

Sponsored by:

get **IT** here ►►► download a **FREE** whitepaper

NETWORKWORLD

This story appeared on Network World at <http://www.networkworld.com/research/2008/010708-data-leak-prevention-watch.html>

Five data leak prevention companies to watch

Not all the data-leak start-ups have been snapped up by the big guys. Here are five data-leak-prevention companies to keep an eye on.

Feature By Network World Staff, Network World, 01/07/08

1. [Code Green Networks](#)

Sponsored by:

When founded: October 2004

Headquarters: Santa Clara

CEO and background: CEO Sreekanth Ravi co-founded Code Green Networks in 2004 with Sudhakar Ravi, the company’s CTO. Previously, the two co-founded SonicWall, where Sreekanth Ravi served as chairman and CEO and Sudhakar as CTO and vice president of engineering.

Funding: In three funding rounds, the company has secured \$32 million from Bay Partners, Sierra Ventures, and the company’s founders.

What does the company offer? DLP appliances designed to protect customer information and safeguard intellectual property.

Why is it worth watching? The company recently released a modestly priced appliance targeted at small-to-midsize businesses (SMB) and branch offices. In contrast, most vendors focus on large enterprises, giving Code Green a solid niche in which to establish itself.

Two key features in the DLP space are data-in-motion (or network) monitoring and data-at-rest discovery. Code Green does not currently offer data-at-rest discovery, a feature it will need to add as Code Green moves upstream to target large enterprises.

Sreekanth and Sudhakar Ravi have a solid track record in the SMB market based on their previous experience at SonicWall, and this experience has translated into features, such as a wizard-driven setup and pre-packaged policy templates, that are tailored to organizations that don’t have in-house security experts.

How did the company get its name? Code Green Networks was named after the Homeland Security Threat Index. A “code green” indicates the lowest threat level.

Who’s using the product? Customers include Signal Financial Federal Credit Union, SonicWall, and Sourcefire

Make the **most** of your IT investments.

Get real-world tips from industry experts on how to get the most value from your IT assets.

CLICK HERE

2. [Proofpoint](#)

Founded: June 2002

Location: Sunnyvale, Calif.

CEO and background: Gary Steele previously served as CEO of Portera, a venture capital-backed [applications](#) company that targeted the professional services industry. Prior to Portera, Steele served as vice president and general manager of the Middleware and Data Warehousing Product Group at Sybase.

Funding: \$58 million from Benchmark Capital; Bridgescale Partners; Inventures Group; JAFCO Ventures; Meritech Capital Partners; Mohr, Davidow Ventures; and RRE Ventures.

What does the company offers? E-mail security and DLP solutions.

Why is it worth watching? Proofpoint has an impressive pedigree, founded by Eric Hahn, the former CTO of Netscape. The company's DLP strategy emerged from its original focus on e-mail security. Proofpoint's strength is monitoring and enforcing messaging policies, protecting users from both inbound and outbound messaging threats.

A lack of data-at-rest discovery features may be an issue for some potential customers. However, with e-mail still being the biggest threat and the most likely conduit for data theft, a DLP strategy that relies on messaging security as the foundation makes sense.

Where did the company get its name? Proofpoint is intended to communicate the company's focus on statistical analysis techniques, as with a mathematical "proof," while "point" references the fact that the solution provides a single "point" of administration, analysis and policy application.

Who's using the product? Proofpoint claims more than 1,300 customers worldwide, including Bank of America, DeKalb Medical Center, Hertz, Hitachi Data Systems, Kaiser-Permanente, Mary Kay, NTT Communications, Outback Steakhouse, Pitney Bowes and T-Mobile.

3. [Reconnex](#)

Founded: October, 2003

Location: Mountain View, Calif.

CEO and background: John Peters was previously the CEO of several venture capital-backed companies, including Yipes, Netli, and Sigma Concentric.

Funding: \$37 million from NorWest Ventures, August Capital, Levensolhn Partners and Outlook Ventures.

What does the company offer? DLP appliances that combine network data monitoring and data-at-rest discovery features into one platform, while also providing features for controlling portable media and storage ports.

