

Product Section

BEST OF 2007

How we do what we do



Overall, the quality of the products we saw this year was higher than ever. For many groups we had a very hard time selecting Best Buy and Recommended rated entries. We never do competitive testing. We test against a set of internal standards derived, in spirit at least, from the common criteria. This was a departure from earlier years.

There were other departures from *SC Magazine* tradition this year. In the past we treated testing as an isolated lab exercise. Products came in, got tested and popped out the other end with a review. Last year we turned that isolationist concept on its head and opened the SC Labs to the vendors.

This approach allowed us to focus on the user experience instead of only the products. If a vendor normally provided a particular suite of services to its customers, we allowed that same interaction in the SC Labs. We often had vendors making installations under the watchful eye of Mike or Justin.

There are two schools of thought about this approach. On one side, one could argue that the vendors had undue influence over the reviews and testing. The other viewpoint is that the process more closely represents what the purchaser is likely to see. We favor the latter. Responding to the former, our position is that the vendor still needs to adhere to our process. We have a quality control procedure that precludes dishonesty on the part of the vendor and we do all of the testing. The vendor usually is involved only in installing and setting up the product. The bottom line in evaluating the vendor participation is whether or not, over the past year, there has been any hint of undue influence. The answer is that there has not.

Potential products come from Judy's research and from interactions with the vendors and their PR representatives. Judy then sends out invitations, usually to 20 or more vendors per group. Out of those 20 or so invitations, we get between six and 12 qualified, interested vendors.

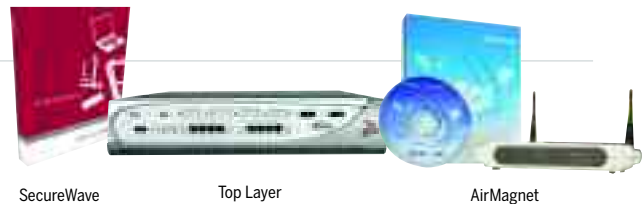
Mike and Justin set up the test beds, I work with them on definitions and test procedures while John makes sure the products arrive on a staged schedule so that products arrive as close to the planned day of testing as possible. Then Mike or Justin performs the testing and writes the draft reviews. I qualify check the tests and edit the reviews, or, in some cases, write the reviews.

The whole process takes about two months, but the actual testing often progresses at the rate of two products per day per lab because test procedures are, whenever possible, automated or scripted for speed and consistency. Products are rated individually on our scale (not against each other) and, at the end of the process, we look at the star ratings and the write-ups and select a Best Buy and a Recommended product.

I hope that answers the questions as to how we selected our winners this year. Those winners are in the pages that follow and I commend them to you as 2007's best. — Peter Stephenson, technology editor

SECTION CONTENTS

Anti-malware management . . . 7	Managed security services . . . 5
Application vulnerability 8	Policy management 4
Biometrics 11	Secure content mgmt. 10
Data leakage prevention . . . 12	SSL VPN 10
Email content filtering 4	Two-factor authentication . . . 8
Email security 9	USB security 6
Firewalls 11	Unified threat management . . 7
First Look 11	Vulnerability assessment 2
Forensic tools 5	Web content filtering 3
Identity management 3	Whole disk encryption 2
IDS/IPS 9	Wireless security mgmt. 6



How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme.

The general test process is a set of criteria built around the six review areas (Performance, Ease of Use, Features, Documentation, Support, and Value for Money). There are roughly 50 individual criteria in the test process. These criteria were developed by the SC Lab in cooperation with the Center for Regional and National Security at Eastern Michigan University and have been in use and refined over the past four years.

What the stars mean
Our star ratings indicate how well the product has performed against our test criteria. These are marked as follows:

- ★ Seriously deficient. An "F" on the product's report card.
- ★★ Fails to complete certain basic functions. A "D" on the product's report card.
- ★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.
- ★★★★ Carries out all basic functions very well. A "B" on the product's report card.
- ★★★★★ Outstanding. An "A" on the product's report card.



What the recognition means

Best Buy goes to products that the SC Lab rates as outstanding. **Recommended** means the product has shone in a specific area. **Lab Approved** is bestowed to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

Vulnerability assessment

This group looked at vulnerability assessment and penetration test tools. The leading difference between last year's tests and this year's is that this year we saw more hybrid products that offered both vulnerability scanning and penetration testing. We also reviewed a passive scanner

for the first time and saw a lot more attention to meeting regulatory requirements.

