

Research Report

Abstract:

The Endpoint Security Paradox

*By Jon Oltsik, Senior Principal Analyst and Bill Lundell, Senior Research Analyst
With Jennifer Gahm, Senior Project Manager and Kyle Prigmore, Associate Analyst*

January 2015

Introduction

Research Objectives

In order to accurately assess organizations' endpoint security technologies, policies, and processes, ESG surveyed 340 IT and information security professionals representing large midmarket (500 to 999 employees) and enterprise-class (1,000 employees or more) organizations in North America. All respondents were responsible for evaluating, purchasing, and managing endpoint security technology products and services.

The survey was designed to answer the following questions about:

- Endpoint security knowledge and opinions
 - Do IT organizations believe that endpoint security is becoming more difficult? If so, why?
 - What is driving endpoint security strategy?
 - What are the biggest endpoint security challenges for organizations?
- The organization(s) responsible for endpoint security
 - Do organizations have the right skills and staff levels to address endpoint security?
 - Which groups are responsible for endpoint security today? Are they merging with different groups, or becoming more independent? Do these groups communicate well?
- Endpoint security technologies
 - What types of security controls and technologies are used today? How are these changing?
 - How are organizations adopting specific types of security technologies such as endpoint forensics, endpoint analytics, and advanced anti-malware products?
 - What are the most compelling features of these products?
- AV/host-based security software sentiment
- "Next-generation" endpoint security software sentiment
- Endpoint security strategies
 - Are organizations looking at endpoint security with a long-term perspective? Or are they making tactical purchases to solve immediate problems?
 - Are customers trying to integrate their endpoint security with other things, such as their network security solutions or threat intelligence feeds?

Survey participants represented a wide range of industries including financial services, manufacturing, retail, business services, communications and media, and government. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and information security professionals from private- and public-sector organizations in North America (United States and Canada) between September 10, 2014 and September 22, 2014. To qualify for this survey, respondents were required to be IT professionals directly involved in evaluating, purchasing, and managing endpoint security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 340 IT and information security professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

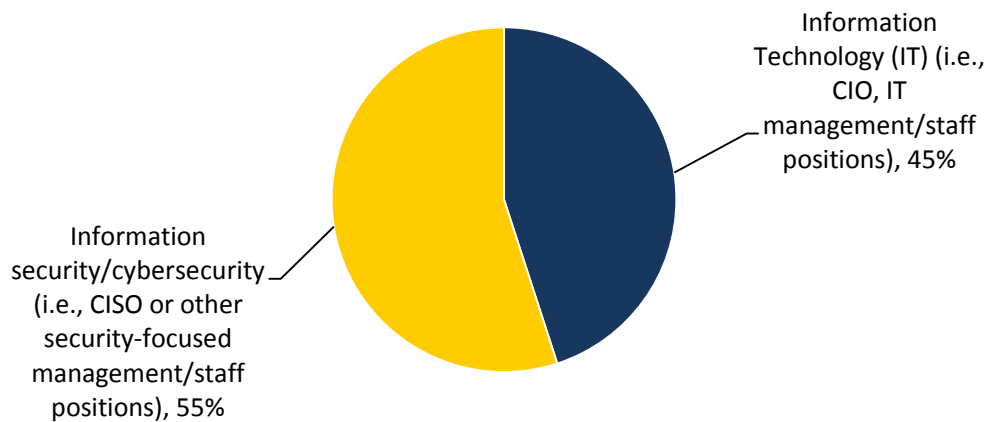
The data presented in this report is based on a survey of 340 qualified respondents. Figures 41-44 detail the demographics of the respondent base, including individual respondents' current job function, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Respondents by Current Job Function

Respondents' current job function within their organizations is shown in Figure 1.

