



Comprehensive System Security Management - Eliminating rogue systems

A Datamonitor research paper commissioned by
McAfee

IT security has been a major concern for CIOs now for a number of years, leading to heavy investment in a number of IT security systems such as firewalls, anti-virus and intrusion prevention. These systems, however, are only effective to a certain degree and a comprehensive system security management strategy is needed to ensure that rogue systems are dealt with and that a heterogeneous environment can be cost-effectively managed.

Publication Date: November 2004

www.datamonitor.com

Datamonitor Europe
Charles House
108-110 Finchley Road
London NW3 5JJ
United Kingdom

t: +44 20 7675 7000
f: +44 20 7675 7500
e: eurinfo@datamonitor.com

Datamonitor USA
245 Fifth Avenue
4th Floor
New York, NY 10016
USA

t: +1 212 686 7400
f: +1 212 686 2626
e: usinfo@datamonitor.com

Datamonitor Germany
Kastor & Pollux
Platz der Einheit 1
60327 Frankfurt
Deutschland

t: +49 69 9750 3119
f: +49 69 9750 3320
e: deinfo@datamonitor.com

Datamonitor Asia Pacific
Room 2413-18, 24/F
Shui On Centre
6-8 Harbour Road
Hong Kong

t: +852 2520 1177
f: +852 2520 1165
e: hkinfo@datamonitor.com

Datamonitor Japan
Aoyama Palacio Tower 11F
3-6-7 Kita Aoyama
Minato-ku
Tokyo 107 0061
Japan

t: +813 5778 7532
f: +813 5778 7537
e: jpinfo@datamonitor.com

ABOUT DATAMONITOR

Datamonitor plc is a premium business information company specializing in industry analysis. We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt, Hong Kong and Japan.

ABOUT THE AUTHOR

Ian Williams has been an analyst with Datamonitor for almost six years, covering the networking and IT security markets. He is currently the program manager of Datamonitor's global Enterprise Security Strategic Planning Program (SPP).

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Datamonitor plc.

Eliminating rogue systems

© Datamonitor (Published 11/2004)

Page 2

INTRODUCTION

It is impossible to open an IT magazine today without seeing a reference to the importance of IT security. Surveys consistently report that IT security remains a principal concern among CIOs. The rising number of security breaches have led to a strong investment by many organizations in IT security systems such as anti-virus, firewalls and intrusion prevention. In 2003 alone, Datamonitor estimates that global businesses spent approximately \$8.3bn on such products. Much of this investment has been, however, uncoordinated and haphazard, with customers rarely buying all of their security products from a single vendor – instead favouring the ‘best-of-breed’ approach.

Mergers and acquisitions further compound the problem – creating a vast, complicated and typically heterogeneous infrastructure needs to be effectively managed. To do this properly, however, can be an expensive, time-consuming business. Most organizations don’t have the resources to effectively manage their system security or monitor for other potential dangers such as rogue systems. The aim of this document is to highlight the danger that ignoring the need for effective system security management brings and to implore the reader to take such threats more seriously.

In order to understand the scale of the dual issues of rogue systems and managing a heterogeneous environment, Datamonitor conducted a survey of 246 European organizations in August 2004. The aim of the survey was to not only examine system security strategies but also determine how many organizations were affected by rogue systems, to identify the damage they cause and discover whether organizations were moving to eliminate such threats. Finally, the survey looked to establish whether organizations source their security solutions from a single vendor – so as to determine the heterogeneity of their security architectures.

