Intel IT Center

MAY 2012

Peer Research

What's Holding Back the Cloud?

Intel Survey on Increasing IT Professionals' Confidence in Cloud Security

Why You Should Read This Document

This report captures key findings from a blind survey of 800 IT professionals in four countries—China, Germany, the United Kingdom, and the United States—that provide insight into cloud computing security concerns, and how those concerns might be alleviated. The report provides insights from IT professionals that you can use to better understand:

- Specific issues IT professionals have about cloud security, and how these issues differ between public cloud and private cloud. Concerns include lack of control over data, lack of visibility into cloud infrastructure integrity, and complexity in meeting compliance requirements, among others.
- What the industry—software and hardware providers as well as cloud service providers—can do to overcome adoption barriers and build greater confidence in cloud safety, such as enforcing security policies across clouds and creating data boundaries
- How these issues are the same or different for IT professionals in China, Europe, and the United States

Sponsors of Tomorrow.™ intel®

Intel IT Center

Peer Research

What's Holding Back the Cloud?

Intel Survey on Increasing IT Professionals' Confidence
in Cloud Security

MAY 2012

Sponsors of Tomorrow.™

Contents

About This Report

Cloud computing holds the promise of helping organizations and their IT departments be more agile, efficient, and able to cost-effectively deliver new services that enable their businesses to thrive.

But the promise of the cloud cannot be fulfilled until IT professionals have more confidence in the security and safety of the cloud. We know that IT concerns with cloud computing security are major barriers to business adoption of the cloud. But before the IT industry can address these concerns, it needs to better understand them. What specific issues should the industry focus on solving so that it can boost IT's confidence in cloud computing?

Intel wanted to help answer this question. We conducted the research detailed in this report to better understand:

- The specific issues IT professionals have about cloud security, and how these issues differ between public cloud and private cloud
- What the industry—software solution and hardware providers as well as cloud service providers—can do to overcome these adoption barriers and build greater confidence in the safety of the cloud
- How these issues are the same or different for IT professionals in China, Europe, and the United States

The data we've gathered identifies specific ways the industry can work together to make public and private cloud computing at least as safe—and potentially even safer—for business computing as traditional IT infrastructure is today. IT is concerned with protecting identities, data, and the infrastructure that delivers cloud services, among other areas. The findings of this research provide valuable insight into these issues.

Private versus Public: Definitions

For this report, we define "public cloud" as IT services—including software services, developer platform services, or infrastructure services—that are delivered to an organization over the Internet via a cloud service provider. We define "private cloud" as a data center, often virtualized, that sits behind an organization's firewall and is designed to deliver "IT as a service" to internal users. Cloud security described in this report covers both public and private cloud security.

IT Security Issues: Traditional Infrastructure Compared to Cloud Infrastructure

In traditional IT environments, IT infrastructure sits behind the organization's firewall, and both virtualized and nonvirtualized servers are typically dedicated to a specific line of business. IT professionals can choose from an arsenal of mature security tools that give them a high degree of control over the security environment and the organization's compliance with regulatory mandates.

With cloud infrastructure, in contrast, servers are typically virtualized and shared across multiple lines of business or even among multiple organizations rather than dedicated to specific lines of business. When IT wants to link multiple cloud data centers together to gain efficiencies—linking a public cloud data center based in Singapore, for example, with their private cloud based in the UK—the tools to secure this far-flung infrastructure are still evolving. The result is that IT loses a degree of control and visibility into workloads and data. This makes it difficult for IT professionals to determine whether the organization is meeting specific compliance requirements, which in turn lessens their confidence in security across cloud environments.

Who We Talked To

For this research, we gathered input from 800 IT professionals in four countries: 200 each in Germany, the United Kingdom, the United States, and China. We recruited across a variety of company sizes; respondents were spread evenly among companies with 100–499 employees, 500–999 employees, and 1,000 or more employees.

The IT professionals in our survey participate in strategic IT planning for their organizations and are deeply involved in their companies' cloud initiatives. The majority of the organizations they work for are already in some stage of cloud delivery and are already offering, currently implementing, or currently evaluating cloud technology. For complete details on the IT professionals who participated in our survey, please see the Appendix of this report.

Resources on Cloud Security for IT Pros

This research report is part of an ongoing effort by Intel to help IT professionals understand and implement improved cloud security. IT professionals can find additional resources from the following:

- The Intel® IT Center
  Advice and information on cloud security from Intel's own IT professionals, Intel product experts, third-party analysts, and peer IT decision makers:
  intel.com/cloudsecurity

Executive Summary

IT Pros Have Significant Concerns about Cloud Security

To set the context for our research, we wanted to understand the general level of concern IT professionals have about cloud computing. Concerns are high—particularly when cloud computing opens the door to an increased number of security breaches—and threats are coming from both inside and outside the organization.

Key findings:

- **Companies are seeing a higher number of security breaches than they experience with their traditional IT infrastructure.** Of those surveyed, 28 percent have experienced a public cloud–related security breach.

  Regardless of the number of breaches they've experienced, 65 percent of IT pros who have had a security breach in the public cloud report that this number is higher than what they experience with their traditional IT infrastructure. Full details on page 10.

- **IT pros report that nearly one-third of the security threat faced by their companies comes from internal sources.** Regardless of IT environment—traditional or cloud—IT professionals report that a third of their total security threat comes from inside their own companies. While many of these threats are likely to be more accidental than malign (employees falling prey to viruses and other schemes rather than actively planning unauthorized access to company resources), internal threats represent a significant source of concern for IT professionals. Full details on page 11.

IT Pros' Specific Concerns with Cloud Security

Delving into the specific concerns of IT professionals, we asked about issues with private cloud, public cloud, and compliance. We also investigated concerns about hypervisor vulnerabilities.

Key findings:

- **In the private cloud, IT professionals are most concerned with lack of control.** The top three security concerns of IT professionals related to private cloud are rooted in concerns about control—or rather the lack of control they're experiencing in the private cloud environment. The number-one concern of IT professionals is a lack of controls to enable them to effectively limit access to data and services to authorized users.

  Second was their concern about lack of visibility into abstracted resources. When resources are abstracted—made virtual and shared across multiple lines of business or multiple customers sharing the same servers—it is a challenge for IT professionals to have the same level of control as they do in traditional IT environments. The third major concern is uneasiness about adequate firewalling. Full details on page 12.

