GroupTest: Anti-malware

Malware is the catch-all for most malicious and unwanted software, and includes viruses, worms, trojan horses, bots, rootkits and spyware.

In this month's issue, we not only wanted to test the tools that we use to fight malware, we wanted to test the capabilities of these tools to handle the multiple threats we lump into the malware definition. We also were interested in their ability to centralize management, reporting, alerting and deployment of the malware solutions.

Why is this important? There are numerous solutions for fighting malware. We have anti-virus, anti-spyware, anti-spam, anti-adware, rootkit detection, host-based intrusion detection and prevention, and personal firewalls. For those who have deployed just one of these in an enterprise environment, you will appreciate the challenge in deploying multiple non-integrated or centrally managed solutions to thousands or tens of thousands of users.

The approaches from the vendors we reviewed this month took on this challenge in some very creative ways. Some solutions were endpoint focused, while others were gateway solutions. As well, some were software-based, some purpose-built appliances, and others virtual appliances. We were interested in the kinds of malware these solutions could manage, and in the approach the vendors took for addressing the new blended threats we face today. We were also interested in a product's ability to centrally alert and report on threats.

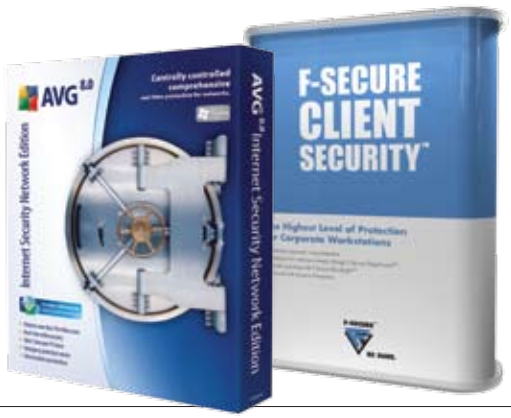
All of the products reviewed provided multiple components of our malware definition. Most provided anti-virus and anti-spyware, while some took a different approach and relied on other products to deliver the traditional signature-based virus and spyware protection (i.e., protecting against the threats we know), while taking a more focused approach on protecting from the unknown threats through a more host-based IDS-like solution. Some were gateway solutions focused on providing web content protection and email protection from virus, spyware, spam and malicious code in HTTP, FTP, POP3 and SMTP traffic.

We did not test the products for their catch rates. For this test, we assumed they all have very similar catch rates for signature-based threats. We were looking for the product's ability to identify, alert and stop zero-hour threats. Some products used firewall and IDS-like approaches to lock down executables, applications and registry items. Some used advanced heuristics for threat detection. Others provided scripting tools to allow for a wide range of additional management and alerting options.

We were also interested in a product's ability to provide near real-time updates to virus and spyware engines and databases through a centralized means that would reduce the load on network bandwidth.

All in all, we were pleased with the solutions. They attacked the malware problem on multiple fronts and provided a means for alerting that allows for rapid remediation once a threat is detected. In a perfect world, where budget is never an issue, the combination of the gateway technologies with the endpoint solutions would provide a very effective malware defense for your enterprise.

Product	Vendor	Our verdict	URL	Rating
Internet Security Network	AVG Technologies	Strong features, good protection, easy to use and manage. We rate this product Recommended.	www.avg.com	SC MAGAZINE RECOMMENDED
Client Security 8	F-Secure	Very nice solution for any size organization. Provides a diverse yet integrated offering, protecting the endpoints against today's new breed threats. This is a solid product and we give it our Best Buy designation this month.	www.f-secureusa.com	SC MAGAZINE BEST BUY



GroupTest: Firewalls

The technology that is the primary security mechanism has just had its 12th birthday, and while the internet, networks and attacks have all changed, the firewall is still the firewall.

As they were being developed, firewalls were a technology meant to protect devices and applications, and they were never intended to provide security. Now, operating systems and applications (and soon IPv6) will all have been developed from the start with security playing a central role.

It used to be precaution enough to block Telnet to a UNIX-based firewall, but attack sophistication was changed forever when, in 1996, Aleph One released "Smashing the stack for fun and profit." This paper enabled the hacker community to stand on the shoulders of giants. Now, attackers didn't need to know the level of operating system architecture – everything was simplified.

In today's environment, the port blocking by most firewalls mostly provides a sense of false security. The first major change hit when encryption became almost a de facto standard for many common applications. Firewalls can't see into the encrypted activity to determine what the traffic actually holds. For the non-encryption problem, the actual solution is to turn off all non-business critical ports on the target device itself, instead of depending on a device blocking the connection attempt one step closer to the internet.

As attacks have evolved, the arguments for firewalls have evolved as well. If a port needs to be open for business reasons, the port needs to be left open through the firewall. If a port is non-business critical, the port should be turned off. In fact, I would say that firewalls solve the wrong problem. We need ports to be open, we need to connect to the internet, and turning off the business is counterproductive. The real problem with network traffic is not the destination, but rather who sent the traffic in the first place. Authentication is the key, not paranoid blocking and passing all encrypted traffic.

You may have already guessed that this month we tested firewalls – both application- and network-based firewalls. Previously, we tested network access control (NAC), and – from concept through implementation – that seemed like a better solution than firewalls. But if we at the SC Lab have learned one thing, it is to test before forming an opinion.

In this month's review, we decided to focus on the improvements to the firewall over the last 12 years. In short, we were looking for what used to be the non-firewall that now is part of the firewall. And the results were surprising. The devices we tested were more like some sort of mutant security device than the firewall of 12 years ago. These devices read into the data portion of packets to determine the attack from legitimate requests. There were other firewalls that terminated encrypted tunnels in order to first judge the contents of the request. There were even devices that could hardly be called firewalls anymore.

We saw these firewalls with new eyes, because they could actually block attack traffic on business critical ports – in other words, they could function more like an IDS, than an IDS could 10 years ago.

Product	Vendor	Our verdict	URL	Rating
Web Site Firewall Model 460	Barracuda Networks	A feature-rich product at a low cost, making it our Best Buy.	www.barracudanetworks.com	SC Magazine Best Buy
NSA 240	SonicWALL	A superior product, which offers a huge number of features for the price. This makes the NSA 240 the Recommended network firewall.	www.sonicwall.com	SC Magazine Recommended

GroupTest: ID management

Identity management has been a sort of fuzzy term encompassing a lot of different functionality. We have seen this in the past, and this year the picture is not much different. That said, the functionality that ID management products include has been increasing, and a picture may be emerging that illustrates what really is meant by the term identity management.

This month, we saw products ranging from simple single sign-on to full-featured appliances that cover all of the functionality currently thought of as required for a solid ID management product. However, the down side is that the nature of the functionality still seems loosely defined.

In 2007, Gartner's Ant Allan grouped ID management into directory technologies, ID administration, ID auditing, ID verification and access management. These systems, according to Allan, must exhibit administration, authentication, authorization and auditing functionality.

