Intel IT Center

SEPTEMBER 2011

Peer Research

Cloud Security Insights for IT Strategic Planning

Intel's IT Manager Survey on Cloud Security

Why you should read this document:

This report describes key findings from a survey of 200 IT professionals that can help you plan security into your cloud initiatives, including the following:

- Protecting platform and infrastructure resources are top concerns.
- Security plays a foundational role in the decision to implement a private cloud.
- Nearly half of the overall organizational investment in cloud initiatives is security related.
- Security drives outsourcing decisions.

Sponsors of Tomorrow.™ intel

Intel IT Center

Peer Research

Cloud Security Insights for IT Strategic Planning

Intel's IT Manager Survey on Cloud Security

SEPTEMBER 2011

Sponsors of Tomorrow.™ intel

Contents

About This Report

The issue of cloud security is keeping many IT managers from fully embracing the cloud—even with large potential savings in infrastructure costs and improved business flexibility. With Gartner predicting an acceleration of cloud computing in the enterprise,[1] we wanted to find out how IT professionals are addressing the challenges of cloud computing, especially the issue of security.

We surveyed 200 IT professionals[2] about a wide variety of cloud topics, including the key business and technology drivers behind their implementation plans, the importance of security in determining how the cloud is implemented, and their level of investment in security as part of cloud initiatives.

The aim of this report is to provide benchmark data you can use for your own cloud security planning.

The results of our survey are detailed in this report. The goal is to provide you with data that can serve as a benchmark for how your peers are approaching cloud security, so that you can use it in your own IT planning efforts.

1 *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010.* Press release. June 22, 2010. gartner.com/it/page.jsp?id=1389313

2 Respondents are IT professionals in organizations of 100 to 1,000-plus employees across a variety of industries. See "Appendix" for detailed information on the respondent profile.

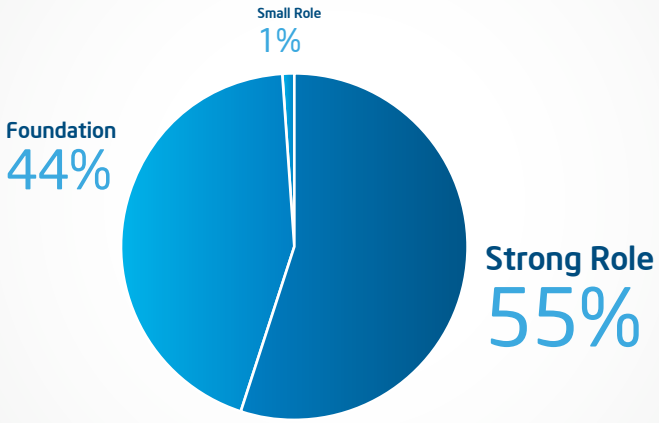
Executive Summary

Security a Key Driver for Cloud Planning

The IT professionals surveyed for this report represent companies across the continuum of cloud computing experience, from early consideration to deployed services. One in five companies surveyed is already offering cloud services (18 percent). Two in five are currently in the process of implementing (42 percent), and another two in five are in the evaluation stage (38 percent) or planning to evaluate cloud initiatives (4 percent).[3]

Not surprisingly, security plays a major role in the selection of a deployment model for 99 percent of the companies surveyed. However, for 44 percent, security issues are the foundation for their decision making in selecting a private versus public cloud delivery model.

Role of Security in Decision *(n=200)*



Q: *Which of the following best represents the role security played or is playing in your decision to implement your cloud initiatives via a private versus public cloud?*

Key Finding:

Security plays a major role in cloud model selection.

3 Those who are not yet investigating cloud computing or have decided not to implement cloud computing were excluded from the survey sample.

How Do Security Issues Influence Planning for Cloud Initiatives?

Protecting data, platform, and infrastructure. The most common drivers of security plans for cloud initiative issues are related to protecting customer, vendor, and employee data (80 percent); protecting servers and other platform/infrastructure resources from attack (76 percent); and protecting financial data (72 percent).

High levels of investment. The level of investment to protect these vital enterprise assets is significant. When averaged across our sample group, nearly half (48 percent) of the overall organizational investment in cloud initiatives is security related.

A clear preference for deployment model. The leading deployment model today is a private cloud, utilized (or most likely to be utilized) by a little more than half (52 percent) of organizations surveyed. A hybrid cloud is preferred by 31 percent and a public cloud by 11 percent.

Security drives outsourcing decisions. Security was cited as the biggest concern by 66 percent of those surveyed about outsourcing some IT to a cloud service provider.

Key Finding:

Protecting platform and infrastructure resources is a top concern for more than three-quarters of IT professionals.

Other Key Findings from the Survey Include the Following:

Implementing security is no easy task. Most report having experienced moderate (60 percent) or major (22 percent) challenges.

Security concerns are similar for outsourcing. Similar to general concerns about security in the cloud, data loss and compromised platform or infrastructure assets are the biggest concerns for two-thirds (66 percent) of IT professionals when it comes to outsourcing to a cloud provider. Not surprisingly, the security capabilities and assurances offered are extremely important to 60 percent of IT professionals when making a selection.

