

McAfee Acquires Sentrigo

McAfee has acquired privately owned Sentrigo.

1. Who is Sentrigo?

Sentrigo is a leading provider of database security, monitoring and intrusion prevention solutions. Sentrigo offers a complete suite of database security technologies including vulnerability management, real-time change monitoring, database activity monitoring, database audit, and virtual patching – ensuring databases are protected without impacting performance or availability. McAfee has had a partnership with Sentrigo through our Security Innovation Alliance (SIA) program and in 2010 entered into a successful OEM relationship with Sentrigo enabling us to offer our current McAfee Vulnerability Manager for Databases, McAfee Database Activity Monitoring, and McAfee Integrity Monitoring for Databases.

By implementing Sentrigo solutions, companies stop database attacks, ensure compliance audit and reporting, minimize the risk of a data breach of Personally Identifiable Information (PII) or other sensitive information, and reduce the costs associated with breach notification.

Sentrigo's software was designed from the start to monitor database activity from the inside out. By monitoring memory on the actual database servers, the Sentrigo architecture with its autonomous sensors and centralized management is the basis of a database security implementation that:

- Best meets compliance requirements, by protecting databases from ALL threats (including 0-day threats) in ALL of its vectors:
 - Network-based, host-based, and intra-database attacks
- Is faster to deploy and more efficient, saving customers money
- Identifies attacks as they occur – and acts on them – reducing risk and liability
- Fits today's IT infrastructure, working seamlessly in virtualization and cloud environments

Sentrigo:

- Was founded in 2006 and has 41 employees
- Is headquartered out of Santa Clara, with a Sales office in Boston, and an R&D center in Israel
- Currently serves 160+ enterprise customers
- Has well over 100 channel partners around the globe
- Installation and configuration is so intuitive that most sales start with a free trial download.
- Has a distributed architecture that fits well in cloud and virtualization environments. Sentrigo products are available as images for Amazon EC2 and GoGrid, and have been installed as part of MSSP implementations, for example with Swisscom.

2. Why did McAfee acquire Sentrigo?

According to research from Verizon, more than 92 percent of records breached involved a database, with more than 87 percent based on exploits requiring significant technical skills. These are exactly the threats that Sentrigo solutions are aimed at preventing.

An increase in the number of severe data breaches coupled with additional regulatory pressure is forcing an urgent and immediate expansion of the database security market, including database activity monitoring (DAM) and database vulnerability management (DVM). This is a large and rapidly growing opportunity that is still primarily a green field (i.e. companies have no solution deployed). According to Forrester the Database Security market is growing at a 20% compound annual growth rate (CAGR) and estimated to reach \$612 million by 2012.

After evaluating other players in this market, McAfee recognized that Sentrigo has the best technology, best go-to-market approach, and strongest team to bring into McAfee. McAfee has sold Sentrigo solutions under an OEM agreement for six months so we are already familiar with the market opportunity, technology, how to sell it, and who to target. The Sentrigo solution is complementary to what McAfee already sells and fits perfectly into our Security Connected approach (<http://www.mcafee.com/securityconnected>)

We believe Sentrigo has the DNA to become the market leader for cloud security of databases. The Sentrigo architecture is unique in the database security market, utilizing autonomous sensors that can be deployed locally wherever cloud systems are provisioned. Other solutions are highly dependent on network topology.

The acquisition is expected to help McAfee:

- Establish itself as the market leader in Database Security
- Deliver best-of-breed solutions in vulnerability management of databases, protection of databases, and activity monitoring of databases.
- Provide worldwide database solutions to all markets McAfee serves and in all the languages into which ePolicy Orchestrator (ePO) is localized.
- Continue to broaden our security portfolio to now secure databases, in addition to endpoints, networks, email, web and the cloud—reinforcing our position as the largest dedicated security company in the world.
- Leverage security expertise and customer experience to deliver more comprehensive solutions to customers and hence more value.
- Combine the skills and resources of both companies to develop and deliver world class, scalable security solutions for databases, applications, endpoints and networks.

3. What products does Sentrigo currently offer?

Hedgehog Enterprise is the flagship Database Activity Monitoring solution, optimal for organizations that require breach prevention, end-user identification, virtual patching, integration with existing security infrastructure, IT governance and operate with enterprise-wide database deployment.

Hedgehog DBscanner is Sentrigo's enterprise-class Vulnerability Assessment solution for databases. DBscanner evaluates risk from virtually all known threat vectors, providing information that can then be used to demonstrate compliance for audit purposes, and to improve security overall for an organization's most valuable data.

Hedgehog vPatch is a subscription-based offering that augments the protection offered by Hedgehog Enterprise with continuous virtual patches from Sentrigo's "Red Team" to detect and prevent attempted exploits of DBMS vulnerabilities, including newly discovered vulnerabilities not yet covered by vendor patches.

Repscan is a vulnerability assessment and security scanning tool designed primarily for auditors and pen testers, with comprehensive coverage of Oracle, Microsoft SQL Server (including SQL Azure), IBM DB2, MySQL, PostgreSQL, and Sybase Databases.

4. How are the Sentrigo products being packaged and sold within McAfee?

McAfee has been selling Sentrigo's software through an OEM agreement and the following three offerings have been on the McAfee Price List since August 2010:

- **McAfee Vulnerability Manager for Databases**
 - Based on Sentrigo Hedgehog DBscanner, this solution scans databases for more than 3000 vulnerabilities and provides customers with comprehensive reporting and an enterprise-wide view.
- **McAfee Database Activity Monitoring**
 - An integrated solution consisting of Sentrigo Hedgehog Enterprise plus Sentrigo Hedgehog vPatch. It tracks database changes so that customers can better manage risk and regulation compliance **plus** protects customers from attacks with virtual patching, which prevents vulnerabilities from being exploited.
- **McAfee Integrity Monitoring for Databases**
 - A simplified version of Sentrigo Hedgehog Enterprise, with some basic checks from DBscanner, this solution tracks database changes so that customers can better manage risk and comply with regulations, but doesn't offer all the policy and reporting customization that Sentrigo Hedgehog offered. This is

a slimmed down version of the offering for cost-conscious prospects and cost-competitive situations.

