# Blind Trust Is Not A Security Strategy

## Lessons From Cloud Adopters

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for iland

May 2016

EMA™
*IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING*

## Table of Contents

Abstract ..... 1

Trust in the Cloud – But is it Blind Trust? ..... 1

- Which Cloud Services? ..... 1
- Demographics Overview ..... 1
- Factors Influencing Cloud Provider Selection ..... 2
- Perception Finally Meets Unchecked Reality: Cloud is More Secure! ..... 3
- More Than Technology: Security Management Improvements ..... 4
- Cloud Security Deployments vs. Data Center Security Deployment ..... 5
- Top Cloud Deployed Security Technologies ..... 5
- To "Cloud" or "Not to Cloud"...That is the Question ..... 7

EMA Perspective ..... 7

About iland ..... 8

# Blind Trust Is Not A Security Strategy: Lessons From Cloud Adopters


## Abstract

Enterprise Management Associates recently conducted a research project that investigated multiple aspects of cloud service providers and the adoption of their services. The research looked to identify major motivators and inhibitors of adopting cloud services for both compliance and non-compliance constrained workloads. Security emerged as the top adoption concern.

The research showed that though they have differing responsibilities, both IT and security agreed that implementing proper security in their cloud environments is better than accelerating deployment speed but achieving a less secure environment. IT respondents admitted that they would rather suffer a delay for a new cloud application deployment than rapidly deploy an application into a potentially insecure environment and, even better, if they help the businesspeople understand the issues, the businesspeople agreed in nearly a 3 to 1 margin. IT sided with security to delay a product launch due to security concerns rather than suffer a significant security breach by a margin greater than 2 to 1.

Cloud adoption is a long-term partnership between the business and the provider. It provides a new toolset to address both traditional and new IT service delivery challenges. Within that toolset security, elasticity, and agility are all available to accelerate business service delivery, but the organization must evaluate its needs to determine not only current requirements but also expected future needs to ensure how each provider under consideration can or will meet those needs.


## Trust in the Cloud – But is it Blind Trust?

### Which Cloud Services?

For the purposes of the research, EMA included a list of the cloud services that were encompassed in the research and the breakdown of what percentage of respondents are using them:

1. Infrastructure as a Service (IaaS) – 83%
2. Storage as a Service (StaaS) – 76%
3. Software as a Service (SaaS) as a provider reselling or providing other services – 74%
4. Platform as a Service (PaaS) – 71%
5. Software as a Service (SaaS) as a consumer – 70%
6. Backup as a Service (BaaS) – 63%
7. Disaster Recovery as a Service (DRaaS) – 62%

All participants in the survey were users of IaaS, DRaaS or PaaS, but were also broad consumers of many types of cloud-based IT services.

### Demographics Overview

The project surveyed a pool of 669 respondents. However, based on filtering and other criteria the maximum respondent pool for any of the core questions was one hundred. Respondents were composed of enterprise (62%) and midmarket (38%) respondents located in North America, with large enterprises with 20,000 or more employees comprising 11% of the total population. All of the respondents worked in IT and IT security in various operations and management positions. Their organizations varied in industry, including Finance/Banking/Insurance (34%), Hi-Tech (25%), Manufacturing (13%), Healthcare/Medical/Pharma (10%), Retail/Wholesale (10%), and other industries (8%).

Cloud has been growing in attention, function, and revenue for the last six years. It is interesting to note that 78% of the organizations are using cloud in some official business workload and 32% used one or more cloud service for between four and ten years, while only and 14% were engaged in a cloud service for less than one year.

Of the organizations that are using cloud, 41% of the enterprises have been using one or more cloud service for seven to ten years. That is a significant number of early adopters, especially for the enterprise segment. Only 27% of the large enterprise organizations have used cloud for more than three years. Given the level of investment in their own infrastructure, this was much more in line with expectations.