We had a nice bunch of products that included appliances and software-only. We had one product that is strictly a penetration testing tool and, as we had some other products that included vul-

nerability assessment and penetration testing, this forced us to break the group up into three sub-groups: vulnerability assessment, penetration testing and hybrid (both).

In general, we were impressed with their utility, ease of use and comprehensive reporting.



Net Clarity Branch Auditor 5.0

Product	Vendor	Our verdict	URL	Rating
Branch Auditor 5.0	NetClarity	We were amazed at the power of this little handful of an appliance.	www.netclarity.com	
NeXpose	Rapid7 LLC	An impressive hybrid – vulnerability scanner and penetration test tool.	www.rapid7.com	
Core Impact 6.0	Core Security Technologies	A pure penetration testing tool optimized for production use.	www.coresecurity.com	
Saint Scanner + Exploit	Saint Corporation	A solid combination of scanner and pen testing tool that is easy to set up from Linux.	www.saintcorporation.com	
Passive Vulnerability Scanner	Tenable Network Security	Truly passive product that does not perform active scans of any kind.	www.tenablesecurity.com	
Tenable Nessus 3	Tenable Network Security	The world's most widely supported vulnerability scanner.	www.tenablesecurity.com	

Whole disk encryption

This group looked at seven whole disk encryption products. All products tested were standalone software packages that were separate from the underlying operating system (OS). One of the products tested was an open source product that has developed a large following in

the industry, while all other packages were commercial products. Several of the offerings were bundled with hardware tokens for authentication. The devices were all USB, while several vendors offered other options such as SCSI and PCMCIA token devices. All of these products were not com-

bined with other desktop security packages, such as personal firewall or anti-virus software.

As a group, these packages performed well and many offered unique features. We evaluated these products as both a single-user install and also as enterprise products.



DriveCrypt Plus Pack

Product	Vendor	Our verdict	URL	Rating
Whole Disk Encryption	PGP Corporation,	Provides the easiest to install hard drive encryption package we tested.	www.pgp.com	
DriveCrypt Plus Pack	SecurStar	If James Bond had encryption software he would have the DriveCrypt Plus Pack.	www.securstar.com	

Web content filtering

It was a new year in web content filtering. There are several new trends this time. First, products are displaying a variety of architectures. These range from in-line gateways that sit behind the firewall to a proxy device that re-routes web-bound traffic through itself. Of course,

we also saw the traditional client-server products as well.

Last year, most of our products were software based. This year we saw several appliances.

The final trend we noted in performing this test was the inclusion of tools that do not apply directly to, but integrate

nically with web content filtering.

Our overall impression is that web filtering products have come a long way in a short time. They are beginning to show a level of maturity that fits well as a countermeasure to some of the most pervasive security problems we experience today.



Web Security Suite 6.3

Product	Vendor	Our verdict	URL	Rating
R3000	8e6 Technologies	A superb appliance that was easy to set up, performed well, is well documented and is feature rich.	www.8e6.com	SC BEST BUY
Web Filter	Barracuda Networks	Blocks access to websites based on content, content category, domain or URL.	www.barracuda.com	SC RECOMMENDED
Web Security Suite 6.3	Websense	A collection of capabilities in a single software package that addresses most challenges.	www.websense.com	SC RECOMMENDED

Identity management

This group looked at one of the hot-button products from the 2006 landscape — identity management. For years identity management has been defined by the triple A acronym: Authentication: confirmation that a user is truly tied to the username provided; Autho-

rization: granting access to specific services based on the authentication; Accounting: a process for logging access and authorization.

For submissions to this review, we required that the products exhibit the following characteristics: password management, user

provisioning, and enterprise access management.

Additionally, it had to be enterprise-centric. Some products were complex and would be required only in the largest enterprises. Some were software-only, while others were appliance-based.



M-Tech ID Synch and P Synch

Product	Vendor	Our verdict	URL	Rating
ID Synch and P Synch	M-Tech	For full-featured identity management, the M-Tech products were among the best that we tested.	www.mtechit.com	SC BEST BUY

Email content filtering

If you thought that buying an email content filtering product would get you an email content filtering product only, think again. Today's batch of products sport a range of capabilities that make these products an absolute must for enterprises of just about any size. From spam filtering, anti-virus and

anti-phishing to centralized management of email security, these products do just about anything you can think of relating to email security.