Trust in cloud service providers is mixed. Slightly more than half (54 percent) of IT professionals have some trust in the ability of their cloud service provider to secure assets in the cloud, while 43 percent have a great deal of trust.

Hardware-based security provides greater assurance. A cloud service provider with additional hardware-based security measures is viewed as delivering a higher level of security by 78 percent.

Minor differences by company size. In general, our data reveals no significant differences in results among the diverse range of company sizes in our survey: 100 to 499 employees, 500 to 999 employees, and 1,000-plus employees. However, of those companies with 1,000 or more employees, 24 percent are already offering cloud services, compared to 10 percent for each of the other segments.

Key Finding:

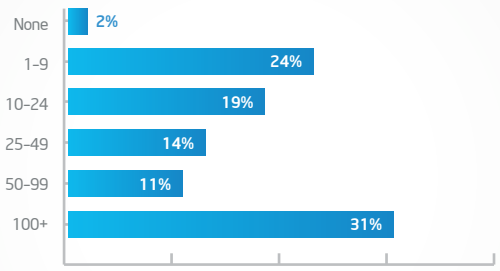
Nearly half of the overall organizational investment in cloud initiatives is security related when averaged across our sample group.

Key Security Drivers

Virus and Malware Attacks Are Relentless

We asked IT professionals to tell us about security in their current IT environment so we could understand what they were most concerned about. Nearly a third of those surveyed (31 percent) are regularly thwarting 100 or more virus or malware attacks every month.

Attacks Thwarted Monthly *(n=200)*



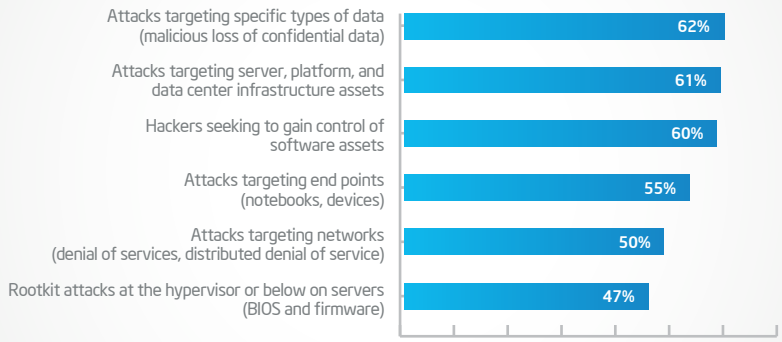
Q: *On average, how many virus or malware attacks are you thwarting each month?*

There is no statistical relationship between the size of the company and the number of attacks thwarted. However, companies with 500 or more virtualized servers are more likely to be thwarting an even greater volume of attacks. In this category, approximately 31 percent report thwarting more than 500 attacks every month, and 24 percent are thwarting 1,000 or more attacks.

High Threat Potential across the Data Center

IT professionals report a wide variety of potential security concerns to keep them up at night. Three top the list: attacks targeting specific data types (62 percent); attacks of server, platform, and data center infrastructure assets (61 percent); and hackers seeking to gain control of software assets (60 percent). Almost half are concerned about rootkit attacks at the hypervisor level or below, network attacks, and attacks targeting end-point devices.

Concern for Security Threats *Percent Highly Concerned (6–7 ratings) (n=200)*

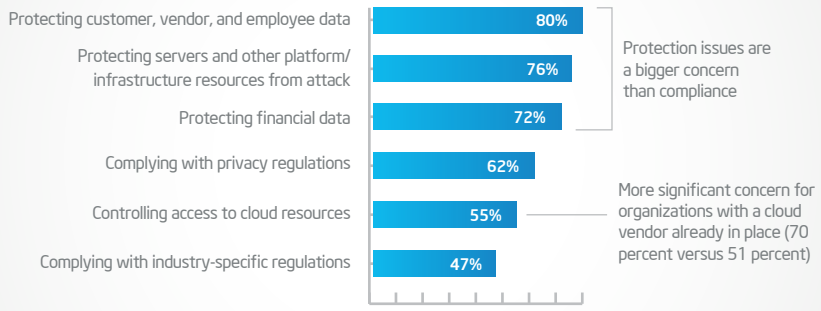


Q: *How concerned are you about each of the following potential security threats to your IT environment? (1=not at all concerned, 7=very concerned)*

Asset Protection Drives Cloud Security

When it comes to security plans for cloud initiatives, companies are most often driven by a desire to protect data and infrastructure resources, with compliance as a secondary concern.

Business/IT Needs Driving Security Plans *(n=200)*



Q: *What specific business or IT needs drove/are driving your security plans for cloud initiatives?*

For those organizations with a cloud vendor already in place, *controlling access to cloud resources* becomes a more significant concern (70 percent versus 51 percent).

