Key Considerations for Effective Data Loss Prevention
Among the various vulnerabilities and potential intrusions that your network is subject to, a data breach is one of the most damaging and costly. It’s not only about the data loss that happens due to a security breach, but also the impact of the loss. ESG estimates that the cost of recovery per breached record can go up to $150 each, which can add up fast when thousands to hundreds of thousands of records are compromised. But it doesn’t stop there; data breaches can also result in loss of customer loyalty, damage to corporate reputation, lawsuits, legal fees, compliance violations, criminal penalties, and more.

The sheer volume of data in a typical IT environment makes it difficult to control data loss through multiple endpoints. Typically, data loss happens when security is compromised and sensitive data is accessed. In other words, it is the unauthorized, intentional or unintentional, infiltration of confidential information on a secure network.

**What is Data Loss Prevention?**

Data Loss Prevention (DLP) is a strategy to ensure that your sensitive data doesn’t move outside of your network. It helps you reduce the risk of confidential information getting into the wrong hands. And, with the continuous increase in cyber-crimes, both internally and externally, it has become even more imperative to protect data across its various stages.

In terms of DLP, there are three key data stages that need to be addressed:

- **Data in Motion/Transit (DiM/DiT)** – Any data that is moving through the network outside of your organization via the Internet
- **Data at Rest (DaR)** – Data that resides in your databases and other methods of storage
- **Data at the Endpoint/Data in Use (DiU)** – Data at the endpoints of the network (e.g. data on USB devices, external drives, and many other mobile devices)

**Where and How Does Data Loss happen?**

Data loss and data leakage can occur from multiple endpoints on your network. It’s important to remember that sensitive data can be accessed through a wide range of devices and applications—spanning across desktops, mobile devices, emails, and more.

In recent years, we have heard about the loss of sensitive information through USB drives and other mass storage devices that make it easier than ever for data to walk out the door. The usage of thumb drives is a common practice in most workplaces given their convenience and ease of use. Unfortunately, the use of such devices poses a real internal security threat, especially from a data loss/data leakage standpoint.

Here’s how:

- Whether intentional or unintentional, USB devices can be the source of data loss given their extreme portability and high likelihood of “walking out the door” with the employee.
- The increasing capacity of flash drives, along with techniques like “pod slurping”, make it easy to quickly copy large volumes of data and steal sensitive/confidential information.
Impact of Data Loss

As mentioned at the beginning of this paper, the loss or leakage of sensitive data can result in serious damage to an organization, including:

- Loss of Intellectual property
- Loss of copyrighted information
- Compliance violations
- Damage to corporate reputation/brand
- Loss of customer loyalty
- Loss of future business opportunities
- Lawsuits and ongoing litigation
- Financial and criminal penalties

To help you protect sensitive data and reduce the risk of data loss, we’ve compiled some key DLP considerations and tactics in this whitepaper.
#1 Know your threats

You can help prevent data loss by knowing your network and threats well. To do this, you need to first identify critical systems and assets within your IT infrastructure, and then begin monitoring for vulnerabilities that might allow access to potentially sensitive information. For example, if your firewall isn’t configured properly, a hacker can spot a port that is accidentally left open and gain access to your network. Similarly, rogue access points, misconfigured routers, and botnet malware can all serve as entry points for hackers to access your network.

Monitoring and analyzing event logs against an established baseline of “normal” network activity provides the insight required to effectively detect and respond to threats. Each log file contains valuable information to help identify intrusion attempts, misconfigured devices, anomalous network patterns, and many more network-related events. SIEM tools like SolarWinds® Log & Event Manager (LEM) help you enhance security and optimize troubleshooting by understanding the relationship between various activities using multiple event correlations and alerting you when your network encounters a threat or other vital issue.

SolarWinds LEM employs a proactive approach to help you identify and respond to threats in real time. LEM automatically collects and aggregates log data from network devices, systems, and applications throughout the IT infrastructure. It then normalizes this data into a consistent format and performs multiple event correlation, along with the distinct ability to set independent activity thresholds per event or per group of events. The end result is security intelligence you can count on and reduced false positives.

#2 Don’t miss the forest for the trees

The sources for data loss aren’t always external. In fact, insider abuse and internal data theft are on the rise. There have been many cases where privileged users, such as database administrators or file server admins were found to have participated in selling sensitive/confidential data. Apart from monitoring the activities across your Web server, firewalls, and endpoints, you need to monitor user activities as well.

Follow SolarWinds: LinkedIn, Facebook, Twitter
Workstation logs can be a good place to start as they can give you some key information like:

- Login/Logoff attempts
- Non-compliant folder sharing
- Accessed URLs
- Insecure file transfer
- Unauthorized software installation
- Malicious processes
- Misappropriation of user privileges

#3 Allow only authorized access on your network

Preventing data loss is not only about protecting your sensitive and confidential data; it’s also about mitigating the risks that come with unsafe or non-compliant behavior on your network. For example, a disgruntled employee may decide to copy sensitive information and leak it externally. Additionally, the absence or lack of enforcement of defined policies around data usage, including BYOD, or lack of understanding of such policies by employees can lead to risky behavior on the network. A common scenario is when employees use personal USB storage devices to transfer or back up data, at which point confidential information can become mobile.