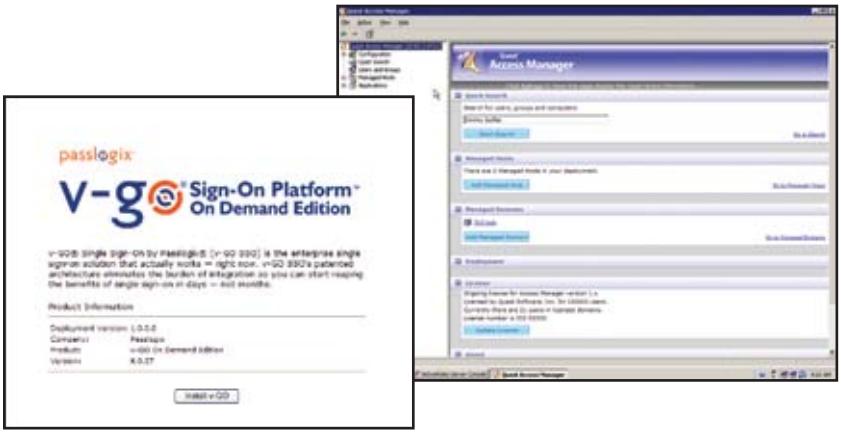
The question, then, is what really is required in an ID management system? Certainly, provisioning is a must. Especially in a large enterprise, provisioning can be a real challenge done manually. For example. single sign-on has become *de rigueur*. Remember when the pundits said that SSO was not practical? All sorts of solutions to the problem were proposed, with few being particularly successful. Today, all that has changed. Lack of SSO weakens an ID management product that claims to be full-featured.

As with any product, one really needs to do a thorough analysis of requirements. That may include determining what products are used currently that might need to integrate with the ID management system. Certainly, it is useful to compare Allan's groupings and recommended functionality with your product choice. Understand how you are managing identities and access control now. Are there solid policies and procedures in place that you will need to automate without losing functionality? Or, perhaps, are your policies and procedures a bit immature and less than robust? That, potentially, can be a blessing in disguise because you can build appropriate policies and procedures that fit nicely with one or more products that are under consideration.

Once you understand the environment in which you will implement ID management, ask the really tough question: do you need to automate ID management at all? All of the products we looked at require some dedication to their implementation. So, if you don't need the functionality, don't cause yourself the pain associated with building a system you could do without.

Some of the indicators that you need to consider for ID management include size of the organization, geographic dispersal, and the number of applications or systems to which your users need access. If the nature of that access is disparate (i.e., not everyone has the same access needs), you may be a candidate for an ID management system. Wide geographic dispersal and large size also are indicators. If you are a multinational organization, make sure that there are no restrictions in host countries against the type of implementation you envision.

Product	Vendor	Our verdict	URL	Rating
v-GO Access Accelerator	Passlogix	Tight integration makes this a solid product, but it requires dedication to get the entire suite up and running. Once implemented, though, it provides real benefits. We rate this product as Recommended.	www.passlogix.com	SC Recommended
Quest One Identity Solution	Quest Software	Top drawer product, easy to manage, and a real value for the money. We rate this as our Best Buy for the month.	www.quest.com	SC Best Buy



GroupTest: Multifactor authentication

Every week there's another article on identity theft and another network is breached. We are all challenged with securing our computers. Whether you are a business securing a global communication system or a home user protecting your personal files and online account information, authentication and identity verification are two challenges we all face. As a business, we want to know that it's really you accessing your private information. As a user of a service, we want to know that no one else can pretend to be "me" and gain access to our information.

User names and passwords are a good start, and we've all gotten better at not using our children's or pet's names for passwords, and not hanging our credentials around the office or home. When we look at the various levels of authentication, the user name and password is commonly known as the first factor of authentication: "something you know."

When a user name and password are no longer sufficient to provide assurance of identity, strong authentication methods are required. Strong authentication has been traditionally defined as two- and three-factor authentication. These additional forms of authentication add "something you have" and "something you are" to the "something you know" factor. Something you have would be technology, such as a token with an additional PIN, or pass-code, to validate that you are, in fact, the person using your credentials. Something you are works in the same fashion and uses such things as a fingerprint or iris scan.

There are numerous solutions addressing the strong authentication market. This month, we focused on solutions that address identification and authentication. We were impressed with both the traditional and unique approaches we found in the products we tested. We were also very surprised with the number of identity and authentication options that were offered. We found soft and hard token offerings (i.e., certificate-based or agent-based as examples of software; and key fob, proximity cards or USB keys as examples of hardware), biometric, PIN-based solutions, out-of-band solutions that would change your cell phone or PDA into a hard token for a one-time password (OTP), and knowledge-based authentication solutions.

Without a doubt, all the solutions we evaluated provided an added layer of security. The plethora of authentication options available today provide organizations a great amount of deployment and management flexibility, and various cost structures to fit most budgets. I did, however, find myself coming back to the traditional definition of strong authentication, and asked myself if authentication forms, such as certificates or agents on computers, machine authentication or even knowledge-based solutions, truly qualified as either something I have or something I am. In the end, I came to the conclusion that any additional level of security is a good thing. We just need to understand that if a notebook or portable device with a soft token install is stolen, and the traditional user name and password is cracked, then that device is compromised.

Product	Vendor	Our verdict	URL	Rating
eToken PRO	Aladdin Knowledge Systems	Definitely one to consider for any enterprise-strong authentication project. We give it our Best Buy rating this month.	www.aladdin.com	SC Magazine Best Buy
IdentityGuard v9.1	Entrust	Nicely integrated platform that provides all the options needed for any small to large enterprise deployment. We rate this product Recommended.	www.entrust.com	SC Magazine Recommended

GroupTest: Email content management

As the reliance on messaging continues to grow and the value of information increases exponentially, organizations are looking to protect messaging services from vulnerabilities and evolving threats. Inbound and outbound email services represent a tremendous risk to any enterprise, whether the threats are malicious outside attackers or simply human error from a corporate perspective. Gone are the days when email security products simply scanned attachments for known viruses, filtered the message body for profanity, or quarantined spam based on a few simple signatures or heuristics. Organizations are dealing with sophisticated spam attacks, phishing, botnets, regulatory compliance mandates and several other risk areas that must be managed in order to effectively secure information.

Email content management vendors have recognized the need for more granular control over email security within the environment. Features and options continue to converge as appliance vendors are responding to the need to secure malicious inbound emails and data leakage concerns for outbound messages.

This month we examined several email content management products. We defined email content management as the ability for a solution to provide most of the following functions: filter inbound and outbound messages, filtering based on content, filtering based on source address or sender, quarantine/notification, overall fit into an enterprise environment.

Overall, we found that most of the products that we reviewed met our criteria for email content management. An interesting observation for this group of products is that some vendors focused on stopping unsolicited and malicious inbound mail through sender or domain validation, reputation scoring and other mechanisms, while others focused their efforts on building more robust data leakage protection for outbound messages. Data leakage is generally secured by the use of keyword filtering and "smart identifiers." The smart identifiers are pre-built data strings that users can apply to policies which search messages for suspicious formats, including possible credit card numbers and Social Security numbers.

All of the products in our group review were hardware-based appliances, except one, GFi MailSecurity, which is a software-based solution. All of the hardware-based solutions were installed in our test network and tested against Microsoft Exchange 2003 with regards to inbound and outbound mail gateway configurations. All email clients that we used for host machine testing included Microsoft Outlook and web-based clients.

In our tests, we focused on several areas, including initial setup and configuration, functional areas of the solution, ease of use and overall administration. Our testing included how easy or difficult it was to configure the options and apply them to a relative domain, organization or list of users.

These solutions removed a chunk of the administrative burden from its users and come highly recommended. With economic uncertainty, administrators are wise to invest in products that cover the largest risk area with the most administrative functionality.