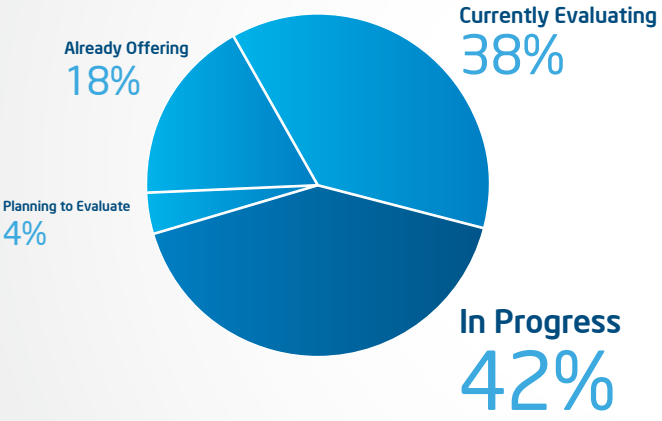
Key Finding:

Protection issues are by far the biggest business/IT drivers for security, but compliance isn't far behind.

Current Cloud Environments

Cloud computing is considered an important strategic investment by almost all the companies we surveyed. One in five (18 percent) is already offering cloud services or capabilities, and three-quarters (76 percent) of those currently evaluating or planning to evaluate expect to implement cloud services within the next year.[4]

Current Phase of Implementation *(n=200)*



Q: *Which of the following best describes your company's current situation regarding cloud computing?*

Implementation Timeline *(n=82)*

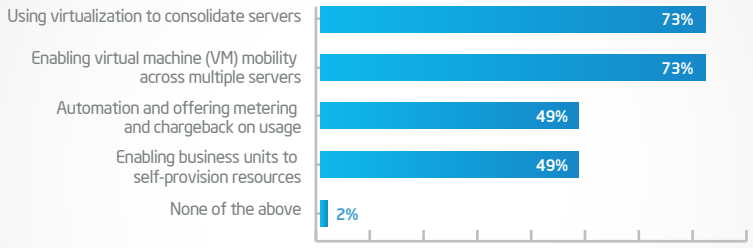
Q: *When do you plan to implement cloud computing capabilities to your end users?*

4 Those who are not yet investigating cloud computing or have decided not to implement cloud computing were excluded from the survey sample.

Increasingly Sophisticated Virtualization

We asked IT professionals to tell us what technologies they were currently deploying that support a current or planned cloud environment. Nearly three in four are currently *using virtualization to consolidate servers and enabling virtual machine (VM) mobility across multiple servers* (73 percent) in order to support a cloud. Nearly half offer *automation and metering and chargeback based on usage* and *enable business units to self-provision resources.*

Technologies to Support Cloud Environment *(n=193)*

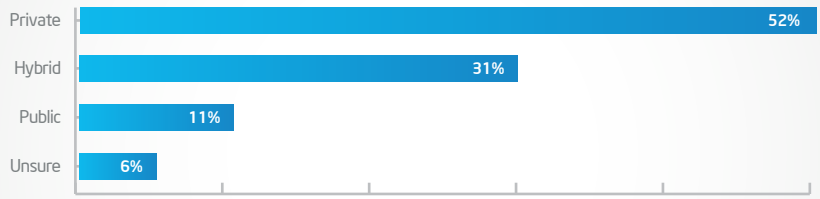


Q: *Which of the following technologies are you currently deploying in your data center that support a current or planned cloud environment?*

Private Clouds Lead the Way

A *private cloud* is the leading deployment model for 52 percent of those surveyed—no matter what phase of implementation. It's most common among those already offering cloud computing (63 percent), those in the implementation phase (51 percent), and those still evaluating (49 percent).

Preferred Cloud Deployment Model *(n=193)*



Q: *Which of the following cloud deployment models is your organization using and/or most likely to use?*

Key Finding:

Private cloud is the leading deployment model.

Public clouds are more likely to get consideration from companies with:

- 500–999 employees (29 percent versus 5 percent among smaller and larger companies)
- Less than 10 worldwide locations (17 percent versus 5 percent among companies with 10 or more locations)
- 250–499 virtual servers (31 percent versus 3 percent among companies with 500 or more virtual servers)
- Less than $10 million U.S. dollars (USD) in revenue (21 percent versus 7 percent among companies with USD $10 million or more).

Although there is a clear preference for delivery model, the same is not true for the cloud service being considered or already implemented. All three of the major services get equal consideration across our sample: software as a service (SaaS), 58 percent; infrastructure as a service (IaaS), 57 percent; and platform as a service (PaaS), 56 percent.

