IT-Harvest

The Future of Data Protection

May 1, 2012

Answers the question: What are the future challenges to effective data protection and how will they evolve?

The introduction of mobility and the cloud into business IT environments is creating a host of new data protection challenges. As data fragments to multiple mobile platforms and coalesces in the cloud organizations must re-think their approach to the data protection problem. An integrated Data Loss Prevention strategy must evolve to incorporate the challenges of cloud and mobile environments.

Data protection in its first stage tended to focus on data residing on servers and accessed by endpoints within a controlled environment: the enterprise IT infrastructure. While the emergence of integrated DLP solutions is enabling enterprises to surmount the deployment challenges that hobbled first-generation, overlay data protection solutions, many are now struggling to extend that protection to mobile devices and the cloud.

Mobile devices — laptops, smartphones, and tablets — are rapidly being deployed with the same access to critical data that traditional, company-owned desktop machines have. Even the simplest device can store documents, spreadsheets, and diagrams and thus expose them to the danger of loss or theft. Of greater significance, and a greater challenge, is the fact that more and more frequently these mobile devices are not owned by the company, but are instead owned and maintained by the employee. As a result, the predictability of when, how and who would access corporate data is rapidly being lost, with profound implications for data protection approaches. In order to adapt to this unpredictability, integrated DLP will have to either be deployed to employee owned devices, the apps they use, or to a network access point.

In order to deliver data securely to these mobile platforms, many enterprises are either extending their data centers or already using cloud based services, such as Salesforce.com, to manage critical data. DLP will have to integrate with cloud platforms to restrict access to critical data and control how that data is used. Extending a data protection regime to the cloud will be the biggest challenge in the future.

KEY POINTS:

- Virtual environments are becoming the primary repository of critical data.

  By now it is evident that the flexibility, availability, and resilience of cloud computing is rapidly drawing enterprise data processing away from the corporate data center. Even those that continue to maintain those data centers are spinning up cloud environments as backups and sometimes relegating the existing data center to back up duty as the cloud becomes the primary repository of critical data. But cloud data, as fluid and transient as it is, still needs to be protected. The key to cloud data protection is encryption, and the key to encryption in the cloud is key management. Encryption keys were already becoming difficult for the enterprise to manage. In the cloud, the important factor is protecting those keys from the cloud provider while making sure they are always available to those that are authorized to access data.

This paper is sponsored by Trend Micro.

Trend Micro integrates Data Loss Prevention into their products at each layer of defense, unified by central policy management and visibility through Trend Micro Control Manager 6. For Trend Micro customers with DLP-ready products already deployed, a deployment scenario involves simply licensing and activating the integrated DLP capability.

Trend Micro products that support integrated DLP modules are:

- **Trend Micro OfficeScan**
- **Trend Micro ScanMail**
- **Trend Micro Portal Protect**
- **Trend Micro InterScan Messaging Security**
- **Trend Micro InterScan Web Security**

Trend Micro and mobile security solutions:

- **Deep Security**
- **SecureCloud**
- **SafeSync for Business**
- **Mobile Security**

Central policy management, monitoring, and reporting are provided by the Trend Micro Control Manager.

- Centralized key management and cloud encryption are the primary solution for data protection in the cloud. For both cloud and mobile environments encryption is vital. Easy and real time access to those keys must always be available to authorized users and protected from public cloud administrators and attackers.

- Both virtual desktops for users and cloud storage for big data are points of weakness.

  Virtual desktops are becoming an alternative to traditional thick clients with buggy and vulnerable operating systems and applications. The virtual desktop offers advantages for protection, and ultimately makes it easy to repair and clean up environments, post infection. The standard image is nursed and coddled so it is always patched and the latest versions of applications are in place. Every time a user initiates a connection they are in the most protected state. When they sign off, any advanced persistent threats that have managed to successfully employ a zero-day vulnerability and bypass any software defenses are eradicated. Yet what about data the user has been working on or creating? It too has to be protected in real time from exfiltration, downloading to portable data devices, or misuse by trusted insiders. Advanced data protection, integrated into virtual desktops and physical security layers, will have to protect data in the transient world of desktop virtualization.

- Be prepared for monitoring for data policy violations in cloud deployments that mimic endpoint data protection requirements. Data protection solutions discover and keep track of instances of documents, and even segments of documents, that may be cut and pasted for re-use. Whether those documents reside on mobile endpoints, virtual desktops, or cloud repositories.

Ultimately, data protection must follow the data. As that data migrates to the cloud, and access is through a plethora of mobile devices, a management console integrated with existing security and policy technology must evolve to monitor and control data creation and dissemination everywhere.