Product	Vendor	Our verdict	URL	Rating
MIMEsweeper Email 2.7	Clearswift	Great value that scales well in most any enterprise environment makes this our Recommended product.	www.clearswift.com	SC Magazine Recommended
Messaging Security Gateway	Proofpoint	Although the solution is the most expensive one we tested, the granular features make this an excellent value and earn it our Best Buy.	www.proofpoint.com	SC Magazine Best Buy

GroupTest: Web content management

As I mentioned in my opening column this month, the notion of web content management is a bit convoluted. When you look for a solid definition of web content management, you find that it is focused at the server end. So what we really have at the client end is content filtering. In that regard, the purpose has not changed much since we first started discussing content filtering years ago. And, ironically, when SC Lab Manager Mike Stephenson ran the web products through the lab, his major comment was that we saw all of this last year – with the exception that there are some new protocols being covered.

Most of the products we saw were appliances. Generally, we like that because setup and administration are easier than with software-based products.

As always, the key to any kind of content management is policy and we looked hard at that. Policy in a product, however, is of little use unless it translates organizational policy into configuration easily and quickly. We are picky about how products make that translation. The old days of needing to program filters in what feels like a scripting language are – or should be – over. Time is money and precision counts a lot. We look carefully for precise, easy to configure, hard to fool policy engines.

As with any product, especially products that can have a potential impact on network performance and user satisfaction, web content filters need to do their jobs as unobtrusively as possible. A web filtering product should not be noticed unless it has to do something, such as block a website.

Fitting into the enterprise is important, and what that means is not intuitively obvious. I have seen products that do what they do very well, but drive their users nuts with interruptions and pop-up messages that many of the users don't fully understand. Not all enterprises are the same. For example, enterprises in organizations that have a culture of high security often are more tolerant of severe restrictions while more open enterprises, such as universities, have a culture of low tolerance for restrictions. The product you select should allow you to match it to the culture of your organization while offering adequate protection.

We set up each system to get a feel for the product's intuitiveness. We then completed the implementation according to quick-start guides to ensure that we had the configuration correct.

Our next stop was the policy engine where we started with the default policy set if there was one. We used a series of tests that attempted to defeat the policies in place as a default. Then we created a policy and attempted to defeat it. We were interested, especially, in the number of ways that the product accomplished its filtering. We looked for URL, key word and protocol filtering.

Finally, we looked at how well the product was documented in conjunction with its complexity. More complicated products – and a product may legitimately be complicated depending on its functions – require more complete documentation. Some products require little because they are intuitive. In addition to documentation, we are concerned about support options and the support website.

Product	Vendor	Our verdict	URL	Rating
Web Filter 310	Barracuda Networks	A highly capable web and application filter with protection from malware at an affordable price for any environment, all of which makes the Web Filter 310 our Recommended product.	www.barracudanetworks.com	SC Magazine Recommended
iBoss Web Filter	Phantom Technologies	A highly comprehensive appliance with a great amount of flexibility makes the iBoss this month's Best Buy.	www.iphantom.com	SC Magazine Best Buy

GroupTest: UTM

UTMs have broken the traditional mold and now contain just about anything that you can conceive of putting on the perimeter. We saw anti-spam, anti-malware, firewalls and the rest of the usual gateway tools all neatly packaged into 10 appliances – no software or virtual appliances.

The breadth and depth of covered protocols improves every year. We saw emphasis on P2P and IM added to those products that did not have them last year.

The game is changing. There now are very competent endpoint security products – we look at several this month in our other group review – so the notion of spreading defense-in-depth across the enterprise now is viable. In the case of the UTM, we now have come to expect a lot of functionality. However, functionality at any cost is not the goal. For example, many organizations have excellent anti-malware gateways and do not need additional functionality in a UTM. So, review your security and network architecture at the perimeter and decide what you need before you decide what to buy.

Manageability is a key aspect of a successful UTM deployment. If you have a widely distributed enterprise, figuring out how to manage remote appliances can be a challenge. Pick products that fit into your existing architecture and are able to be managed centrally. The same is true of reporting and alerting. Make sure the capabilities of the UTM fit your needs in both respects.

Network architecture is a key issue as well. If your architecture at the perimeter is based on a DMZ or multiple perimeter networks (such as online banking systems), you might want to consider mixing the UTM with a traditional firewall. This adds defense in depth at a very sensitive part of the enterprise. It also increases your control.

The last issue to consider is performance. The UTM sometimes can pose a bottleneck at high traffic perimeters. Be sure that your choice has high availability capability in those situations.

UTM testing is great fun. We set up some of our meanest attack tools and threw everything we could at the products. We set up a complete network of targets that we protected by the devices. Then, we set up an attack machine on its other side (the WAN side).

We started with the firewall wide open to see if the IPS would stop attacks. Generally, we found the default state was 'report only.' Admins are faced with configuring before the IPS can be used effectively. However, you can use the reporting to characterize the traffic that is passing through the UTM. That helps you tune effectively.

Once we knew what was passing through our devices, we tightened them down and ran Nessus again. The idea was to get past the UTM and hit the targets it was protecting. If we saw anything inviting, we opened up our big guns – Core Impact – and let fly. Those of you who attended the SC World Congress may recall that we demonstrated a UTM test there. The difference is that Core has continually updated its attacks and each month there are more tests for us to try.

The results this year were quite satisfactory. Bottom line? If you can't find what you need in the way of a UTM here, it probably doesn't exist.

Product	Vendor	Our verdict	URL	Rating
Proventia Network MFS	IBM	A pleasant surprise this year. Solid performance and a very good price make this our Recommended choice this month.	www.ibm.com	SC Magazine Recommended
TZ 210 Wireless-N	SonicWALL	Solid performance, good pricing and excellent functionality all combine to make this our Best Buy for the month.	www.sonicwall.com	SC Magazine Best Buy

GroupTest: Endpoint security

Both my desktop PC and my notebook computer allow me to perform the tasks associated with my job. These same devices also provide me with the ability to print to a local printer, sync to a PDA device, plug in my camera and transfer images, add new software, attach to my private secured wireless network, as well as any public unsecured wireless network, burn CDs and DVDs, plug in USB devices, and so on.

As our technologies continue to expand to meet the challenges of component integration and data sharing, and as the mobile workforces continue to grow and more people access corporate resources over unsecured public networks, the challenge becomes controlling what data should be allowed to reside on those endpoints or mobile devices and, when allowed, securing that data while at rest and while in transit.

Audit after audit, I am always amazed at the amount of data that can easily walk out of organizations. These challenges have far-reaching implications, such as the protection of the corporate data and of personal identifiable information, and the obvious compliance and audit requirements.

I find myself always weighing the security advantages of totally locking down an endpoint so no applications can be loaded, no port will be active and no unauthorized communications can occur versus the productive gains of allowing people to use the technology we give them to be more effective, productive and innovative. To be effective, endpoint security must balance the security risk with the productivity benefits. The right solution must also address the IT challenges we all face today – mainly, overburdened and understaffed IT departments.

We reviewed endpoint security solutions. The criteria for the submissions focused on solutions that could manage, assess or control security at the endpoint, were centrally managed, and provided centralized reporting and alerting.

We classify the products into four categories: network security – providing protection like firewalls, antivirus and spyware; encryption – the ability to encrypt the local drive or partitions, as well as any removable media that would be allowed; port management – providing tools to manage everything from USB ports to printers, CD/DVD devices, communication ports (serial or parallel ports), smart card readers; and various wireless interfaces, such as Bluetooth, infrared and Wi-Fi. The final category addresses the host-based intrusion protection aspect with solutions that monitor and prevent application loads, registry changes, privilege escalation, and block use of copy/paste features and kernel event management.

We focused our testing efforts on the server side management, reporting and alerting along with the product's ability to integrate with various directory structures for setup, agent/client deployments and management of the environment. Most of the products required the use of a backend database engine. One or two shipped with their own embedded database, the rest required us to load either a MSDE [Microsoft Data Engine] or SQL database prior to loading the application. This will be something to pay attention to when evaluating these products in your own test labs.