Role, Level of Investment, and Experiences

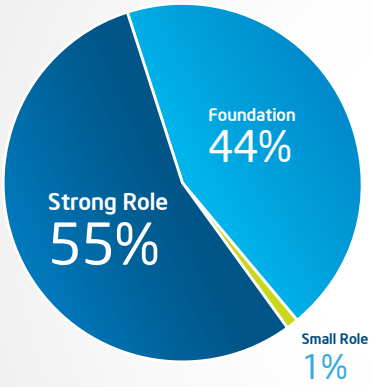
Security Influences Cloud Decision Making

Security plays a major role for nearly all IT professionals (99 percent) when considering or implementing a private versus public cloud. Significantly, for nearly half (44 percent), it is *the foundation of the decision.*

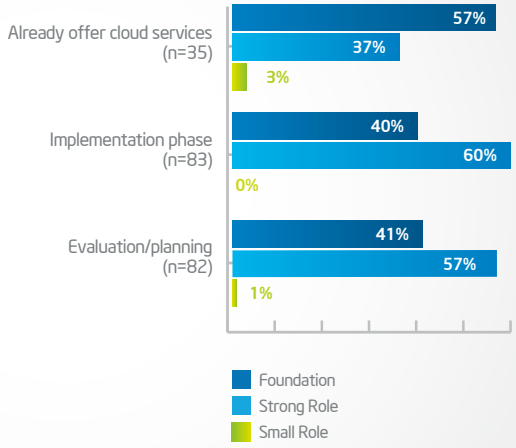
Security plays a more substantial role for those already offering cloud services (57 percent foundational role compared with 37 percent strong role) than those in either the implementation stage (40 percent versus 60 percent) or evaluating stage (41 percent versus 57 percent).

Since IT departments have been facing security challenges for decades, the overwhelming importance of security in cloud decision making isn't unexpected. Those surveyed are well aware that the effort to thwart attacks and prevent breaches will be ongoing even as delivery models continue to evolve.

Role of Security in Decision *(n=200)*



Role of Security by Phase



Q: *Which of the following best represents the role security played/is playing in your decision to implement your cloud initiatives via a private versus public cloud?*

Key Finding:

Security plays a foundational role in the decision to implement a private cloud model.

Investment Levels Support Value of Security

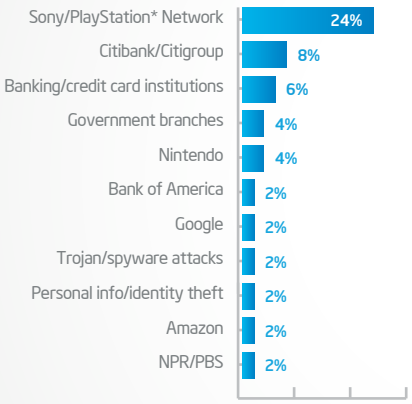
The IT professionals we surveyed recognized the importance of security across delivery models and for both internal and external implementations. They back up their concern with a high level of investment in security as part of the overall investment in cloud initiatives. For example, when averaged across our sample group, almost half (mean equals 48 percent) of the investment in cloud initiatives is related to security.

Bad News Taken in Stride

We were curious about whether high-profile security breaches reported in the news had any impact on cloud decision making. When asked to recall recent newsworthy breaches or attacks, one-quarter (24 percent) mention the high-profile public security breach of the Sony* PlayStation* Network. Nevertheless, most (70 percent) say the breaches they recall have no impact on their decision to move forward with cloud initiatives.

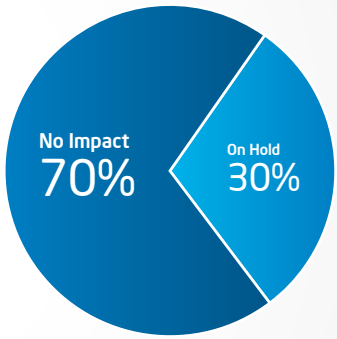
One-third (30 percent) are on hold while they deepen their evaluation of their security plans and controls.

Unaided Recall of Security *(n=200)*



Q: *What recent high-profile breaches/attacks have you heard about on the news or in trade publications?*

Impact of Security Breaches *(n=79)*



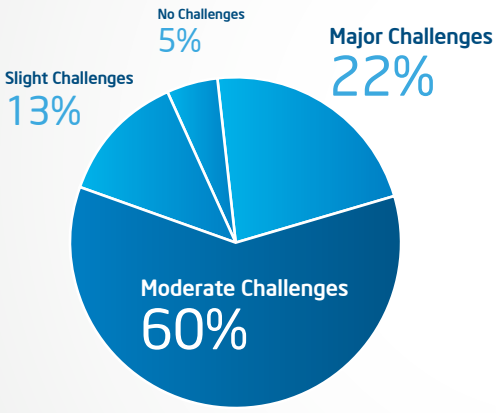
Q: *How have these recent breaches/attacks impacted your plans to pursue cloud initiatives?*

Why don't these high-profile breaches cause more anxiety? The allure of cloud computing is very powerful these days. It may be that cloud computing is seen as so strategically important that IT professionals are willing to move forward with a thoughtful, risk-based approach.

Cloud Security No Walk in the Park

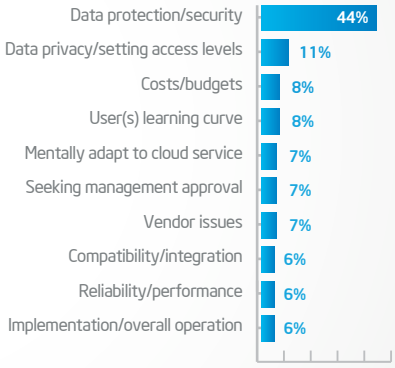
We asked survey respondents to tell what they experienced as the greatest challenges to implementing security. Nearly all (95 percent) who are already implementing or offering cloud services have experienced slight challenges in implementing security for a private or hybrid cloud. One in five (22 percent) indicated that they had experienced major challenges. The biggest headache? Data protection challenges, experienced by 44 percent of those surveyed.

