



Rajesh Parthasarathy

## Company Spotlight: By Jayakishore Bayadi



# MENTIS Software

## Answering the What, Where, How, & Who of Sensitive Data

When a major American public company decided to do more to protect the personally identifiable information (PII – name, address, Social Security number & driver’s license number) of its customers, their Head of Financial and HR Systems turned to MENTIS Software.

The executive described the problem: “We hear about data breaches every day. Not wanting to be a negative headline is an obvious motivator, but doing what’s right to protect the information of our customers and employees is our driving force. To adequately protect this information, we first needed a comprehensive map of all of the locations of PII data across all our enterprise databases. We looked to MENTIS because this critical capability was built into their Framework, which is shared by all their solutions.”

The company used MENTIS’ data classification capability to first document WHAT was sensitive to its organization. Next, they deployed the MENTIS data crawling and pattern recognition software to scan their databases to determine WHERE sensitive data was located across their databases. “MENTIS was able to document known locations of sensitive data as well as unknown locations – where sensitive data had been propagated through internal processes or through the efforts of tenacious application users – locations that our existing documentation

had missed,” the executive explained.

Such experiences are common among MENTIS’ customers. The firm, which provides information security solutions for databases and applications, was founded in 2002 by Rajesh Parthasarathy. As a Chartered Accountant turned technologist, his skills include an ability to see the vulnerabilities in the information technology stack, often far in advance of current security trends. Parthasarathy and the MENTIS team have built a culture of innovation and thought leadership, which enables them to remain on the cutting edge of information security. “We keep coming back to one idea: that you have to know your risk, understand your exposure,” said Parthasarathy. “And we’re finding that sensitive data is literally everywhere in an organization’s systems.”

“Sensitive Data Creep,” Parthasarathy continued, “is what we call a phenomenon where sensitive data in databases is propagated into unknown and unexpected locations. In addition to the known fields and columns where PII is expected to be stored, we’re seeing that in fact very often it is also stored in description columns, attribute fields, log and debugging messages, etc. – areas that are intuitively not critical in the lay person’s eyes. Think of it as a behind-the-scenes movement and

storage of data as a result of everyday use.”

PII can be stored in hidden tables thrown off by a common application process, through developers’ test tables, or even by software code written before the more stringent era of breach notification laws. “And sometimes we find that tenacious users have created tables with bits of PII in order to expedite a process that tends to be repeated quite often.” Given the very nature of the relational database, these locations, and the sensitive data within them, can multiply geometrically, undermining even the best security programs. Over the last several months, MENTIS has been evangelizing the need for sensitive data discovery as a necessary first step to any data protection strategy.

### HOW is my sensitive data utilized?

The next challenge facing MENTIS’ customer was to determine how to protect the various tables and columns where sensitive data was located. “Once we knew where the information was, we had to take steps to protect it. However, without knowing how the data got to the location, or whether an application was using that location, we wouldn’t have been able to proceed,” the IT executive told us. “What is really powerful about MENTIS’ solu-

tions is that all of their products are built on a common platform and can share intelligence. So it was an easy matter for MENTIS’ iCatalog (which automates source code review) to determine the various ways in which each location was utilized within our applications.”

### WHO has access?

“With this customer, our solutions were able to identify WHAT data is sensitive to his organization, WHERE it is used, and HOW it is being used. The next step was to review WHO has access to sensitive information. Since this customer has several applications and databases, understanding who has access to sensitive information can only be answered if we look at enterprise users and their ability to access information from more than one application or database. For example, User A could get access to Name and Address in Application 1, Name and Social Security Number in Application 2 and Name and Driver’s license number from Database 3 – all the elements of PII from not one source, but collectively. Traditional user access reviews focus on one application at a time, but using MENTIS iAudit and iDocument, our customer can document enterprise users and their accesses across all enterprise applications and databases,” says Parthasarathy.

“This level of granular control and documentation is unprecedented. We would not be able to accomplish these tasks without the speed and accuracy that is provided by the MENTIS suite of products,” noted the IT Executive. “Our Security and Audit teams are heavily involved in the roll-out of the MENTIS suite to all enterprise applications and databases. Their participation in this process has helped created a culture of compliance in what is a vast organization.”

### The MENTIS Approach

Since its inception, MENTIS’ mission has been to provide solutions with a risk-based Best Practices approach. Products range from those that enable the protection of PII in Production applications (data

masking), Production databases (intrusion prevention, data masking and access monitoring) and Nonproduction databases (data masking) to those that allow for code reviews that ensure that developer code doesn’t inadvertently expose sensitive data.

In a single suite of products, customers can gather intelligence on current access rights across the enterprise and then deploy the appropriate preventive or detective solution across the application and database technology stacks. This Best Practices approach drives innovation and invention – currently MENTIS has an industry-best line-up of products that cover the entire lifecycle of PII in an organization’s database and application layers.

Yet for all their technological innovation, MENTIS understands the need for all involved groups to buy in. “Our solutions have been unique in terms of their business-driven approach, rather than a nerdy technological approach. We’ve intentionally designed our solutions for their ease of use and accessibility by stakeholders in the IT, Security, Audit, Application & Data Owners, and Compliance groups.” Enabling stakeholders to pinpoint the problems and take a giant step toward compliance within days, not weeks or months, has been a key advantage offered by MENTIS.

In fact, last year, the Gartner Group singled the firm out for notice as a “Cool Vendor in Risk & Compliance,” citing the company’s ability to keep up with evolving business objectives that are affected more by business cycles than by technology innovation. Also last year, Yale University named Parthasarathy a “Rising Star” in Corporate Governance.

### The Road Ahead

“The legislative landscape is quickly changing and there will be more laws coming up in near future pertaining to data security and protection. Organizations will look to solutions that are both

MENTIS Software at a Glance	
Founded:	2002
Headquarters:	New York
Founder:	Rajesh Parthasarathy
Investors:	Self-funded
Headcount:	18
Products:	iScramble, iMask, iMonitor, iCatalog, iProtect, iAudit, and iDocument
Website:	<a href="http://www.mentissoftware.com">www.mentissoftware.com</a>

collaborative and comprehensive. We are well ahead in this area and have a strong offering,” stated Parthasarathy.

Rather than following the conventional method of developing a product first and then marketing it, MENTIS works with its customers to understand their critical needs, and then develops innovative solutions to address them. The company profits from a highly experienced technology team with several decades of combined experience in the kind of security challenges its customers face.

“We will continue to develop solutions that are driven by customer pain points, and will stay ahead of the information security curve. Our great relationships with our customers prove an advantage for us, too, as we get tremendous feedback which enables us to continually enhance our solutions.”

The company, which is now 18 people strong, thrives even in tough times. “We are adding new customers and new partners who recognize what we bring to the table,” Parthasarathy continued. MENTIS has announced several new products over the last few months, and is expanding support for all its products across the major enterprise platforms.

“We believe that our disruptive approach – bringing out product innovation and acquiring customers and building a successful business around our way of doing things – will take us to the next level and keep us going in a difficult economic climate,” concluded Parthasarathy. 