## Factors Influencing Cloud Provider Selection

The research project provided cloud consumers with a list of fifteen options and asked them to identify the top three that influence their consideration for a cloud provider. The figure below shows how each of the fifteen affects the consumer's choice of public cloud providers.

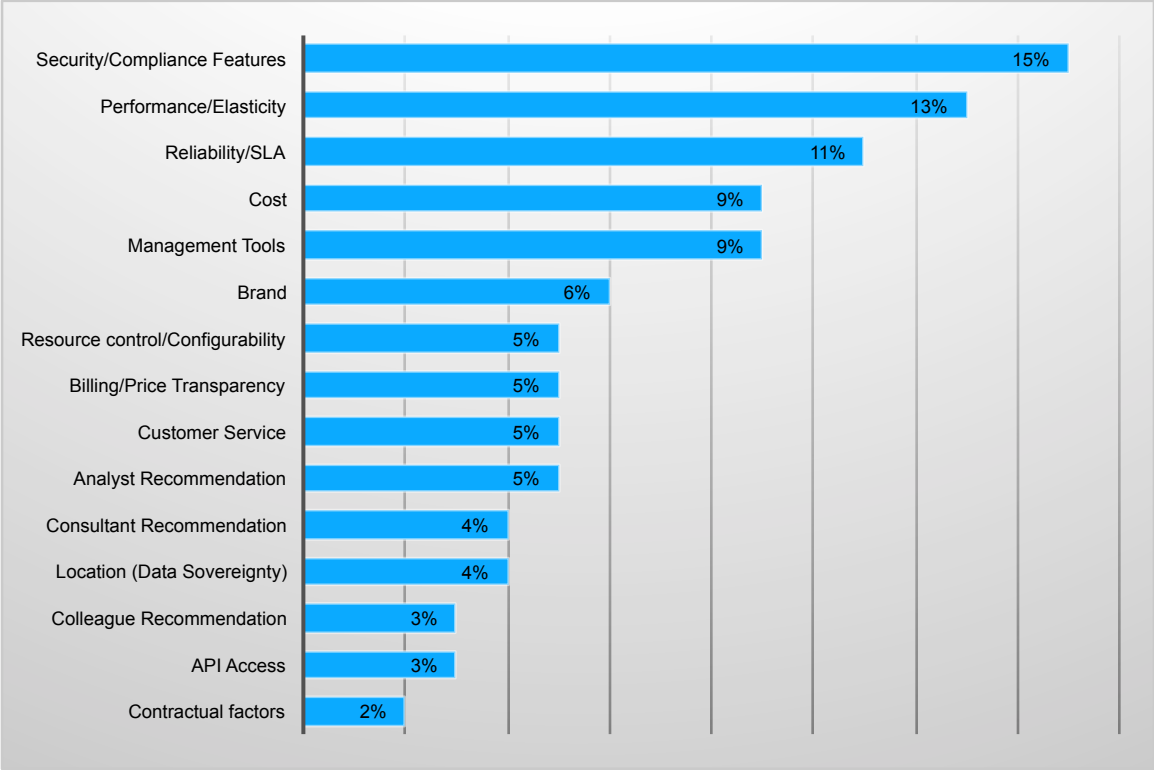


Figure 1: Consideration Factors When Choosing a Cloud Provider

None of these results should be a surprise as being a top selection, though it was interesting to have security in the top spot. This demonstrates the heightened security awareness that took place over the last two years. All of the breach notifications and the ensuing loss of brand confidence, revenue, and breach-related costs pushed security to the forefront, both on the provider and the consumer side. No one wants to be the subject of a breach, but the cost is more poignant for cloud providers since a single breach that was tracked back to a lack of controls on the provider's side would mean certain death for any, but possibly the largest, cloud provider.

As seen in Figure 1 above, performance and reliability are strongly linked to the selection of the cloud providers. Some hypervisors, like VMware, provide more native tooling to support these priorities than others, so the underlying hypervisor platform should be a point of questioning when investigating a cloud provider.