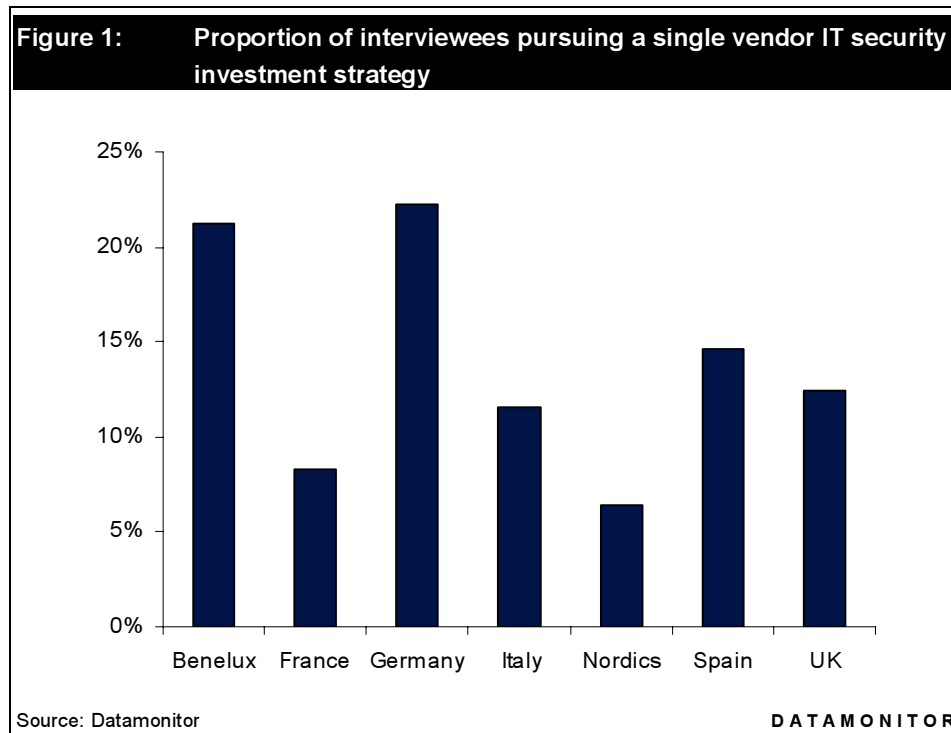
THE NEED FOR EFFECTIVE SYSTEM SECURITY MANAGEMENT

The growing concern for IT security among businesses worldwide has led to a strong uptake of IT system security such as anti-virus software, intrusion prevention, firewalls and identity management solutions. Research conducted for this paper revealed that this year, organizations will spend approximately 4% of their overall IT budgets on IT security, of which around 40% will be spent on IT security hardware and software solutions. Because organizations have been investing in IT security

products for a number of years, it is not uncommon for them to have built a comprehensive IT security architecture, consisting of solutions at the gateway level, between different sub-networks and on servers and desktops.

Those observing the security market for a number of years, such as Datamonitor, have noted that very few organizations buy all of their IT security solutions from a single vendor – even though there are a number of vendors positioning themselves as a single source of firewall, anti-virus and intrusion prevention technologies (among others). The research conducted for this paper reveals that within Europe, only 14% of organizations pursue a single vendor strategy for desktop, laptop and server security. One of the main reasons why this has occurred is the desire to buy the best-of-breed technology for each product set.

This has not only been the case for different security technologies but for where they are deployed: so a customer may deploy a different brand of anti-virus at the desktop to that at the server level. In some cases, organizations even deliberately deploy security solutions from more than one vendor to solve the same issue – for example deploying more than one brand of anti-virus at the gateway level. The idea is that if one solution misses a particular virus, the other brand may pick it up – therefore greatly reducing the chance of infection.



From the customers perspective such strategies aim to increase the level of protection and ensure that each technology deployment is the best technology on the market in the client's eyes. The network environment can become heterogeneous in other ways too. Mergers and acquisitions, for example, bring together two systems that have evolved at completely different stages and will, in all likelihood, consist of completely different technologies. Very few organizations can afford to harmonize the network environments by standardizing on technologies and accept that they will have to work instead within a multi-vendor environment.

The problems of deploying a heterogeneous architecture

There are a number of problems, however, that operating with a heterogeneous architecture brings. Typically, the biggest trade-off for a customer choosing a best-of-breed approach over a single solutions-source is management. Most vendors deploy common management interfaces for all of the technologies within their product families making them easier to centrally manage. In a heterogeneous environment, each device will need to be configured and monitored on an individual basis. This can be an enormous drain on IT resources because staff need to be trained to understand each management interface and will be unable to carry out configuration changes and monitoring on a product-by-product.

By stretching the IT resources even further, security lapses become commonplace. Staff simply do not have the time to effectively monitor all of the security alerts generated by each device alone and therefore incidents may slip through the net. For you the customer this can be a no-win situation. Either you effectively monitor each device, which is expensive – particularly as this needs to be carried out on a 24 hour a day, 7 day a week basis or you do the best you can with limited resources. If this is the case, you must understand the trade-off in terms of security.

