

DATA MATION™

Verdasys Digital Guardian: Policy-Based Enterprise Security

February 19, 2008

By James Maguire

As Broadcom CIO Ken Venner tells it, several years back his company urgently needed an enterprise-wide security solution. The company, a global leader in semiconductors, had suffered some serious data leaks – from its own employees.

Trusted staffers had taken key intellectual property with them when they left the company. It's every CIO's worst nightmare: to spend vast energy protecting against external threats, only to face a deep threat from within.

"The people you fear the most are the people you trust the most," Venner tells me.

Action was required. To take full control of dataflow, Venner needed a rock-solid security solution that addressed both internal and external threats. The solution, he explains, had to "be able to track, manage, understand, report, do post-analysis and trending, [monitoring] what is IP, where is IP going, who's had IP, and does anyone go after, take, or steal IP?"

Furthermore, given that many employees work on laptops, the solution had to be geared for the individual rather than the data. Upping the challenge, in a single day a sensitive document might visit a half-dozen digital mediums. What solution could supervise all these transactions?

Venner chose Digital Guardian, by Verdasys. The security solution recently won a Datamation Product of the Year Award in the Enterprise Security category. (The other nominees were Code Green Networks, Data Domain DD580 Appliance, Kazeon Information Server IS1200-ECS, Bluesocket v6.1 software platform, and nuBridges Secure Transaction Manager.)

The Digital Guardian platform touts itself as a veritable octopus of data control. It handles file and mail encryption, content inspection, context management, application logging and masking, and other sensitive tasks.

Once Venner began using Digital Guardian's monitoring and control capabilities, security at Broadcom improved. "I could actually control what was IP, how it was flowing, who could do what with it, could you copy and paste, could you transfer, could you email it, those kinds of activities."

Adaptive Encryption

Broadcom recently upgraded to the Digital Guardian 5.0 platform; this platform's adaptive encryption capability is of particular interest to Venner. (Adaptive encryption encrypts and decrypts files selectively and automatically based on data context, rather than using a "one size fits all" approach.)

Venner explains the value of adaptive encryption: "By default our policy is if you copy a file to an external USB drive, we will encrypt it

so that only other Broadcom PCs can read it, unless we capture information around why you're passing it in an unencrypted fashion."

"We're also thinking of using adaptive encryption to control certain files that are tagged appropriately, so that they're always stored on your laptop or desktop, raw in an encrypted format. Every time that document flows, it flows as an encrypted object, never becoming unencrypted in an unprotected space. Even though we're implementing disk encryption technology, this would be even a layer on top of that for IP protection."

This heavy-duty encryption method would protect data that Venner calls the "crown jewels of the organization," information so sensitive that only a tiny cadre should be viewing it.

"And if anyone was to steal their device, you hope [the employee] started an encrypted directory on the machine so they couldn't get to it. But even if they could hack the encrypted directory, it has a second layer of encryption to ensure that they could never get to the file."

Security Policy Implementation Engine

The rationale behind the development of Digital Guardian, says Verdasys president Nick Stamos, is that companies need a centralized encryption platform that implements company policies. So the DG solution is not DRM-based (because DRM methods are proprietary, so if the provider goes out of business it's a problem). And it's not disc based (because if someone steals your machine, the default mode is decrypt).

Instead, Digital Guardian is what Stamos calls a "security policy implementation engine."

"With DG, before it actually decrypts the file, it takes into account: what's the document classification? And, based on who you are, what are you allowed to do or not do with that particular document?"

The focus is on a comprehensive solution that handles every data transfer scenario. And significantly, DG doesn't require end users to be aware of what's going on in the background.

"Once you have one system that both provides the protection and the information policy enforcement, it's much easier to now manage a large company...because it's all centralized, it's all one policy," Stamos says. "There's no longer a need to make clearance decisions on an individual basis."



DATAMATION
PRODUCT OF THE YEAR™

VERDASYS™

GLOBAL DATA SECURITY SOLUTIONS

www.verdasys.com