Figure 1. Survey Respondents by Current Job Function

Which of the following best describes your current job function? (Percent of respondents, N=340)



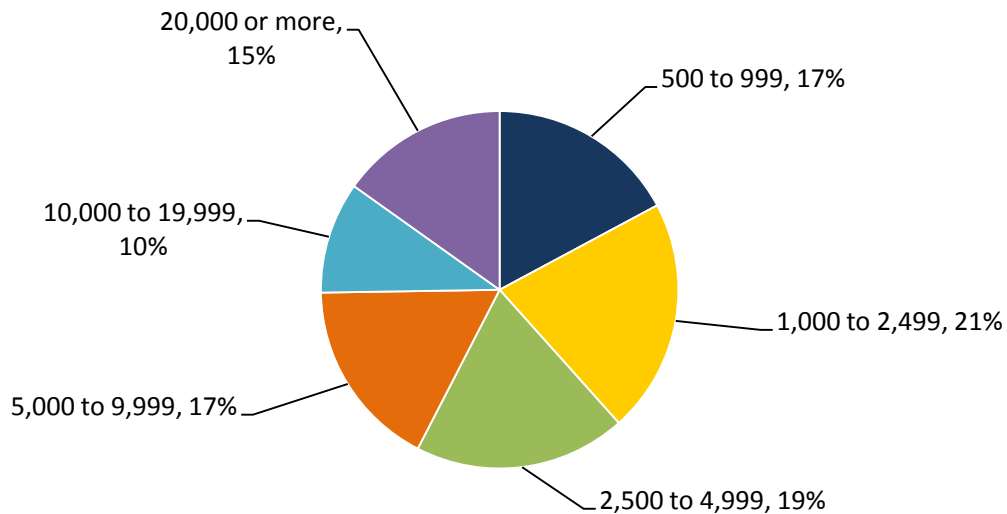
Source: Enterprise Strategy Group, 2015.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 2.

Figure 2. Survey Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of respondents, N=340)



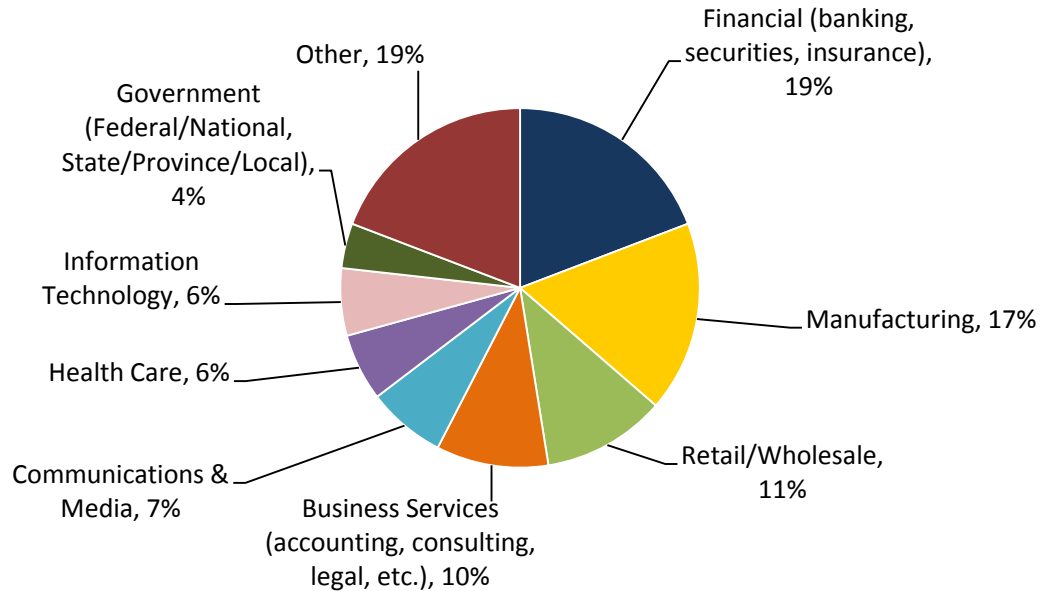
Source: Enterprise Strategy Group, 2015.