Third party security management solutions

There are, luckily, a number of options available to customers looking to deploy best-of-breed solutions and yet centralize their system security management. One option is outsourcing. Today, a number of managed security solution providers offer customers the option of outsourcing the management of their security architectures. Many customers, however, are not comfortable with outsourcing because often these solutions only solve half the problem. When dealing with a security incident, a decision needs to be taken that may affect business operations such as closing ports

or taking a server offline. Because they are unlikely to understand the business implications of such decisions, third parties are rarely trusted with such responsibilities.

This state of affairs typically reduces the role of the third-party to that of simply monitoring the architecture and alerting the client to potential problems. This can reduce the burden of security management to some degree but still requires a significant amount of client interaction. An alternative option is a third party software solution with the ability to monitor a number of systems from the main security vendors. This gives you the benefits of centralizing security system management in terms of reduced cost and more effective monitoring, while retaining in-house security decision-making.

Other system security management concerns

System security management, of course, is more than just monitoring the devices to ensure that they are working, are up-to-date and that their alerts are considered. There are a number of other tasks that must be carried out by security administrators. These include:

- **Patch management.** Most worms and viruses today exploit vulnerabilities with systems that would be safe if the appropriate patches were applied. The widespread chaos caused by such malware indicates that many of the patching programs today are woefully inadequate. In today's hostile Internet environment, a comprehensive patch management program is a prerequisite.
- **Security policy enforcement.** Your security policy effectively sets out your aims as a secure on-demand business – detailing how you believe you can best protect your system. Not only must this policy be regularly updated as your business changes but it must also be regularly monitored to ensure that violations are swiftly dealt with.
- **Eliminating rogue systems.** Enforcing your security policies on your own devices can be difficult enough. 'Rogue systems' such as employee-owned laptops and PDAs, which are beyond the administrative control of your IT department, may be introduced into the network environment, however, creating a potential threat in terms of malware spread. Clearly, steps must be taken to control or prevent their introduction.

THE PROBLEM OF ROGUE SYSTEMS

One of the critical problems highlighted by an ineffective security management problem is the infiltration of rogue 'systems'. Datamonitor defines rogue systems as unidentified, unaccounted for and unmanaged systems with access to the corporate network, including desktops, laptops and other mobile devices. The main problem with such systems is that they will typically not conform to the policies laid down in the organizations security policy and, more importantly, that they may not have deployed the same levels of endpoint security as sanctioned devices. The penetration of anti-virus and personal firewall technologies among consumers is very low and as a result the possibility of virus or worm infection is high. Once these systems are connected to the network, the whole system itself can be infected.

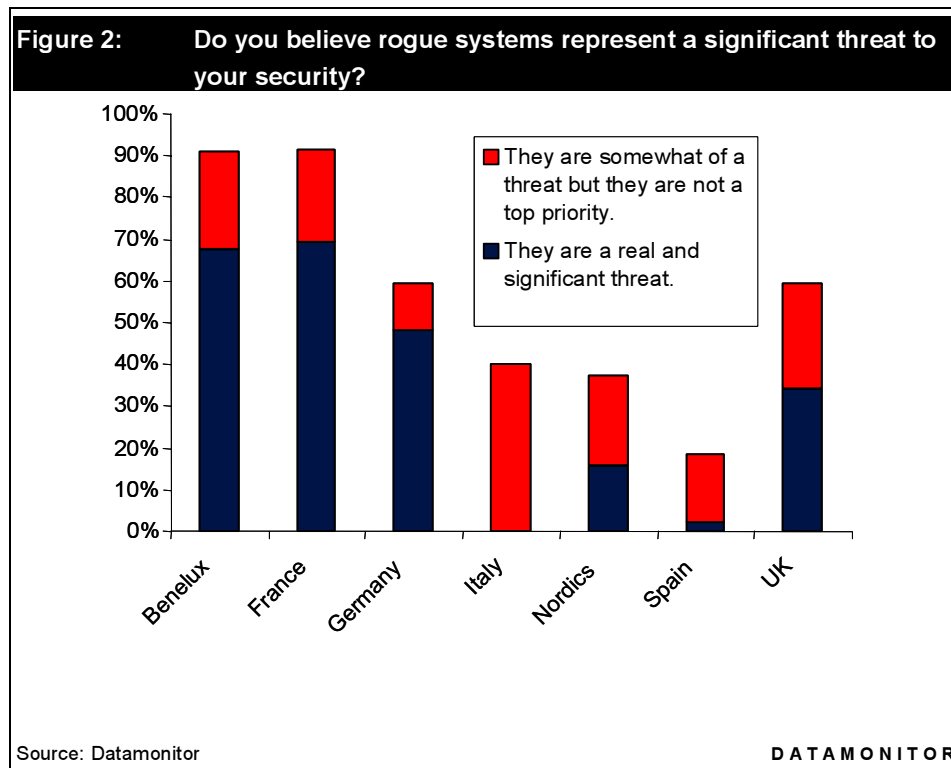
There are a number of ways in which these rogue systems can arise:

- **Employees.** As your employees become accustomed to using IT devices at work such as laptops and PDAs and start using these solutions for work purposes, it is inevitable that many will bring these mobile devices into work and connect them to the network. Because your IT department has no control over these elements, they are unable to insist on comparable levels of security on such devices.
- **Contractors.** When an organization hires third parties such as consultants or workmen it is not uncommon for them to bring their own IT equipment with them to connect with the networks of their employers. Unless these contractors have the same security concerns as your organization you could be exposing your network to malware infection.
- **Wireless LAN war driving.** Penetration rates of wireless LANs among medium sized European organizations reached 31% in 2003 and 44% among large organizations. Unless the appropriate security measures have been taken it can be easy for unauthorized users to access system resources and potentially spread viruses or steal Internet bandwidth.
- **Other visitors.** Often when partners or customers visit your offices they may wish to do some of their work when not busy. As a courtesy, they may even be allowed to access to the corporate network to allow them to browse the Internet. Again, there are no guarantees that your visitors take IT security as seriously as you and the risk of infection increases dramatically.

- **Forgotten legacies.** Not all of the 'rogue systems' within your network may be introduced from the outside. Among large organizations it is not uncommon for systems to be "forgotten" when security audits are carried out and as a result they may not have up-to-date anti-virus pattern information. This leaves these systems in serious danger of infection that would be prevented the latest anti-virus systems.

Are rogue systems a threat?

The research conducted by Datamonitor for this paper indicates that the existence of rogue systems within an organization is commonplace – with 86% of the interviewees stating that they knew 'rogue systems' were present within their systems. This was a common experience across Europe with 100% of French organizations, 97% of organizations within the Benelux region and 91% of organizations within the UK acknowledging their presence. Many organizations have indicated that they also recognize the potential threats of these systems in terms of a source of malware or data theft.



One of the prime reasons why organizations feel that rogue systems are a significant threat is because they are source of infection. While corporations may spend thousands of Euros filtering their emails for viruses, home users are rarely as diligent. An employee may unwittingly download a virus at home to their laptop and may then wish to copy a resource from the corporate network onto their own PC.

As soon as the laptop reaches the network it can seriously expose that environment to infection. Of the interviewees that admitted they had rogue systems, 46% stated that rogue systems had been a source of infection, with some reporting that this accounted for more than 50% of their infections over the last 12 months.