A tool like SolarWinds LEM can help protect your network from unauthorized access in multiple ways, including the ability to monitor user activity, such as logon attempts, and then correlate events with other log activity to identify suspicious behavior and malicious activity. LEM can then automatically disable user access.

Another key way LEM can prevent access to sensitive data is through its real-time detection and automatic detachment of unauthorized USB devices. Plus, LEM enables you to monitor what files and processes are accessed on the device.

The following steps explain how to allow only authorized USB access using SolarWinds LEM:

**Step 1:** Create a user-defined group in the LEM console and enable **USB Defender** on the systems you want to authorize USB access.
Step 2: Add the group of “authorized” devices to SolarWinds LEM rules and also set up Active Response rules to detach the unauthorized USB devices. You not only allow authorized USB access on your network, but also block all other unauthorized connections.

LEM’s powerful correlation rules alert you in real time when unauthorized USB devices try to access your network. You can also automate the reporting of your network’s USB usage and policy violations over time for network security audits.

#4 Secure your file transfers

There are chances that your employees may accidentally leak data when they use 3rd-party websites or cloud storage services, especially when there are file transfers. If employees send files or upload company documents though servers out of your network control, you in turn lose control of your data.

The problem with typical file transfers:

- Files are sent without encryption
- No control over the transferred files
- Lack of advanced options like session auditing

What’s needed is a secure managed file transfer (MFT) server that enables you to maintain the integrity of data shared between two entities. Below is a set of criteria for a managed file transfer solution:

- Security: Both at rest and in motion
- MFT Access: Limit access by role, individual, and time
- Certificate-based authentication
- File Storage: Limit access after upload, default file access policy, and security logs
- Monitoring: View “real-time” file transfer progress
- Reporting: Transfer activity and access
- Internal Resource Protection (Proxy Server): DMZ resident, conceal internal IP addresses
- Endpoint Management: Create, edit, and remove trading partner profiles

SolarWinds Serv-U Managed File Transfer (MFT) Server allows you to support secure file transfer and secure file sharing from your own datacenter. It supports FTP, FTPS, SFTP, and Web transfer (HTTP/S) services to support uploads and
downloads from almost any FTP client, Web browser, or Web-enabled mobile device. It also includes an ad-hoc file sharing interface that allows your end-users to safely send files and request files with anyone. Here’s how Serv-U Managed File Transfer Server can help you:

Security:
- Optional passwords protect individual sets of shared or requested files
- Automatic IP lockouts prevent brute-force attacks
- HTTPS sessions use the SSL certificate (X.509) of your choice
- FIPS 140-2 validated cryptography is available

Control:
- Files automatically expire and are deleted after a configurable period of time
- Complete control over the content lifecycle thus minimizing non-compliance

Auditing & Monitoring:
- Sessions are displayed in real time, with options to kick-out or drill-down into active sessions
- All activity may be written to disk for additional analysis
- Email alerts and Windows® Event Logging may be configured with Serv-U events
#5 Stay compliant, stay secure

Industry regulations, federal mandates, and privacy laws are all about protecting confidential information and preventing sensitive data loss. Being in line with IT compliance regulations, such as PCI DSS, GLBA, SOX, NERC CIP, and HIPAA require businesses to protect, track, and control access to and usage of confidential/proprietary information and private customer data. Unfortunately, many organizations treat compliance as just a “checkbox” to pass an audit, instead of focusing on putting truly effective controls in place to better secure their network resources and critical data.

With SolarWinds Log & Event Manager’s real-time log analysis and powerful cross-device/cross-event correlation, you can quickly uncover policy violations that could leave your network vulnerable to a breach. And, with over 300 predefined, customizable reporting templates, you can ensure the right controls are in place to not only maintain compliance, but keep your network and the data it holds secure.

Resources for Additional Learning

- Creating Rules in SolarWinds LEM (Video)
- Using nDepth and Reports to Analyze Log Data (Video)
- IT Security Checklist: 9 Key Recommendations (Whitepaper)
- How to use SolarWinds LEM for Fault Diagnostics and Prevention (Whitepaper)

About SolarWinds Log & Event Manager

SolarWinds Log & Event Manager (LEM) delivers powerful Security Information and Event Management (SIEM) capabilities in a highly affordable, easy-to-deploy virtual appliance. It combines real-time log analysis, event correlation, and a groundbreaking approach to IT search to deliver the visibility, security, and control you need to overcome everyday IT challenges and an ever-growing threat landscape. SIEM software has never been easier to use or more affordable.
SolarWinds Log & Event Manager Feature Highlights:

- Easy Collection of Network, Security, Machine, Application and Cloud logs
- Real-time, In-Memory, Event Correlation for Immediate Threat Detection
- Built-in Active Responses for Automated “Hands-Free” Remediation
- Automatic USB Device Detection and Detachment for Protecting Sensitive Data
- Advanced IT Search and Intuitive Data Visualization for Fast and Easy Forensic Analysis
- Predefined, Customizable Templates for Simplified Security, Compliance, and Operations Reporting
- Affordable, All-in-One Virtual Appliance for Quick and Easy Deployment and Use

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.