Respondents by Industry

Respondents were asked to identify their organizations' primary industry. In total, ESG received completed, qualified respondents from individuals in 20 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 3.

Figure 3. Survey Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=340)



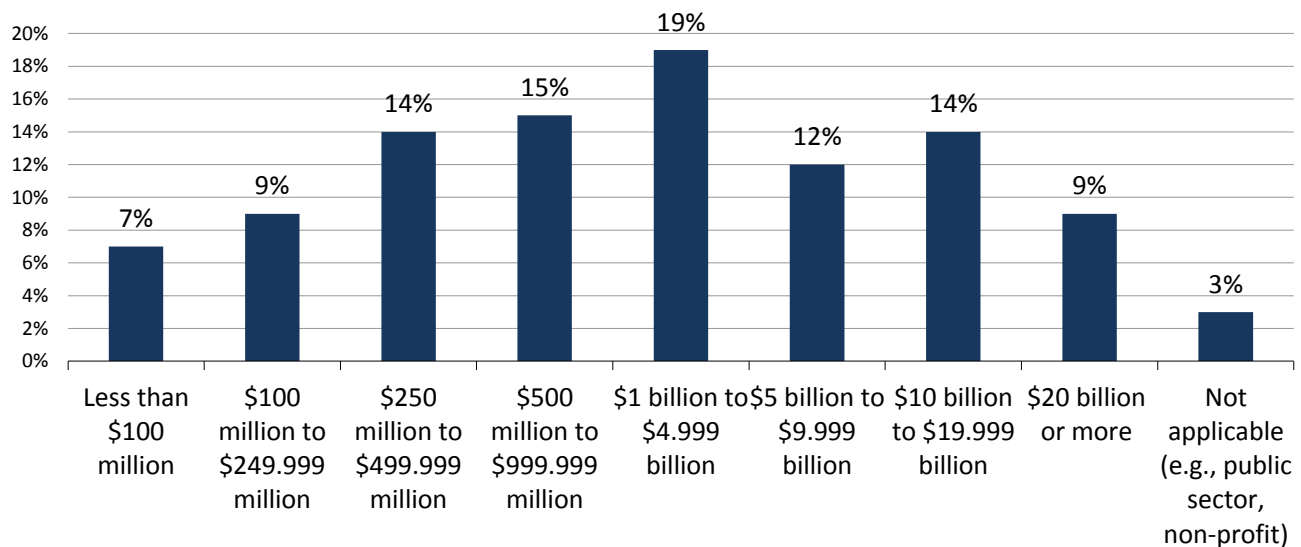
Source: Enterprise Strategy Group, 2015.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 4.

Figure 4. Survey Respondents by Annual Revenue

What is your organization's total annual revenue (\$US)? (Percent of respondents, N=340)



Source: Enterprise Strategy Group, 2015.



Contents

List of Figures	3
List of Tables	4
Executive Summary	5
Report Conclusions	5
Introduction	7
Research Objectives	7
Research Findings	8
The Endpoint Security Landscape.....	8
Endpoint Security Technology	19
Endpoint Security Services	35
Future Endpoint Security Strategy Decisions	37
Conclusion.....	39
Research Implications for Information Security Vendors	39
Research Implications for IT and Information Security Professionals.....	41
Research Methodology.....	45
Respondent Demographics.....	46
Respondents by Current Job Function	46
Respondents by Number of Employees	46
Respondents by Industry	47
Respondents by Annual Revenue	47

