



Systems and Security Management: A Survey of Mid-market Organizational Readiness

■ INTRODUCTION

The complexity of managing end-node (desktop and laptop) computers has skyrocketed, security breaches pose ever greater threats to businesses, and IT organizations are continually under pressure to keep costs down and service levels up. There are a plethora of tools available that claim to help IT departments with these challenges, so much so that learning and using these tools effectively has become a major challenge for IT organizations – particularly those in mid-sized companies with limited staffing resources.

The following report is based on a survey of IT professionals conducted in February 2007. The goal of the survey was to gather data on their approach to unifying systems and security management including the perceived need for integrated end-node systems and security management, types of management tools in use, the current state of security readiness, and the personal consequences of security issues.

■ SUMMARY OF FINDINGS

- The majority of mid-market IT professionals, 73%, are concerned that they may lose their job in the event of a major security breach.
- 62% of participants who are personally responsible for IT security report that responsibility for affects them in a personal way by causing them to worry about security issues outside working hours, giving up personal time to deal with security issues, or both.
- Systems management activities are applied inconsistently in the security strategies of most mid-market companies. Only 35% of participants included end-node vulnerability scanning, although 81% included patch management as part of their security strategy.
- Most IT organizations, 87%, are confident in their ability to deal with viruses, spam, spyware and malware, but very few, 35%, feel they are equipped to deal with lost corporate or personal data.
- Mid-market IT organizations report a large number of disparate user-interfaces (six on average) in use for systems and security management which creates challenges in learning and using the tools effectively.
- Use of an integrated end-node systems and security management tool is perceived as useful by mid-market IT teams, with 69% of participants citing increased efficiency as the most important benefit.

■ Mid-market IT professionals believe a security breach may cost them their jobs

Participants at mid-market companies who have responsibility for security were asked if they were concerned that they might lose their job in the event of a major IT security breach. 73% reported that they would be concerned about losing their job (**Figure A**).

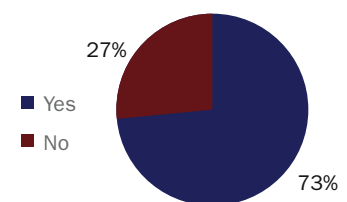


Figure A: Concern About Job Loss in the Event of Major Security Breach

Security responsibility appears to have a personal impact. Among those who have ownership for IT security, 62% report that this responsibility affects their personal time either by causing them to worry about security issues during personal time, giving up personal time to deal with security issues, or both.



Systems and Security Management: A Survey of Mid-market Organizational Readiness

■ LACK OF END-NODE VULNERABILITY SCANNING A WEAKNESS IN SECURITY STRATEGIES

Participants were asked about the activities that are directly considered to be part of their organization's security strategy. While anti-virus software and firewalls were ubiquitous among mid-market participants, automated desktop configuration was reported for only half (50%) of the security strategies of participants and about one third (35%) of participants included end-node vulnerability scanning (**Figure B**).

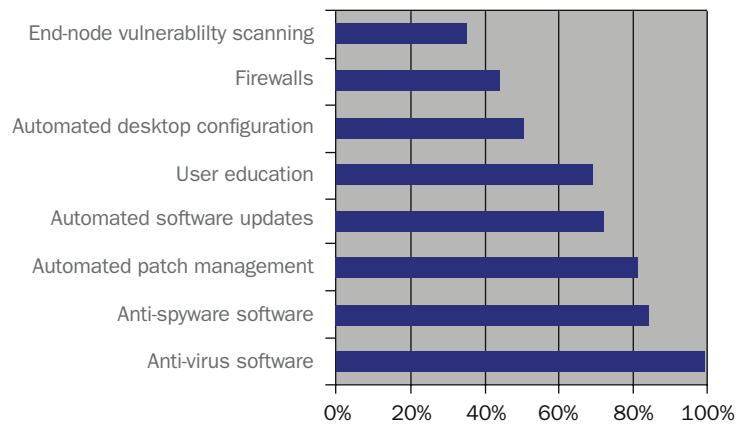


Figure B: Security Activities

■ IT SECURITY TEAMS READY FOR VIRUSES, BUT NOT THEFT

Participants were asked about their readiness for potential security issues including:

- Stolen equipment resulting in lost corporate or personal data (i.e. stolen laptop)
- Mis-configured systems (i.e. a user modifies their browser security settings)
- Viruses, spam, spyware, and malware.

