike Full Disk Encryption (FDE) solutions, Laptop Data Encryption is focused on a customer’s need to control and monitor their data. FDE solutions are only effective if the encryption key is properly protected by end users – a task at which they are notoriously not very effective. In addition, FDE emphasizes pre-boot authentication whereas Laptop Data Encryption uses Windows authentication and tracks the logon attempts, eliminating the user certificate if hacking is attempted. Laptop Data Encryption encrypts files using the same algorithms used by standard FDE software: 256- bit AES or 3DES.

Some of the advantages of Data Encryption over FDE:

• With Laptop Data Encryption, the current logon method is maintained, eliminating need for any end-user training or changes to the IT and support infrastructure – FDE does require these changes to function properly.
• Laptop Data Encryption monitors the status of all client PCs, even after a loss or theft, and secures the data even if the thief has the password (as often happens if the user wrote the password down or if the user is the thief - insider threats are amongst the largest ones) with either the timeout triggers or the online kill switch.
• Unlike FDE solutions, client PCs protected with Laptop Data Encryption continue to report back so that the enterprise knows that its data is secure.

Summary

Dell Distributed Device Management helps reduce the risks and costs of managing client PCs by allowing IT managers to centrally track assets, distribute software, manage patches and enforce polices. IT administrators can manage any Internet connected, Windows-based PC (Dell and non-Dell) virtually, regardless of the PC’s location. These services:

• Provide management visibility and control over remote client PCs via the Internet without requiring the PC to be connected to the company network (no WAN/LAN or VPN required).
• Are designed to provide policy-based centralized management to update and maintain thousands of PCs by type or use.
• Are Cloud optimized and delivered as a SaaS services that leverage the Internet, so the services require no up-front expense and can be deployed more rapidly than competing on-premise solutions. Subscription-based pricing provides a predictable cost structure with virtually no upfront investment.

Contact Dell Today

For additional information on Dell ProManage Modular Services such as pricing and a free demo, please visit www.dell.com/modularservices.

©2009 Dell, Inc. Dell is a registered trademark of Dell, Inc.
Microsoft, Microsoft Windows, Windows XP, and Microsoft Office are all registered trademarks of the Microsoft Corporation.