

# SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

## REVIEWED IN THIS ISSUE

### StillSecure VAM P76

Implementation of the StillSecure VAM is intuitive and easy



### ISS Proventia P75

Network Enterprise Scanner has power when properly deployed



### SecurStar P90

Gives you the option to hide the key inside any music or graphic file



## FEATURES:

## THE VERDICT ON

# VISTA

Microsoft's Scott Charney says security is improved, but others say not so fast. **P26**

## Guarding the exit

Organizations gradually are realizing the value of intellectual property **P36**

## Fast growing threats

Cybercriminals are finding holes in company web applications **P41**

## GROUP TESTS

### » Vulnerability assessment

The platform du jour **P73**

### » Whole disk encryption

This niche is maturing **P83**



# GUARDING

Organizations gradually are realizing the value of intellectual property, reports **Dan Kaplan**.



Illustration by Si Hyunh/Imagezoo

**W**hen Verdasys co-founder and CEO Seth Birnbaum was heading up engineering at NeoGenesis Pharmaceuticals, three employees thought they had a foolproof plan to steal drug formula secrets in hopes of forming their own company. “We wouldn’t have known anything about it if they didn’t order CD-ROMs through our IT purchasing department on the same day,” he recalls of the incident, which happened about four years ago. “That’s the only reason we interdicted that. We had never even thought this kind of thing could happen.”

Company officials agreed that up until that point, they had hardly considered the possibility that an inside job might breach their deepest and darkest secrets, despite a drug discoverer’s heavy reliance on intellectual property (IP), Birnbaum says. Organizations like NeoGenesis were mainly concerned with the external hacker. The possibility that an unauthorized employee was going to email out some IP or store it on a disk or flash drive, well, that was a risk they were willing to take.

Birnbaum and his fellow co-workers’ initial reaction to the planned heist was far from unusual. Although organizations — especially those in manufacturing sectors — have revolved their bottom lines and competitive edges around IP for as long as they have been in exis-

# THE EXIT

tence, a rare few stop to think just how valuable those digital assets are, experts say. Yet, according to the U.S. Department of Commerce, IP theft costs American businesses \$250 billion a year and 750,000 jobs.

“People really don’t appreciate the full scope of what has value to themselves and their competitors,” says Ira Winkler, a global security strategist and author of *Spies Among Us*. “Frankly, if you lose IP, people might not care, but conversely, if you lose hundreds of thousands of credit card numbers, you’re going to end up on the front page of newspaper.”

Still, some industry leaders say that mindset is changing — and the proof is in a fast growing market segment that tracks content *leaving* the organization.

Compliance regulations such as *Sarbanes-Oxley (SOX)*, combined with an increased reliance on outsourcing to keep costs down, high-profile data losses and the ability to easily store many gigabytes of company secrets on removable devices, have forced enterprises to study their security posture from the inside out. As a result, more companies are realizing the importance of leak prevention and are no longer willing to roll the dice that they can stave off an insider attack, be it malicious or accidental.

And, most importantly perhaps, technology is starting to catch up with the problem, as a host of vendors have arrived on the scene in the last three years — including Birnbaum’s three-year-old data security firm Verdasys, based in Waltham, Mass. (an idea

borne out of the NeoGenesis incident) — to tackle a threat that industry experts expect to continue to grow.

Safeguarding 16-digit credit card numbers and nine-digit Social Security numbers are still priorities, of course, but many companies are now also focusing efforts at protecting trademarks, copyrights, patents, business strategy and trade secrets — be it source code for a new Microsoft soft-

ware program or the 11 secret herbs and spices for Col. Sanders’ famous KFC recipe. (Almost ironically, Silicon Valley is now considered America’s home base for corporate espionage).

“More and more customers are saying that it’s not just about compliance, it’s not just about privacy, it’s about IP,” says Faizel Lakhani, vice president of marketing at Mountain View, Calif.-based Reconnex. “Now they’re actually making sure their company’s doing well by protecting their IP and making sure it doesn’t get exposed.”