## Perception Finally Meets Unchecked Reality: Cloud is More Secure!

Perception is catching up with reality. When cloud first emerged and for some time after, people perceived cloud as less secure than on-premises data centers. This was not an unexpected. The general populace does not want to get burned when the new "widget" is put to the test. Consumers, not businesses, are first to adopt new technologies, then that acceptance bleeds over into their professional lives, increasing commercial adoption. Today, cloud is in full tilt and thus far has stood the test of time. If we evaluate the number of data breaches over the past two calendar years, there were thousands reported for compromised, on-premises data while there were no cloud vendor compromises or significant breaches, supporting the perception that clouds are more secure.

In the research study, 77% of individuals reported they felt cloud security was superior to their organization's traditional on-premises data center security. The figure below depicts the breakouts of the aspects of cloud security that made up that group.

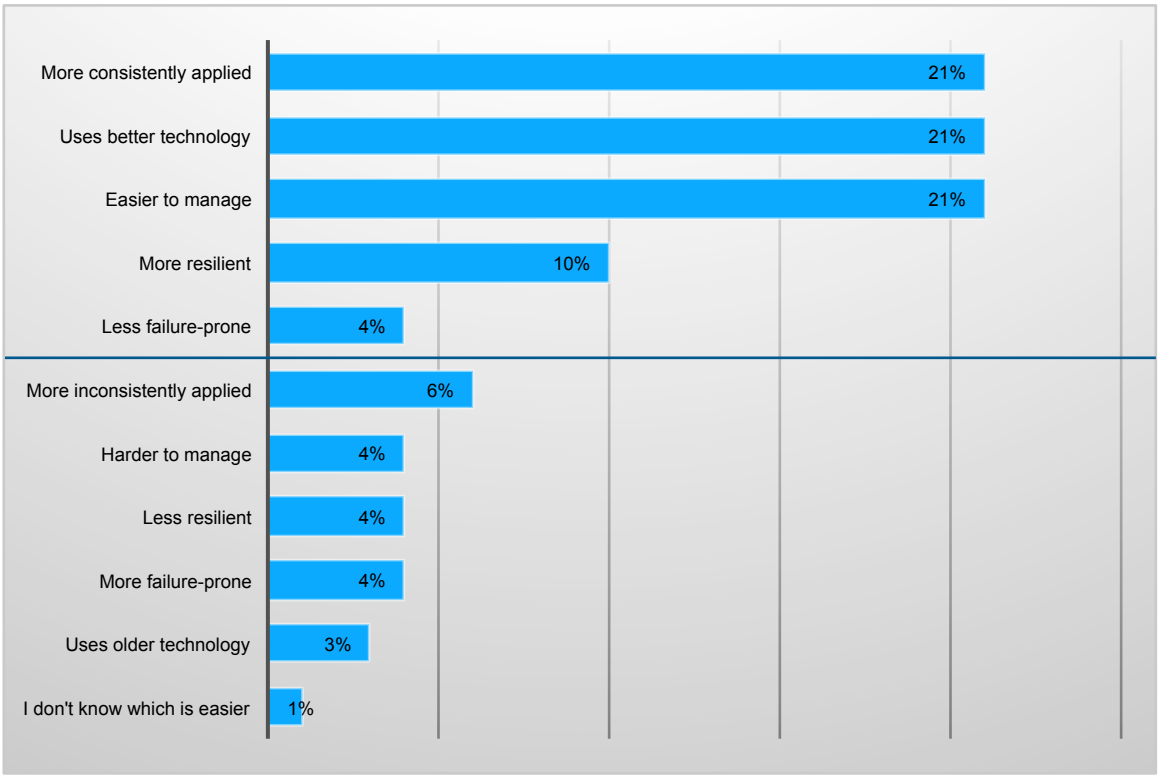


Figure 2: How Security of Public Cloud Compares to Your Organizations On-premises Data Center

The interesting issue is that while so many feel security is better in the cloud, many organizations seem to take that perception as fact without verifying it for themselves. When asked how they ensure their cloud workloads are secure, 47% of security respondents said they, "simply trust that the provider is delivering on their agreements." This was the most common answer.