As we looked through these products we were struck by one very important differentiator: the policy engine. Regardless of the

added features an email filtering product may offer, if the policy engine is not extremely strong, the product cannot be a superior performer. Some of the products we looked at had a large number of pre-built policies and most had the ability, at some level, to create new policies or to modify existing ones.



IBM-ISS Proventia Network Mail Security System

Product	Vendor	Our verdict	URL	Rating
IronMail	Secure Computing	Can protect against many outside email threats, including viruses, spam and phishing.	www.securecomputing.com	
Proventia Network Mail Security System	IBM Internet Security Systems	Many customizable easy to set up rules that can be based on a large number of categories.	www.iss.net	

Policy management

System configurations are getting more complex, and systems no longer are defined as just workstations. Devices such as smart phones, wireless access points and printers are all devices that are capable of storing a security configuration, but they are also devices capable of

introducing vulnerabilities or other security weaknesses into an environment. When new clients or endpoints are combined with the constantly moving target of new vulnerabilities being released and new organizational directives, the task of ensuring policy compliance is often a quickly evolving one.

Many of the products that we reviewed this month used unique approaches to tackle the problem of device policy management. Some products focused on specific types of devices, while other clients focused on more traditional systems, such as workstations and servers.



BigFix Enterprise Suite, Version 6.0

Product	Vendor	Our verdict	URL	Rating
GPAnywhere, Version 2.5	FullArmor	Installs an extension into the Microsoft Windows 2003 Global Policy Management Client (GPMC).	www.fullarmor.com	
Enterprise Suite, Version 6.0	BigFix, Inc.	BigFix Enterprise Suite (BES) is a product that can really do it all in the world of policy management.	www.bigfix.com	

Managed security services

Managed security service providers (MSSPs) often are an enigma for information security professionals. Many MSSPs have been driven out of business as more organizations have looked to outsourcing as the best option for managing security devices. When

outsourcing of security services is discussed, the focus immediately moves to the large telephony and internet service providers.

We invited over 25 service providers to take part in this Group Test. In the end, we ended up with many organizations unable to participate for a

myriad of reasons, and we eventually were left with just four providers to test.

Overall, we concluded from this testing that if you need an MSSP, don't be dazzled by the big guns in the marketplace. There are some little guys that want your business and can really produce for you.



Solutionary ActiveGuard

Product	Vendor	Our verdict	URL	Rating
Threat Manager	Alert Logic	The portal provides a lot of information that is easy to navigate and to comprehend.	www.alertlogic.com	SC BEST BUY
ActiveGuard	Solutionary	Includes hosting, managed firewall and managed intrusion prevention.	www.solutionary.com	SC RECOMMENDED

Forensic tools

This group looked at a wide variety of digital forensic tools. This category has been growing rapidly, diversifying and maturing in the past two years. However, there are some interesting aspects to those growth phenomena. First, we are beginning to see real innovation

in tool sets, but virtually none of it is in traditional computer forensics tools. In that class, we saw, essentially, nothing new since we reviewed them last year.

In many respects, the computer forensics product leaders are indistinguishable from each other. Advances that have come at all

have been in areas that are intended to keep pace with emerging forensic requirements, such as the increasing number of media types that need to be analyzed.

This year our observation is that there really is very little difference among the leaders beyond a feature here or there.



WetStone Technologies Gargoyle Investigator

Product	Vendor	Our verdict	URL	Rating
Gargoyle Investigator	WetStone Technologies	An important addition to any lab, it is an excellent tool for compliance and vulnerability testing.	www.wetstonetech.com	SC BEST BUY
ProDiscover IR v 4.9	Technology Pathways	If you need an over-the-network forensics tool at an affordable price this is just the ticket.	www.techpathways.com	SC RECOMMENDED
LiveWire Investigator v. 3.1.1C	WetStone Technologies	Extremely powerful tool for analyzing computers without taking them off-line.	www.wetstonetech.com	SC LAB APPROVED

USB security

When we started looking at USB security products, we actually had no idea what we would find. Vendors of many types of products — from those that protect USB ports to those that protect data at USB ports — presented their wares. We found something

interesting in all of the sub-categories.

The most obvious types of USB security products, at least in the enterprise environment, are those that allow direct management of the USB ports on enterprise computers.

The bottom line for this group

of USB devices and software was that there are ways - with improved functionality and granularity over last year - to manage what is and what is not allowed at the endpoints of the enterprise, especially relating to the USB ports and the data that may be accessible through them.



