The Drive for Data Protection

April 17 2007

Not finished with updating your organization's payroll for the day? No problem - just save the documents to a USB thumb drive, drop the drive in your briefcase, stick it in one of your family PC's USB slots and finish up in the comfort of your own home.

But wait. Your kids were downloading some cool IM (instant messaging) icons, and now your home PC - and the USB devices connecting to it - are infected with a virus. Or, you thought you had stuck the USB drive in your briefcase. Or was it your pocket? In any case, where the heck is the drive?

Yes, it's easier than ever to take the data and run - a blessing for many users, but a curse for administrators charged with securing company information.

Employees need access to data to do their jobs, but IT implementers and corporate executives need to weigh the productivity benefits of allowing users to take data home against the security implications of private data lost via a rogue or misplaced device.eWEEK Labs recommends that companies not allow unfettered usage of portable storage devices with corporate machines.

However, the knee-jerk reaction of gluing employees' USB ports shut can hamper productivity significantly, because those ports could be used for card readers, digital signature devices and VOIP (voice over IP) handsets, among many other devices and functions.

Rather, we recommend the establishment of written data-handling policies, backed by policy-based security controls and accountability via reports and logs to ensure against data loss.

Microsoft's Windows XP provided the bare-minimum protection against device-borne data loss, but required some creative workarounds to get going. Windows Vista promises more granular controls to block device installation, plus read or write behavior blocking - albeit with some odd and unfortunate dependencies.

But the operating system is not the place to look for the current utmost in protection against accidental data loss, and oversight over and privacy for data that is permitted to be copied to devices, and proof of action for audit and compliance purposes. For these types and levels of protection, companies need to look to third-party solutions.

Indeed, the security market for products that protect against data loss from the endpoint is white-hot right now, with dozens of companies vying for a place on the corporate desktop.And it's a market that an increasing number of organizations are tapping into as a pre-emptive strike.

"We put something in place with - Microsoft - Active Directory that would block the use of USB ports, CDs or floppy disks, but it was not easily administered," said Miriam Neal, vice president of IS at South Western Federal Credit Union in California. Neal eventually settled on SecureWave's Sanctuary 4.1, which we have reviewed. We also reviewed Secuware Security Framework 4.0.

Both products offer policy settings to deny read or write actions to removable storage devices, approve the use of standard devices and enable the use of encryption.

Security Framework's strength lies in its ability to easily enable encryption on the enterprise level, providing a centralized way to encrypt off-the-shelf USB drives as well as primary operating system hard drives.

Sanctuary offers many of the same high-level capabilities as Security Framework, but it also drills deep down to provide administrators with incredibly in-depth control over the use of just about any port, device or connection type.

Sanctuary also provides the ability to log - or even keep a copy of - data permitted to be copied from the desktop.

Closer watch

In the months to come, we expect to see increased interest in content-aware technologies. Network DLP (data loss prevention) vendors, including Vontu, Vericept and Reconnex, have recently released new endpoint agents that promise not only to lock down the use of unauthorized storage devices but also to provide policy-based detection of proprietary data content copied to an approved device.

For example, if an authorized user copies a Social Security number or intellectual property to an unapproved location, this new breed of endpoint security would block and log the attempt.

However, content detection historically has been a network-based technology, so vendors will need to prove that their products will work on the desktop, intercepting disk IO behavior rather than a network stream without causing harm to the local system.

Many of these networking-based vendors have looked outside their own development teams to get going - with one notable exception: While

Vericept bought Black White Box back in 2005 and Reconnex partnered with an unnamed third-party endpoint security vendor, Vontu went it alone, developing its own endpoint solution in house.

There are drawbacks to cooperative products, as customers need to make sure that the same detection algorithms that are used at the network level are used at the endpoint. Also, the network and endpoint management functions should be fully integrated, with policy management, logging and reporting tied together for better trending and forensic analysis.

But Vontu's ground-up development comes at a cost as well, as its endpoint product appears less mature than the competition's. We learned in conversations with Vontu representatives that the company's Data At The Endpoint product is a log-only solution.

It cannot, at this time, block the copying of data to removable storage, but only notifies an administrator of policy violations via e-mail. While such a notification is marginally useful for accountability reports, the horse has already left the barn at that point.

Steve Roop, Vontu's vice president of products and marketing, in San Francisco, asserts that the risk for false positives currently outweighs any reward for automatic blocking: "Our clients value accuracy as a higher priority than automated blocking," Roop said. "If you block things that are false positive, you will aggravate a large number of your employees."

Roop added that the same detection algorithms Vontu uses at the network level are available for the endpoint. Automated blocking will come in the next revision, he said, after customers have gotten a handle on exactly what data flows are present and what they mean.

eWEEK Labs recommends that corporations evaluate their systems and assess risk tolerance to determine the mix of network and endpointbased products that will provide necessary auditing features, forensic analysis capabilities and - most importantly - peace of mind.

Citation: The Drive for Data Protection (2007, April 17) retrieved 19 April 2024 from https://phys.org/news/2007-04-the-drive-for-data-protection.html