Though history supported that approach in the lack of disclosed cloud provider data losses, this is not a recommended strategy. Blind trust is never a preferred strategy, but many cloud providers are very shrouded or vague about the security measures they put in place at a foundational level. Many organizations must "blindly" trust in their cloud provider's security because they lack qualified staff to ask the right questions (68%), or when they are given responses, they don't have the technical acumen to understand the answers (34%) so they just go with it.

In addition to trust, the next two most popular responses were much more in line with best practices; "We test and verify all claims" (21%) and "We implement our own security measures on top of the provider" (21%). The latter is evident by the number of security services being purchased by cloud subscribers, and especially by IaaS consumers. EMA highly recommends that cloud consumers understand where their cloud provider's security measures stop and where they need to pick up to appropriately protect their cloud workloads and data.

## More Than Technology: Security Management Improvements

These influencing factors created an interesting dichotomy in perception. While 77% of organizations feel that cloud does have better security, there were concerns about a number of items that cloud providers could improve. The top six challenges that organizations needed their cloud providers to address better were security related! The following figure shows which needs were identified when asked for cloud subscribers' top 3 issues they need assistance with.

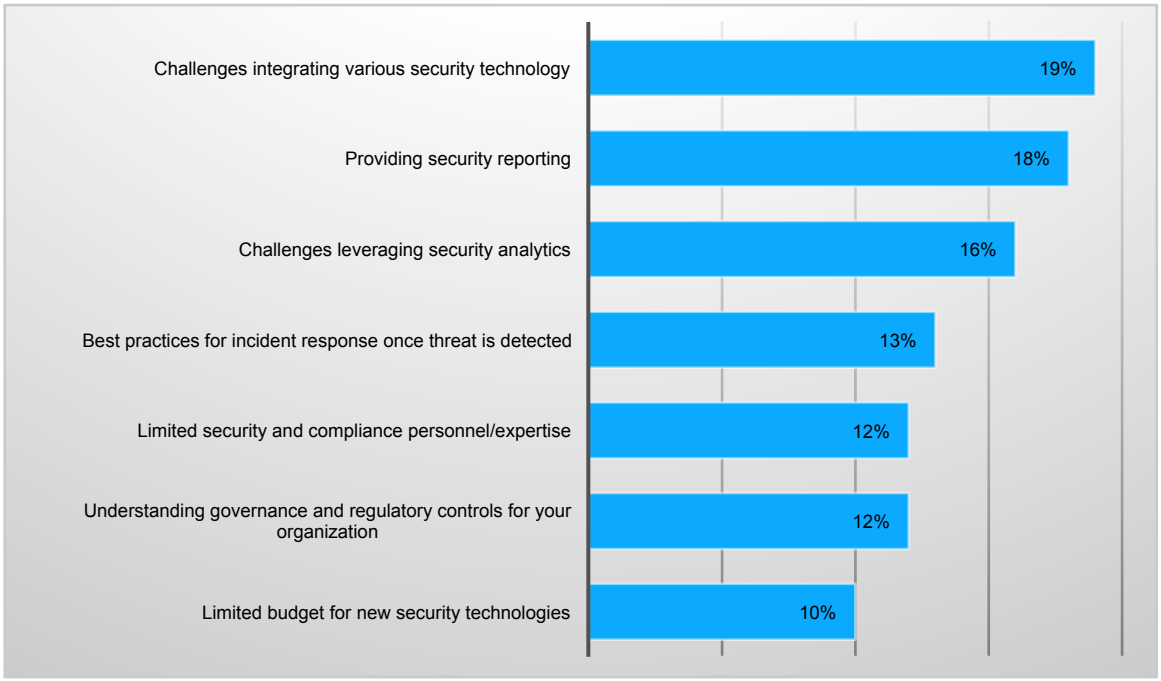


Figure 3: Top 3 Issues Clients Need Cloud Services to Improve on

Too often organizations purchase a wide variety of security tools that they then have to manage from separate interfaces and/or processes within the provider, so they either are not able to get full functionality or proper function, thus yielding the net effect of spending money to provide less than expected security. Solving this particular shortcoming seems to be a no-brainer on the part of both the cloud vendor and the security solution providers. If security solution vendors invest in getting tools integrated into the cloud services up front, then both they and the cloud vendor will see increased revenue.

