

Fidelis announces XPS 5.2 with scanning within local network, and a granted US patent

Analysts: Nick Selby, Lauren Eckenroth
Sector: Enterprise Software

Anti-data-leakage vendor **Fidelis Security Systems** has announced several new developments to its business and product line. It has been granted US patent number 7,467,202, for its 'high-performance network content analysis' system, and launched Fidelis Extrusion Prevention System (XPS) 5.2. New to this dot-release is the Fidelis XPS Internal sensor for discovery of data moving within the network – not just as it tries to leave.

The 451 Take

We don't aver a patent makes a product successful (see US patent number 6,368,227) or even that it makes a product necessarily work (7,062,320) – though it does make the case that a technology is unique and useful. Fidelis' patent is noteworthy because it addresses its core claims as a company – specifically, that it seeks to prevent unintentional dissemination of data at gigabit speed without being limited to port. The strength of the patent is in its very breadth (it's also, shockingly, a good read), and at the least gives Fidelis concrete IP to sell in addition to its partnerships and reputation. Monitoring the flow of data inside the network as well as on the gateway is something we have been harping on for quite some time. It strikes us as far more valuable to see a sensitive piece of data moving within your LAN than to get a notice that an email that just left to the public Internet contained valuable information.

Context

Bethesda, Maryland-based Fidelis Security Systems was founded in 2002. The company raised in March 2005 a \$6.8m series A funding round from **Ascent Venture Partners**, **Inflection Point Ventures**, **Maryland Department of Business and Economic Development**, and **WS Investment Company**. Its \$22m series B round closed in April 2008 from **Tudor Investment Corp**, **Inflection Point Ventures**, **Point Judith Capital Partners** and **Maryland Venture Fund**. Fidelis has about 50 employees and sells about 50% through its channel.

Fidelis has asked us not to mention its current customer numbers, but it is up from 21 in May 2008. Included in the new customer list is the city of Washington DC. It claims an average deal size of around \$335,000, with deals ranging from \$35,000 to \$2.3m.

Products

Fidelis claims that XPS protects all ports and channels, providing visibility to data as it flows within and outside of the network. The system is sold as appliances with five sensors sitting on the network. The XPS Direct sensor is deployed at the gateway to monitor outbound traffic; the Internal sensor seeks to discover and classify in-network traffic. Fidelis says that it works to integrate with existing business processes to monitor data flow within an organization. This is the kind of activity that we had said in our summer 2008 long-form report, Mind the Data Gap, would be an important trend.

Fidelis also offers the XPS Mail sensor, for SMTP and email traffic; the Proxy sensor for communicating via ICAP to Web proxy servers; and the Scout sensor for auditing network traffic.

As the central management console for the XPS sensors, policy and alert management, sensor configuration, and reporting capabilities are rolled into Fidelis' XPS CommandPost.

Technology

While we don't want go too in depth in covering all of Fidelis' technology (we've already done that [here](#)), there is something to be said about this patent and its implications to the anti-data-leakage market. The patent covers Fidelis' method of sending data streams through proprietary decoders (most ADL vendors license theirs from either **Oracle** Outside In or **Verity**), stripping off application wrappers and then analyzing the raw data using keyword scanning and digital fingerprinting. The data is then filtered into separate multi-dimensional content profiles. Each profile may have policies around it; for example, traffic can be shut down, or files can be quarantined if Fidelis' scanners, packet sniffers, TCP session trackers, etc., catch something amiss.

Now, other than the proprietary protocol decoders: If sniffing for traffic, cracking open documents, hashing the text, creating overlapping hashes of text within and storing this as a profile sounds like the way almost everyone does data leakage, that's because it is. We don't think that Fidelis is a lawsuit shop; in fact, the customers we know of show us that Fidelis is in the business of selling boxes rather than concerning itself with capitalizing on a patent by suing everyone in sight. But the patent may make others somewhat uncomfortable – even if competitor X does do things substantively differently, we wouldn't want to have to pick up the legal tab to explain exactly how.

Strategy

The world of data-leakage prevention (which comprises anti-data-leakage, disk encryption, port and device control and database transaction monitoring) is rapidly converging. We have already seen the integration of data loss prevention (DLP) technologies as another layer of enterprise security in the way **McAfee**, **Symantec**, **Sophos** and **Trend Micro** are bundling DLP with antivirus suites (see their acquisitions,

respectively, of **Onigma, Reconnex and SafeBoot; Vontu; Utimaco Safeware; and Provilla**). What we are beginning to see, in the **EMC/Microsoft** and **McAfee/Liquid Machines** partnerships, are higher-level integrations of DLP with information rights management.

We have been talking about the confluence of anti-data-leakage, rights management and identity and access management for the past few years. The Fidelis XPS Internal sensor has the potential to serve as a bridge between DLP and identity and access management, and DLP and policy framework.

We think Fidelis' is among the most sophisticated network-based approaches to the problem of internal data movement, and while we won't get into an agent-versus-network debate, we think it's by any measure faster and less costly to deploy ADL on the network (OK, a well-functioning, well-maintained agent is theoretically more efficacious because it would be able to see documents before they are encrypted and stop them from being transmitted in the first place – but as we've said many times, building an ADL agent for a Windows machine is easy. Building one that doesn't hork up the works and blue-screen everything is really, really hard).

In the future, we see the market moving toward further consolidation of basic data-leakage technology that can be sold with anti-malware suites. The well-financed companies with strong technology will look to add specific value for their customers in more specialized deals. **CA Inc's** acquisition of **Orchestria** is almost exactly this, pulling together agent- and network-based approaches to ADL and eventually tying it to identity and access management (IAM). **IBM** may be in the market for an acquisition as well, considering its close partnership with **Verdasys** and Verdasys' partnership with Fidelis, inked in May last year.

Competition

Fidelis competes with anti-data-leakage vendors **CA Inc (iLumen and Orchestria), Chronicle Solutions, Code Green Networks, EMC (Tablus), GTB Technologies, McAfee (Reconnex and Onigma), Raytheon Oakley Networks, Websense (PortAuthority Technologies), Trend Micro (Provilla), Symantec (Vontu), Sophos (Utimaco, which licenses ADL from Trend Micro's Provilla), Varonis Systems, Verdasys, Vericept** and others. Data encryption vendors include **BitArmor, Bluefire Security Technologies, Check Point Software Technologies (Pointsec), Credant Technologies, GuardianEdge, WinMagic, McAfee (SafeBoot), Sophos (Utimaco) and PGP Corp.**

Port and device control comes from **Check Point, RedCannon Security, Safend, GuardianEdge, WinMagic, Credant, PGP** and others. Database transaction monitoring comes from **Sentriigo, Guardium, Imperva, Secerno and Application Security Inc.**

SWOT analysis

Strengths

Fidelis tells a good technical tale, and its price point in terms of what you get for what you spend is quite compelling. The patent will at the very least help its trade sale valuation, when one comes.

Weaknesses

Fidelis fights the perception that it's wildly expensive; whether this is true is irrelevant, the fact is that a significant portion of the Fidelis sales conversation regards its price versus its competition's.

Opportunities

With the internal passive classification capability now fully launched, Fidelis opens partnership possibilities with IAM and DRM vendors, and those in turn could lay groundwork for an eventual trade sale.

Threats

Symantec's Vontu has solidified a commanding lead in the space as the name to beat – and Vontu customers tell us they are happier than ever with the product. McAfee, Sophos, Trend, Microsoft and CA – and others – will join this fight soon, and Fidelis will be competing against increasingly huge names.

About The 451 Group

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company's analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com