- **In the public cloud, IT professionals are concerned with measurement of security capabilities as well as with control.** IT professionals feel they lack a way to measure the security services of their public cloud providers—a concern that landed at the top of their list of concerns related to public cloud use. This worry was closely followed by another concern about lack of control: in this case, the general lack of control they are experiencing over the data stored in public cloud data centers. Full details on page 14.

- **Compliance concerns are keeping some types of workloads and data out of the cloud.** Companies worldwide are being required to comply with government mandates that regulate the flow and storage of certain information—typically healthcare information, financial information, and other types of sensitive data—within or across national boundaries.

  Seventy-eight percent of IT professionals report having to comply with such regulations. For 57 percent of these respondents, security and other concerns are preventing them from moving these workloads and data into the cloud. Specific concerns IT professionals have about compliance in a cloud environment include their ability to meet audit and reporting requirements; worries about legal responsibilities and whether they fall with their organization or a service provider's; and a general concern that public clouds won't allow them to meet certain mandates required of their organization.

  Of the 43 percent of organizations surveyed that are moving regulated data and workloads to the cloud, the vast majority are doing so without an automated way of tracking their regulation compliance. This can add significant IT overhead and put an organization at risk of a compliance liability. Full details on pages 17–18.

- **For both public and private cloud, hypervisor vulnerabilities are a widespread concern.** Hypervisors—a critical piece of virtualized cloud infrastructure—provide the software layer that sits between the hardware and virtual machines (VMs) and allows multiple VMs to share a single hardware platform. Eighty-seven percent of IT professionals are concerned about hypervisor vulnerabilities that could enable hackers to access data or introduce malware into the IT environment. Full details on page 16.

How the Industry Can Respond

Our research provides insight into the specific steps that software and hardware providers, cloud service providers, and others in the technology ecosystem can take to alleviate IT's security concerns about cloud computing. Taking these steps will help increase IT professionals' confidence in moving business data and services into cloud environments, whether they use private or public clouds.

Key findings:

- **In the public cloud, IT professionals identified four key confidence boosters.** Public cloud service providers and others in the technology ecosystem can increase confidence by giving IT professionals the ability to:
  - Set and enforce security policies across clouds, which would give IT a common way to manage and ensure the consistency of security policies across both private and public cloud environments.
  - Create data boundaries, which would give IT greater control over where certain workloads can be run.
  - Ascertain whether public infrastructure is high integrity and free of potentially damaging malware.
  - Compare the security services offered by different public cloud service providers.

Full details on page 21.

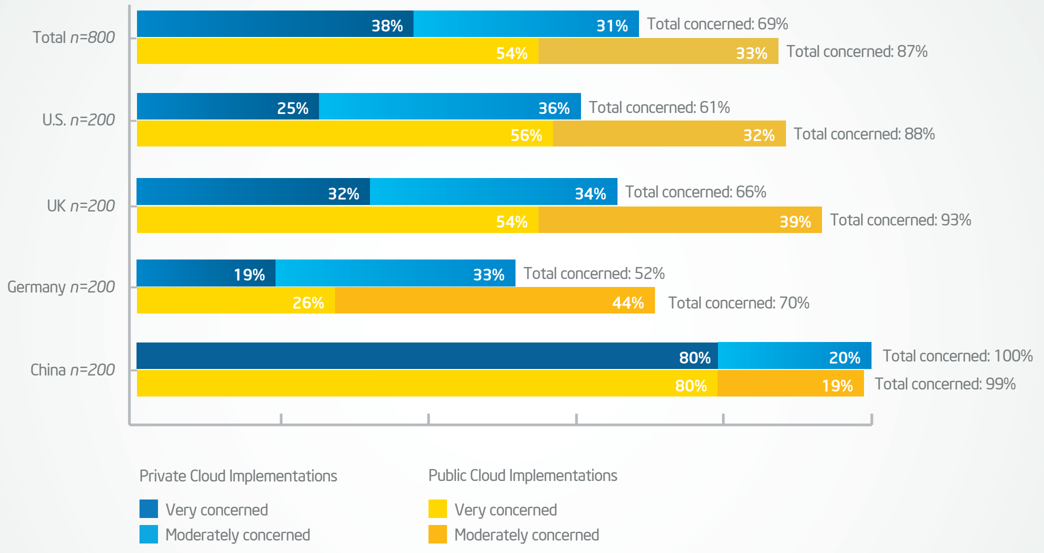
- **Also key for public cloud: 98 percent of IT professionals want a way to measure cloud service providers' security posture.** The vast majority of IT professionals are interested in a service that would enable them to see, in real time, the security controls put in place by the provider and the security status of their environment. Seventy-six percent of IT professionals report being "extremely interested" in such a service, and a full 96 percent say having this ability would increase their confidence in public cloud computing. Full details on page 22.
- **In the private cloud, IT professionals identified three key confidence boosters.** Software and hardware providers in the private cloud space can increase confidence by giving IT professionals the ability to:
  - Create data boundaries, which, as mentioned above, would give IT greater control over where certain workloads can be run.
  - Attest to the integrity of their private cloud infrastructure, which enables them to determine, for example, whether their IT infrastructure is free of malware.
  - Ensure that network packets have not been compromised—that is, that network traffic has not been altered, intercepted, or compromised with malware or other malicious software. Full details on page 23.
- **IT professionals want a way to measure their regulatory compliance.** Fully 98 percent of IT pros are interested in a service that would improve their ability to know whether they are meeting compliance and regulatory requirements, with 65 percent saying they are "extremely interested." Full details on page 24.
- **IT professionals need the ability to access or disable data stored on client devices that are lost or stolen.** With the adoption of HTML5, data stored locally on devices will enable users to keep working even if they are not connected to the cloud service—which raises significant security issues when devices are lost or stolen. Being able to access or disable data on lost or stolen devices is important to almost every IT professional (99 percent), with 73 percent saying it is "very important." Full details on page 25.

Rising Security Anxieties in the Age of the Cloud

Cloud computing has introduced a new world of security issues for today's IT professionals. Some of these issues are completely fresh; others are traditional IT issues that are now amplified in a cloud environment, where multiple lines of business and organizations may share the same virtualized servers.

We first wanted to understand IT professionals' overall level of concern with cloud computing and how this concern may differ between public and private cloud. While concerns are considerable for both, in general the level of concern is higher for public clouds than for private clouds.