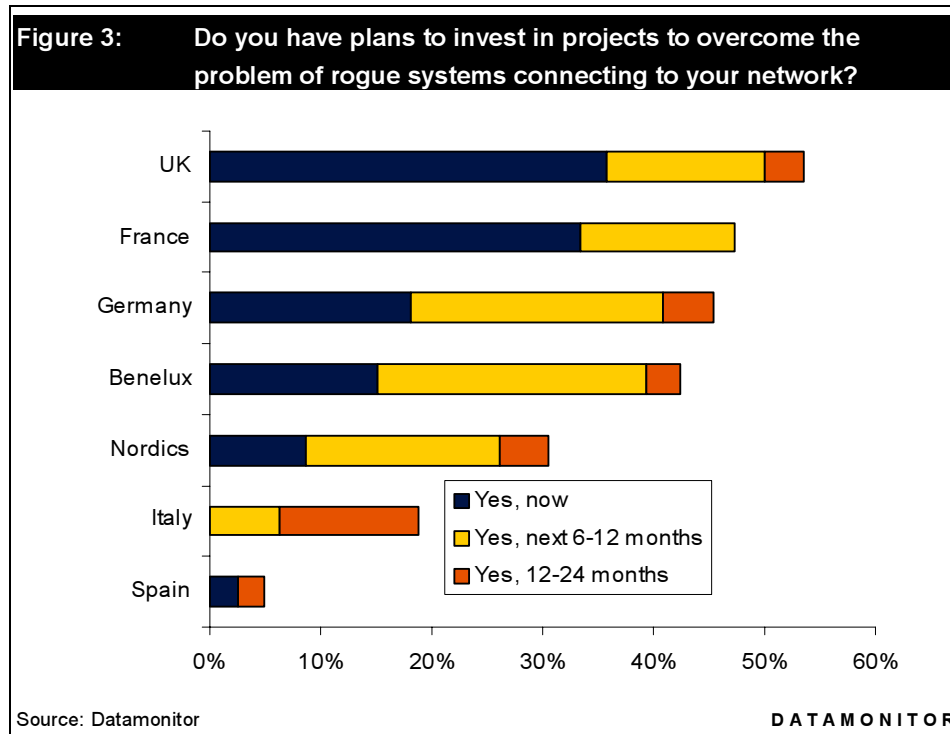
Dealing with rogue systems

While some organizations may not have considered that the presence of such systems to be a threat, those organizations that claim to take security seriously must surely recognize the potential threat that unmanaged systems represent. The 2004 DTI security breaches survey revealed that on average each security incident costs around €45,000 and that it only takes a single incident to cause widespread devastation.

Clearly, the best way to deal with 'rogue systems' is to invest in solutions that monitor the network for their presence, allowing administrators to take the appropriate action. This can include:

- **Preventing access.** IT departments often have enough to worry about with their own systems without having to worry about dealing with other peoples. As a result some organizations have policy banning all unauthorized devices from the network.
- **Restricting access.** In some cases there is a legitimate reason why a system may not have the latest anti-virus patterns – for example if the owner has been away for a period of time. As a result, it is often wise to limit network access to the system but allow the laptop to update the anti-virus patterns. Once the device meets the security policy again, unfettered access can be restored.

Datamonitor believes that applying both principles is the best way to achieve a happy medium of access and security – depending on the organization's security policy.



Sadly, Datamonitor's research reveals that few companies plan to take the necessary measures to prevent such a threat – with on average only 17% in the process of doing so. Additionally, 66% have admitted that they currently have no plans to deploy the relevant countermeasures. The UK emerged as the market with the greatest will to invest in the appropriate technologies to prevent rogue system access but even here only 36% of the interviewees were in the process of addressing the problem. Datamonitor believes that the reliance of modern organizations on their IT systems means that they can no longer be so complacent about IT security.

The reason why such systems are a problem is because there is no way for an organization to enforce its security policy on such devices. The bare minimum for any effective malware control policy is to ensure that all devices connecting to the corporate network have anti-virus and that the anti-virus solution in question has the latest anti-virus patterns. If this is not the case and given the prevalence of viruses and worms today, it is only a matter of time before your system becomes infected - making a mockery of the thousands of Euros invested by organizations on anti-virus systems.

The business impact of worms and viruses

Datamonitor firmly believes that the increasing reliance on IT systems by organizations to support their business processes necessitates a high degree of resiliency within these systems – creating a stronger argument for the deployment of IT security mechanisms to protect systems. Those organizations that need convincing need only look at the devastation caused by the Sasser worm, which hit earlier this year, causing widespread devastation.

The Australian press, for example, reported that 300,000 rail travellers in New South Wales were left stranded as a result of a computer outage on the railway system that lasted several hours before being rectified. The virus has also been confirmed as the source of extensive outages in banking systems operated out of post offices in Taiwan. About a third of branches were affected. Other prominent organizations affected include a major American airline (who had to cancel or reschedule several flights), the European Union Headquarters and several Spanish courthouses.

Even the threat of the worm caused problems – with a large Finnish bank, reportedly closing down 130 branches for a few hours out of fear of being infected by the worm, to give technicians time to apply patches to its systems. Those organizations that do not take such threats seriously will inevitably fall foul of such a calamity themselves and Datamonitor urges those businesses that rely on their IT infrastructure to do more to protect their mission-critical systems. Given that this is the vast majority of organizations in Europe today, immediate action needs to be taken.

