Finding mobile security in the cloud.

Software as a Service (SaaS) will help protect your laptops, their data, and will even help recover them if necessary.

By John Dodge

Today's increasingly mobile workforce means making sure workers have technology tools that give them access to data wherever and whenever they need it. That also means a company's hardware and data assets can be anywhere at any time — and therefore vulnerable to theft and loss.

Security for mobile devices will be top-of-mind for IT leaders for years to come. The mobile workforce is growing by leaps and bounds: IDC predicts it will expand from 919.4 million in 2008 to 1.19 billion workers worldwide. In the U.S., the mobile workforce is growing even faster: by 2013, it is forecast to be 119.7 million workers, accounting for 75.5 percent of the entire workforce, according to IDC's Worldwide Mobile Worker Forecast from December 2009 to 2013. Such dramatic growth in the mobile workforce poses a security challenge for IT. IT must protect the assets of their employers, and above all ensure the security of the company's sensitive and confidential data that resides on those devices.

Empowering employees to be productive and mitigating the risk of mobility is a balancing act, but there are tools that can make the job easier. The bottom line is that IT must ensure security and prevent data loss even if the laptop is lost or falls into the wrong hands. These are critical IT mandates when managing a mobile workforce.

All one has to do is search "stolen laptops" on Google to find hundreds of horror stories about data stolen from laptops. Indeed, a study conducted by Intel Corp. and the Ponemon Institute in 2009 found that each lost or stolen laptop costs corporations an average of $49,245.

That study was summarised in October 2010 in a report entitled "The Billion Dollar Lost Laptop Problem." Other studies say the figure is even higher. The same study reported that the main worry is data breach, which represents 80 percent of the loss. The value of the notebook itself by comparison is incidental. And it's not just financial loss companies should worry about. Compromised data can also mean regulatory noncompliance, legal exposure, negative publicity and just plain embarrassment.

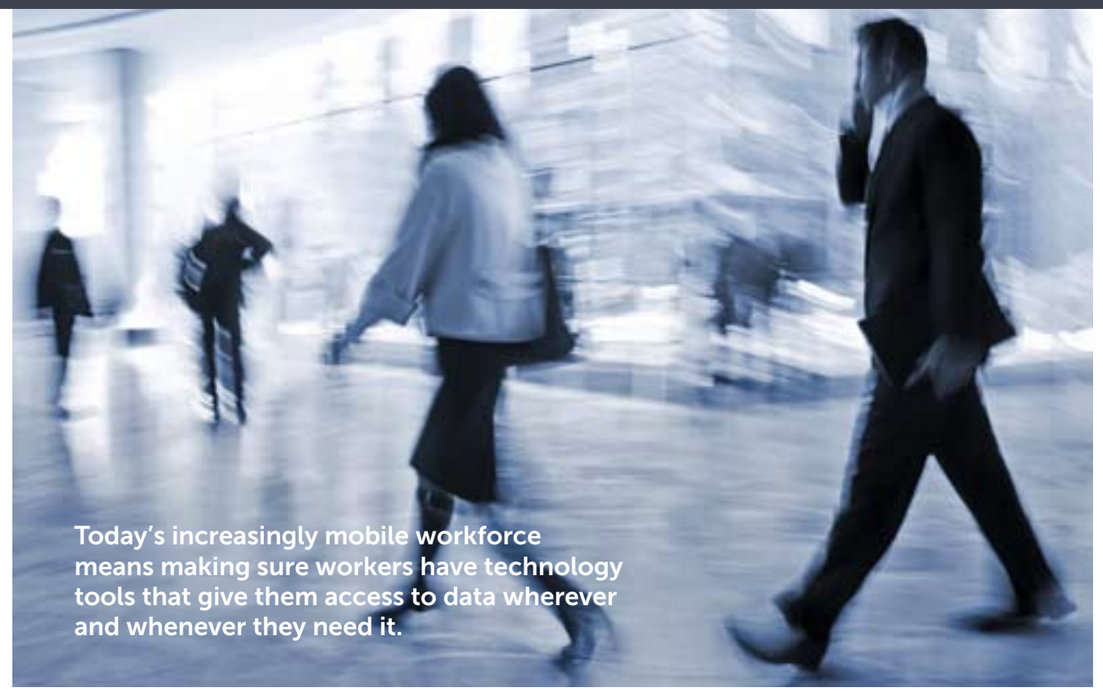
And the problem is getting worse. The Safeware Insurance Agency Inc., which specialises in policies for systems and electronics, estimates that 1.4 million laptops were stolen in 2004. Today, Safeware says that figure has grown by 70 percent to 2.6 million, which translates into a laptop being stolen every 12 seconds.