Level of Security Concern with Public and Private Cloud Implementations



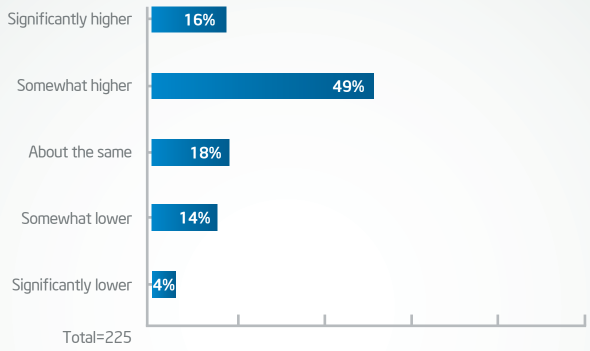
Q: *Please rate your level of overall concern when it comes to security and data protection in adopting ... public cloud.*

Q: *Please rate your level of overall concern when it comes to security and data protection in adopting ... private cloud.*

Public Cloud Users Seeing More Security Breaches

Our research shows that IT concerns with cloud security are justified. Twenty-eight percent of IT professionals surveyed have experienced a public cloud–related security breach. Regardless of number of breaches seen, 65 percent of these companies say this number exceeds the number of breaches they experience with their traditional IT infrastructure.

Number of Breaches: Public Cloud Compared to Traditional IT Infrastructure



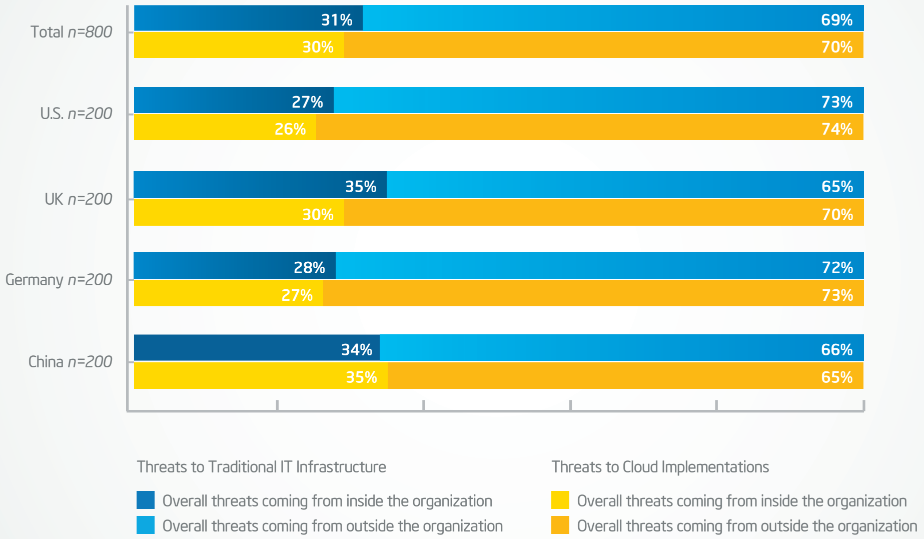
Q: *Compared to your traditional IT/enterprise environment, would you say the number of security breaches you've experienced in a public cloud is ... (Base = users of public and hybrid clouds who have experienced a public cloud security breach.)*

Where Do Threats Come From: Inside or Outside the Organization?

To better understand the nature of the security breaches they face, we asked IT professionals what percentage of threats to their IT security came from inside versus outside their organization. We also asked whether that percentage changed when using a traditional IT infrastructure versus a cloud implementation (public or private). Two key findings resulted:

- IT professionals believe that nearly one-third of the threats come from inside their company.
- That percentage is virtually the same for both traditional infrastructure and cloud computing.

Inside or Outside? Threats to Traditional IT Infrastructure and Cloud Implementations



Q: *Thinking about your traditional IT/enterprise infrastructure and security profile, what percentage of overall threats do you believe come from ...*

Q: *Thinking about your company's cloud security profile, what percentage of overall threats do you believe come from ...*

Understanding the severity of IT professionals' concerns, and the nature of the threats they face, set the stage for questions concerning the specific security issues they are experiencing in public and private cloud environments.

Specific Security Concerns of IT Professionals

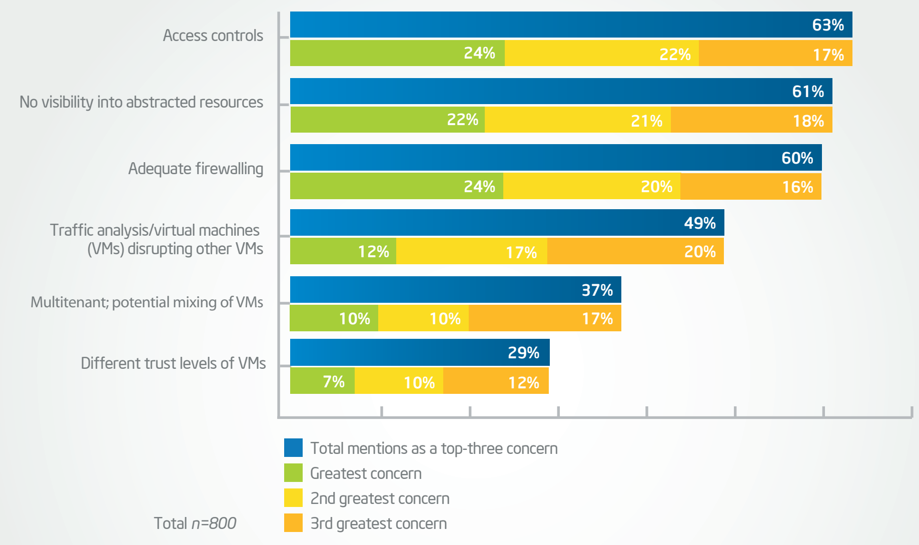
The focus of our research was to identify the specific concerns IT professionals have about security in public cloud and private cloud environments. IT has significant security concerns about both public and private cloud, but the research shows that IT professionals are most concerned about the safety of the public cloud.

Private Cloud: It's All about Control

We asked IT professionals to identify their three greatest security concerns with private cloud computing. Their answers are all about control—or, rather, the lack of control they experience in the private cloud environment. Topping the list of concerns is access controls: the availability of controls they can use to make sure access to corporate data and services is provided only to authorized users.

