

Part 4: A guide to buying extrusion-prevention products

Danny Lieberman, Open Solutions Israel

October 28, 2004 (Computerworld)

*To be able to do something before it exists,
sense before it becomes active,
and see before it sprouts.*

The Book of Balance and Harmony (Chung-ho chi).

A medieval Taoist book

In my previous articles ([see story](#)), I introduced the concept of extrusion, or the unauthorized network transfer of sensitive digital assets. Here are a few true examples:

- cc'ing a supplier by mistake on a classified RFP document
- Production servers with anonymous file transfer protocol (FTP) turned on
- Break-ins, bribes and double agents (workers who spy for other groups or companies)
- The actuary who went to work for the competition

As new technologies are developed to meet the extrusion challenge, more customers are evaluating and implementing solutions. This article examines the threats that drive business makers to buy extrusion technology, and the industry players that provide the products. The shopper's guide will help you choose the product that best fits your business and your threat profile.

Who are the buyers and what drives the decision?

A common question I hear is, "Who should 'own' extrusion-prevention technology?" Is it the vice president, internal auditor, chief financial officer, CIO or CSO, or is it IBM Global Services?

The business need drives directly to the CEO and his management team, and in firms with outsourced IT infrastructure, the need for extrusion prevention becomes more acute as more people are involved with less allegiance to the firm.

To help you qualify your organization's commitment to extrusion prevention, let's look at the decision drivers, or what compels companies to buy security products, and the decision-makers, or those who sign off on the products. We'll look at seven industries: banking, credit card issuing, insurance, pharmaceuticals, telecommunications, health care and technology.



INDUSTRY		
BANKING	<ul style="list-style-type: none"> ■ A real event, such as theft of confidential customer account information by trusted insiders ■ Privacy regulations such as the Gramm-Leach-Bliley Act, HIPAA ■ The Sarbanes-Oxley Act, for transparency and timeliness in reporting of significant events 	Vice president of internal audit who mandates a technical evaluation to the CSO or the CIO that directs the information security group to act.
CREDIT CARD ISSUERS	<ul style="list-style-type: none"> ■ Ongoing theft of customer transactional information by customer service reps ■ Extrusion threat to credit card numbers that haven't yet been printed on plastic cards and issued to card holders ■ Privacy regulations, Sarbanes-Oxley, nondisclosure agreements with business partners 	The security officer or information security officer (many issuers have separate functions for physical and information security)
INSURANCE	<ul style="list-style-type: none"> ■ A real event, such as theft of customer lists by competitors ■ Fear of losing actuarial data ■ Exposure to extrusion of credit card numbers in online systems 	General counsel, VP of internal audit, CFO
PHARMACEUTICALS	<ul style="list-style-type: none"> ■ Theft of chemistry, manufacturing and control information, product formulation and genome data by trusted insiders ■ Difficulty in preserving secrecy of sensitive intellectual property prior to patent filings ■ Sensitivity of company records during due diligence processes 	General counsel, CFO, chief compliance officer
TELECOM/ONLINE BUSINESS (Telecom service)	<ul style="list-style-type: none"> ■ Prepaid code files ■ Pricing data 	VP of internal audit, VP of technologies

<p>providers and large online operations such as Yahoo collect and aggregate huge quantities of data, and the higher up the value chain you go with data aggregation, the more valuable and vulnerable the asset.)</p>	<ul style="list-style-type: none"> ■ Strategic marketing plans ■ Call detail records (analogous to credit card transaction records, these are extrusions by customer service representatives to private investigators and difficult to detect) ■ Customer credit card records 	
<p>HEALTH CARE</p>	<ul style="list-style-type: none"> ■ Privacy regulations/HIPAA ■ Need to protect pricing data of drugs and supplies purchased by the health care organization 	<p>CSO, VP of internal audit</p>
<p>TECHNOLOGY COMPANIES</p>	<p>Theft of:</p> <ul style="list-style-type: none"> ■ Source code ■ Designs, pictures and plans of proprietary equipment ■ Strategic marketing plans 	<p>CEO, CTO</p>

What kinds of technology are there?

Now that you see why companies need technology for preventing data theft, let's take a look at the options. There are three architectures for extrusion-detection and -prevention: agent, proxy and sniffer.

Agent: An agent-based solution is similar in concept to host-based intrusion detection. The agent, which needs to be distributed to all the PCs in an organization, provides a software solution for Windows with shims to network services, file systems, Windows clipboard, removable media and CD burners. Events are generated according to a set of predefined rules, for example, copying a Word file from a file share marked as "sensitive" and then pasting text into a browser.

Proxy: A proxy-based solution is typically used for monitoring e-mail traffic. It requires placing an application-layer proxy next to your Exchange servers or installing a server agent. Events are generated according to a set of predefined rules and content profiles.

Sniffer: A sniffer-based solution is a Windows or Linux-based appliance located next to the firewall that provides off-line content profiling and online packet sniffing and TCP session reassembly. Some solutions operate in real time, while others may log the sessions first for later batch analysis. After the session payload is decoded, the content is analyzed and events are generated according to a set of predefined rules and content profiles. A good sniffer solution will send events to a database for reporting and data mining.

Shop by threat

Our shopper's guide is organized around typical threat profiles. Your profile will contain one or more threats to your company's digital assets: human error, system holes, criminal and terrorist activity, and trusted insiders.

