

THINK

Data Protection

Unmanaged removable media, such as thumb drives, effectively open a floodgate within federal organizations today, allowing data to escape, whether by accident or some sort of malicious intent.

Government organizations are increasingly bombarded with data leakage problems caused by removable media, and the regulatory consequences can be overwhelming. Think of it this way – the easiest way to ‘lose’ data nowadays is by allowing individuals to plug in thumb drives and walk sensitive information out of the door, or by enabling them to use such devices to introduce viruses, spyware or other malicious programs.

Industry experts such as the Ponemon Institute, estimate that slightly over half of all organizations don’t know what data is missing following a loss event. Without the ability to quantify data lost or track data movement, federal agencies face stiff financial penalties when accidents happen. By now, everyone is familiar with the situation at the U.S. Department of Veterans Affairs (VA), which is estimated to have spent more than \$100 million to ‘fix’ problems in the aftermath of a stolen external hard drive containing sensitive information on millions of veterans. Expenses included mailing multiple letters to each veteran, and providing credit protection services as well.

Accidents aside, an even bigger headache involves protecting against theft or espionage. Robert Hanssen, the CIA spy who went to jail for selling secrets to the former U.S.S.R., stored much of that organization’s top secret information on a PDA.

Fortunately, it’s possible to manage, control and audit data moved onto removable devices. Lumension Security, a global leader in security management formed by the combination of PatchLink and SecureWave, provides a solution that puts controls and audit trails on the use of removable devices to ensure sound protection of data-at-rest and data-in-motion.

Lumension’s Sanctuary Device Control enables even the largest federal institutions to create specific rules to allow granular access

for the download of data onto removable devices, when work situations require that flexibility. Device use and data movement is only allowed by permission, with the ability to trace data throughout the process.

Nothing underscores the success of Lumension’s Sanctuary more than its recent contract award to assist the VA. Also, a range of other DoD and intelligence organizations already use Lumension’s solution. Sanctuary enables the VA to create a ‘whitelist’ of allowed devices, denying all others by default. Sanctuary’s ability to assign permissions based on dozens of granular parameters allows the VA to implement flexible policy enforcement.

Achieving Compliance

To comply with the Office of Management and Budget’s M-06-16 mandate, which requires agencies to safeguard the integrity and availability of information, Lumension’s Sanctuary enforces encryption when data is copied to removable media and controls what devices are used by whom, and on what machines. And Sanctuary also helps agencies comply with Director of Central Intelligence Directive (DCID) 6/3, the established security procedure for storing, processing and communicating classified intelligence information in information systems.

Meanwhile, Lumension also recently obtained a patent for its ‘data shadowing’ technology, which enables organizations to monitor all information transferred to or from removable media, creating a centrally stored, complete copy of the information. This Sanctuary feature provides customers with a comprehensive audit trail for robust security and compliance.

As federal organizations continue to learn, being ‘reactive’ costs so much more than being proactive when it comes to protecting against data loss or theft. That’s why Lumension stands ready to assist public sector organizations in overcoming data protection challenges.



For more information, please visit www.lumension.com, call (443) 889-3291, or email patchlink.federalsales@lumension.com.