Participants from mid-market companies are generally confident about their ability to deal with viruses, spam, spyware, and malware with 87% reporting that they were properly equipped to handle these issues. However, only 35% of participants reported that they are equipped to manage the security and intellectual property risks associated with stolen equipment. See **Figure C** for more detail.

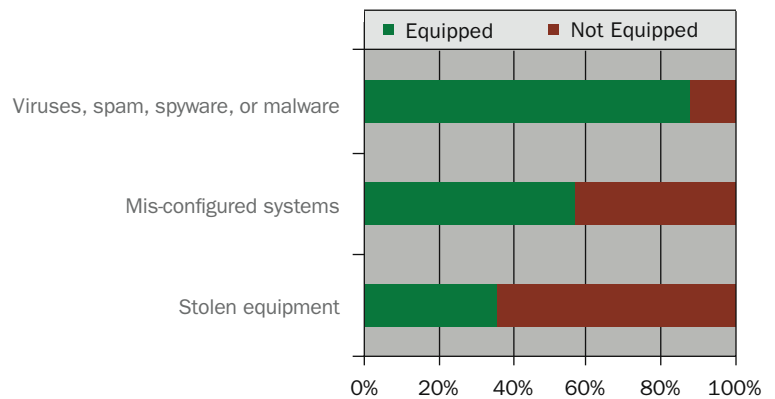


Figure C: Readiness to Deal with Security Risks



Systems and Security Management: A Survey of Mid-market Organizational Readiness

LEARNING TO USE MULTIPLE APPLICATIONS CITED AS GREATEST CHALLENGE WHEN DEALING WITH RANGE OF SYSTEMS AND SECURITY MANAGEMENT TOOLS

Participants were asked about the number of disparate tools they used for systems and security management, firewalls, anti-spyware, anti-malware, anti-spam, patch management, and configuration management in order to discover how many unique and different user interfaces IT organizations were using among this variety of tools. According to the responses of participants from mid-size companies, IT teams are, on average, required to access six different product interfaces to manage their desktops and laptops.

Participants were asked about the greatest challenge when using these multiple product interfaces. The most frequently cited challenge (47%) was learning to use the different applications effectively. See **Figure D** for a detailed breakdown of responses.

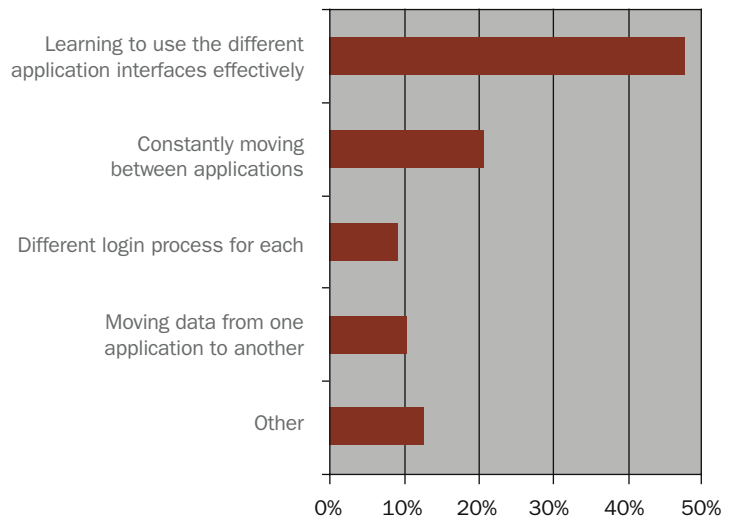


Figure D: Greatest Challenge of Working With Disparate Toolsets

INCREASED EFFICIENCY CITED AS GREATEST BENEFIT OF FEWER PRODUCT INTERFACES

When asked about the most important benefit to consolidating the number of user interfaces for end-node systems and security management, participants consistently identified increased efficiency with 69% of participants from mid-size companies citing it as the most important benefit (**Figure E**). Other benefits of fewer product interfaces reported by participants include:

- Greater quality of service as a result of faster resolution times
- Improved security
- Ease of use
- Consistency
- Decreased costs

