



New security tools focus on the data

02/16/05

By William Jackson,

SAN FRANCISCO—The increasing mobility of digitized data and a growing concern over privacy is driving security from the network perimeter down to the data level.

"The United States is just now starting to accept this," said Todd LaPorte, channel sales manager from Utimaco Safeware AG of Germany. "The U.S. market is absolutely exploding."

Utimaco is one of a host of companies showcasing data security and management tools at the RSA Security Conference this week. The company's flagship product, SafeGuard Easy, is a disk encryption tool that protects data on desktop and mobile devices.

"It is for data at rest," LaPorte said. "Once it has been decrypted and is being used, it's out of our purview."

For data in use, Digital Guardian from Verdasys Inc. of Waltham, Mass., monitors system calls that have data components.

"We do data security at the point of use," said Verdasys CEO Seth Birnbaum. New Technology such as finger-sized USB drives with multigigabyte storage makes it imperative to keep track of how data is being used. "You can take everything out of an enterprise through a desktop."

For sensitive data on the move, Beachhead Solutions Inc. of Santa Clara, Calif., offers the nuclear option. Lost Data Destruction is a software agent that wipes data from mobile devices that have been lost or stolen. The need to make sensitive intelligence both readily available and secure from misuses was the driver for creating LDD, said vice president of marketing Jeff Rubin. "You can't keep it all on one server at Langley today," Rubin said. "You have to have access to it."

The shrinking security perimeter has been a trend for several years, with more security moving inside the network. But the process is speeding up because of government regulations that make custodians of information accountable for it. The Federal Information Security Management Act and California's privacy disclosure law essentially require administrators to be able to protect data and to document the safeguards.

"Now it's no longer an option," Birnbaum said.

Utimaco's SafeGuard Easy uses the Advanced Encryption Standard with 128- or 256-bit keys to encrypt

Sponsored By

An advertisement for Ciena. On the right side, a man in a dark suit and tie stands with his arms crossed. On the left, the text reads: "More Bandwidth for less?" in red, followed by "We bet you can save at least 15%." in black. Below this is an orange button with the text "TAKE ASSESSMENT NOW" in white. At the bottom left, the "ciena." logo is displayed in red. The background features a faint grid pattern.

either entire disks or disk sectors, rather than files.

"It encrypts any form of portable memory device you can think of," LaPorte said, including notebook PCs, removable disks and USB drivers.

The first encryption of the entire disk with a 256-bit key can take as long as 90 minutes, LaPorte said. "It's a one-time process, though," he said. After that, it becomes transparent to the user calling up data. "As a user, you don't see it. It's always on."

Similar disk encryption tools introduced several years ago failed because they required a five-to-eight-minute cycle at startup and shutdown of a machine.

Access to the encrypted data can be controlled with passwords, tokens, smart cards and digital certificates for multifactor authentication.

The product is running on several thousand individual devices in the U.S. military, the Federal Reserve and the FBI, LaPorte said. But it has not yet been deployed agencywide. "They don't make it easy," LaPorte said of government adoption. "It can take years to do business with the feds."

Digital Guardian from Verdasys consists of a central management console and client agents that sit on PCs or servers to monitor data use. Policies pushed out from the console can control how data is used, based on file type, storage location, users, location on network or other factors. Files can be blocked, users can be warned about improper use and administrators can be alerted of problems.

"Because we intercept the system calls, we have all the controls you want," said chief scientist Dan Geer. "We do not do content inspection. All of this is about how data moves." Simply opening a document can produce from 200 to 2,000 system calls. This data must be reduced to "user X opened document Y." Beachheads Lost Data Destruction is intended to protect high-value data that is not irreplaceable. "The whole point is to avoid compromise or misuses of the data, not to protect the device," Rubin said.

A small agent sits on the client and checks in regularly with the management console when online. Under specified conditions, such as a theft report logged on the console, a number of consecutive unsuccessful log-in attempts, or too long an interval between network sign-ons, the agent can wipe out the data.

Beachhead offers LDD either as a stand-alone product or as a managed service with an annual subscription. The cost for the service is about \$129 per user per year.

The Lenovo logo is displayed in white lowercase letters on a black background.

Lenovo PCs come with built-in security features.

© 1996-2008 1105 Media, Inc. All Rights Reserved.