SecureWave Sanctuary Device Control v4.1

Product	Vendor	Our verdict	URL	Rating
Sanctuary Device Control v4.1	SecureWave	Secures against many I/O devices, it has excellent control of USB devices.	www.securewave.com	SC BEST BUY
DeviceWall v4.5	Centennial Software	Goes way beyond typical USB security features. A good value for almost any size enterprise.	www.centennial-software.com	SC RECOMMENDED

Wireless security management

Wireless networks are not about to go away any time soon. The convenience of losing the copper tether and gaining the ability to roam from one end of a campus to another without re-authenticating is just too practical.

In the earlier days of wireless

networks, the security controls were riddled with flaws, but today's updated wireless networks have security controls that - when appropriately configured - provide greater security than a traditional wired network.

However, owing to the number of wireless standards, there is still

a great deal of confusion due to all the standards that exist just for wireless networking.

All of the wireless security management products in this Group Test scored well in detecting the rogue access point, the rogue client and unauthorized configuration changes.



AirMagnet Enterprise 7.5

Product	Vendor	Our verdict	URL	Rating
800 Mobility Controller	Aruba Networks	A great product for overburdened IT shops wishing to spend more time administering.	www.arubanetworks.com	SC BEST BUY
Enterprise 7.5	AirMagnet	The pre-built policies will make the admin's life easier and the wireless network more secure.	www.airmagnet.com	SC RECOMMENDED

Anti-malware management

This Group Test was dedicated to the tools we use to fight various types of malware. In our product roundup, we list around 75 anti-virus and anti-spyware products that are, generally speaking, best of breed. They all have been through the West Coast Labs certification process and their

catch rates have been verified using the WildList, the authoritative listing of viruses, including BOTs and worms, actually in the wild.

However, in the enterprise, these products pose a few challenges. For example, how does one implement anti-malware in a 10,000-user enterprise spread

around the world? And how does one support it with updates and logging and alerting of events? That is the subject of this Group Test, anti-malware management tools. You might say that these products are the glue that holds an anti-malware program together.



Savant Protection Enterprise Management

Product	Vendor	Our verdict	URL	Rating
Interscan Gateway Appliance	Trend Micro	This is an extremely strong, easy to use product loaded with features.	us.trendmicro.com	SC BEST BUY
Enterprise Management	Savant Protection	A novel approach to managing malware that we found quite effective and attractively priced.	www.savantprotection.com	SC RECOMMENDED

Unified threat management

The unified threat management (UTM) group is maturing rapidly and, in fact, is taking over market share from the multipurpose products. The result is a true UTM that has a lot of anti-malware capability. There is good news and bad news here.

The bad news is that this creates a single point of failure. It also creates a bit of a dilemma for security architects. If one buys a first rate UTM, especially one with a lot of anti-malware capability, how does one justify purchasing an additional anti-malware gateway?

The good news is that the UTMs we tested all are competent. In fact, in some cases, we were hard-pressed to find significant differentiation between some of the products, and the dashboards even look similar. There is no doubt that this product category is taking off.



eSoft InstaGate 604

Product	Vendor	Our verdict	URL	Rating
InstaGate 604	eSoft	Can be built up to have as little or as much functionality as needed by the environment.	www.esoft.com	SC BEST BUY
PRO 5060	SonicWALL	Includes the usual suspects of firewall, IPS/IDS and anti-virus, but also includes web/email tools.	www.sonicwall.com	SC RECOMMENDED

Two-factor authentication

With today's network environments, perhaps the greatest vulnerability is the loosely defined perimeter of an organization. In times past, an organization's computing took place inside of a brick-and-mortar computer room. This model evolved into distributed computing where

processing took place anywhere inside the physical building. Once the laptop was introduced, the perimeter was extended again.

What is the easiest solution to all of these problems, as well as the most efficient path to compliance with the latest legislation? Two-factor authentication often is

the best answer. Regardless if the authentication is inside a VPN connection, to a wireless network, to a web-enabled application, or to a critical device like a router or a firewall, two-factor authentication provides greater assurance that the user on the connection is authorized.



MXI Stealth MXP

Product	Vendor	Our verdict	URL	Rating
IdentityGuard	Entrust	Authentication occurs at the application level and can be used for easily authenticating web traffic.	www.entrust.com	SC BEST BUY
Stealth MXP	MXI	Unique in offering the option of a USB-based token that includes a fingerprint biometric scanner.	www.mxisecurity.com	SC RECOMMENDED

Application vulnerability assessment

Today, many legacy applications are either web-enabled or in the process of becoming web-enabled. Consequently, these applications — which were never designed to be used in this fashion — are now being exposed in new ways to larger and larger user communities, as

well as attacking communities with increasing sophistication.

