

1.0 Introduction and Report Overview

As computers and networking become ubiquitous, information security is no longer a backroom issue in the enterprise. It's everyone's concern. Information security depends on balancing cost and risk through the appropriate level of technology and policy. Too little security can be dangerous and costly — but so can too much. How do you decide the appropriate level of security for your enterprise?

This Executive Report provides recommendations, action items and planning guidance on how to identify and achieve winning strategies for implementing information security. The report describes how CEOs, CIOs and security organization managers — as well as other concerned enterprise personnel — can safeguard their enterprises against cybercrime and other cyberattacks.

CIOs must ensure that their enterprises have formal methods to monitor threats, assess defenses and balance risks. CIOs generally understand information security threats, but some IS organizations may be weak on risk analysis and prioritizing effective preventive actions. Because the risks and the costs of defenses are high and increasing, achieving the right balance is more important than ever.

This Executive Report describes ways in which IS and security organizations can monitor risks, assess defenses and create more secure enterprises. It provides answers to the question: How should an IS organization plan and implement a level of digital security that's appropriate for the enterprise? The report provides comprehensive guidance on the strategy, tactics, implementation plans and supporting technologies and services that enterprises need to develop, launch and monitor to achieve successful security initiatives.

This report is designed to serve the diverse needs of executives involved in security-related strategic planning, budgeting and investment management, technology acquisition and implementation, and application and service vendor evaluation. Some of the key topics addressed in this Executive Report are:

- Gartner's "Cyber-Threat" Hype Cycle, which details the progression of a number of important cyber-threats
- The role of government in fighting cybercrime

- Security philosophies adopted by enterprise type
- Gartner's Information Security Hype Cycle, which discusses the progression outlook for key new security management technology
- Intrusion detection, and why the industry will move increasingly to intrusion protection
- An assessment of the firewall vendor arena, including Gartner's Firewall Vendor Magic Quadrant
- How to implement effective antivirus architectures and how to negotiate with antivirus vendors — Gartner's Antivirus Magic Quadrant is presented
- Gartner's Managed Security Service Provider Magic Quadrant, and what to look for in evaluating a vendor
- How to implement effective organization structures of information security
- How to build and manage a computer incident response team
- Why an enterprise security architecture for Web services is so important
- Gartner's Web Services Hype Cycle, and the outlook for various new technologies
- How enterprises should develop security strategies for Microsoft Windows
- The trends and outlook for public-key infrastructure and digital signatures
- The most important issues and strategies for IT security management
- Business continuity and disaster recovery planning
- The importance of implementing wireless and mobile security measures
- Major elements of risk the art of risk mitigation, including procurement of cyberinsurance policies
- How to measure information security effectiveness
- And much more

This overview has been tailored for executives who need a high-level summary of the issues, forecasts, guidelines and recommendations offered in each chapter of this Executive Report.

- The remainder of this introductory chapter provides a general guide and overview to the research elements and high-level concepts presented in the report.
- Section 1.1 reviews the standard Gartner research elements used in the report.
- The subsequent sections provide an executive overview of each of the 15 remaining chapters of the report.
- Each section number corresponds to the chapter summarized — for example, Section 1.2 summarizes Chapter 2, Section 1.3 summarizes Chapter 3, and so on.

1.1 Research Elements Used in This Report

This Executive Report is based on Gartner's extensive research facilities and archives, which include conference presentations, Research Notes and Strategic Analysis Reports. The report is structured around Gartner Key Issues and corresponding Strategic Planning Assumptions and Tactical Guidelines.

- *Key Issues* pose questions that embody an important concepts or problems facing decision makers in a given topic area. Gartner develops Key Issues about markets, technologies and business strategies.
- *Strategic Planning Assumptions* are forecasts — usually framed within a defined, multiyear time horizon — that are assigned probabilities denoting Gartner's level of confidence in the outcome (see Section 1.1.1).
- *Tactical Guidelines* are analytical statements addressing important tactical factors enterprises will face in addressing a Key Issue.

In addition, selected sections conclude with Action Items — statements that convert a section's analysis into

concise, actionable advice. High-level recommendations, spanning the overall content of the chapter, may also be offered in the concluding section of the chapter.