List of Figures

Figure 1. Approximate Total Number of Endpoint Computing Devices Supported by IT Organization	8
Figure 2. IT Organization’s Support of Endpoint Device Platforms.....	9
Figure 3. Approximate Percentage of Employees Who Connect to the Corporate Network Remotely Via VPN on an Average Day	9
Figure 4. Considerations That Have the Most Significant Influence on Organization’s Endpoint Security Strategy Moving Forward.....	10
Figure 5. Most Important Security-related Endpoint Provisioning Tasks Performed	11
Figure 6. Security Professionals Rate Aspects of Their Organization’s Endpoint Security.....	12
Figure 7. Endpoint Security Challenges.....	13
Figure 8. Actions Organizations Have Taken Over the Past Two Years with Regard to Endpoint Security	14
Figure 9. IT Organization’s Ability to Support Endpoint Security Technologies and Processes with Necessary Number of Trained Staff	15
Figure 10. Survey Respondents Rate IT/Security Staff in Endpoint Security Areas	16
Figure 11. Weakest Area with Regard to the Individuals Responsible for Endpoint Security	17
Figure 12. Is There a Dedicated Individual/Group Responsible for Endpoint Security?.....	18
Figure 13. How Organizations Address Endpoint Security and Endpoint Management/Operations.....	18
Figure 14. How Organizations Keep Track of Endpoint Assets	19
Figure 15. Approximate Number of Security Agents Installed on a Typical Endpoint	20
Figure 16. Installation of Antivirus Software on the Endpoint Devices that the Organization Formally Supports ..	20
Figure 17. Survey Respondents Rate Their Organization’s Standard Antivirus Software.....	21
Figure 18. Antivirus Software Supplementary Functionalities Currently Used	22
Figure 19. Challenges Experienced with Antivirus Products as Part of Organization’s Endpoint Security Strategy.	23
Figure 20. Approximate Number of Unique Antivirus Software Products Deployed	24
Figure 21. Antivirus Upgrade Patterns.....	24
Figure 22. How Often Organizations Change Antivirus Vendors	25
Figure 23. Why Organizations <u>Do Not</u> Change Antivirus Vendors	26
Figure 24. Why Organizations Are <u>Not Averse</u> to Changing Antivirus Vendors.....	26
Figure 25. Likelihood of Replacing Commercial Antivirus Software with an Alternative Free Antivirus Product	27
Figure 26. Usage of Security Software Technologies to Protect Sensitive Data on Endpoint Devices	28
Figure 27. Challenges of Data Security Software on Endpoint Devices	29
Figure 28. Familiarity with Types of New Advanced Malware Detection/Prevention Products	30
Figure 29. Deployment of Advanced Malware Detection/Prevention Software.....	30
Figure 30. Reasons for Deploying or Considering Deploying Advanced Malware Detection/Prevention Software	31
Figure 31. Familiarity with Endpoint Forensic Solutions.....	32
Figure 32. Deployment of Endpoint Forensics Solution.....	32
Figure 33. Reasons for Deploying or Planning to Deploy/Interested in Deploying an Endpoint Forensics Solution	33
Figure 34. Interest in Integration Between an Endpoint Forensics Solution and Other Types of Security Analytics Systems	34
Figure 35. Usage of a Managed Security Service for Any Aspect of Endpoint Security	35
Figure 36. Endpoint Security Services Currently in Use or Expected to Be Used	35
Figure 37. Reasons for Using or Planning to Use Managed Services for Endpoint Security.....	36
Figure 38. Type of Endpoint Security Technology Approaches Most Attractive to Organizations.....	37
Figure 39. Functionality Most Desired in a Comprehensive Endpoint Security Product Offering.....	38
Figure 40. Importance of the Inclusion of Remediation and Recovery Capabilities in an Endpoint Security Suite .	38
Figure 41. Survey Respondents by Current Job Function	46
Figure 42. Survey Respondents by Number of Employees	46
Figure 43. Survey Respondents by Industry.....	47
Figure 44. Survey Respondents by Annual Revenue.....	47



List of Tables

Table 1. Endpoint Security Challenges among Organizations with <u>Sufficient</u> Endpoint Security Resources.....	16
Table 2. AV Product Challenges, by Organizations that Rate Their Standard AV Software as <u>Very Effective</u>	23

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group | **Getting to the bigger truth.**