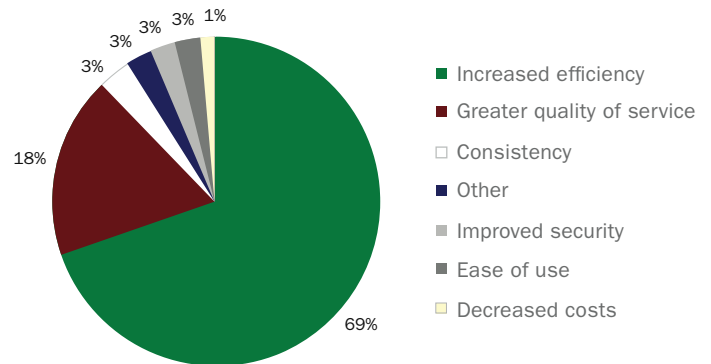


Figure E: Benefit of Fewer Product Interfaces

Clearly these benefits are compelling to IT teams. 61% of all participants from mid-market companies who had five or more product interfaces for systems and security management reported that they have made a product purchase specifically to minimize the number of product interfaces their staff was required to use for systems and security management.



Systems and Security Management: A Survey of Mid-market Organizational Readiness

■ PARTICIPANT PROFILE

A total of 256 participants completed the survey, with 156 of those from mid-market companies. Each participant had some responsibility for managing their organization's desktops and laptops with a portion having multiple areas of responsibility. See **Figure F** for a detailed breakdown.

I am a hands-on systems administrator	38%
I manage a team of systems administrators	32%
I have business responsibility for our systems	34%
Other	13%

Figure F: Role in Managing Desktops and Laptops

Among participants there was a wide adoption of tools for end-node management tasks, particularly with systems and security management tools and anti-spyware, anti-malware, or anti-virus software. See **Figure G** for a detailed breakdown.

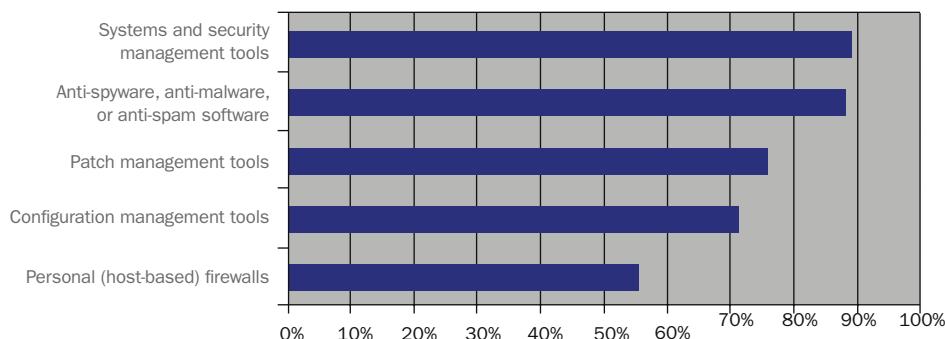


Figure G: Use of Desktop and Laptop Management Tools

■ SURVEY METHODOLOGY

An independent database of IT professionals responsible for systems and security management was emailed and invited to participate in the survey. A total of 256 respondents completed the survey. Of those, 156 respondents worked at mid-sized companies, with anywhere from 100 to 5000 employees. The survey was conducted using Zoomerang, an online survey tool. Respondents were not compensated for participating in this survey but were offered a copy of the final report. This survey was sponsored by KACE, a provider of IT automation appliances. This sponsor was not revealed to participants.

■ ABOUT KING RESEARCH

King Research provides marketing research and consulting services in the high-tech and enterprise computing markets using proven research methodology combined with in-depth technical expertise. Our projects result in our clients gaining a clear understanding of opportunities, priorities, perceptions, motivations and requirements in markets in which they wish to build their business. For more information see www.kingres.com.

■ ABOUT KACE

KACE™, a privately held technology company, is the leader in IT automation appliances. The KBOX™ family of appliances deliver easy-to-use, comprehensive IT automation that is affordable and really work. The KBOX 1000 Series Systems Management Appliances automate routine and complex IT maintenance tasks for end-point nodes on a network. The KBOX 2000 Series Systems Deployment Appliances provide centralized provisioning and remote system recovery.