Product	Vendor	Our verdict	URL	Rating
Endpoint Protection v11.0.4	Symantec	Full protection, easy to install and manage, and good reporting and alerting, all for what most would pay for anti-virus.	www.symantec.com	SC Magazine BEST BUY
StormShield Security Suite	SkyRecon Systems	Very nice offering, providing a lot of security at the endpoint for the price. This is the complete package.	www.skyrecon.com	SC Magazine RECOMMENDED

GroupTest: Vulnerability assessment

This was an interesting year for our vulnerability assessment test. Last year, we separated application vulnerability assessment from network vulnerability assessment. This year, we grouped them together. This revealed a few interesting differences.

The primary difference is that network vulnerability assessment tools are converging with penetration testing tools to provide both capabilities in the same tool. This is important because penetration testing is an extension of vulnerability assessment. In a proper network security assessment, one begins with the large view and progresses toward the specific. Two years ago, there were no solid combination tools. Last year, we had a couple that got pretty close. This year, we had solid entries that are really single security assessment tools.

I make a distinction between vulnerability assessment, penetration testing and security assessment. Vulnerability assessment (VA) reveals the global picture of possible vulnerabilities. I say "possible vulnerabilities" because VA tools can give false positives and, sometimes, the existence of a vulnerability does not constitute a risk. In order to have a risk, the vulnerability must be reachable by a threat and there must be a threat to exploit it.

We have learned that when there is a vulnerability we should pay attention to it. With SQLSlammer and now Conficker, we have exploits of vulnerabilities that were announced and patches provided months before an exploit appeared. So, when we identify a vulnerability, we need to test it thoroughly to determine if it can contribute to a risk. We do that by focusing on potential vulnerabilities with a tool to attempt to exploit the vulnerability. That means penetration testing.

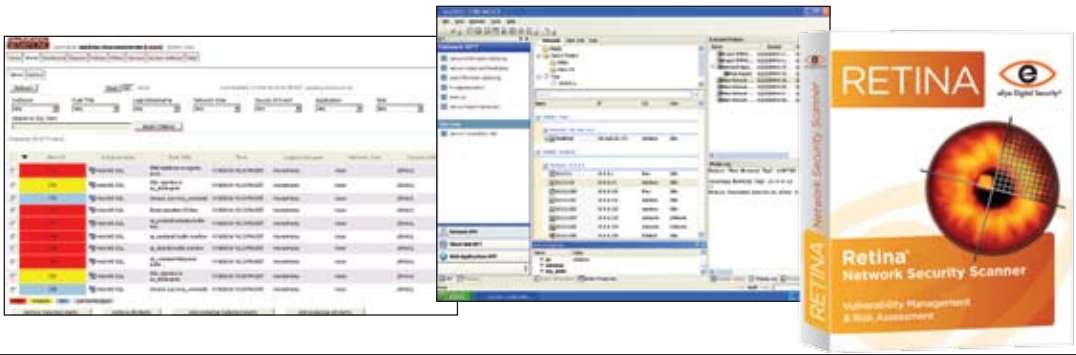
Having all the tools in one network security assessment tool – from discovery and footprinting through VA to pen testing – is very useful. This offers consolidated reporting, simplified point testing where appropriate, and easier compliance testing and reporting. Unfortunately, application VA tools have not progressed quite to that maturity yet.

However, given what we saw this year, that maturing process is not far off. Perhaps we'll see the same kind of consolidated testing in applications as we do in networks. Of course, we'll know that security assessment has come to full maturity when all the tools are converged into a single product.

Compliance is probably the number one driver in information assurance currently. VA tools are responding by providing scan and testing templates that address specific regulatory requirements. This is an interesting twist on many other kinds of products that test or manage systems generally and then create specialized compliance reports.

The jury is out on this approach, because if you need to look at a comprehensive set of possible vulnerabilities, it's good to test completely and refine at the reporting stage. There is the potential to support what I call the "tick-in-the-box" syndrome. This happens when an organization opts to make sure that they can defend the checkmarks on the audit report, instead of making the enterprise truly secure.

Product	Vendor	Our verdict	URL	Rating
DbProtect	Application Security	A solid database vulnerability assessment product with a high, but certainly not prohibitive, price tag. For its solid performance and ease of use, we make this product our Recommended product this month.	www.appsecinc.com	SC Recommended
Core Impact Pro 8	Core Security Technologies	The absolute top of the line for network security assessments at all levels. Again, this year, we award Core Impact our highest rating of SC Lab Approved.	www.coresecurity.com	SC Lab Approved
Retina	eEye Digital Security	An excellent vulnerability scanner at a good price. This one gets our Best Buy.	www.eeye.com	SC Best Buy



GroupTest: Digital forensics

Gone are the days in which conducting a forensic analysis meant pulling the plug and imaging the hard drive. We now know that valuable investigative data resides in a large variety of locations throughout the digital continuum. A successful investigation may rely on the ability to find and interpret a variety of data from these multiple locations.

As a result, the number of tools being designed and marketed with forensic capabilities is growing. The traditional media analysis tools definitely still have a firm place in the investigative process, but they now often include the ability to carry out all the traditional tasks over the network. Adding to those traditional tasks, some of these tools also include the ability to complete a live analysis of a target system over the network as well. Once you've moved past the more traditional products, they become more specialized, and in some cases, less obvious.

On the media front, one category of specialized tools we tested is mobile device forensics. The most obvious application for these tools is to analyze cell phones and PDAs, but devices such as GPS units and digital cameras are also gaining support. These tools can acquire data, such as deleted SMS messages, call logs, stored media, contacts, etc. Additionally, we tested some tools with specialized memory forensics applications. This type of functionality could be useful in analyzing instances of malware or network intrusions.

We also tested products that provide a wide range of network-based forensics capabilities. Many of these are focused on log aggregation, correlation and analysis, with other features spread throughout. The ability to actively monitor and receive alerts based on criteria, such as link analysis and system status, could also be considered a defensive mechanism. While ironing out the normal event levels, system states and statistics can be an intensive task, the final result can be extremely beneficial.

In order to determine what you must look for, you need to examine what you already have. Your answer will help determine which type of forensic tools you should consider purchasing next.

Acquiring tools over time will help you build a comprehensive forensics solution. Not only will this help ensure that you resolve your investigations, but you will be able to do so more quickly and efficiently with a large toolset at your disposal.

Knowing how you plan on using your new tool is one of the most important aspects of making a decision. If you have special analysis tasks that will need to be performed, then you may move in the direction of a specialized tool. On the other hand, more general purpose tools will provide a wider range of features. Deciding on one product may be difficult, but your decision should be based on whether or not the tool meets all of your data analysis requirements within its respective genre.

While many of the media forensics tools often have a clear purpose and selection criteria, this isn't always the case with the network tools. It's even more important to know how you plan on using the product in this category. Depending on your needs, you'll have to choose between an over-the-network forensic tool, a network forensic tool, and the more specialized log aggregators.

Product	Vendor	Our verdict	URL	Rating
ProDiscover IR v5.5	Technology Pathways	This is the tool for your over-the-network forensic needs. We make it our Recommended product this month.	www.techpathways.com	SC Magazine Recommended
LR-1000-XM	LogRhythm	Powerful product with plenty of easy-to-use features, this one is our Best Buy.	www.logrhythm.com	SC Magazine Best Buy

GroupTest: Biometric tools

A few years ago, we wrote about biometrics coming out of science fiction and becoming a very real and feasible option for high security applications, such as government agencies and high level areas in airports. Since that time, we are seeing these products and devices becoming affordable for almost any enterprise that wants to play. From scanners for access into physical areas to fingerprint scanners at every workstation, these devices are finding their way as everyday applications. Simply put, biometrics are becoming mainstream. We are seeing this product space continually growing, and the technology is becoming more and more affordable, as well as reliable.