The second greatest concern is their lack of visibility—and therefore their lack of control—over resources that are abstracted; the third major concern is with adequate firewalling.

Greatest Security Concerns: Private Cloud



Q: *Of the private cloud computing security concerns listed, which would you say are your three greatest concerns?*

These concerns are generally consistent across the four countries included in the survey: the United States, the UK, Germany, and China.

Greatest Security Concerns by Country: Private Cloud

Private Cloud Computing Security Concerns	U.S. (n=200)		UK (n=200)		Germany (n=200)		China (n=200)	
	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns
Adequate firewalling	**26%**	**60%**	24%	**60%**	22%	**56%**	**24%**	**64%**
Access controls	25%	**66%**	**28%**	**64%**	20%	**62%**	23%	58%
Resources are abstracted/ no visibility	24%	**66%**	18%	**56%**	**24%**	**59%**	22%	**62%**
Traffic analysis if virtual machines (VMs) are disrupting other VMs	10%	42%	10%	47%	14%	48%	16%	**62%**
Multitenant; potential mixing of VMs	10%	37%	12%	40%	12%	45%	8%	30%
Different trust levels of VMs	4%	29%	9%	34%	8%	30%	6%	22%

Q: *Of the private cloud computing security concerns listed, which would you say are your three greatest concerns?*

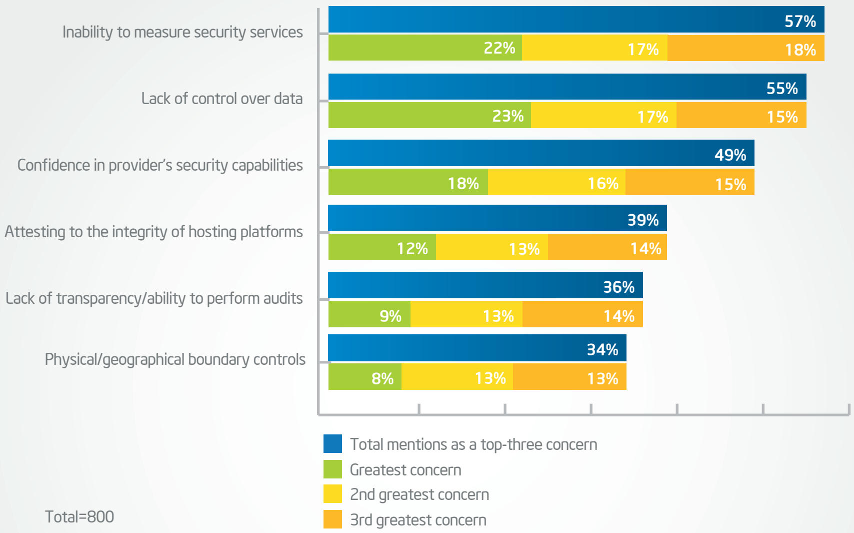
Public Cloud: IT Pros Want Improved Measurement of Security Services

IT security concerns ratchet up a level when considering the public cloud, in which IT cedes a level of security control to a third-party provider whose data center infrastructure is generally shared across its customers.

And, as with private clouds, in the public cloud, IT professionals are worried about lack of control. But they're even more concerned by their inability to measure the security services being offered by their public cloud provider—which, in turn, erodes their confidence in their provider's overall security capabilities.

These concerns are generally consistent across all countries included in the survey with the exception of Germany, where a major concern is physical and geographical boundary controls.

Greatest Security Concerns: Public Cloud



Total=800

Q: *Of the public cloud computing security concerns listed, which would you say are your three greatest concerns?*

Greatest Security Concerns by Country: Public Cloud

Public Cloud Computing Security Concerns	U.S. (n=200)		UK (n=200)		Germany (n=200)		China (n=200)	
	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns	Greatest Concern	Top 3 Concerns
Lack of control over data	22%	**52%**	24%	**56%**	**24%**	**60%**	20%	**51%**
Inability to measure the security services	**28%**	**67%**	**24%**	**58%**	10%	38%	**23%**	**61%**
Confidence in provider's security capabilities	22%	**55%**	14%	**50%**	18%	**50%**	16%	42%
Attesting to the integrity of hosting platforms	10%	42%	12%	41%	9%	28%	19%	**45%**
Lack of transparency/ability to perform audits	7%	33%	8%	36%	12%	36%	10%	41%
Physical/geographical boundary controls	6%	25%	8%	30%	14%	**48%**	6%	34%
Lack of legal governance & indemnification	6%	26%	8%	30%	13%	40%	6%	26%

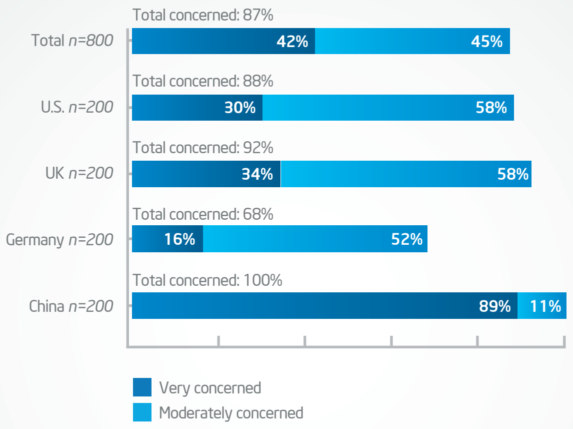
Q: *Of the public cloud computing security concerns listed, which would you say are your three greatest concerns?*

Hypervisors a Common Concern of IT Pros Worldwide

Hypervisors—a critical piece of virtualized cloud infrastructure—provide the software layer that sits between the hardware and VMs and allows multiple VMs to share a single hardware platform. Not surprisingly, hypervisor vulnerabilities are a major source of concern for IT professionals. If a hypervisor is vulnerable to security attacks, then the integrity of the entire public or private cloud implementation is at serious risk. While IT professionals are moving ahead with virtualization and are using hypervisors to gain significant efficiencies in their IT infrastructure, our research shows that they remain concerned about the vulnerabilities of the hypervisors they are using or evaluating.

While concern with hypervisor vulnerabilities is expressed by nearly all IT professionals, the level of concern varies by country. IT professionals in the United States and the UK show similar levels of concern, while their colleagues in Germany are less concerned. In China, however, there is a heightened level of concern.