Cloud Security Challenges *(n=95)*



Q: *How would you describe the challenges you've experienced in implementing security for a private or hybrid cloud?*

Top Challenges Experienced *(n=90)*



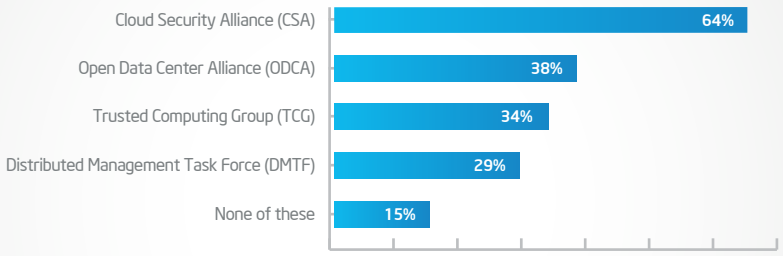
Q: *What, specifically, were these challenges?*

Asked how they overcame their challenges, those surveyed reported that their top method was to increase or upgrade security measures, as well as to research thoroughly and leverage vendor relationships. Other approaches included training, hiring consultants, and increasing budget. A number of companies continue to grapple with unresolved issues.

Best Practices

The explosion of interest in cloud computing has inspired several key industry groups to work on establishing best practices and standards around security. Nearly two-thirds (64 percent) of companies surveyed have had their planning efforts influenced by the Cloud Security Alliance (CSA), and more than a third mentioned the Open Data Center Alliance (ODCA) and the Trusted Computing Group (TCG), followed by the Distributed Management Task Force (DMTF).

Influence of Best Practices *(n=200)*



Q: *Which groups have influenced your planning with their best practices and/or standards concerning security and trust in the cloud?*

Best practices advice from your peers:

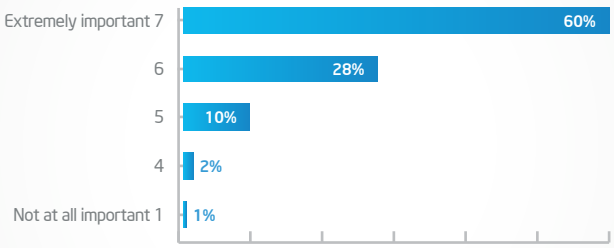
"Researching, learning, understanding, and implementing best practices [was] the first step. Speaking with colleagues who have dealt with similar challenges gave us a comfort level that we lacked." [5]

5 Verbatim response from one of the participants in this benchmark study.

A Trusted Cloud Service Provider

Of the IT professionals surveyed, three in five (61 percent) are *currently evaluating* a cloud service provider, and nearly a quarter (23 percent) *have selected* a cloud service provider. Most reported that the security component offered by the cloud service provider is *important*, with 60 percent considering it *extremely important*.

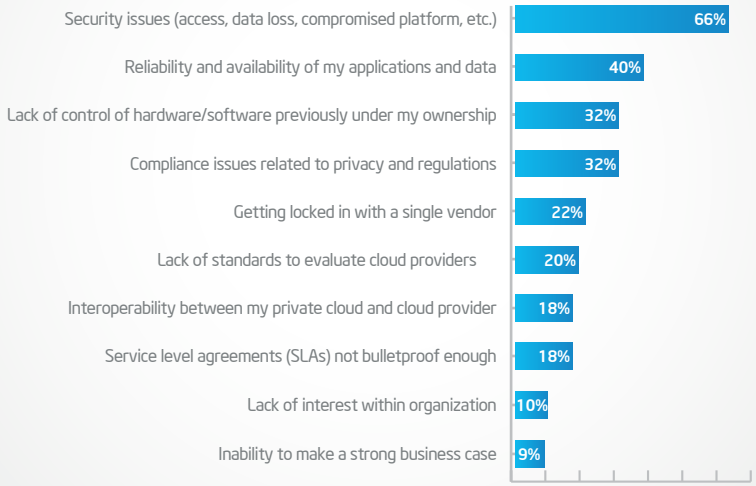
Importance of Security *(n=200)*



Q: *How important is the security component offered by the cloud service provider in your vendor selection decision?*

The leading concern of those surveyed about outsourcing some IT to a cloud service provider is security—by a wide margin (66 percent). One in three cited compliance issues related to privacy and regulations as one of their greatest concerns.