Unfortunately, we did not have a lot of products to include in the group this month. Many of the vendors we contacted are getting ready to launch new products in the coming months and they did not want to have us feature an old and outdated product at the time of publication. This is becoming the hallmark of the industry – with maturity comes both technological and business acceptance.

Interestingly, I have a discussion question that I pose to my students that addresses this phenomenon. Three years ago, the students were posing all sorts of alternatives. This year the general answers were: why worry? Biometrics are affordable and there are so many new types of reliable, low-cost products that there is something for just about any application.

The problem, of course, is that new versions, new models and new applications are beginning to sprout like weeds in this space and not all vendors were ready to show their wares.

It used to be easy. If you had an average network, you would use passwords and save the expensive biometrics for the high security applications. Then, you would bite the financial bullet and go for the appropriate product.

A year or so ago, it began to get easier. Many networks, and even individual users, could benefit from biometrics of some sort, and we even began to see thumb drives with biometric authentication.

This year, there is almost no security application where strong authentication is required for which you cannot find an appropriate biometric device. While it is true that some are trivial, all have advantages and all should be considered. For example, notebook computers with built-in biometric authentication are becoming commonplace.

The bottom line in buying biometrics is fairly simple. First, match the application to be protected to the appropriate level of biometric type and device. If you have a large population to protect, be sure that there is some form of centralized management, provisioning and deployment.

Second, be sure that the product you are buying cannot be bypassed simply by removing it. This is a problem with some add-in PC biometric access control products.

Finally, be sure that you are not spending $100 to protect $10 worth of assets. It really is that simple to move from reusable passwords to biometrics. The debate about biometrics versus one-time passwords is one we will save for a future issue, but even here, today's biometrics come out credibly.

Product	Vendor	Our verdict	URL	Rating
Combination Model	ACTAtek	Rich with options and straightforward to manage, this is our Recommended product this month.	www.actatek.com	SC Magazine Recommended
DigitalPersona Pro	DigitalPersona	This venerable product gets better every year, and this year we award it our Best Buy.	www.digitalpersona.com	SC Magazine Best Buy

GroupTest: Smart cards

This month, we are reviewing smart cards. A smart card is defined as a pocket-sized device containing integrated circuitry that can process data. There are many different types of smart cards. Some contain basic circuitry and non-volatile random access memory (NVRAM) and provide very specific functions. Others have onboard microprocessors and can receive, store and transmit information.

Smart card technologies are not new, they have been around for over 10 years. The applications have evolved from access control to time-keeping/tracking to credential storage to storing certificate or token-based keys. Smart cards are still widely used for physical security in access control applications and digital time-keeping. Today, this technology has evolved to provide two-factor authentication, secure network logins, secure remote access, secure web authentications, secure email and e-transactions, and digital signature management.

Some of the cards we reviewed this month were purpose built to provide a single function, such as time clock/time tracking. Some of the solutions were focused on credential storing and provided the multifactor authentication through public key infrastructure (PKI)-based strong authentication. Others were flexible in their offering and provided identification, authentication and data storage capabilities.

The ability to store additional information on these cards provides numerous benefits. The same card that a user carries to gain access to their office can also securely authenticate them to their PC or corporate network. As well, the same card can securely provide access to various web-based or email applications, and identify users through digital signatures by storing various public key encryption certificates and digital signature credentials.

As with past reviews, we took an enterprise perspective in reviewing these products. Our focus was on ease of deployment, ease of use, centralized enrollment/pin changes/revocation, centralized management, centralized reporting, user features that can address self-enrollment and support for recovering from lost or bad cards. Some of the products focused on the end-user deployment and management of the smart card. Others had integration with Microsoft for deployment of end-user software and/or centralized PKI management. Some did provide server-side applications for deploying and managing the remote end-user and their smart cards and card readers.

Most of the products reviewed provided basic eight hours a day/five days a week web-based support. Some also offered eight hours a day/five days a week phone support. Those products that had a server-side offering provided additional options for purchasing upgraded support to cover the server software and provide up to 24/7 phone support.

As we mentioned earlier, these technologies have been around for some time. While we were somewhat surprised at the maturity of the server-side offerings for management and the documentation that accompanied these solutions, from an enterprise deployment, management and support aspect, most of the products, with a couple of exceptions, came up a bit short.

Product	Vendor	Our verdict	URL	Rating
En-Sign v7.0.0.7	SPYRUS	Great product, nice price; only lacks enterprise management. We choose this as our Recommended product of the month.	www.spyrus.com	SC Magazine Recommended
Sphinx Enterprise v4.1.9	Open Domain Sphinx Solutions	Nice solution, easy to use, has the enterprise-class requirements to support a large deployment. We designate it our Best Buy of the month.	sphinxenterprisesltd.com	SC Magazine Best Buy

GroupTest: Encryption tools

At this point in time, there aren't too many states that haven't enacted some sort of disclosure legislation. This particular influence has surfaced in many of the encryption products that we see today. The trend this year indicates that protection is spreading to different OSs and devices other than Windows-based desktops and laptops.

As we expected, we're seeing a slight convergence between overall endpoint protection features and encryption solutions. Suites of products are still offering the standard features – such as whole disk encryption, protection for various partitions, and encryption of removable media. However, we're also seeing a growing trend in these policies to either allow or deny access to devices based on certain rules and criteria. Even if the software does not have the ability to encrypt an external device, it may have granular controls and rule sets on how to treat the device if it's connected to the host.

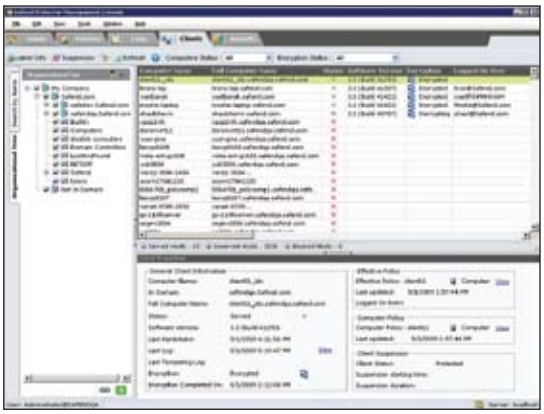
When making a buying decision, many of these newly converged features may be attractive. Your enterprise's policy should ultimately drive the investment. In some organizations with highly confidential data, whole disk encryption may be mandatory for all mobile assets. However, not all of the products available, or even in our review, have the ability to encrypt the entire hard drive, and require pre-boot authentication before accessing the device. But, many products that do not have whole disk encryption capabilities may have other useful features, such as centralized management consoles or the ability to push clients remotely to all host machines. IT and security stakeholders should make sure that company policies and standards are covered when asking questions and making purchasing decisions.

For this particular review, all of the products we assessed were software-based encryption applications. They did not require any special chipsets within a hard disk, and all of the products contained either a client installation or client-server architecture. Some of the features we looked for were the ability of the product to secure the entire disk, secure files and folders, secure removable media, and whether or not the product could be centrally managed through an administrator interface. Whole disk encryption products secure all of the contents on the hard disk and require a pre-boot authentication screen (PBA) before accessing the disk. Products that did not offer whole disk encryption methods usually encrypt a partition or allow for certain files or folders to be encrypted.

