

FINANCIAL IT SECURITY

December 2006

Securing Financial Enterprises from the Inside Out

THE FUTURE NOW LIST

BY REBECCA SAUSNER,
MICHAEL SISK, MICHAEL
DUMIAK AND HOLLY SRAEEL



WHEN TALKING SECURITY IN 2006—AND, REALLY, WHO WASN'T?—two movements dominated the industry: authentication and consolidation. Thanks to proactive moves by the FFIEC, authentication became priority number one last October, triggering a spending spree by financial institutions

that, Y2K aside, had many corporate officers blanching. That two-factor authentication was mandated by year-end was bad enough, but companies also had to foot the bill for rigorous compliance spending. Security, it seems, comes at a price: Institutions were expected to spend \$700 million to \$1 billion on anti-fraud technology this year, according to Fortent, an enterprise risk management technology provider.

The urgency of security in financial services is also creating new job opportunities, and prompting institutions to rethink security roles. In 2006, there were an estimated 1.5 million IT security professionals worldwide, an increase of 8.1 percent over last year. That number is expected to hit two

million by 2010. The demand for expertise can be spotted in what IDC says are the top areas for additional IT security training in the Americas: information security risk management, forensics and application development. “The traditional corporate security organization is less involved in day-to-day compliance activities; they’re not the one with the hammer anymore,” says Jon Darbyshire, CEO of Archer. “Business people have to either accept or not accept risk, and that information is being reported back up through the governance group [and] audit committee—that’s who has the hammer now.”

Some would argue otherwise. The game-changing rules dispensed by Washington had dramatic effects not only on financial institutions, but also on vendors, hastening consolidation from more than a dozen companies to a handful of credible players. Some of the largest deals of the year were EMC’s buy of RSA Security for \$2.1 billion and IBM’s purchase of ISS for \$1.3 billion. Other notables include Viisage and Identix’s biometric merger, estimated at \$770 million, and Secure-Computing’s acquisition of CipherTrust for \$273 million. No M&A discussion is complete without discussing Symantec, which bought IM Logic and Relicore this year, and has been on a buying binge since 2004, acquiring 10 companies, including Veritas for \$13.5 billion in 2005.

Consolidation has not been limited to the authentication space. Managed security service providers saw a good number of their brethren snapped up, while many point solutions were bought in the hopes of coming up with more advanced and integrated offerings to capture the imagination, and dwindling budgets, of chief information security officers—many expected to do more with less in 2007. “The security budget sometimes touched 10 percent of an organization’s overall IT spend,” says Khalid Kark, senior analyst at Forrester. “Those days are gone, and security managers now face decreasing budgets and increasing expectations from executive management.”

It is apparent that data needs security, and preferably encryption, wherever it travels. With CISOs fed up with managing too many point solutions that can’t be integrated, companies such as BT and IBM sought out Counterpane and ISS, respectively, to round out their security portfolios and provide CISOs with one-stop shopping capabilities. Smaller MSSP deals came with the merger of Lurhq and SecureWorks, and SurfControl buying BlackSpider to become one of the first content-filtering companies to offer its services any way customers want to buy them. “The days of standalone security companies are dead,” maintains Ross Brown of eEye Digital Security.

Yet budget constraints—security is pegged at nearly 8 percent of an institution’s overall IT spend in ’06—do little to sway expectations in the executive suite. And public awareness of fraud and information security threats grows stronger with every data breach and identity theft case reported. This leaves financial institutions in search of technologies and providers that will enable them to comply with state and federal data privacy and loss reporting regulations, while also meeting the stronger authentication mandate. But it also has institutions looking for technology that will extend protection beyond their perimeters—whether physical or virtual—to the laptops and data centers of vendors and their subcontractors. The long-term agenda for institutions is on identifying and implement-

ing solutions that embed rights, access privileges and authentication into the workflow processes, systems, devices and partnerships related to information management. Progressive institutions are using security as a springboard to protect and enhance the equity of their intellectual property and information firmwide.