Why is it worth watching? Most DLP solutions do a good job of protecting fixed-format data such as Social Security and credit card numbers. Guarding unstructured data, on the other hand, is a more difficult proposition. Much intellectual property, such as source code, has no fixed format and requires more sophisticated search techniques.

Reconnex relies on indexed searches, which "enable organizations to automatically mine data and define group associations." Indexed searches allow organizations to find sensitive data via keywords, communication parameters, content types or other customer-defined concepts.

Where did the company get its name? Reconnex is a combination of the words "reconnaissance" and "exposure," highlighting the importance of having network visibility in order to control the flow of sensitive data.

Who's using it? The company claims more than 45 Fortune 1000 customers, including WebEx, Sirva, Medstar Health, BCD Travel and George Washington University.

4. [Vericept](#)

Founded: 1999

Location: Waltham, Mass., and Denver

CEO and background: Dave Parkinson was most recently with Sigma Partners, where he was executive-in-residence. Prior to that, he was president and CEO of Books24X7, an e-learning company, and he was director, partner and CFO of Boston Consulting Group.

Funding: \$52 million from Sequel Partners, Sigma Partners, William Blair Capital Partners, Visa International and Globespan Capital Partners.

What does the company offer? DLP solutions that discover and analyze stored data, while also analyzing all Internet-based communication and attachments, including e-mail, instant messaging, peer-to-peer file sharing, chat rooms, blogs, Web postings, FTP and Telnet.

Why is it worth watching? Vericept was one of the earliest entrants into the DLP space. The combination of data discovery and content analysis positions it well for large enterprises.

Vericept has a programmable content detection and analysis engine that adapts to an organization's specific content requirements, which is critical for detecting unstructured data such as IP. The analysis engine can also look for patterns or broader concepts that may be markers of sensitive data, rather than simply searching for specific data matches.

Where did the company get its name? The name Vericept is intended to indicate that the company's products intercept information, perform content analysis, and verify that what is confidential stays that way.

Who's using it? 750 organizations worldwide, including Walgreen, Anadarko Petroleum, Inova Health System, LifeSpan and Baker Hughes.

5. [Verdasys](#)

Founded: 2003

Headquarters: Waltham, Mass.

CEO and background: Seth Birnbaum previously co-founded NeoGenesis Pharmaceuticals, a privately held biotechnology company, and served as its vice president of engineering.

Funding: Verdasys has not sought venture capital backing, with funding instead coming from company officers and private investors. According to Verdasys, the company is profitable and able to reinvest based on current sales.

What does the company offer? Data security platforms that protect against data loss through integrated file encryption, e-mail encryption, data discovery, forensic reporting, offline data protection and network access control.

Why is it worth watching? Verdasys takes an endpoint-based approach to the data-loss problem. Agents reside mainly on desktops and laptops, but in the more recent versions of the product, Digital Guardian, they can also protect applications and [servers](#).

Verdasys argues that its end-point based focus has advantages over network-based control, which has its roots in the old [firewall](#), 'you're-in-or-you're-out' approach to security. An endpoint approach, in contrast, shifts the focus to where information is actually created, altered and moved – desktops, laptops and other end devices.

Verdasys Digital Guardian discovers, classifies and monitors data use on endpoints, preventing misuse by alerting users to policy violations or blocking high-risk activities while also creating audit trails and triggering alarms when necessary.

Where did the company get its name? Tomas Revesz, executive vice president of customer service, prevented a data-loss incident at NeoGenesis Pharmaceuticals, so when the time came to name the new DLP start-up, the founders gave the job to him. A native of Mexico City, Revesz wanted a name that meant “truth in systems,” so he blended the Spanish word Verdad, which translates to “truth,” with “systems” and arrived at Verdasys.

Who’s using it? Verdasys has more than 100 customers, including Cigna, Humana, Convergys, Broadcom, DuPont, Genzyme, OKI Electronics, Tomin Bank and TD Ameritrade.

All contents copyright 1995-2008 Network World, Inc. <http://www.networkworld.com>