Rich Mogull, vice president of information security and risk research at Gartner, Stamford, Conn., says the content monitoring and filtering market is one of the fastest maturing sectors percentage-wise in the security space. It was worth \$25 million last year and is expected to grow to \$60 million to \$80 million this year and as much as \$160 million next year.

“This kind of crime has happened forever,” Mogull says. “We just have new tools and new vectors of loss. We’ve always known someone can put something on a floppy and walk out the door. Now we know they can email it.”

Yet while the market is soaring relative to previous year’s performance, the overall numbers remain minimal compared to other facets of enterprise security.

Sreekanth Ravi, president and CEO of Santa Clara, Calif.-based Code Green Networks, a new player in the content monitoring arena, compares its growth to the firewall market of the early 1990s.

## TOP 5 TIPS: Intellectual property

**1 Define** intellectual property. An effective plan should require IT administrators to classify data using multiple techniques in order to ensure that unstructured data is protected.

**2 Know** what is leaving your network. Deploy a content monitoring appliance to discover if private data or IP is leaving the network or if employees are using the network inappropriately.

**3 Establish** and enforce security policies. Educate employees on your approved applications and security policies while communicating that these policies will be enforced.

**4 Define** authorized users. Create rules that define who can access IP both inside and outside your organizations.

**5 Identify** and protect data at rest. An information protection system must be able to identify pre-registered known sensitive content and protect it before it leaves the network.

— Ratinder Paul Singh Ahuja, CTO, Reconnex

“There’s so much awareness and talk around it, but the deployment is being done by visionaries or early adopters or people who have been affected by it,” he says. “Pretty soon, though, it’s going to be off the rack. Everyone will be designing it in as a standard because everybody has something they want to protect.”

With a market sector still in its infancy comes a slew of new vendors — including Verdasys, Code Green Networks, Tablus, Reconnex, Vericept and others — trying to make a name for themselves with appliances and software. The solutions vary in their protocol monitoring breadth and analysis techniques, but essentially all of them track and potentially flag network communications traffic that contains IP. Looking at the threat from the inside out is starting to take hold across organizations, especially companies that heavily deal in the area of IP.

“My whole company is R&D,” says Ken Venner, CIO of leading wireless semiconductor maker Broadcom.

Based in Irvine, Calif., but with 47 design locations worldwide, Broadcom has 5,200 employees. Seventy-one percent of them were hired to design the chips that propel Bluetooth and Ethernet technology.

“The core assets of the company are the algorithms and the circuit layouts that these engineers generate,” Venner says. “IP protection is the business I’m in.”

Broadcom deploys Verdasys’ Digital Guardian solution as a way to monitor outbound data flow, without limiting productivity. “It’s a collegiate environment here,” Venner says. “It’s a bunch of intellects working their thing. I want to make security invisible to them. I want them go where they need to go. The doors are open, but the camera is watching.”

While companies such as Broadcom are being driven to secure IP by value



**People really don’t appreciate the full scope of what has value to themselves and their competitors.”**

— **Ira Winkler**, global security strategist and author of *Spies Among Us*

propositions, compliance is also playing a role. SOX, for example, compels companies to disclose incidents of data losses that could impact an investor’s decision to pour money into a stock, Ravi says. In other words, you might think twice about buying Microsoft shares if you heard the proprietary design specs to Windows Vista fell into the hands of a competitor.

Still, software solutions can only take an organization so far in protecting IP. Some have opted to employ less costly, but potentially equally helpful ideas, such as blocking USB port access entirely, or instituting employee awareness training programs.

“When you start going through all the permeations, you learn that most networks are like Swiss cheese,” says Willy Leichter, director of product marketing for Redwood City, Calif.-based Tumbleweed Communications, a messaging security firm. “There’s so many ways things could get out. Email is the most likely place something will leak, but if somebody is hell-bent on stealing your secrets, and they’re inside your organization, frankly it’s going to be very difficult to stop them.” ■



**VERDASYS**<sup>™</sup>

950 Winter Street, Suite 2600  
Waltham, MA 02451  
781.788.8180

info@verdasys.com • www.verdasys.com