Level of Security Concern with Hypervisor Vulnerabilities



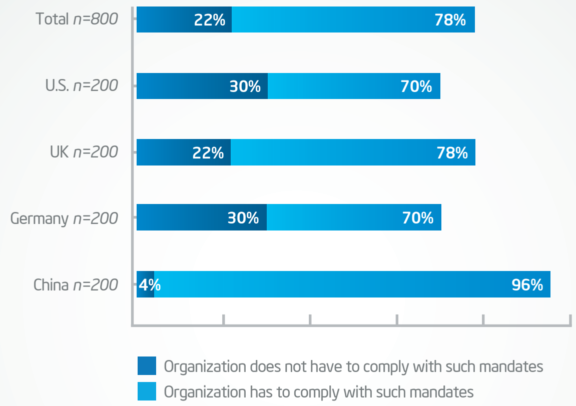
Q: *How much of a concern are hypervisor vulnerabilities for your confidence in private and/or public cloud computing infrastructures?*

Public and Private Cloud: Compliance Is a Major Issue

Realizing that compliance is a major issue for many companies, particularly those in heavily regulated industries such as banking, finance, and healthcare, we asked IT professionals several different questions about how compliance issues affect their planning for cloud computing. Their answers show that compliance issues have a significant effect on the movement of certain workloads and data sets into the cloud.

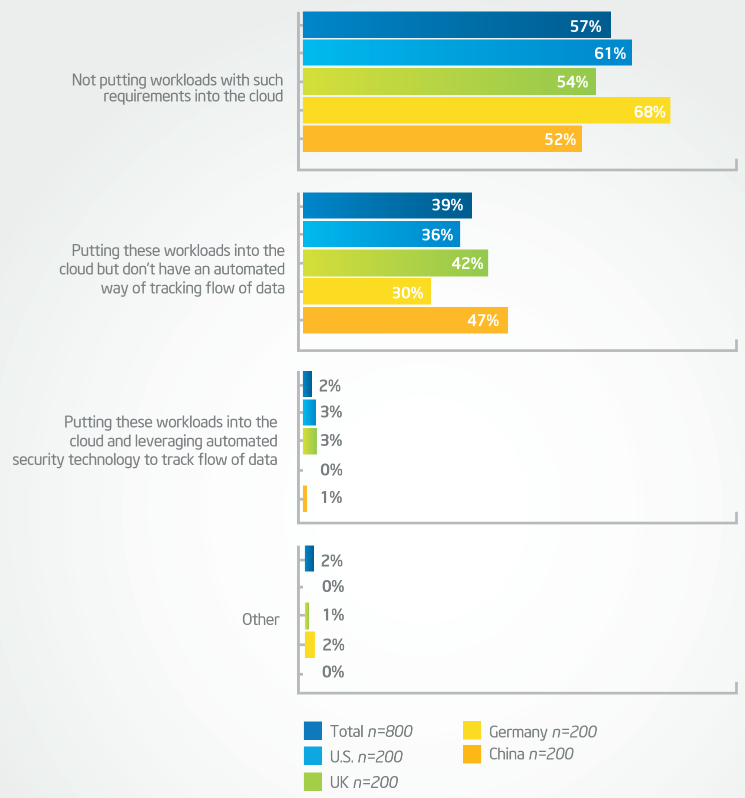
Seventy-eight percent of IT professionals report having to comply with regulations that govern the flow and storage of certain information (typically sensitive information such as healthcare and financial data) across national borders. Of the IT professionals that do have to comply, the majority (57 percent) are not putting compliance-regulated workloads and data into either private or public clouds. Forty percent of IT professionals who are putting these types of workloads and data into the cloud report that they are tracking compliance manually; they don't have an automated way of tracking the flow and storage of data within or across national borders. This can add significant IT overhead and put an organization at risk of a compliance liability. Only 2 percent of IT pros who report that they are subject to regulation say that they are using automated security technology to track compliance.

Compliance with Regulatory Mandates



Q: *There are dozens of mandates that govern the flow and storage of data across national borders. Does your organization have to comply with such mandates?*

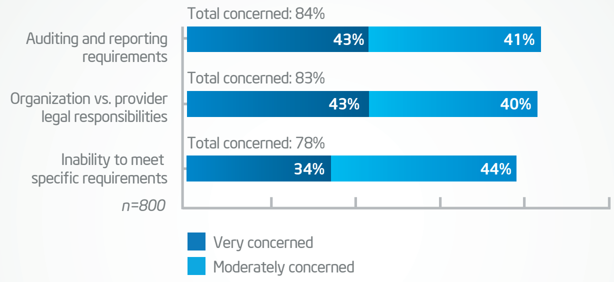
Putting Regulated Workloads and Data into the Cloud



Q: *How do you attest to [regulated workloads] today in a private or public cloud setting? (Base = IT professionals who report having to comply with mandates that govern the flow and storage of data across national borders.)*

To better understand the specific compliance concerns of IT professionals, we followed up with questions about their biggest worries as they relate to the public cloud. The data shows widespread concern with audit and reporting requirements, understanding the legal requirements of their organization versus the cloud service provider's, and their inability in the cloud environment to meet the particular legal requirements their organization faces. However, the level of concern is higher in China, and lower in Germany, than in the United States and the UK.

Concerns with Public Cloud Compliance Issues



Q: *Please rate your level of concern with compliance issues as they relate to a public cloud.*

Concerns with Public Cloud Compliance Issues: Top Concerns by Country

Percent of Respondents Who Are "Very Concerned"	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
Auditing and reporting requirements	42%	38%	22%	69%
Organization vs. provider legal responsibilities	39%	39%	25%	68%
Inability to meet specific requirements	34%	28%	16%	58%

Q: *Please rate your level of concern with compliance issues as they relate to a public cloud.*

How the Industry Can Increase IT's Confidence

While the focus of our research was to identify the specific concerns IT professionals have about security in both public and private clouds, we also wanted to explore the specific actions the industry can take to address these concerns and build IT professionals' confidence in public and private cloud solutions.