Actually, a reasonably accurate number of stolen and lost laptops is hard to come by because many incidents go unreported, according to the 2010/2011 Computer Crime and Security Survey from the Computer Security Institute about cyber-crime. Fully a third of the 285 respondents reported laptop theft in describing cyber attacks at their companies.

Leverage SaaS to protect your laptops — and the data stored on them

Suffice to say laptops are the apple of many a criminal's eye. But there are multiple ways to protect the data and even recover the laptops.

Data should be encrypted and backed up before something bad happens — and when it does, laptops should also be able to be tracked and recovered, and the data either remotely retrieved or deleted.



Dell offers a suite of Software-as-a-Service (SaaS) tools that help companies protect their laptops and the data stored on them.

SaaS offers several advantages over buying software outright and maintaining and upgrading it yourself. Given that SaaS operates over the Internet, it is available anytime and anywhere, and you pay only for what you use. Upgrades are automatically distributed as the service is used, so they do not have to be pushed out to users, and it easily scales as your business grows and the number of mobile employees increases.

Almost all stolen business laptops contain confidential data, much of it highly sensitive. How do you recover the data or at minimum prevent the data from being compromised?

The first line of defense is to encrypt the data, and there are multiple ways to do it.

For instance, data can be encrypted just on the hard disk or on everything that comes in contact with that notebook. Dell Laptop Data Encryption allows all of the information stored on a laptop or PC to be encrypted, so if it falls into the wrong hands, the data cannot be accessed. The information can also be automatically secured based on predefined events like hard disk removal or a lack of timely login. All of this is easy to install and requires minimal management, because Dell takes care of the encryption process and keys.

While encryption renders the data useless in the wrong hands, it still has value to the company. That's where Dell Online Backup & Restore for laptops comes in.

Laptops are the most vulnerable from data loss (and don't forget hard disk failures as well). Dell offers an SaaS solution that IT can set to automatically back up laptop data when it is connected to the Internet.

Dell technology can also help track and recover missing laptops with Dell System Track and Recovery (STR) service. This service allows an IT manager to monitor connection status and locate laptops when they connect to the Internet. STR further protects data and laptops with remote data deletion, system lock and emergency file retrieval.

The same service can also help locate and recover missing laptops. This functionality is managed through a customisable Web-based console that can be accessed from anywhere.

Besides protection from theft and loss, these far-flung systems must also be managed on a daily basis. IT has to make sure mobile users have the latest software versions and patches and correct security policies. What's more, laptops need to be tracked as company assets.

Sounds complicated and time consuming, doesn't it? It's not using Dell Distributed Device Management (DDM), an efficient and cost-effective portfolio of Internet-hosted management services. With no up-front investment, DDM allows IT to centrally manage 500 or 50,000 laptops regardless of location as long as they have access to the Internet. DDM's benefits are numerous: It's highly scalable, quickly deployed, and easily configured and managed. New features, users and capabilities can be added rapidly and no VPN is required to securely perform all of these activities.

The age when a company's computers were securely locked away in data centres has long since passed. The explosion of laptops and mobile applications has created a critical need for new, flexible types of security solutions that can keep up with the demands of an ever-expanding mobile workforce. SaaS solutions efficiently and effectively answer that need.

John Dodge is a veteran technology and business writer based in Massachusetts.

More Information @

dell.co.uk/ddm

Boomi will help companies migrate to cloud computing.

You've probably heard a lot about how cloud computing can help lower costs, speed application deployment and allow you to easily scale.

But how can businesses fully leverage cloud applications? The answer could be Boomi, Inc., a cloud integration company Dell acquired in November of 2010.

Boomi's specialty is connecting on-premise applications and data with popular cloud applications from companies such as Salesforce.com, NetSuite, Coupa, Taleo, SuccessFactors, and RightNow Technologies.

"Dell is undergoing a transformation to be more focused on the cloud. Integration is a natural first step into the cloud," says Boomi chief technology officer Rick Nucci. "We help companies automate their business processes by integrating their apps."

"Mid-size business on-premise applications are typically finance-related, from companies such as Great Plains, Intuit (QuickBooks) or Peachtree. Larger companies typically connect apps from companies like SAP and Oracle to the cloud," Nucci says.

As a result of connecting business applications to the cloud, Boomi eliminates costs associated with inaccurate data entry.

"Cloud integration most often replaces the most labor-intensive processes, such as data re-entry, into different applications. With Boomi, you enter data once in an application and it's automatically synchronised to your other applications," said Nucci. "Data entry is a pretty easy cost to calculate: The bigger the company, the bigger the pain."

It's simple to get started: By using an intuitive drag-and-drop menu, customers can connect their on-premise applications to cloud applications with Boomi.

If the result to the business is lower costs and increased innovation, then all parties concerned will benefit.

More Information @

dell.co.uk/boomi