Greatest Outsourcing Concerns *(n=200)*

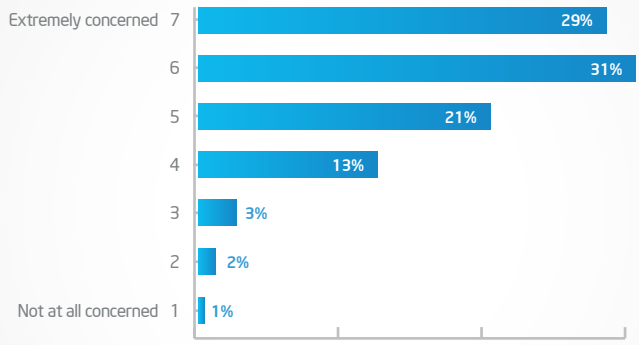


Q: *What are your greatest concerns about outsourcing some of your IT to a cloud provider?*

Vendor Infrastructure Concerns

Among IT professionals who are evaluating or have already chosen a cloud provider, more than half (54 percent) have *some* trust in the ability of their cloud service provider to secure assets in the cloud, and 43 percent have a *great deal* of trust. However, almost 60 percent reported that they were extremely or very concerned about the infrastructure their cloud provider uses. This is even higher for those thwarting 10 or more attacks a month (35 percent versus 15 percent for those fighting off fewer attacks).

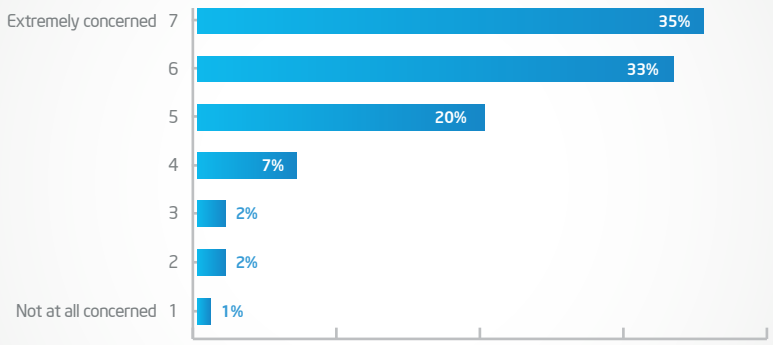
Infrastructure Concern *(n=168)*



Q: *How concerned are you about the infrastructure your cloud provider uses?*

In this same group, two-thirds (68 percent) are *concerned* about rootkit hypervisor attacks, and 35 percent are *extremely concerned.* Again, those IT professionals thwarting 10 or more malware attacks per month are more likely—twice as likely—as those fighting off fewer attacks to be *extremely concerned* about rootkit hypervisor attacks (40 percent versus 19 percent).

Level of Concern for Rootkit Hypervisor Attacks *(n=168)*



Q: *How concerned are you about rootkit hypervisor attacks (for example, "blue pill") or other malware infecting the cloud provider's server environment?*

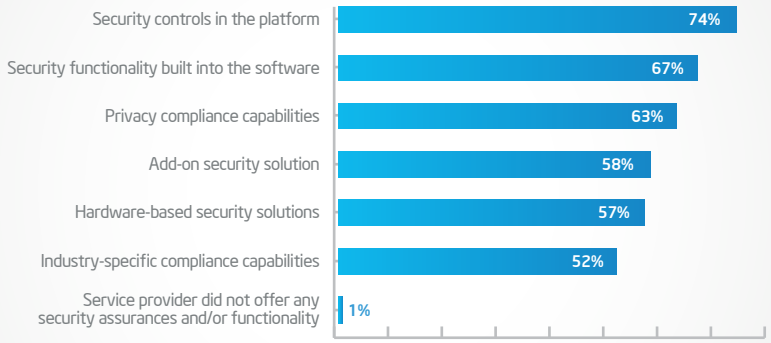
Key Finding:

Two-thirds of IT professionals worry about rootkit hypervisor attacks or other malware attacks on their cloud provider.

Vendor Security Assurances

Providing the right security assurances goes a long way toward building trust in a cloud service provider. According to those who have chosen or are evaluating cloud providers, *security controls in the platform* (74 percent) are the most common security assurances provided. Those already using a cloud service provider are significantly more likely to be assured of *security controls in the platform* than those IT professionals still evaluating vendors (85 percent versus 70 percent).

Security Assurances Provided by Cloud Service Providers *(n=168)*



Q: *What security assurances and/or functionality does/do the cloud service provider(s) offer?*

Just over three-quarters (78 percent) believe a cloud service provider with additional hardware-based security measures to reduce some forms of malware provides a *higher level of security*. This was higher for those companies thwarting 10 or more attacks per month (62 percent versus 42 percent for those fighting off fewer attacks).

Visibility into Security and Compliance

IT professionals report that cloud service providers make their security assurances *moderately* (48 percent) or *highly* (45 percent) visible. *Regular, periodic reports on security incidents* (73 percent) are the most common methods used by vendors to document compliance with privacy or other regulatory requirements, followed by *specified level of responsibility for a security breach* (60 percent) and the *ability for the organization to conduct compliance audits* (60 percent).