To this end, *Financial IT Security* has compiled its “Future Now List,” the first-annual ranking of the 25 best security innovations for 2007. Of the companies chosen, one thread is consistent: the technological sophistication of the products is so significant as to dramatically improve the enterprise’s ability to secure its data and devices going forward, while changing the way businesses manage information, internally and externally. Whether it’s EMC’s acquisition of RSA, Symantec’s partnership with VeriSign, or Liquid Machine’s machinations in enterprise rights management, the critical mission of information security is in protecting and managing data—wherever it resides or is being used.

Also included in this year’s ranking are Fortify/Watchfire, Archer, CyberTrust, PortAuthority Technologies, Imperva, Trend Micro, eEye, MarkMonitor, SkyBox, 3VR, AirMagnet, PGP, Secured eMail, RedSeal, BigFix, 41st Parameter, **Secuware**, nCircle, ArcSight, AXS-One, Incard Technologies and MessageLabs.

2006

TOP RANKINGS

Javelin rates banks based on how well they protect their customers from identity theft. Overall rankings are out of 100 points. Detection scores, out of 35, indicate how easily customers can detect fraud. Prevention scores, out of 45, refer to proactive steps to prevent ID theft.

»»OVERALL

- 80 »» BANK OF AMERICA
- 79 »» JPMORGAN CHASE
- 77 »» WASHINGTON MUTUAL
- 73 »» KEYBANK
- 64 »» FIFTH THIRD BANK
- 64 »» WELLS FARGO
- 63 »» MARSHALL & IISLEY
- 61 »» SUNTRUST
- 60 »» CITIBANK

53 »» MEAN

»»DETECTION

- 35 »» JPMORGAN CHASE
- 32 »» BANK OF AMERICA
- 32 »» KEYBANK
- 23 »» CITIBANK
- 23 »» SUNTRUST
- 23 »» WACHOVIA
- 23 »» WASHINGTON MUTUAL
- 20 »» FIFTH THIRD BANK
- 20 »» PNC BANK
- 20 »» WELLS FARGO

18 »» MEAN

»»PREVENTION

- 34 »» MARSHALL & IISLEY
- 34 »» WASHINGTON MUTUAL
- 33 »» BANK OF AMERICA
- 29 »» FIFTH THIRD BANK
- 29 »» JPMORGAN CHASE
- 29 »» NAVY FCU
- 29 »» REGIONS BANK
- 29 »» WELLS FARGO
- 26 »» KEYBANK
- 26 »» NETBANK

22 »» MEAN

»»TOP IT SECURITY PRIORITIES FOR 2006*

- 50% »» MULTI-FACTOR AUTHENTICATION
- 42% »» DATA ENCRYPTION/ PROTECTION
- 42% »» INTERNAL SECURITY PERMISSIONS
- 33% »» WIRELESS SUPPORT
- 17% »» COMBATING PHISHING
- 17% »» VENDOR RISK ASSESSMENT
- 17% »» AWARENESS/EDUCATION

TWENTY

Virtualization Hits the Desktop With Secuware's Authentication Scheme

CATEGORY: NETWORK, AUTHENTICATION **CLAIM TO FAME:** SECURES THE SPANISH CIA **BENCH STRENGTH:** 500,000 EXISTING USERS



OPENING A U.S. HEADQUARTERS in October, Spain-based Secuware offers desktop virtualization as a unique approach to securing applications. The concept is in pilot testing with two Spanish banks, and essentially allows users to run a caged application on the desktop preventing any types of malware or man-in-the-middle attacks from interfering with the session. The security is ensured through a pre-boot authentication process

that precedes the startup of Windows, booting from a CD or USB and utilizing 256-bit encryption.

This type of application is part of Secuware's security framework which is used by the Spanish equivalent of the CIA to secure its internal networks. Unique in the marketplace, Secuware's product line offers features of network access control, data leak protection, network encryption and enterprise content management. (rs)

About Secuware Security Framework (SSF)

SSF extends the security of Windows networks by creating closed circuits for information in which only authorized individuals using authorized devices and authorized applications can access authorized data, preventing information leakage and delivering a more stable computing environment.