All of the products we reviewed contained strong encryption schemes (AES in various bit strengths). Most offered incrementally less intense encryption algorithms for organizations that might have performance issues on older hosts. Encryption is also applied differently, either using passphrases or key ring technology.

Since most of the products can deploy some sort of strong encryption scheme to protect your data, the decision criteria for purchasing isn't the algorithms, but the ease in which clients are deployed and managed. Decision-makers should review whether or not the product helps to support organizational policies, as well as the ease of configuration, deployment and support from the vendor.

Product	Vendor	Our verdict	URL	Rating
Data Protection Suite	Safend	Excellent product at a great price point.	www.safend.com	SC Magazine Best Buy
SafeGuard Enterprise	Sophos (acquired Utimaco)	A great enterprise product with tons of useful features.	www.sophos.com	SC Magazine Recommended



GroupTest: DRM & DLP tools

This month's Super Group focuses on protecting data under a variety of circumstances. First, we look at digital rights management (DRM). DRM lets us send data wherever we want while dictating what can be done with it.

Data leakage prevention, sometimes called extrusion prevention, has a different objective. In this case, we want to keep our data where we put it and we do not want unauthorized users to remove it.

Finally, we have a twist on DRM: license protection. In this case, we usually have some sort of app that we want to control the use of in accordance with our end-user license. This is the familiar copy protection dongle that we see regularly, especially on big ticket applications.

DRM has multiple levels of protection depending on the product and the data being protected. One of the simplest functions is watermarking. This places a notation, or "watermark," in the file, such that it cannot be removed. Other functionality present with some products includes prevention of printing, emailing, copying, deleting and editing protected files. Some products allow a self-destruct policy for the file.

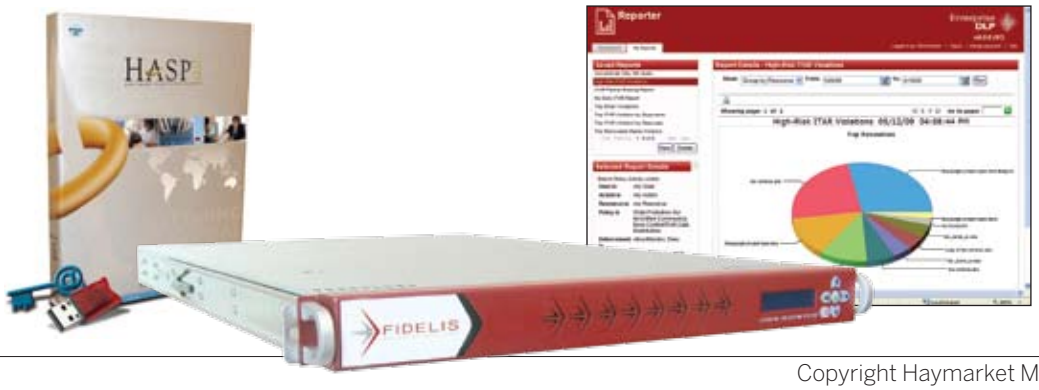
When buying a DRM product, consider carefully why you are applying it. DRM is not a substitute for encryption. It is intended to allow controlled access, rather than to deny all access. However, like all of our product types this month, it might include encryption.

Data leakage products sometimes can be confused with endpoint management products. Many endpoint protection systems do a rudimentary form of DLP by preventing the use of thumb drives or other peripherals. However, for this review we concentrated on products whose primary function was to protect data, wherever it lies in the enterprise, from being removed without authorization. Perhaps the most insidious type of data leakage is that facilitated by malware. Unfortunately, positive control of that problem still is a bit of a Holy Grail. There are some good efforts, but this is a very hard problem.

When buying DLP, look at what types of extrusion you are addressing. Also, look at what endpoint protection you have in place – or plan to have – and focus on augmenting them in functional areas over which you do not have control. Here, as with most enterprise products, centralized management is a key issue. This means the ability to deploy, provision and manage the product over the enterprise. It means that where identity management of some sort is required there are clear connections to something, such as lightweight directory access protocol (LDAP) or Active Directory. The user should be able to access the benefits of the product transparently from any workstation in the enterprise where they have authorized access.

Finally the twist on DRM: license protection. These are products that offer some sort of copy protection. For high value products, the cost of the hardware key (USB dongle) is absorbed easily in the price of the product. Piracy of such products may have serious consequences – from the proliferation of pirated copies of very expensive software to uncontrolled availability of dangerous products, such as penetration testing tools.

Product	Vendor	Our verdict	URL	Rating
HASP SRM	Aladdin Knowledge Systems	These guys pioneered this dongle approach and they still lead the field with first-rate products, making them our Recommended product for license protection.	www.aladdin.com	SC Magazine Recommended
Fidelis XPS	Fidelis Security Systems	We really liked this one. Its high performance and ease of use make it our Recommended extrusion prevention product.	www.fidelissecurity.com	SC Magazine Recommended
Enterprise DLP	NextLabs	Serious functionality and fine performance at an acceptable cost of ownership over its life cycle, made this one our Best Buy this month.	www.nextlabs.com	SC Magazine Best Buy



GroupTest: Password management

There comes a time in the lifecycle of every product type when it starts to become mature. When that happens, the number of new entries starts to decline and feature sets start to become stable across most of the products in the group. That is what has happened to password management. We saw very limited differences in feature sets, so the big differentiators now are how well the product does what it does and how well it integrates into the rest of the enterprise.

The market leaders still are the market leaders, largely because of creativity, innovation and solid integration across the enterprise and suites of complementary products. This, for password management, is a very interesting evolution, however, and part of what makes it interesting is that the category ought to be dying instead of stabilizing. That's a pretty controversial statement, but it fits the facts.

First, security experts agree that multiple-use passwords need to become a thing of the past. They are far too easy to compromise. That leaves us with single-use passwords and tokens of various types. These markets – largely due to cost and complexity of implementation and management – are slow to take hold, so we're stuck for now with multiple-use passwords as the baseline for most users. Of course, high-risk accounts and systems that require the highest security are beginning to use strong identification and authentication routinely. But that does not apply, usually, to the average user in the average organization.

That is what this month's Group Test reviews are all about: How well do the participants manage a very high risk identity and access (I and A) process. The answer is that all do a credible job, but there were a couple of standouts.

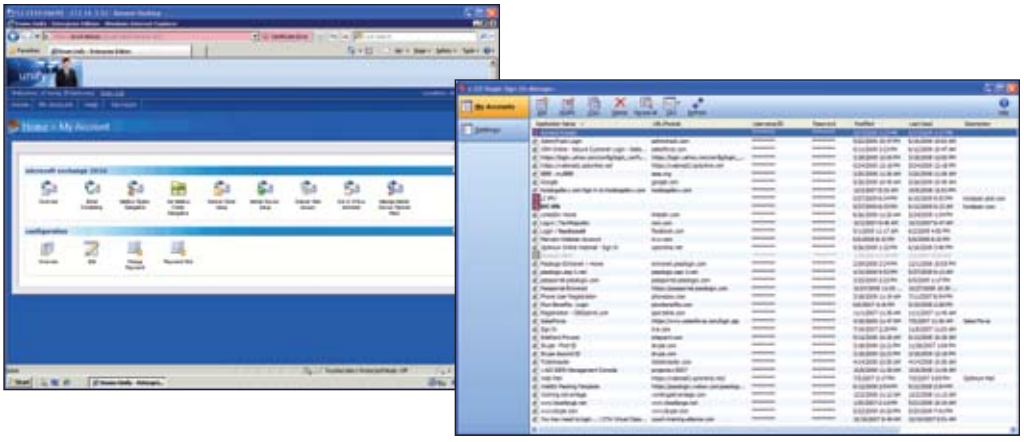
These products were standouts because they built very carefully on what we know about password management, what the enterprise has to offer, and the other products that the vendor is able to integrate into the mix. For example, we need a solid way to manage very high-risk passwords if tokens are not deployed. For reusable password systems, this sometimes is called "password carving." It refers to breaking up high risk accounts, such as superuser accounts, into smaller, lower risk pieces, and removing the top level administrator or root account.