In many cases, the process of web-enabling an application exposes critical assets, such as large databases with personal client information.

To mitigate these risks and also for compliance with industry

best practice standards, application vulnerability assessment must be performed.

This type of assessment is different from the more common network vulnerability assessment because of the need for a greater understanding of web-based vulnerabilities.



SPI Dynamics Assessment Management Platform

Product	Vendor	Our verdict	URL	Rating
Assessment Management Platform	SPI Dynamics	Adds enterprise use and role management for strong management of web vulnerabilities.	www.spidynamics.com	SC BEST BUY

IDS/IPS

This year there are two noticeable changes in IDS/IPS products. First, the footprint we are seeing is decidedly distributed. Second, the functionality continues to approach universal threat management.

There is another trend that, really, is an outgrowth of the function-

ality trend. There are fewer real IDS/IPS products in the market.

But, there still are very credible IDS/IPS products, and from our perspective, that's a good thing. The use of a distributed IDS/IPS is a step forward for most large enterprises. To date there have been ways to gather data from

multiple sensors, but the emerging architecture of separating the control center from the sensors is a step forward.

The products are becoming more versatile, more powerful as analysis tools, and more distributed.

And that's good news, indeed.



Top Layer IPS 5500-150E v 5.12

Product	Vendor	Our verdict	URL	Rating
IPS 5500-150E v 5.12	Top Layer	Capable of handling a wide range of threats, including worms, viruses, spyware, and P2P applications.	www.toplayer.com	
NitroGuard IPS	NitroSecurity Inc.	A solid product with good integration to other NitroView products.	www.nitrosecurity.com	

Email security

We found that email security products for the enterprise tend to be of three broad types: appliance, software or integrated tool kit. The first thing to look for is enterprise management capabilities. There needs to be a way to push out encryption to the user.

The second issue that needs to be considered is key distribution. The average office worker has neither the time nor the interest in managing public and private keys. Thus, key distribution and management needs to be as transparent as possible.


Finally, there is key recovery.

When a user leaves their password, critical information in emails that are encrypted must be recovered.

We found that most products performed well. Because Group Tests are never shootouts, the final choice may well come down to your preference.



PGP Desktop Enterprise Email 9.6

Product	Vendor	Our verdict	URL	Rating
Desktop Enterprise Email v9.6	PGP Corporation	This product continues to set the standard for pure email security in an enterprise environment.	www.pgp.com	
Secure Messenger v6.3	Tumbleweed Communications	Incorporates email encryption and a full content security manager.	www.tumbleweed.com	

Secure content management

This Group Test examined secure content management (SCM) products. As defined for this review, secure content management devices are gateway devices that have multi-feature/multi-purpose functionality, which includes filtering incoming and outgoing traffic for malicious code,

inappropriate content and network attacks.

SCM protects an organization from malicious code outbreaks by scanning email, web and file transfer traffic for viruses and worms. SCM devices also protect an organization from unauthorized use of systems.

SCM devices also safeguard an organization from spam emails. Most SCM devices use a combination of blacklists, whitelists, heuristics, reverse domain name service (RDNS) checks, sender policy framework SPF checks, as well as learning mechanisms which update the spam filtering.



McAfee Secure Internet Gateway 3000

Product	Vendor	Our verdict	URL	Rating
Secure Internet Gateway 3000	McAfee	This product performs all tasks for secure content management.	www.mcafee.com/us	
ThreatWall	eSoft	Provides SMTP mail filtering and web traffic filtering, with medium range costs.	www.esoft.com	

SSL VPN

Connectivity is more important than ever. Most members of a mobile workforce must be able to access critical files, print services, company intranet applications and even their workstation desktops outside of normal business hours. Whether a user connects to a branch, main or

home office, access is the key.

To maintain secure access remotely, many organizations are turning to or have already implemented virtual private networks (VPNs). The VPN allows a remote user to connect over the internet to the remote office in a secure manner.

The VPN connection uses encrypted tunnels to protect the confidentiality of the information, as well as making the connection appear to the user as if they are on the corporate LAN.

IPsec is a standard written to specify running on top of internet protocol (IP) networks.