Documenting Vendor Compliance with Regulatory Requirements *(n=168)*

Q: *How do you document the vendor's compliance with privacy or other regulatory requirements?*

Your Peers Speak Out

We asked those surveyed for the single most important piece of advice they could offer to another IT manager just starting the process of planning cloud security. We then grouped the answers under similar categories. Experienced IT managers most often would encourage others to *be thorough in their cloud computing research* and to *continuously prioritize security* in their future cloud initiatives. Specific advice suggests reaching out for information sources beyond vendors, as well as pressing for more security assurances, flexibility, and references from vendors. Those surveyed also recommended comparing vendors, working with reputable vendors, and using third-party recommendations. They also suggested that IT managers should take their time planning.

"When you are looking into the cloud, be sure to evaluate security, as your decision will affect you and your company for years to come."

Sample Verbatim Responses

"Evaluate all aspects of this new technology. Read everything you can get your hands on. Talk to people that have implemented this technology."

"Research all the options out there and take your time in making a decision."

"Get all the information up front and implement training for the whole IT department."

"Ensure that you have control and ability to implement monitoring [of] auditing measures to ensure security is adequate."

"Focus on integration and security from the get-go and make sure your vendor can be flexible to meet your requirements."

"If you are not convinced about the security aspects of the process, do not move forward! Even better, hammer out ways to be able to test as to how effective the security options provided by the vendor are."

Cloud Security Profiles

From the data, we are able to develop security profiles for organizations already offering, implementing, and evaluating or planning to evaluate cloud initiatives. In general, it appears that while security is an important issue no matter the phase of implementation, those surveyed who were already offering cloud services had more confidence in their ability to protect assets in the cloud than those in the early stages of planning and evaluation. This suggests that while security concerns never go away, they can be identified and addressed. As IT professionals get further along in the process, their thinking evolves as part of the experience of researching, evaluating, implementing, and then finally offering cloud capabilities.

Security Is Foundational to Those Offering Cloud Computing

By far the biggest business and IT drivers for security are protection of data and server platforms. Compared with companies implementing or evaluating cloud computing,those companies already providing cloud-based services are more likely to:

- List their top two IT drivers as the need to protect data (74 percent) and the need to protect servers and other platform and infrastructure resources from attack (66 percent)
- Say security was the foundation of their decision for implementing a private cloud initiative versus a public cloud (57 percent versus 41 percent)
- Report high visibility into the security assurance provided by cloud service providers (67 percent versus 40 percent)
- Have considered or implemented SaaS over PaaS or IaaS (86 percent versus 52 percent of those implementing or evaluating cloud services)
- Be deploying technology that enables business units to self-provision resources (71 percent versus 44 percent)
- Have an enterprise-class data center (60 percent versus 21 percent) with more than 500 virtualized servers (34 percent versus 13 percent)
- Be from companies with more than 1,000 employees (24 percent versus 10 percent)

High Level of Concern about Security in the Early Planning Stages

Those evaluating or planning to evaluate cloud computing are inclined to be significantly more worried about security than those already offering services or in the implementation stage. Those in the earlier stages tend to be:

- Driven most by the need to protect data (87 percent) and to protect servers and other platform and infrastructure resources from attack (76 percent)
- Least confident that their current network and data center assets are adequately protected (43 percent very confident versus 64 percent not confident)
- Able to recall more high-profile breaches and attacks (55 percent versus 33 percent)
- Least trusting of the ability of cloud service providers to secure their assets in the cloud (20 percent have a great deal of trust versus 58 percent)
- Least likely to be influenced by industry standards groups

Midsize Companies Are Implementing Cloud Initiatives Now

In our sample group, those in the process of implementing cloud computing are inclined to be from midsize companies with 100–999 employees. They tend to be:

- Driven more than any other stage of implementation category by the need to protect servers and other platform and infrastructure resources from attack (81 percent) and to protect data (75 percent)
- More likely to consider a public cloud (23 percent versus 2 percent of those already offering services or in the planning and evaluation stage)
- More likely to have a localized or regional data center (57 percent versus 41 percent of those already offering services or in the planning and evaluation stage)
- More likely to be from companies with less than 1,000 employees (59 percent versus 41 percent of those already offering services or in the planning and evaluation stage)

Conclusion

Our benchmark report of 200 IT professionals in various stages of cloud deployment confirms what other studies have shown, with some interesting additional insights. While security is clearly a primary concern, respondents who have already deployed cloud services, often in the form of private clouds, generally feel confident in their abilities to manage security in the cloud. The strategic value of cloud computing is compelling enough that companies are still moving forward—despite concerns about protecting data and infrastructure and reports of high-profile attacks in the news.

Our survey reports that for the majority, security issues are a significant factor in the decision to deploy a private versus public cloud—in some cases the foundation of that decision. This reinforces other industry studies that have shown that the journey to the cloud often starts with a private delivery model—typically because of security concerns.

While security challenges are many, our results indicate that they can be overcome by a solid investment in security controls, including solutions that protect data and data center infrastructure from attacks—top security drivers for those surveyed. Organizations are making substantial investments in cloud security to protect assets, thwart infrastructure attacks, and meet compliance requirements.

The IT professionals in this survey are managing security challenges by prioritizing security as part of their cloud planning, conducting in-depth research, and leveraging or establishing strong vendor relationships. The good news is that as IT professionals move through the planning, evaluation, and implementation stages, they gain valuable knowledge and experience with security that really pays off in the final deployment. As several respondents recommended, when it comes to cloud security, "do your homework."