Public Cloud: IT Pros Want Control, Assurance, and Measurement

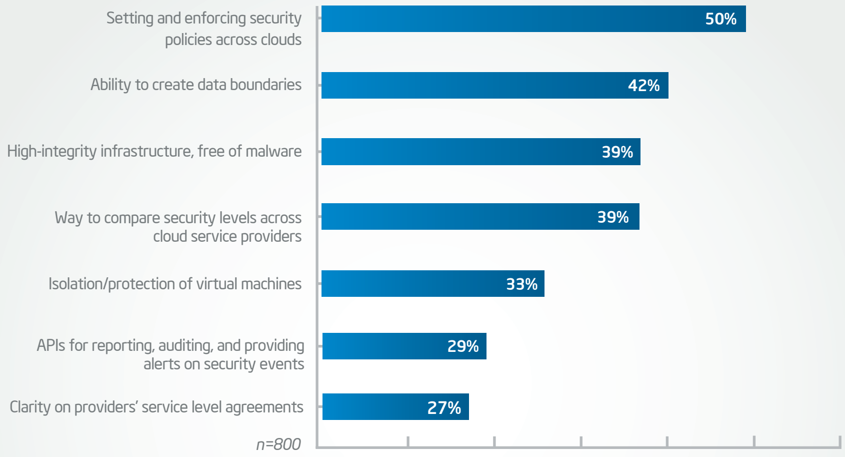
We asked IT professionals to rate the importance of seven actions the industry could take to improve their confidence in moving to the public cloud. In aggregate, they told us that the number-one issue to address is the challenge of setting and enforcing security policies across clouds. This capability would give IT a common way to manage and ensure the consistency of security policies across both private and public cloud environments.

IT professionals also want the industry to address:

- Providing the ability to create data boundaries—which would enable them to control where certain workloads can be run
- Providing the means to help them understand if a provider's infrastructure is high integrity and free of malware
- Providing ways for them to compare security levels across a number of cloud providers

This question, however, revealed some interesting differences among countries. China, for example, showed significantly more interest than other countries in having the industry address the isolation and protection of VMs—not surprising given their level of concern about hypervisor vulnerabilities (discussed on page 16 of this report). The United States showed significantly more interest than other countries in being able to compare security levels across multiple public cloud service providers.

Public Cloud Confidence Builders



Q: *Which of the above, if addressed, would most increase your confidence in adopting public clouds? Please select up to three responses.*

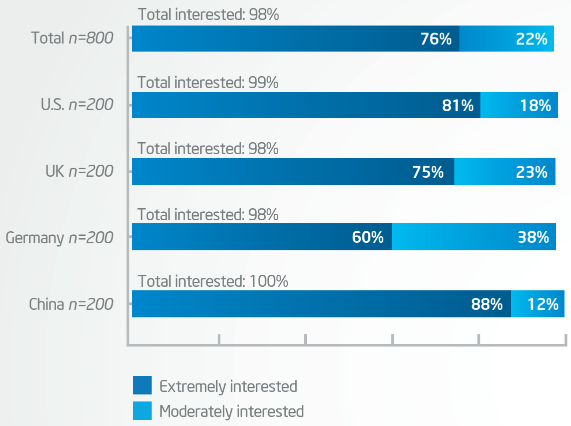
Public Cloud Confidence Builders: By Country

	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
Setting & enforcing security policies across clouds	42%	**50%**	**53%**	**56%**
Ability to create data boundaries	42%	36%	**47%**	42%
High-integrity infrastructure, free of malware	**43%**	36%	33%	43%
Way to compare security levels across cloud service providers	**50%**	**38%**	36%	32%
Isolation/protection of virtual machines	26%	26%	32%	**49%**
APIs for reporting, auditing & providing alerts on security events	26%	28%	28%	36%
Clarity on providers' service level agreements	24%	30%	24%	31%

Q: *Which of the above, if addressed, would most increase your confidence in adopting public clouds? Please select up to three responses.*

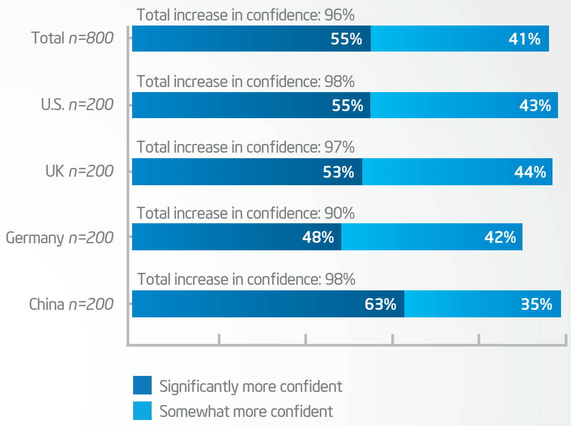
We also asked IT professionals whether having a way to measure their public cloud providers' security services would improve their confidence. As detailed earlier in this report, the lack of this type of measurement was the number-one concern IT professionals have about public cloud. It is no surprise, then, that 98 percent of IT professionals are interested in a real-time service that would enable them to measure the security posture of their providers—and that 96 percent report that having such a service would improve their confidence in the safety of moving services and data to the public cloud.

Interest in Service for Measuring Security of Cloud Providers



Q: How interested would you be in a service that enabled you to measure the security posture of your cloud service provider's infrastructure in real time?

Effect of Security Measurement Service on Confidence in Cloud Providers



Q: How much impact would [a real-time security measurement service] have on your confidence of security in moving services and data to a public cloud?

Private Cloud: Three Key Confidence Builders

As discussed earlier in this report, IT professionals' key concerns about the private cloud all relate to feeling a lack of control. When we asked IT professionals what would most improve their confidence in the private cloud, their number-one answer is about gaining control.

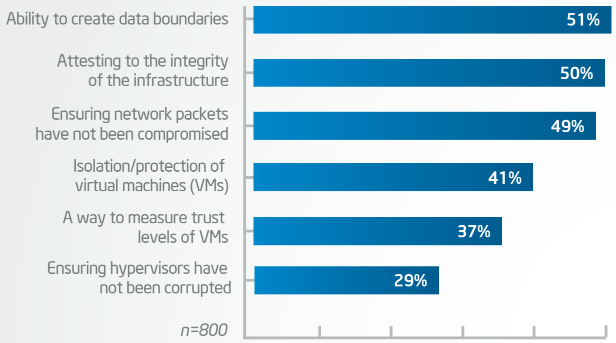
In aggregate, the majority of IT professionals believe that having the ability to create data boundaries would most increase their confidence in the safety of the private cloud. The ability to create data boundaries would give IT greater control over where certain workloads are run, which in turn would help them comply with regulatory mandates.