Billion Electronic Co. BiGuard S10

Product	Vendor	Our verdict	URL	Rating
BiGuard S10	Billion Electronic Co.	The SSL VPN provides access to many types of common applications.	www.billion.uk.com	
SPX2000 Universal Access Controller	Array Networks	Allows remote file access through SMB, internal mail servers and standard TCP-based services.	www.arraynetworks.net	

Biometrics

Today's crop of biometric products is innovative, work well and is acceptably easy to implement.

It is quite common to be able to perform multiple tasks with current biometrics. You can gain logical access to computers and networks, you can gain physical

access to doors, and you can create biometric profiles of individuals using facial recognition.

We saw an interesting trend in the area of false acceptance and rejection rates: adjustability. Many products allow you to determine your tolerance for these two anomalies. This is

important because in order to tighten these parameters you must sacrifice usability.

Another trend is the emergence of standards, both in the U.S. and internationally. We found that most of the products that we reviewed conformed to one standard or more.



Bioscrypt VeriSoft v2.0

Product	Vendor	Our verdict	URL	Rating
VeriSoft v2.0	Bioscrypt	Features a fingerprint scanner for biometrics, but is also capable of managing use	www.bioscrypt.com	
Pro Workstation/Pro Server	DigitalPersona	Easy to install and deploy with integration into Active Directory.	www.digitalpersona.com	

Firewalls

In today's business world, there are two great tools used by almost every organization to help protect the computing environment. These two tools are the firewall and the virtual private network (VPN). The firewall is still the primary mechanism for protecting the infrastructure of an

organization, where the VPN is more about enabling connectivity to the infrastructure.

The firewall can be a proxy-based firewall. Proxy-based firewalls are firewalls which, as the packet is processed, terminate the time to live (TTL) field in the IP header. These firewalls must pro-

tect all layers of the OSI (open systems interconnection) model, including the application layer. A proxy-based firewall must maintain two separate data streams. The most complex type of firewalls, proxy firewalls are often referred to as third-generation firewall technology.



SonicWALL PRO 4100

Product	Vendor	Our verdict	URL	Rating
Corporation Sidewinder 7.0	Secure Computing	A complete enterprise firewall loaded with more features than most organizations will ever need.	www.securecomputing.com	
PRO 4100	SonicWALL	A good product with a large number of features and an easy-to-use interface.	www.sonicwall.com	

Data leakage prevention

One of the most important security functions today is protecting organizational secrets. We finally have entered a world where everything important is on a server or workstation somewhere in our organi-

zations. Certainly we're nowhere near paperless, but the important stuff lives happily as data bits and bytes. How do we ensure that critical corporate data, intellectual property, private information and the like don't fly our

nically protected coop?

The short answer is that today we cannot offer that assurance. But we can close many of the escape routes effectively, and that is what this month's data leakage prevention products intend to do.



Oakley Networks SureView v5.0

Product	Vendor	Our verdict	URL	Rating
SureView v5.0	Oakley Networks	If you need very strong data leakage protections with powerful forensics, this is the product for you.	www.oakleynetwork.com	
DLP 1.1	BigFix, Inc.	Powerful agent-based endpoint data leakage protection at a very good price.	www.bigfix.com	

First Look

A new offering this year in *SC Magazine* has been the First Look column. Its purpose is to address products that may not fit neatly into any product group. Tech editor Peter Stephenson looks for products that have the potential to define the group they are in or a new group if they

don't fit neatly into an existing one.

We will be revisiting many of those products in the future to see if they lived up to their promise.

In 2007, three new First Look products received SC Magazine Lab Approved designations — NitroView Receiver 7.2.0/ NitroView ESM 7.2.0 from

NitroSecurity, the Mu 4000 from Mu Security, and the LogLogic LX Release 4.0.

This distinction means that these products are extraordinary standouts that fit into the SC Lab environment, and will be used subsequently in our test bench for the coming year.



Mu Security Mu 4000

Product	Vendor	Our verdict	URL	Rating
NitroView Receiver 7.2.0 and NitroView ESM 7.2.0	NitroSecurity, Inc.	Speed, depth of analysis, comprehensive log management, enterprise scalability — this has it all.	www.nitrosecurity.com	
Mu 4000	Mu Security, Inc.	This is the most powerful vulnerability analysis tool I have used.	www.musecurity.com	
LogLogic LX Release 4.0	LogLogic	We liked the improved reporting and log analysis features	www.loglogic.com	