Providing security reporting is a tricky situation. Struggle with achieving the desired granularity, accuracy, and/or automation from the reporting engines within their cloud portfolio causes them a great deal of manual work. Grey area, especially in their compliance-related workloads, reduces their willingness to continue moving their most critical workloads into the cloud. To maintain and attract these premium workloads, the reporting has to meet all three of those criteria (granularity, accuracy, and/or automation).

Choosing the right cloud provider makes all the difference in addressing these issues. The perception that cloud does security better but simultaneously looking at cloud's general shortfalls in security creates a dichotomy. Therefore, while most organizations agree that cloud security is superior to on-premises security, this perception is based more on the surplus of technology and faith in the system than on the actionable, integrated security data that is being thrown off their cloud environments. So, as is often the case in tech, the focus of trouble shifted from the technology of securing the cloud to the operations and management – the people side – of securing the cloud.

## Cloud Security Deployments vs. Data Center Security Deployment

Cloud is increasing security in several ways. First, EMA identified 18 categories of security capabilities from security alerting to IP Geo-fencing for data sovereignty. EMA asked participants to identify which they had deployed in their on-premises data center and which they had deployed in their cloud workloads. Without exception, respondents had more security deployed in the cloud than on-premises. On average, security services were deployed 1.5 times more often in the cloud than in the data center. Some services were deployed greater than twice as often in the cloud over the data center.

## Top Cloud Deployed Security Technologies

This report discussed cloud security adoption, so now it is time to discuss the security technologies that are included in that conversation. The types of solutions and features available will vary by cloud provider, so EMA recommends that IT and security collaborate to identify both what the organization already has in place and what they may want in the future, choosing a provider that best meets both of those lists.

The following figure depicts the deployment rates of all of the identified cloud security services and what percentage of the respondents identified each as a premium service that they were willing to pay more to use.