Following close behind, however, are two issues that relate to confidence:

- IT professionals would like the ability to verify the integrity of their private cloud infrastructure—so they can be assured that their workloads are running on trustworthy infrastructure and can provide the proof needed to satisfy the compliance requirements.
- They would also like the ability to ensure network packets have not been compromised.

This question also brings to light some interesting differences among the IT professionals in different countries. China's concern with hypervisor vulnerabilities surfaces again, with the majority of their IT pros reporting that isolation and protection of VMs would most increase their confidence. For German IT professionals, the number-one issue by a significant margin is the ability to ensure the integrity of network packets.

Private Cloud Confidence Builders



Q: *Which of the above, if addressed, would most increase your confidence in adopting private clouds? Please select up to three responses.*

Private Cloud Confidence Builders: By Country

	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
Ability to create data boundaries	**56%**	**52%**	46%	52%
Attesting to the integrity of the infrastructure	54%	50%	42%	52%
Ensuring network packets have not been compromised	40%	48%	**58%**	52%
Isolation/protection of virtual machines (VMs)	40%	31%	36%	**57%**
A way to measure trust level of VMs	42%	43%	30%	34%
Ensuring hypervisors have not been corrupted	28%	25%	26%	38%

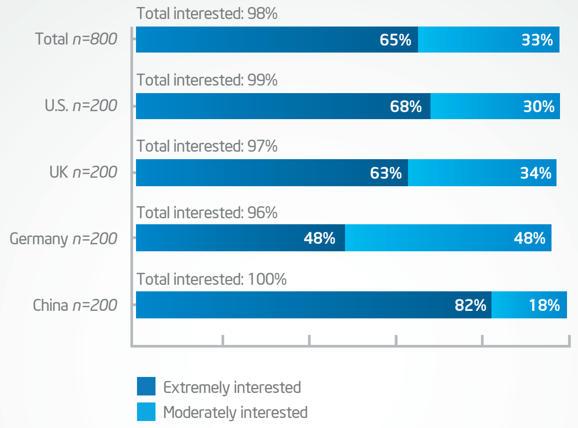
Q: *Which of the above, if addressed, would most increase your confidence in adopting private clouds? Please select up to three responses.*

IT Pros Want Compliance Measurement

As discussed earlier in this report, 57 percent of IT professionals who report having to comply with regulatory compliance requirements are responding by not moving the associated workloads and data into either a private or public cloud. Those who are moving sensitive data into the cloud are doing so, the vast majority of the time, without having an automated way to track the flow or storage of this data.

This likely explains the 98 percent interest of IT professionals in a report service that would enable them to report against multiple compliance standards using a common framework. While interest in this type of service is high across all countries, it is particularly high in China—where 96 percent of IT professionals say they are required to comply with mandates regarding the flow and storage of data.

Desire for a Compliance Reporting Service



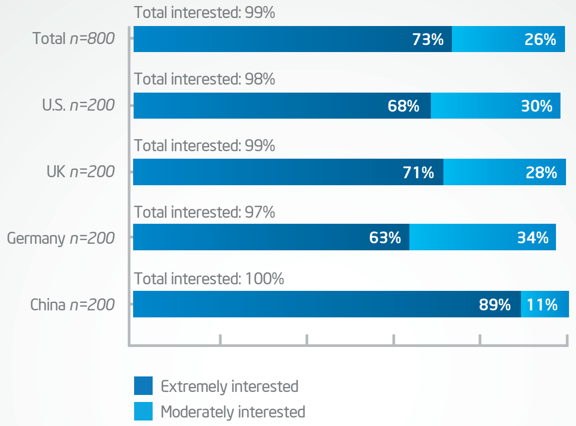
Q: *How interested would you be in a reporting service that enabled you to report against multiple compliance standards that use a common framework?*

Near-Universal Desire to Disable Lost or Stolen Devices

With the adoption of HTML5, data stored locally on devices will enable users to keep working even if they are not connected to the cloud service. While this ability has the potential to raise business productivity and efficiency, this "cached environment" also raises significant security issues for IT professionals when devices are lost or stolen.

It therefore becomes very important to IT professionals to be able to deal with missing devices. With near universal agreement, IT professionals would like a service that enables them to disable the data on a missing device before hackers can gain access. If, for example, a PC were left in a taxi or lost in an airport, IT would be able to remotely disable access to the device or to its data before it falls into unsafe hands.

Desire for "Cache Control" and Ability to Disable Lost/Stolen Devices



Q: *Given this cached environment [of HTML5], how important would it be for your organization to disable the device or access to the data stored on the device if it were stolen?*

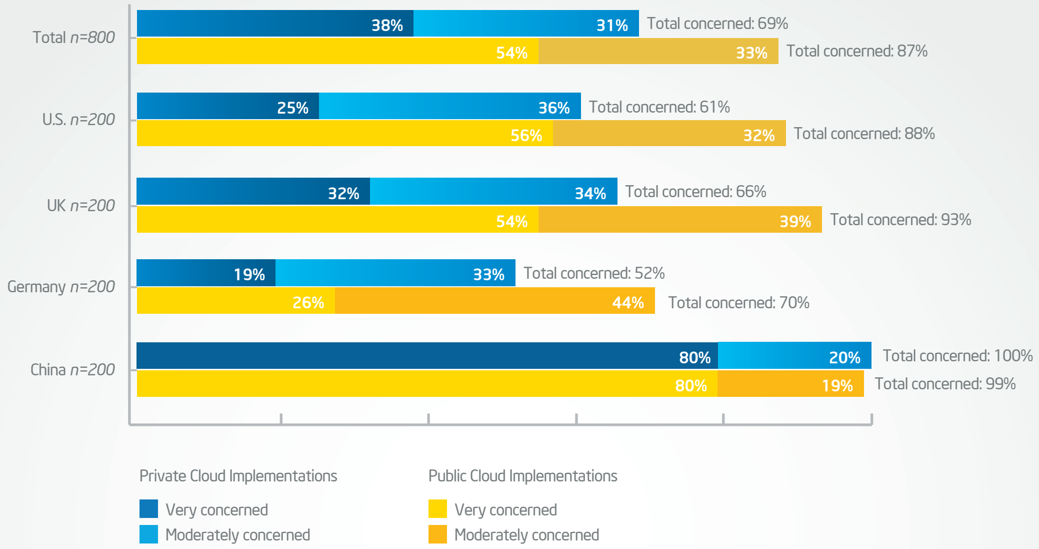
Global View: Differences among Countries

One of our objectives with this study was to identify differences in security concerns among IT professionals in the four countries included in the survey: the United States, UK, Germany, and China.