Another issue is how well the product allows integration with or conversion to stronger identification and authentication methods. This allows the enterprise a path forward as multiple-use passwords are phased out and strong I and A phased in.

First, decide what your identification and authentication strategy is. Are you going to stick with reusable passwords? Do you plan to mix strong I and A, such as tokens or single-user passwords with reusable passwords?

Next, look for a product that appears to support your strategy. You probably will find more than one. So look at how they integrate into the existing enterprise. This includes integration into the infrastructure of the security architecture, but it also includes such intangibles as cost of deployment, cost of ownership, and ease of administration and provisioning.

Product	Vendor	Our verdict	URL	Rating
Unify Password Manager	Ensim	For its ease of use and good value, we make Unify our Recommended product this month.	www.ensim.com	SC Magazine Recommended
v-GO Access Accelerator Suite	Passlogix	For its power and value, this venerable product and its complementary product suite rates as our Best Buy this month.	www.passlogix.com	SC Magazine Best Buy



GroupTest: Portable device security

Cell phones, PDAs, smartphones and BlackBerry devices all have one thing in common: They do far more than make phone calls. We live in a connected world today and our personal communication devices are our lifelines.

We reviewed endpoint security tools in April. In that review, we talked about the risks and challenges with securing mobile devices and media. Your corporate or personal information resides on mobile PCs, CD ROMS, USB drives. There is open access to your data over wireless networks and/or Bluetooth. The issues we summarized then are the same we face in this month's review. Only now, we add on top of that, a device such as your cell phone that you take to your children's events, family picnics, the bar after work, leave lying around on your desk, or leave sitting in your car to charge. The same device may have additional wireless access via Bluetooth and standard 802.11 capabilities, and in most cases, will be in an always-on state.

There is no doubt that the benefits of having email, data exchange, data storage and various network access options available on our portable devices provides substantial productivity, efficiency and customer service advantages. To be effective, portable device security must balance the security risk with the productivity benefits. The right solution must also address the IT challenges we all face today, mainly overburdened and understaffed IT departments. The right solution should deploy easily, provide centralized policy management, provide centralized reporting and tunable alerting.

In this month's issue, we review portable device security solutions. Products in this Group Test deal with not only a collapsing perimeter, but also consumer-owned and consumer-controlled devices being used to get at corporate resources. The criteria for the submissions this month focused on solutions that were centrally managed and intended for an enterprise environment, provided some form of encryption, and included some form of security for portable devices.

The products reviewed covered several security categories, including firewall, anti-virus, encryption and device lock-out. Some products treated the portable device like any other USB or Bluetooth-attached device, and managed security at the port level. Others provided various levels of security for the actual portable device.

The solutions varied in their support for various mobile platforms. Some focused on providing a lockout feature, others provided encryption for the communications with the device and/or the data stored on the device, while others delivered a solution that included firewall, antivirus, anti-spyware, software update management, theft protection, remote wipe, and various encryption and lockout features.

We were pleased with all the products we tested for this review. All the products were mature, installed easily and were easy to use. Features and functionality varied across all the products reviewed. When choosing the right product for your use, it will be important to understand and document the needs you are trying to address before evaluating technologies to support those needs.

Product	Vendor	Our verdict	URL	Rating
DeviceLock v6.4.1	DeviceLock	Good endpoint product for securing access via ports and drives to corporate assets. For ease of use, documentation and excellent support we rate DeviceLock Recommended.	www.devicelock.com	SC Magazine Recommended
Mobile Security TMMS v5.1	Trend Micro	Nice solution for portable device security. Delivers a feature-rich set of tools for securing portable devices. For performance and value, we make this our Best Buy.	us.trendmicro.com	SC Magazine Best Buy

GroupTest: IDS/IPS MSS

There are several aspects to managed security services that have evolved over the past 10 years of their history. A decade ago, managed security services were restricted to applying the output of sensors to some sort of collection and display device. Usually this took the form – in the beginning, anyway – of a homogeneous system allowing only a single sensor type. The first evolution of that approach was the use of Snort sensors to overcome the problem of feeding the collector.

It was not long, though, before we began to see the development of translators that could take many of the most popular data sources and feed them into the collector. This forced the collector to become a correlator, taking the pressure off of the human operators and placing it on machines. When that happened, the race for the market was on. Today's refinements are a direct result of the development of compact, high performance log correlators. These devices usually are either unified threat management systems (UTMs) or something similar to security information and event management (SIEM). In either, log feeds now are completely heterogeneous and correlation is in near real time, simplifying the job of the analyst.

We found there are a couple of approaches to today's managed security services. In one case, the services are automated and completely managed by the devices. Once the device – correlator, SIEM or other similar device – is tuned for minimum false positives, the device takes over notifying the customer of alerts.

The other case adds a significant human analyst element. In this case, there are human analysts watching the devices and responding to alerts by tracing, analyzing sources, and performing specific actions to protect the customer network.

Today, managed security services are, de facto, services in-the-cloud in that the correlation point is remote and is accessed through a protected internet connection. Where the sensors aggregate varies from vendor to vendor, and many of the service providers are product vendors that have added managed services to their menu.

Buying managed services always has been difficult. Ten years ago, the difficulty had a lot to do with the immaturity of network security and network security tools in general. The challenges were, in part at least, technology driven. Today's technologies have addressed those issues nicely. The other problem, though, is still with us: A combination of cost/benefit analysis and the fear of turning the organization's "crown jewels" over to an outside vendor.

When buying managed services for intrusion detection and prevention, get back to the basics. The first question regards whether managed services are appropriate for your organization in the first place. Managed security services are not for everyone. Of necessity you will lose some level of control.

More data always is better than less, and more types of data also add to the ability of your staff or the vendor's analysts to analyze events and act quickly and effectively. If your vendor can't become a part of your security team, look for another vendor.

This month was a bit different in the SC Labs. Deploying a managed service is quite different from testing an appliance.

Product	Vendor	Our verdict	URL	Rating
Clone Guard Managed IDS/IPS	Clone Systems	Excellent service with a lot of capabilities. We rate this one Recommended.	www.clone-systems.com	SC Magazine Recommended
Managed Protection Service	IBM ISS	A top-notch services suite based on proven technology and infrastructure. We make this one our Best Buy.	www.ibm.com	SC Magazine Best Buy

GroupTest: Fraud prevention

Fraud is a rapidly growing problem for public and private sector organizations of all sizes. Overall operational risk continues to grow at an alarming rate as the fraud component grows. The compounded growth in fraud can be attributed to the ever-increasing levels of sophisticated tools, attacks and methods used to defeat the security infrastructures we have built to identify, alert and remediate this threat. I find more and more organizations struggling to properly deploy technology to combat the risk associated with fraud. Since the threat for fraud can come from the internet as well as from the inside, the risk to your information, customers and shareholders is higher than it has ever been.