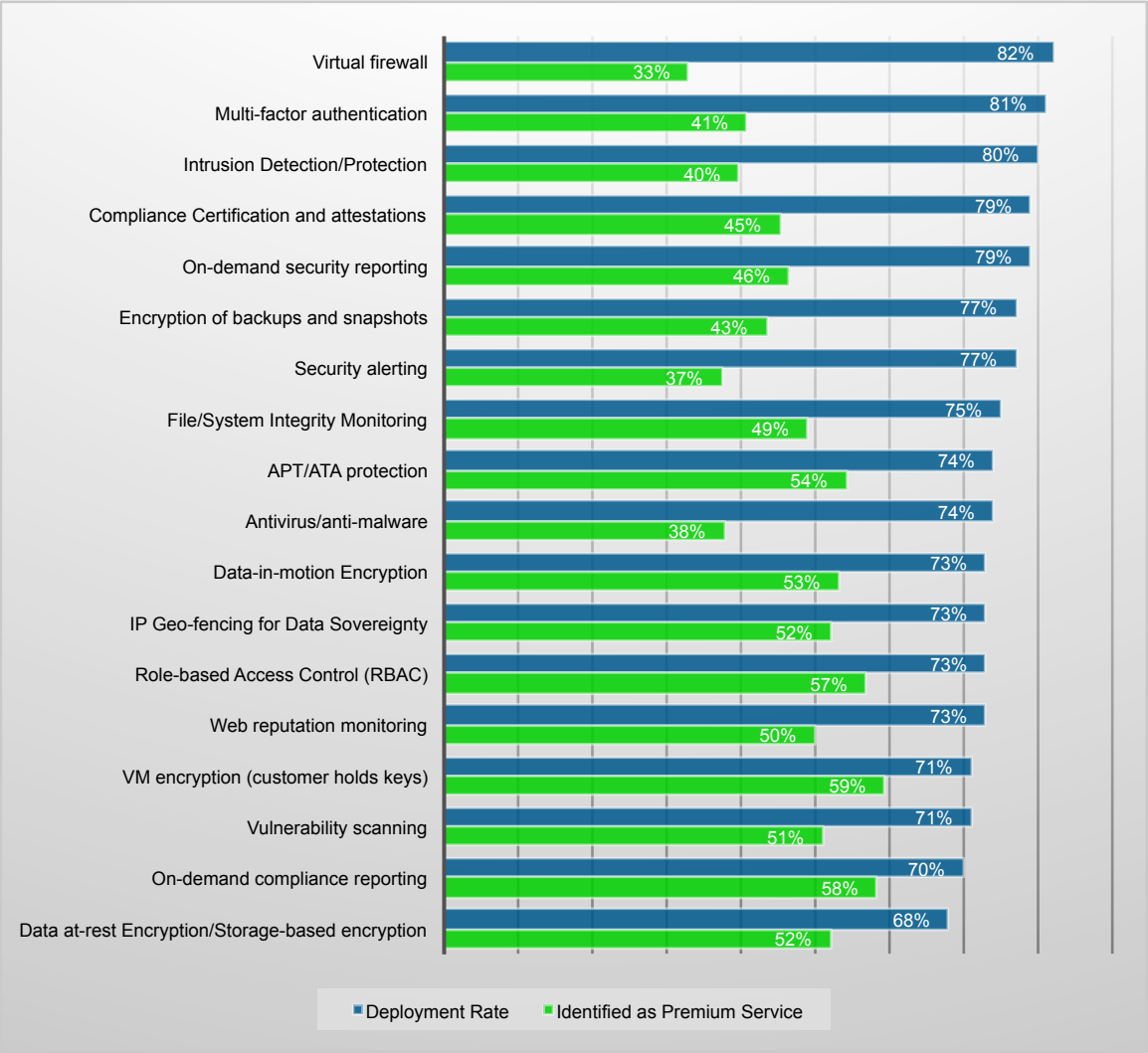


Figure 4: Cloud Security Services

None of these should come as a surprise, but what was interesting was that 48% of the respondents using cloud security were evaluating more services to further increase security. At the same time, only 31% of respondents indicated that they felt they didn't need additional security.

The top five services identified as premium services are: VM encryption (customer holds keys) (59%), On-demand compliance reporting (58%), Role-based Access Control RBAC (54%), and APT/ATA protection, Data-in-motion Encryption (53%). Aside from identifying which services the cloud provider offers as part of their portfolio, cloud consumers should understand up front which security services are included as part of the base price of the service and which are premium services, since those raise the monthly spend.

It is important to note that earlier in the paper, EMA identified the customers' desire for a compliance/privacy-related liaison. This is a role, not a technology, and therefore was not part of the lists above. It was highly interesting that 50% of the participants feel that this should be included as part of the basic services, while only 33% felt it was a premium upgrade. This shows the increase in security pressures for all workloads. Most cloud providers do not offer this support role as an included service, and only a few more offer it as a premium service, making it another point of differentiation among the vendors.

### To "Cloud" or "Not to Cloud"...That is the Question

The security respondents identified that 96% of their organizations have compliance-related workloads in the cloud. This is significantly higher than expected and good news for both cloud providers and cloud consumers. This is good news for cloud providers because the compliance-related workloads often drive more premium security and reporting services. The good news for cloud consumers is the raising of the bar by cloud providers to meet their needs, making them more available from a broader range of providers, which creates positive price pressures for the consumers.