What we found is that the concerns themselves did not differ as much as the level of concern. IT professionals in the four countries are in general agreement about the specific areas of concern and the specific actions that can be taken to increase their confidence. But the general level of concern regarding cloud security is higher among IT professionals in China than it is with their counterparts in the United States and the UK. On the flip side, the general level of concern among IT professionals in Germany tends to be lower than it is with their colleagues in the United States and the UK.

Below, for example, are the responses of IT professionals regarding their overall level of concern related to public and private cloud computing.

Level of Concern with the Security of Cloud Computing: By Country



Q: *Please rate your level of overall concern when it comes to security and data protection in adopting ...*

The most important reasons for differences among countries, however, are likely to be found in the particular business culture, security environment, and regulatory climate unique to each country. Fully understanding these differences will likely require additional research.

Conclusion

We initiated this research to better understand the specific reasons that IT professionals feel less confident in the security of public and private cloud computing than they do with their traditional IT infrastructures. We also wanted to explore the ways that the IT industry can come together to alleviate these concerns and boost IT confidence in the cloud.

No single provider in the IT ecosystem—hardware, software, or cloud service provider—can single-handedly address IT's cloud security issues. The research shows that IT professionals have serious concerns about control and measurement: They seek more control over data and access, and they want better ways of measuring integrity, compliance, and the services offered by external cloud providers. Solving these issues will require efforts across the IT industry.

We believe this research shows the necessity of the industry coming together to build common standards and frameworks. For cloud computing to reach its potential, we have to address security issues holistically and collectively rather than in fragments and industry silos. The cost of not working together is high: Cloud computing will fall short of its promise because organizations will fail to trust their most important data and workloads to cloud environments.

Industry-wide security standards—and common frameworks that enable IT professionals to control and measure their cloud environments—will help ensure that cloud computing becomes not the exception but the rule. If the IT industry works together to advance cloud security capabilities and standards, Intel believes that cloud computing has the potential to offer the same or even greater security and safety than is provided by the traditional IT infrastructures of today.

Appendix: Methodology and Audience

Responses to this blind survey were gathered via an online questionnaire; 800 surveys (200 each in the United States, UK, Germany, and China) were received between January 26 and February 14, 2012. A sample size of 800 has a maximum sampling variability of ±3.3 percent at the 95 percent confidence level; 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 cloud environments in their organization
- Have implemented, are currently implementing, or plan to implement cloud environments

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 Job Responsibilities	Total (n=800)	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
Vendor selection for key components of cloud technology	94%	94%	91%	94%	98%
Participating in strategic technology planning	93%	97%	94%	89%	94%
Working with most senior IT management to set the strategic IT direction for the company	93%	97%	94%	88%	94%
Planning, implementation, maintenance of cloud technology	92%	95%	94%	87%	94%
Leading a team of IT specialists to support business initiatives	87%	87%	86%	81%	93%
"Hands-on" implementation responsibilities	76%	76%	79%	83%	68%

Company Size	Total (n=800)	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
100–499 employees	35%	27%	27%	42%	46%
500–999 employees	31%	33%	20%	38%	35%
1,000+ employees	33%	40%	53%	21%	20%
Median	*735*	*849*	*1,057*	*612*	*565*

Worldwide Locations	Total (n=800)	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
1 location	13%	12%	8%	23%	12%
2–4 locations	29%	27%	19%	33%	37%
5–9 locations	28%	24%	35%	21%	33%
10–14 locations	14%	18%	17%	11%	11%
15–19 locations	14%	18%	19%	12%	8%
Unsure	1%	1%	3%	2%	--

Industry	Total (n=800)	U.S. (n=200)	UK (n=200)	Germany (n=200)	China (n=200)
Manufacturing	17.5%	15.0%	15.0%	15.0%	25.0%
Financial services	14.1%	15.0%	8.0%	17.0%	16.5%
Professional services	11.8%	16.5%	15.0%	10.0%	5.5%
Computer-related business or service	8.5%	10.0%	10.0%	8.5%	5.5%
Retail	7.5%	8.5%	8.0%	5.0%	8.5%
Healthcare	7.1%	9.0%	4.0%	10.0%	5.5%
Construction	6.1%	2.5%	9.5%	5.0%	7.5%
Transportation & logistics	5.9%	5.5%	6.0%	7.0%	5.0%
Education	4.9%	5.0%	6.0%	5.0%	3.5%
Telecommunications	4.3%	1.5%	2.5%	5.5%	7.5%
Wholesale & distribution	3.4%	4.5%	2.0%	4.5%	2.5%
Utilities	2.4%	3.0%	2.5%	1.5%	2.5%
Government	2.1%	1.5%	5.0%	1.0%	1.0%
Media & entertainment	1.3%	0.5%	3.0%	1.0%	0.5%
Agriculture, forestry & fishing	1.0%	0.5%	1.5%	0.5%	1.5%
Hosting	0.4%	--	--	1.0%	0.5%
Nonprofit	0.3%	0.5%	0.5%	--	--

More from the Intel® IT Center

Peer Research: What's Holding Back the Cloud? Intel Survey on Increasing IT Professionals' Confidence in Cloud Security is brought to you by the Intel® IT Center, Intel's program for IT professionals. The Intel IT Center is designed to provide straightforward, fluff-free, unbiased information to help IT pros implement strategic projects on their agenda, including virtualization, data center design, intelligent clients, and cloud security. Visit the Intel IT Center for:

- Planning guides, peer research, and vendor round tables to help you implement key projects
- Real-world case studies that show how your peers have tackled the same challenges you face
- Information on how Intel's own IT organization is implementing cloud, virtualization, security, and other strategic initiatives
- Information on events where you can hear from Intel product experts as well as from Intel's own IT professionals

Learn more at intel.com/ITCenter.

Share with Colleagues

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

0512/JM/ME/PDF-USA 327311-001

Sponsors of Tomorrow.™