1.1.1 Probabilities Defined

Probability statements are most commonly used within Gartner Strategic Planning Assumptions, although they are occasionally used in other research contexts (for example, to qualify the likelihood of a vendor's product availability estimate, or within a graphic illustrating a timeline of future events). In any context, probabilities never exceed 0.9, which represents Gartner's highest confidence level in a forecast. (Because no future outcome is 100 percent certain, a probability of "1.0" is never used.)

Because a forecast is logically phrased in form of the likely outcome, probabilities lower than 0.6 are rarely used. Occasionally, however, probabilities ranging from 0.1 to 0.5 may be used in special contexts — for example, in a "scenario" mutually exclusive possible outcomes, in which all probabilities total 1.0.

Within the context of a formal Strategic Planning Assumption, the probabilities assigned will normally range from 0.6 to 0.9. These probabilities are defined as follows:

- 0.9: This will almost certainly happen, barring a major industry reversal. Gartner would be shocked otherwise. Moreover, the timing is almost certain.
- 0.8: This is likely to happen, barring exceptional circumstances. Gartner would be quite surprised if it failed to happen, but a degree of uncertainty exists. The timing estimate is fairly certain.
- 0.7: There is good reason to believe that this will be true, but there is a fair chance that it won't. Gartner would be surprised, but not shocked, if it did not happen. Moreover, the timing is unclear and may vary from estimates.
- 0.6: For planning purposes, this should be treated only as a general direction, rather than a solid forecast. It is better than a rumor or a guess, but not necessarily by

a wide margin. Most likely, Gartner does not have a firm idea of the timing.

1.1.2 Type A, B and C Enterprises Defined

Gartner often identifies enterprises as "Type A," "Type B" or "Type C" based on the aggressiveness with which they adopt and use technology. These terms are often used to offer different recommendations to different types of enterprises, based on their approach to technology adoption. Briefly defined:

- Type A enterprises are technology-driven, and are often willing to risk using immature, cutting-edge technologies to gain a competitive edge.
- Type B enterprises are moderate technology adopters, using new technologies once they have been proven and have entered the mainstream.
- Type C enterprises are technologically risk-averse and cost-conscious, and are usually among the last to adopt new technologies.

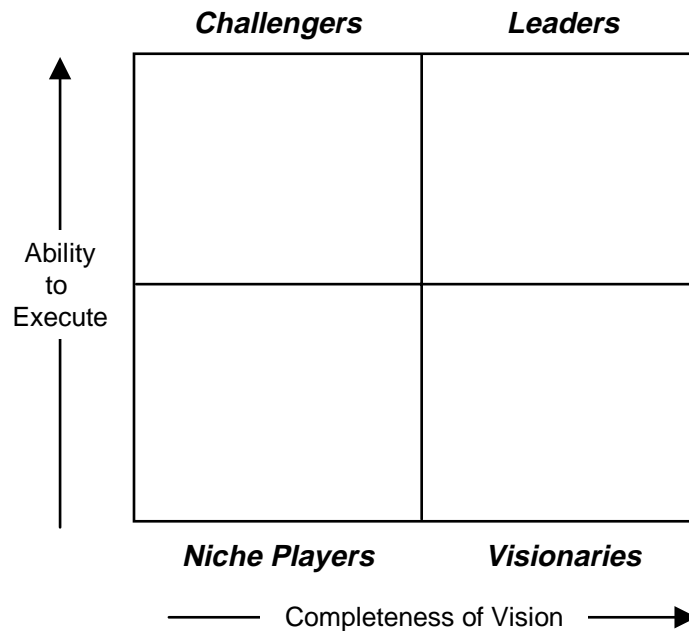
1.1.3 The Gartner Magic Quadrant

Gartner's Magic Quadrant diagrams (see Figure 1-1) are graphical portrayals of vendor performance in a market segment. Within the diagram, vendors are grouped within four categories — Leaders, Challengers, Visionaries or Niche Players — is based on their positioning along two axes.

Completeness of Vision, the horizontal axis, assesses factors such as:

- The existence of clear vision
- Consistency with industry trends
- Product completeness for the target buyer
- Creativity in the plan of attack for the defined market

Figure 1-1: The Gartner Magic Quadrant



Source: Gartner

Ability to Execute (the vertical axis) assesses factors such as

- Senior management talent
- Sales, marketing and distribution capabilities
- The depth of research and development
- The quality of a vendor’s professional services and support
- The strength of a vendor’s finances and alliances

Based on those positionings, vendors fall within one of the following four quadrants:

- *Leaders* are companies that are doing well today and have great prospects for tomorrow.
- *Visionaries* are those that have great ideas for tomorrow, but may not be executing consistently or well in all areas.