Interestingly, the IT respondents did not report the same level of compliance workload deployment. This indicates a significant gap in IT's understanding of compliance requirements and/or the compliance-related workloads in the environment. This gap could lead to exposures for the organization if IT were to place a compliance-related workload into a non-compliant cloud provider.

Drilling down on organizations that did not have compliance-related workloads in the cloud, 19% (<1% of total survey body) are on their way into the cloud looking to engage a cloud service in the next year. Beyond that, 22% (<1% of total survey body) are cloud adoption laggards, indicating that they are looking but with no specific time frames for adoption in mind. Lastly, 59% (2.4% of the total survey body) have no plans to move forward with a cloud workload in the foreseeable future.

Further investigating the participants that have compliance requirements but do not currently have compliance-related workloads in the public cloud, EMA found the two primary drivers were, "can't find a cloud provider that meets reporting requirements" and the organizations are, "not ready to trust a public cloud with compliance-related workloads." Both of these issues received 40% of the respondent votes. Of the organizations that identified as not ready to trust the public cloud, 83% of them said security was their main concern.

## EMA Perspective

The research results bring out several key issues that should be addressed as part of the cloud adoption project. First and foremost, proper cloud implementation can be a secure and cost effective way to provide deployment and lifecycle agility and elasticity to business service delivery. Security can no longer afford to be the "No Guys" looking at cloud as a "non-starter." Security people have to find secure solutions to serve business needs and facilitate business objectives with cloud as one of their tools.

Cloud providers offer a wide array of security options. Be sure that as the organization evaluates cloud providers, it understands the security requirements before signing. The number of organizations currently evaluating additional security technologies to apply to cloud is more than twice any of the other reasons for non-deployment (Cost, Complexity, Availability, or Unnecessary), indicating that moving to the cloud is the opportune time to deploy previously unused security technology.

Organizations investigating cloud must consider the human effort of managing security in the cloud, whether compliance-related or not, selecting cloud providers and security tools that support the organization in evaluating, assuring, and managing security in that cloud and providing security management and reporting to meet the business needs.

IT and security both need to accept that compliant workloads ARE going to the cloud, and architect for that need—to ensure all compliance requirements are met before deployment. This will save the need to move or suffer fines or additional fees.

IT and security need to remember that they are partners in supporting and delivering business objectives.

Both cloud providers and cloud consumers must understand why organizations look to move compliance-related workloads into the cloud. For consumers, it is important to know that they are not experiencing unique and unsolvable business challenges; there are solutions available to address their problems. For providers, it is important to know so they can determine where they are lacking or leading, and prioritize their features and functionality to address the more common problems that can improve their attractiveness and thus their market share.

## About iland

With 20 years of IT experience serving global customers and hosting critical workloads, iland approaches cloud computing with a different goal: to provide customers with secure, easy-to-adopt cloud services while delivering unmatched visibility & customer support.

**Cloud Security:** iland provides built-in advanced security features from antivirus to encryption to file integrity monitoring and more – all easily configured and reported on through our cloud console.

**Compliance:** Our in-house compliance team helps customers from the initial legal agreements they may need (for HIPAA/HITECH) through to configuring their environment and supporting an audit process.

**Integrated Management:** iland built – and continues to innovate upon – our own console that brings together everything from basic cloud management to disaster recovery to security, reporting, backups, and billing.

**Customer Support:** Whether it's initially on-boarding your workloads or adjusting their resource allocations, crafting your DR plan or configuring your network, iland has certified technical support staff located around the world, available by phone for each of our customers.

**Global Presence:** With data centers across the United States, and in Europe and Asia Pacific, iland has a global footprint with global connectivity options.

Built on VMware virtualization atop Cisco and Nimble hardware and best-of-breed security technologies, the iland cloud delivers secure public cloud, hosted private cloud, disaster-recovery-as-a-service and backup, managed through a powerful and intuitive console.

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

---



**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3387.051716