

# THE BATTLE TO SECURE TOMORROW

Ten security innovations with the power to make a difference.

## THE FUTURE NOW

Heartland Payment Systems | IBM | Actimize  
JP Morgan Chase | SAS | Silver Tail Systems | Memento  
ThreatMetrix, Inc | 3VR Security | PhoneFactor

LIST 2009

Banks are the bread-and-butter of many security firms, and despite the theory that even in lean times security budgets survive, many small vendors are scrambling for crumbs. In a horizontal survey, 57 percent of C-level IT executives told RSA Conference that budgetary concerns were the top security challenge they'd face next year. Don't call it cutting though, the word is "optimize," which often means looking for enterprise plays.

This also means a dearth of small companies coming out with must-have security technologies. There have been a few, and we put them on this list. Instead, BTN found enterprise-scale innovation coming from large players, like IBM, SAS, and even JP Morgan Chase. And, finally, the year's biggest security invention was, to turn the phrase around, the child of necessity. **Heartland Payment Systems** takes the honor for its work to further secure its systems, and the rest of the payments chain, with end-to-end encryption.

# 01

## HEARTLAND PAYMENT SYSTEMS

CEO: Robert O. Carr | Product: E3 Encryption System | The big deal: Heartland is the first player in the payments industry to offer end-to-end | encryption for payments from the point of sale to the issuer's front door.



### ENCRYPTION

## Heartland Raises the Table Stakes

Heartland Payment System's E3, an end-to-(almost) end encryption process, has the greatest potential of any new product to impact the security of America's financial system in the coming year. And by bringing it to market just about seven months after the company announced the discovery of its massive data breach, Heartland wins kudos for reacting expeditiously to both save the company and set a standard for the rest of the industry to follow.

Heartland's security breakthrough begins at the point of sale with a new Heartland-branded tamper-resistant module that borrows security technology from the ATM world, and combines it with terminal software that's signed to prevent rogue applications from being installed. From the terminal, Heartland sends encrypted transactions on a route that results in consumer card data being continuously encrypted from the time a card is swiped until the data is delivered to the issuer's front door.

The details: When a mag-stripe card is swiped through the tamper resistant terminal, track one, two, and three data are immediately encrypted using a format preserving AES methodology provided by vendor Voltage Security. Voltage's approach, which emerged from Stanford University, has been called revolutionary for the way it not only maintains the 16-digit card number format, allowing it to integrate more seamlessly with host systems, but for the way its identity-based encryption eliminates the need to manage certificates, simplifying the typically complex problem of key management. Using AES as opposed to triple-DES was intentional, even though TDES is the standard in the ATM and debit world, "We don't feel it's strong enough," says Steven M. Elefant, Heartland's executive director of end-to-end encryption.

From the terminal, the encrypted transaction is sent to the Heartland host security module where it's decrypted then re-encrypted using the host's key, allowing Heartland to store all its transactions with a single key. The encryption process adds only about 200 milliseconds of latency on a typical dial-up transaction, Elefant says, based on the beta tests at 10 small-scale merchants.

As impressive as Heartland's encrypted payments topology is,

a problem remains: The card brands are not yet able to receive encrypted data so Heartland must decrypt everything to make the handoff to the issuers' authorization and settlement centers. The company reports to be in talks with the major card brands about accepting its encrypted data, but no agreements have been announced.

And, it's not only the card brands that have to invest to make Heartland's encryption plan work. Merchants will also have to spend several hundred dollars for new POS terminals. Heartland says its E3 terminals won't cost anymore than competing products, and that it won't charge merchants more to be a part of the secure system. "There's no added fees for doing end-to-end encryption," Elefant says. "We don't believe in that, fundamentally. We don't believe in a tax. This is something the industry desperately needs."

And for the merchants that choose not to buy new POS terminals, Heartland plans to move its entire system to what it calls "earliest point encryption," which involves encrypting the data as soon as Heartland gains control of it.

Heartland's status as the first payments processor to make the necessary investment to offer serious security to its merchants is not only good security, it's great public relations. The move should help the company successfully weather the blow of the massive data breach that exposed the data of up to 100 million consumers, and cost more than \$32 million in the six months since it happened. But the new encryption focus isn't purely a reaction to the breach, Heartland says. The company began developing the end-to-end encryption program in April 2008.

"When the big breach happened to them, Heartland had a choice of trying to paper over it with business as usual, or do what is actually necessary across the industry, which is taking much more aggressive steps to improve the security of the payments system," says George Peabody, principal analyst at Mercator Advisory Group. "That's what encryption does."

—Rebecca Sausner