McAfee ePolicy orchestrator

One third-party management solution available on the market that aims to assist administrators with many of the issues highlighted by this paper is McAfee, Inc.'s ePolicy Orchestrator administration solution. While Datamonitor does not endorse vendor products, it acknowledges that ePolicy Orchestrator release 3.5 has a number of features that can greatly aid administrators when dealing with the many of the security problems highlighted by the results of the research. These include:

- **Third party security solution management.** Because of the heterogeneous nature of many security architectures, a centralized security management solution must be able to manage multi-vendor environments. ePolicy Orchestrator 3.5 tackles this problem within the anti-virus space by managing and reporting on both McAfee and Symantec anti-virus solutions as well as McAfee system firewalls, anti-spyware, anti-spam, content filtering, host-based intrusion prevention systems (IPS) and Microsoft patch assessment.

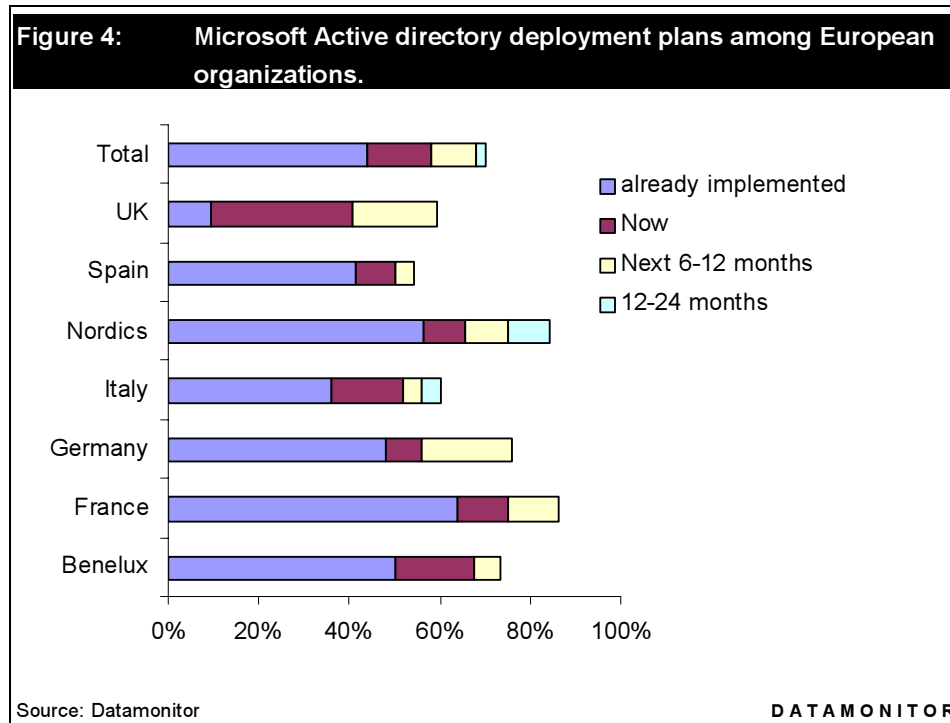
- **Allowing an administrator to manage rogue systems.** The existence of 'rogue systems' on a network can be a serious security concern and your administrators should aim to ensure that such systems are prevented from connecting to the network in compliance with your organization's security policy. McAfee ePO takes a unique approach to mitigating the risk of rogue, non-compliant systems by passively monitoring the network for any LAN-based connections and quickly establishing whether they are currently managed by ePO. ePO then provides a range of policy based responses to these rogue systems. By rapidly identifying unmanaged systems, administrators are empowered to mitigate the weakness of rogue, non-compliant systems.
- **Rapid policy update.** Within a large and complex system there may be a vast number of security solutions that need constantly updating. Updating these agents cannot only be time-consuming but can also place an enormous burden on the network in terms of bandwidth consumption. Using a system of 'super agents' to distribute the workload, ePO spreads the updating tasks throughout the network, avoiding bandwidth drain while ensuring that the relevant security elements are up-to-date.
- **Monitor System Security 24 by 7.** ePO's integrated notification services and graphical reporting provides the 24 hour a day, 7 day a week visibility required to effectively monitor system security, evaluate your policy's status and find your network's weak points. Instant, proactive information is critical for a security professional especially when monitoring compliance and threat activity. ePO delivers integrated alerting and notification on compliance, threat activity and rogue systems. Thresholds, defined by the administrator, will enable critical alerts to be sent to specified individuals via email, SMS, text pager or SNMP trap. Alerts cover threat activity, anti-virus compliance levels and rogue system detections.
- **Enhanced reporting.** Furthermore, ePO can help locate non-compliant systems, trace outbreaks to their source, or determine the effectiveness of security policies via ePO's array of over forty pre-defined reports. These reports can range from one-page, executive security summaries to detailed information on threat activity, system security policy across anti-virus, desktop firewall and host-based intrusion prevention, system vulnerabilities, and spam and content filtering policies depending on the level of granularity you need. Reports can also be customized to meet a customer's specific needs. Administrators may select from a variety of printable and exportable chart types including three-dimensional bar charts, pie charts, line graphs, and tables. Additionally, McAfee ePO is integrated with Seagate Crystal Reports technology and Microsoft's MSDE/SQL server that