SSF returns control of the network to the enterprise by delivering:

- A secure operating system, not just access control and encryption
- Flexible architecture that enables protection to adapt as behaviors, threats, and systems evolve
- Closed circuits of information - security zones within and beyond the borders of the enterprise
- Assured compliance through the prevention of information leakage and blocking of malware
- Scalability and simplified policy deployment through tight integration with Windows and major directory services
- Enhanced internal security by separating IT and information security controls

SSF is designed to sit on top of Windows and adapt Windows' own behavior to deliver greater security. It accomplishes this through the concept of a security grid that encompasses and connects the entire enterprise and its associated ecosystems. Unauthorized changes, whether inbound - such as a malware infection - or outbound - such as information leakage, are detected instantly and the affected systems are isolated, containing infections and pinpointing the source of information leaks.

SSF delivers true multi-dimensional security that's always-on:

Security right from the start

Systems are protected from boot process onwards
Protection cannot be bypassed by low-level access tools

Closed circuits for information

Users get the access they need to do their jobs
Information is protected within defined groups

Devices are locked against unauthorized access

All storage device types - hard drives, USB drives, CD and DVD drives

Authorized users retain transparent access

Logical encoding of data in network folders

Protected data remains protected, wherever it is stored

Encoded data not accessible to administrators - or malware

Increased stability of software and hardware

Software authorization

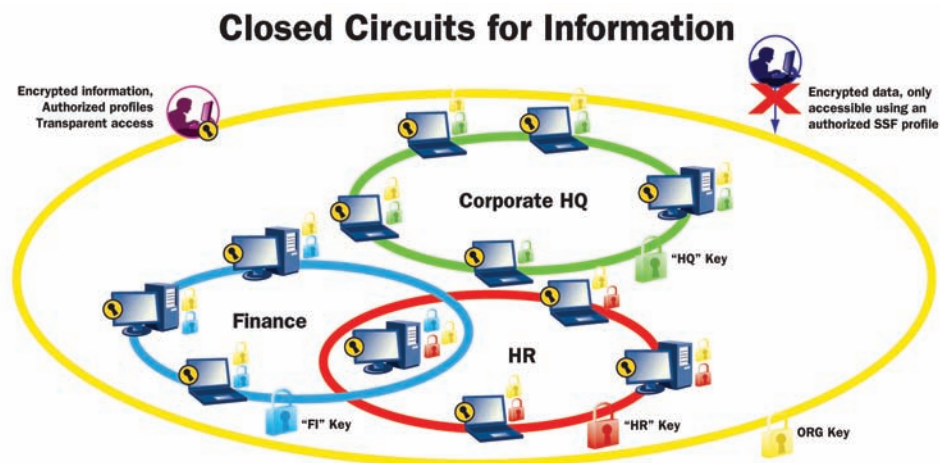
Authorization of devices

SSF's modular framework delivers multi-dimensional security in a single suite that adapts to changing threats, behaviors, and systems over time.

About Secuware

Founded in 1998, Secuware is a leading European developer of enterprise security solutions. The company has grown from a dedicated provider of robust security solutions to the Spanish Ministry of Defense to a broad-based security infrastructure company that now protects more than 500,000 computer users around the world. Commercial customers include Warner Bros, Wal-Mart, Telefonica, Banco Santander, Iberdrola, and every major department of the Spanish government.

The brains behind Secuware is Carlos Jimenez, Spain's leading information security expert. Not yet 40, Carlos is a member of the Commission of Experts for the Ministry of Science and Technology and a contributor to the government's current strategic action plan for the security of electronic information; an invited expert at NATO counter-terrorism conferences, where he has contributed particularly to efforts to combat the Basque separatist group ETA; and has contributed to the protection of the Human Genome Project and a number of other key digital content projects.



Secuware Inc
440 North Wolfe Road
Sunnyvale, CA. 94085
Phone: 408-524-3070
Fax: 408-524-3072
Toll Free 1-800 - 720-0734
www.secuware.com