According to your evaluation of threats, assets, network vulnerabilities and potential economic loss, you're probably shopping for a solution in one of these categories: to prevent trusted insider theft in Microsoft networks; to prevent trusted insider theft by e-mail; to prevent all extrusion threats in a heterogeneous network; or to prevent extrusion threats with a real-time network audit.

Trusted insider threat in Microsoft networks

If your organization is agreeable to installing agent software on Windows PCs, and you're mostly worried about trusted insider theft, then take a look at a vendor such as Verdasys Inc. This company's product doesn't analyze content but monitors flow of information from trusted sources (such as a Windows file share) to untrusted destinations (such as a Webmail browser session) and infers a policy violation.

Pros of agent software

- Covers everything the Windows PC sees
- Solves the disk-on-key issue
- Solves the issue of mobile users

Cons

- Doesn't mitigate threats by intruders
- Doesn't address network or server vulnerabilities
- Scalability challenge of maintaining classifications of Windows shares

Trusted insider threat by e-mail

If your main threat is theft via e-mail, you may want to consider a solution from vendors such as IoLogics Inc. or Vidius Inc. Both companies have workflow features for prevention by quarantining suspect messages. Vidius has recently added domain-specific content recognition in addition to their digital file fingerprinting.

Software proxies have a number of weaknesses:

- You will need to install the proxy or a Microsoft Exchange or Notes server agent.
- Vidius depends on file-system scanning to generate digital signatures; you can miss events in between scans.
- It is arguable that the only extrusion threat is e-mail sent by authenticated Windows users.
- Users can bypass the proxy due to a misconfigured network or Windows PC.
- They don't support popular Unix/Linux mail servers such as sendmail or qmail.
- There are lengthy implementations of four to six weeks, according to some customers.

The IoLogics proxy-based appliance fingerprints actual content, regardless of the type of digital asset (e-mail, Word document, PDF or others). Extrusion control is provided with the ability for violations to be recorded, quarantined or blocked. IoLogics is a relatively new product and, unlike Vidius, should work equally well with any messaging service and scale up with multiple appliances.

All extrusion threats, large heterogeneous network

If you have a large, heterogeneous (Microsoft, Linux, Unix, AS/400, mainframe) network with multiple threats, you should consider one of the sniffer-based products from companies such as Vericept Corp., Tablus Inc., Vontu Inc. or Fidelis Security Systems Inc.

Pros of sniffer-based products

- Scan all channels
- No software installations or changes in network topology
- Controls extrusion
- Can provide a much wider spectrum of threat mitigation than an agent or proxy

Cons

- May not be able to decode all protocols effectively
- Doesn't solve the disk-on-key problem
- Doesn't solve the mobile user issue

In this category, take a special look at Fidelis and Vontu.

Fidelis has a well-balanced offering of content profiling, analysis and the highest performance of sniffer category products. One dual 2.8-GHz Pentium Linux-based Fidelis appliance processes 30GB per hour on all channels of a corporate backbone vs. a similar network that required eight servers and load balancers for a Vericept solution. In a distributed configuration, a single analyst workstation can support dozens of distributed sensors.

Vontu has a solid understanding of the extrusion problem and does a fine job of content profiling and analysis, implementing Windows-based software that scales with multiple servers. Its largest client has deployed a distributed configuration at six locations processing 10GB of e-mail traffic daily and aggregating events to a central database.

Founded in early 1999, Vericept has 600 customers. Vericept's patent-pending software monitors inbound and outbound Internet traffic using pre-set categories. It enables companies to identify activity that falls outside of a company's pre-defined acceptable use policy and provides customized analysis to meet an organization's specific needs.

Tablus deploys a Linux-based sniffer with linguistic content classification. However, their Windows file-system crawler approach raises similar issues to Vidius. A server that crawls the entire Active Directory forest requires comprehensive privileges and could be vulnerable to hacker exploits.

Anticipating extrusion threats with real-time network audit

If you're concerned about mitigating threats before they bite, then this category is for you.

It only takes one leak to cause serious damage, and, unfortunately, most companies don't know what's going on in their network. Think about Cisco Systems Inc. and its source-code theft as a lesson in how network system holes can lead to loss of sensitive assets ([see story](#)).

Going beyond content-flow control we get into the realm of providing real-time visibility into the status of the network, its services and its assets. Customers have told me that the best way to anticipate extrusion is to audit their network in real time. In this category, Fidelis' high-performance appliance alerts and prevents extrusion of sensitive assets and also highlights network anomalies such as anonymous FTP, IP fragmentation and denial-of-service attacks that are precursors to extrusion events.

How do you decide?

I think the best way to decide is to test-drive. Call the vendor on Wednesday and ask them to come into the office on Monday with a box.

Give them one hour to set up on a production network segment. Try a few of your favorite cases; trap a webmail with some keywords, fingerprint a SQL query from the billing system, extrude some C# source code and intercept credit card number thefts.

Allocate one day for a hands-on evaluation and have the vendor in a week later to discuss results. Be patient. This is cutting-edge stuff, but it's worth it in terms of mitigating your No. 1 computer crime threat—extrusion.

Remember: Extrusion prevention starts with management commitment to action and budget before you start shopping.

For a detailed list of questions to ask, try this shopping list on my [Web site](#).