Comprehensive System Security Management - Eliminating rogue systems



McAfee believes provides a balance of simplicity and power that suits every size of company.

- **Leverage existing infrastructure investments.** One burden imposed by most administration solutions is the need to recreate information that may already be held within systems previously installed by the client. Because ePolicy orchestrator 3.5 integrates with Microsoft's Active Directory, clients with this technology can import information directly into the ePO directory and even mirror existing AD groupings. Microsoft's Active Directory is the most widely deployed directory solution on the market today and as the research below demonstrates, will have been deployed by 68% of European organizations within the next 12 months.



System security management is a complex and time consuming process but it is also imperative the organizations take it seriously if they hope to protect their systems effectively. Because of the burden this imposes in terms of manpower, Datamonitor believes that a third-party system security management solution, such as ePolicy Orchestrator 3.5, is the only effective means of avoiding the trade-off between cost and security and allowing organizations to eliminate the threats posed by rogue systems.

CONCLUSIONS

The research conducted for this white paper has indicated that there are a number of important system security management challenges that European organizations must address if they are to improve their system security. These are:

- Only 14% pursue a single vendor purchasing strategy when buying IT security solutions.
- 86% of the organizations interviewed acknowledge the presence of 'rogue systems' within their networks. Further more, of these organizations, 64% acknowledge that they represent a threat to their system security.
- This finding is backed up by the fact that for 42% of the respondents, rogue systems have been a source of malware infection within the last 12 months. This figure is likely to be much higher because many respondents refused to submit an answer because of the sensitive nature of the question.
- Despite this, only 17% of the organizations interviewed are doing something about the problem and within 12 months this will only have risen to 31%.

The results of the survey are clear – rogue systems pose a serious threat to your organization but not enough administrators are taking the threat seriously. The evidence from both the DTI in the United Kingdom, the FBI and Computer Security Institute and countless other surveys is that viruses and worms cost global business billions of Euros a year. If you don't want your organization to be part of these statistics you must act intelligently to minimize the threat,

A call to action

Datamonitor believes there are 3 key action points for readers of this white paper.

Take system security management seriously

No security solution can be added to a security architecture and then autonomously protect your systems effectively. IT security solutions must be constantly updated and reconfigured to both support business requirements and thwart the latest threats. They also generate alerts that typically require an administrator response. Unless these functions are centralized and coordinated some devices are likely to be missed completely because the cost of maintaining each device is likely to be prohibitive.

Failing to do so, however, could lead to a serious virus or worm infection that could cripple your systems and cost thousands of Euros in terms of loss of productivity and clean-up costs.

Act now to eliminate the threat posed by rogue systems

Datamonitor accepts that there are a number of IT investment priorities that must be budgeted for in terms of Euros spent and IT staff time but believes that because IT systems have become such an important part of an organizations operations in terms of supporting its business processes, everything must be done to maximise uptime and avoid data loss and corruption. Malware is a common threat to all organizations and Datamonitor believes that by eliminating rogue systems, the effectiveness of your existing virus prevention measures will increase dramatically.

Evaluate third-party system security management solutions

The only way to centralize security management functions in-house is to invest in a security management solution. Because most organizations operate a heterogeneous security architecture, the solution selected must be able to receive alerts from and be able to assist in the configuration of as wide a number of systems as possible. Such a solution will allow you to continue to enjoy the peace of mind that a best-of-breed purchasing strategy creates without the resulting security management headaches. Ideally such a solution will perform a number of security functions including improved patch management and prioritization, greater policy enforcement and the ability to detect and eliminate rogue system access.