Managed security offerings are not new to the industry, but their growth lately cannot be ignored. As organizations have continued to struggle to manage their own security infrastructure, the value of a managed security relationship has evolved. Managed security solutions have evolved to fit just about any need you may encounter, whether your organization is looking to outsource a complete security offering, partner on a solution that it lacks the time or skill set to address in-house, to have a check and balance for compliance and regulatory reasons, or simply to leverage a second set of eyes to complement the in-house team.

We are looking at companies that strive to deliver a security service as a hosted or managed offering. Our criteria was for the offerings to provide a turnkey approach to an organization's primary technical security needs. These could be either a co-located device at the client organization facility or a completely outsourced solution where the application to be protected would reside at the vendor's data center, network operation center (NOC) or security operation center (SOC).

Our usual testing methodology differed this time. Since this review was based on mostly managed service offerings, there were no actual product submissions for us to install and review. Our examinations were a combination of web demonstrations and online studies of live analyst NOC/SOC tools and functionality and client portals to review reporting, alerting, ticketing and remediation activities.

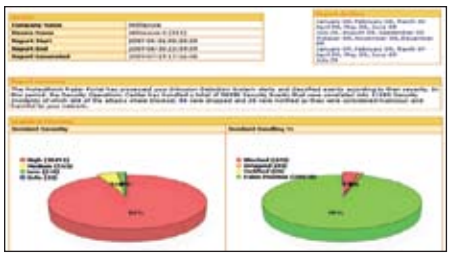
There are numerous managed security offerings available today. Our submissions varied greatly and provided us with a very nice cross-section of the types of services available in the market. We looked at offerings that provide full-service managed security services through fully staffed 7/24/365 security operation centers.

We were pleased with the various web-based user tools and interfaces we saw. The reporting, configuration and alerting functions were easy to use and very powerful.

As we saw from our testing, offerings differ greatly. It is important to fully understand your goals in partnering with a managed service offering. It is also important to remember that this is a partnering arrangement and that your IT and security resources should always be engaged in the day-to-day management of enterprise risk.

As always, our best advice is to do your homework: Research all the options and make the choice that best fits your needs.

Product	Vendor	Our verdict	URL	Rating
ProtectPoint MSS	StillSecure	Very nice full-service managed security offering for organizations that don't have the security expertise on staff. This one gets our Best Buy for the month.	www.stillsecure.com	SC Magazine Best Buy
Managed security services	Trustwave	Great offering for security and compliance management. This one gets our Recommended nod.	www.trustwave.com	SC Magazine Recommended



GroupTest: NAC

Network access control (NAC) tools come in a variety of shapes and sizes. That means that they have different subsets of uses within the greater context of their primary objectives. For example, some NACs are software-only, while some are appliances. Some of the appliances are designed to deliver access control for different-sized enterprises. Many of these are capable of being connected together, feeding a sort of master NAC with data from outlying organizations within the enterprise.

The most important factor affecting your selection is the existing security architecture and infrastructure. While NAC usually can stand alone in a security infrastructure, it works best when tightly coupled to other services within the enterprise.

NAC should be easy to administer. It should have an easily accessible and easy-to-use policy manager, as well as the ability to gather its information from a primary list of authorized users, such as from Active Directory. However, NAC works best when the implementation of the database (Active Directory in this case) is clean. That means organization within groups, for example. Most NACs can take that information and allow individualized controls on a group basis. In addition, many NACs allow even finer-grained control – down to the level of the individual user. An important function for many organizations is the management of non-employees. This can include guests, contractors, consultants, vendors, etc. These users often need access to the internet or, in the case of contract employees, to specific resources inside the enterprise.

What is most important in this case is the control of non-employees without heavy intervention by the administrator. Some NACs allow people other than the administrator to assign visitors to a particular group. This considerably simplifies the generation of credentials.

Another thing to look for in a NAC is how well it ensures that the computer connecting to the enterprise is safe to connect. Options in this regard include virus pre-scanning, and configuration confirmation of the computer attempting to connect.

Finally, as in most enterprise-focused products, scalability is an important issue. In this case, we generally see the ability of the NAC to be distributed. Some NACs, anticipating distribution, have several models that are intended to manage different-sized networks within the enterprise. This not only affects scalability, it improves value for the price of the product, since smaller groups or organizations within the enterprise are not forced to use a product designed (and priced) for a much larger network. This, of course, has the additional benefit of providing NAC for smaller enterprises, such as small businesses that need a high level of access control.

Testing the NAC products this month was quite straightforward. We set up a network with the usual enterprise accoutrements, such as Active Directory, email, DNS, etc. We then installed the NAC under test to attach to our Active Directory. We then went through a suite of operations that exercised the capabilities of the NAC in the context described above.

Product	Vendor	Our verdict	URL	Rating
Veri-NAC Appliance	Black Box	A solid suite of hardcore NAC products with a clear focus on keeping unauthorized systems and users off the network. We give Veri-NAC our Recommended this month.	www.blackbox.com	SC Magazine Recommended
NAC Director	Bradford Networks	Extremely versatile with lots of associated functionality. We designate NAC Director our Best Buy.	www.bradfordnetworks.com	SC Magazine Best Buy

GroupTest: Policy management

Policy management is a challenge for most organizations. It's a formidable duty to periodically review configurations, vulnerabilities, patches, servers, users, network and security rules. Now, imagine that these tasks must be performed in real time, or near real time, to validate the enterprise security posture as it relates to corporate policy. Most corporate governance statements, compliance requirements and various regulatory bodies require us to do this. Fortunately, there are tools to help address this challenge. In this month's review, we are looking at policy management solutions. These products provide the tools for managing, enforcing, auditing and reporting on various security and network system configurations and patch levels.

For this review, we looked for products used to enforce configuration policies of devices in an enterprise. This could include, but was not limited to, network configuration, security configurations, encryption configuration, or software configuration, as well as hardware configuration of any devices in the enterprise. By our definition, these products should be able to audit devices against a policy created by an administrator, as well as provide the ability to make policy changes to devices in the enterprise from a centralized console. These solutions were also required to address compliance management. Additionally, we looked for centralized management capabilities, support for compliance reporting, optional risk management capabilities, and centralized auditing, alerting and reporting.

Our testing methodology for this month's Group Test used vendor-provided, web-based access to their systems. Vendors were allowed to run through a short presentation on the company, product features and value proposition and to describe the implementation process that a typical end-user would experience. We then ran through a full demonstration of the products using our usual evaluation criteria: ease of use, features and functionality, reporting and alerting, documentation and support.

We asked the participants to not only demonstrate the features and capabilities of the offering, but to also run through a typical deployment scenario. The solutions reviewed consisted of client-side software deployments, appliance-based solutions and combinations of both.

We reviewed solutions that focused on the security products (i.e., firewalls, IDS/IPS systems), others that were endpoint-focused, and some that spanned across security, network and endpoint products. Some were very good at managing the assets, as well as the vulnerabilities and patches on that particular asset. Others had very nice compliance- and risk-reporting capabilities. Others addressed the challenge of managing large numbers of security and network systems and synchronizing the configurations of each as policy changed.

Although these tools offer a great service, before choosing a vendor it is important to consider the impact these services will have on your environment. Most solutions are agent-based and require some level of overhead on endpoint resources and network infrastructures.

Product	Vendor	Our verdict	URL	Rating
Firewall Analyzer v5.1, plus	AlgoSec	Great enterprise solution; It may be pricey for smaller organizations.	www.algosec.com	SC Magazine Recommended
Kaseya 6	Kaseya	A strong endpoint management solution. Although it appears pricey, the price is reasonable based on the functionality delivered.	www.kaseya.com	SC Magazine Best Buy