5. What languages do Sentrigo's products currently support and what are the localization plans?

Sentrigo's products, management interfaces and documentation are available in English today and while internationalized, they have not yet been localized into other languages. However, it is important to note that they can be used with databases that contain content in any language.

McAfee plans to localize Sentrigo's products into the same languages supported by McAfee ePolicy Orchestrator (ePO). A full roadmap of this localization plan will be available later in 2011.

6. What database and operating systems do the Sentrigo products (and associated McAfee Products) currently support:

Sentrigo Product	Platforms Supported	
Hedgehog Enterprise Management Server	Windows 2003 or later, Sun Solaris 7 or newer, or any Linux version	
Hedgehog Enterprise Sensor	Databases: Oracle 8.1.7 or newer, Microsoft SQL Server 2000/2005/2008, Sybase ASE 12.5 or 15.0	Operating Systems: Microsoft Windows 2000 or newer, Sun Solaris 7 or newer, IBM AIX 5.2 or newer, HP-UX 11.11 or newer (11.23 or newer on IA64), Red Hat Enterprise Linux (RHEL), SUSE Linux, or other Linux versions (supported but require manual installation)
Hedgehog DBscanner	Databases: Oracle 8.1.7 or newer, Microsoft SQL Server 2000/2005/2008, MySQL v4.0 or newer, DB2 for LUW v8.1 or newer, Sybase ASE 12.5 or 15.0	
Hedgehog vPatch	Any supported by Hedgehog Enterprise	Any supported by Hedgehog Enterprise

7. How does Sentrigo complement the existing McAfee product portfolio?

As part of our Database Security solution that includes products from all business units, the Sentrigo Vulnerability Assessment solution is the starting point – to be able to diagnose and assess the database environment so that McAfee can propose the optimum security solution for a customer's database infrastructure – from network to server to data.

As part of the McAfee Risk & Compliance Business Unit, Sentrigo's solutions and McAfee's vulnerability management solutions will include everything from operating systems, networks, web applications and databases. Likewise our change monitoring solutions now include operating system configurations, networks and databases. With Sentrigo's Database Audit and Database Activity Monitoring solutions, we can now offer complete visibility into all transactions, including privileged users, a requirement of many compliance regulations. Finally, Sentrigo's Virtual Patching capability is an excellent extension to McAfee's existing patch management solutions, providing a strong level of protection for database systems that cannot be patched in a timely manner.

Sentrigo's software-only approach was architected to be fully distributed, enabling solutions for both physical and virtual platforms as well as the cloud – making it a perfect fit for McAfee's strategy.

Because Sentrigo products were already integrated and certified as part of the SIA program and OEM partnership, McAfee's ePO can already report on Database Activity Monitoring, Vulnerability Management of Databases, and Integrity Monitoring of Databases. The integrated products are already deployed in several McAfee accounts. And our roadmap for Sentrigo products includes full management integration with ePO.

8. How does this acquisition and McAfee's database security announcement tie to McAfee's overall server security strategy?

Database security is a key element of McAfee's overall strategy to secure data centers including servers. Organizations are placing more data than ever in their databases and moving to next generation data centers that rely on fewer but far more powerful servers. To meet the needs of server security, McAfee has a complete portfolio of products including McAfee Total Protection for Server and McAfee Management for Optimized Virtualized Environments (MOVE) to ensure server uptime and protection against advanced persistent threats.

9. How does this acquisition benefit customers?

The integration of Sentrigo with McAfee provides customers with the highest level of security across their database environments and allows companies to rapidly deploy a database security strategy in a cost effective manner.

Sentriigo customers:

Sentriigo customers benefit from the following:

- Access to a wide range of comprehensive security solutions and resources from the world's largest, dedicated global security company, including:
 - McAfee Labs research, reports, and software technologies
 - McAfee's award-winning, global technical support
- Continued support and protection of existing investments in Sentriigo solutions
- Localization of Sentriigo products and content
- Further integration of Sentriigo products with McAfee solutions, including McAfee ePO.

McAfee customers:

McAfee customers will now have access to a robust database security management solution. Adding Sentriigo products enables McAfee to provide the following benefits to customers:

- Comprehensive security including:
 - Vulnerability management solutions extending to include everything from operating systems to networks, web applications and databases.
 - Change monitoring solutions expand to include operating system configurations, networks and now databases.
- New solutions and bundles with additional McAfee products providing broader protection to address their complete information security needs.

The integration with McAfee ePO allows existing ePO customers to deploy an enterprise-class database security solution as part of their established security framework with no additional management consoles.

10. What does this acquisition mean to channel partners?

Through McAfee's existing OEM relationship with Sentriigo we are able to offer McAfee Vulnerability Manager for Databases, McAfee Database Activity Monitoring, and McAfee Integrity Monitoring for Databases. These solutions are already available to accredited partners with the Risk & Compliance solution competency via the McAfee Security Alliance program.

Sentriigo channel partners who are not yet McAfee partners may wish to join the McAfee Security Alliance Program – either remaining focused on Risk and Compliance solutions or representing the broader McAfee product portfolio. Additional details and timelines for how Sentriigo partners can join McAfee's partner program will be communicated by the end of April 2011.

For more information about McAfee Database Security and Sentriigo, visit www.mcafee.com/dbsecurity and www.mcafee.com/sentriigo.