- *Challengers* are those that execute well today and may dominate a large segment, but do not fully understand market trends and directions and thus may not have all the elements necessary for future success.
- *Niche Players* are either companies that focus on a small segment of the market (and may do so well), or those that have modest horizons and possibilities owing to their inability to innovate or outperform other vendors.

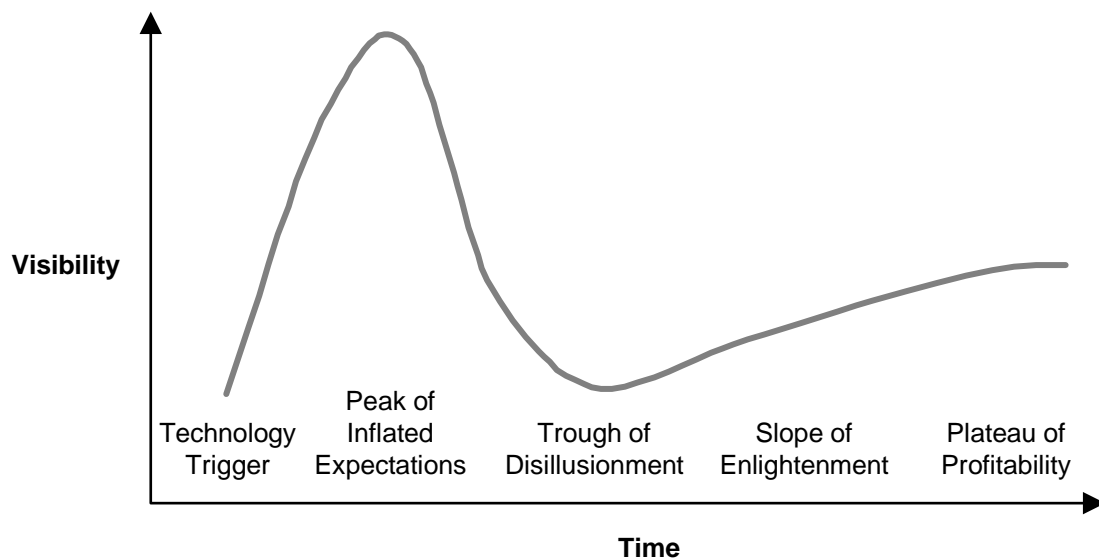
Magic Quadrants can be used to support technology selection decisions; however, Gartner cautions that they should not be used as the sole means of evaluation. Enterprises should not limit their considerations only to vendors that are in the Leaders category, nor should they necessarily reject those ranked as Niche Players. In certain situations, Niche Players’ products may be appropriate tactical choices. User organizations should carefully evaluate vendors based on their own unique circumstances and specific requirements.

1.1.4 The Gartner Hype Cycle

Gartner uses its Hype Cycle diagram (see Figure 1-2) to illustrate the pattern of intense hype, followed by disillusionment, that emerging technologies typically pass through on the road to eventual productive use and mainstream adoption. Technologies or services are plotted on the diagram to illustrate Gartner's estimates of their current maturity, and how far away they are from providing mainstream value. The Hype Cycle contains five phases:

- *Technology Trigger*: This is an event that generates significant press and industry interest, such as a breakthrough, invention, discovery, public demonstration or product launch.
- *Peak of Inflated Expectations*: During this phase of over-enthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The enterprises that make money during this phase are generally conference organizers, magazine publishers and consultants.
- *Trough of Disillusionment*: The technology fails to live up to the inflated promise. As a result, it rapidly becomes unfashionable, and the press abandons the technology or touts its failure deliver on what were, in retrospect, unrealistic expectations.
- *Slope of Enlightenment*: Focused experimentation and hard work performed by an increasingly diverse range of organizations leads to a true understanding of the technology's applicability, risks and benefits. Commercial, off-the-shelf methodologies and tools become available to ease the development process and application integration.
- *Plateau of Productivity*: The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. The final height of the plateau varies according to whether the technology is broadly applicable or benefits only niche markets.

Figure 1-2: The Gartner Hype Cycle



Source: Gartner