Those surveyed are well aware that threat activity is increasing and cyber criminals are continuing to develop more sophisticated methods of attack. Efforts to thwart these will be ongoing even as cloud services delivery models continue to evolve. The challenge for the IT industry is to continue to adapt so that organizations can continue to maintain—or even increase—confidence in the security of their assets.

We provided the information in this report to help you learn from the experience of your peers as you plan and implement cloud security as part of your own cloud initiative. For a practical guide to help you plan cloud security, with recommendations from Intel, see the Cloud Security Planning Guide: Seven Steps for Building Security in the Cloud from the Ground Up. And find more information about Intel and cloud security here.

Appendix: Methodology and Audience

Responses to this survey were gathered via an online questionnaire; 200 surveys were received between June 23 and July 1, 2011. A sample size of 200 has a maximum sampling variability of ±6.9 percent at the 95 percent confidence level.

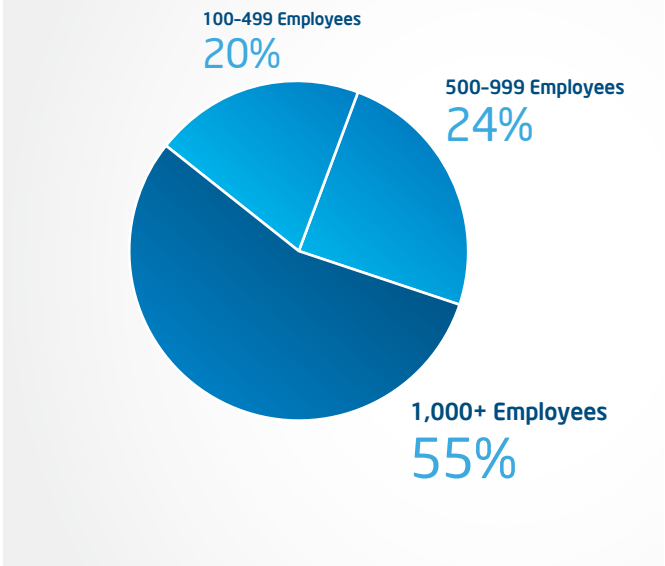
Respondents were screened to ensure that they:

- Work in a company of 100-plus employees
- Are IT decision makers
- Are involved in decision making and strategic planning for clients in their organization
- Have implemented, are currently implementing, are evaluating, or plan to evaluate desktop virtualization
- Represent what Intel terms a "tech enthusiast" company—that is, a company that considers IT to be a driver of its business success

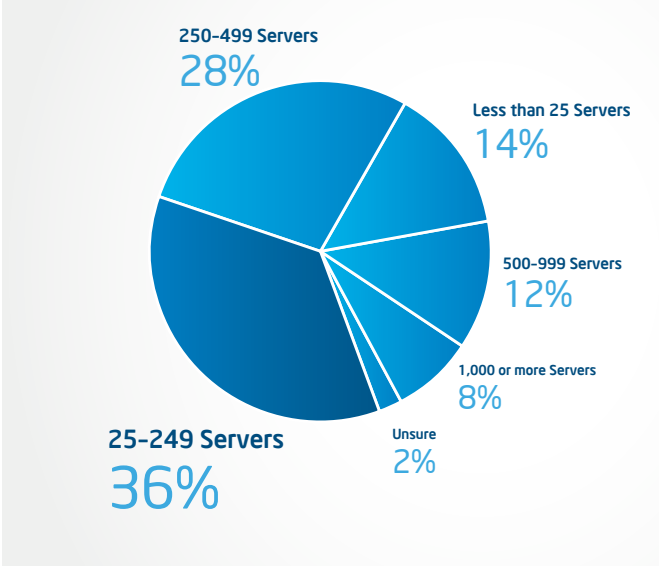
Being an Intel customer was not a consideration for inclusion in the survey. Quotas for company size and industry were enforced to ensure a representative sample.

Respondent Profile Information

Company Size (*n=200*)



Virtualized Servers (*n=200*)



Worldwide Locations (*n=200*)

1 location	6%
2-4 locations	24%
5-9 locations	22%
10-14 locations	20%
15-19 locations	25%
Unsure	3%

Annual Revenue (*n=200*)

Less than $500,000	1%
$500,000-$900,000	4%
$1 million-$3.9 million	10%
$4 million-$9.9 million	14%
$10 million-$49.9 million	21%
$50 million-$99.9 million	12%
$100 million or more	30%
Unsure	8%

Industry (*n=200*)

Manufacturing	14%
Financial services	12%
Computer-related business or service	12%
Healthcare	12%
Professional services	10%
Retail	7%
Education	5%
Telecommunications	4%
Wholesale & distribution	4%
Construction	3%
Government	3%
Transportation & logistics	3%
Media & entertainment	3%
Other (2% or less)	7%

Share with Colleagues

0911/JM/ME/PDF-USA 326043-001

Sponsors of Tomorrow.™