Sponsored content

WHITE PAPER

Market Pulse

Cloud Optimization Shines Spotlight on Need to Integrate Security Measures

THE QUEST FOR ADVANCED SECURITY ranks among the top business drivers fueling cloud migration and usage, but transparency across hybrid infrastructure and integration challenges remain, according to a global IDG Research study of 600 cloud-using companies across multiple industries. To clear the bar, a growing number of companies are partnering with third-party providers, leveraging their specialized security expertise and proven track records to facilitate successful cloud deployments — and realize the cloud's associated operational and innovation benefits.

Migration to the cloud is accelerating, in part, because longstanding security concerns have given way to an understanding that for some organizations cloud platforms can deliver more robust protections than a typical internal IT department. According to survey respondents, an average of 41% of IT infrastructure and applications have shifted to the cloud; all qualified respondents claim at least one-quarter of their total IT infrastructure now runs in public-cloud environments.

More rigorous data security is a top business driver behind the accelerated adoption of public cloud, cited by 38% of respondents (ranking in between cost savings [42%] and shortened time to market [36%]). In addition, companies in the health and safety sectors, in particular, are far more likely (65% of respondents) to count rigorous data security as a top advantage of public clouds.

The IDG survey also found that companies making the leap to the cloud were confident in the security of their deployments. Seventy-four percent of respondents said they trust their cloud-based data to be secure; 75% said they have a good understanding of the security-related regulatory and compliance issues associated with cloud migration; and 71% were confident that the many benefits to be gained from a public-cloud environment overshadow potential security risks.

In fact, as enterprises deploy infrastructure and applications to the public cloud, they are starting to recognize the security advantages. "The [head of security at my company] said that the companies that host applications and services in the cloud do a

accenture | aws

ACCENTURE AWS BUSINESS GROUP

CIO
Strategic Marketing Services

IDG Communications, Inc.

"Cloud infrastructure and cloud security are the things that I outsource. I know my business, I know my app stack, and I need to be responsible for the deployment and maintenance of that app stack. The rest of it, I have a partner do."

— CIO for a health, physics, and safety company

much better job at security than we do," notes the director of IT operations for an industrial products company. "This is what they do. They can't drop the ball on this."

This may be because companies such as Amazon Web Services (AWS) support an expanding array of robust security functions compared to what is typically offered in on-premises deployments, notes Christian Lachaux, security lead for the Accenture AWS Business Group. For example, AWS' 15-plus services in the areas of security and governance include fine-grained identity and access management controls and newer capabilities in areas such as automated security assessments and machine learning-powered security services. This gives cloud platforms an edge over the security practices being implemented by most internal IT departments, he notes. "These kinds of capabilities are much easier and cheaper to implement [in the cloud] than they would be on-premises," Lachaux says.

Despite momentum, challenges remain

While survey respondents and industry players are bullish on the security advantages of the public cloud, they acknowledge the complexity of the landscape and a host of emerging challenges.

Integrating data security was the most challenging aspect of deploying applications to the cloud, cited by 45% of respondents to the IDG survey. This is well ahead of other hurdles, including managing variable cloud costs (36%) and compliance and legal risk management (34%).

Industry sector also plays a role in how well companies are situated to deal with security integration challenges: Respondents in highly regulated industries such as life sciences (53%) and consumer products (54%) were more likely to flag data security integration as a trouble spot compared to those in the industrial products (43%) and financial services (44%) sectors.

Not surprisingly, security integration is also the most in-demand skill set as companies broaden competencies to ensure success of cloud deployments. Forty-four percent of respondents to the survey flagged security integration as a sought-after skill set, and 40% identified risk-management capabilities.

While the most desirable skill sets were similar across the different vertical sectors, the health and safety vertical and life sciences sector were more likely to actively seek security integration skills, cited by 53% and 58%, respectively. In comparison, respondents in the industrial products field cited project management (48%) as their most in-demand skill set, while those in consumer products prioritized data/analytics (49%) and risk management (48%) over security integration (46%).

Security integration for cloud environments has become a focal point because it raises challenges companies haven't dealt with in the past. While public-cloud service providers such as AWS have added high-level security services to their platforms, retraining is sometimes required to get internal IT personnel up to speed on properly configuring the environments and leveraging new protections.

Consider Amazon Macie, a machine learning-powered security service that automatically discovers, classifies, and protects sensitive data in AWS. While Macie provides a clearer understanding of access patterns and automatically delivers detailed alerts when unauthorized access or inadvertent data leaks are detected, it requires a different knowledge set to effectively leverage the new capabilities.

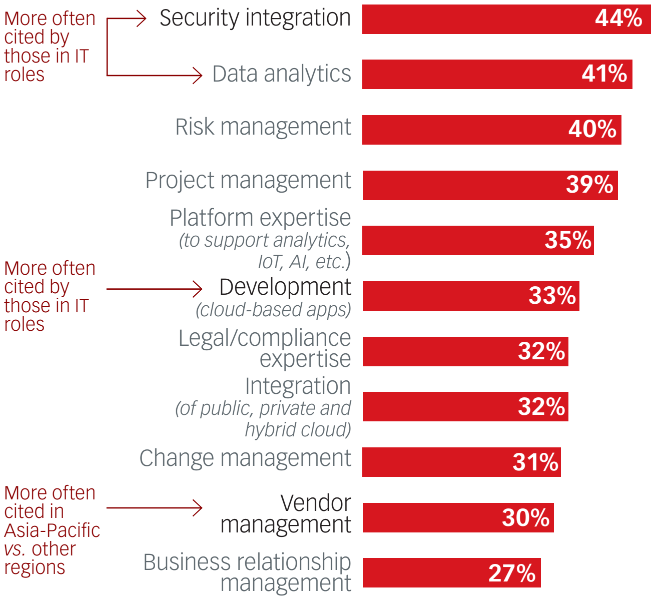
"[Security] services are becoming ever more complex, especially when you start to add machine learning and algorithms into the equation," says Hart Rossman, Director, Global Security Practice, AWS Professional Services. "You need to understand how to use data and feed data to other parts of the security posture. These kinds of services are invaluable, but it would be very complicated and time-consuming for a company to try and build them on its own."

At the same time, most cloud providers don't yet offer the full spectrum of necessary security services, requiring gap analysis and additional third-party tools to achieve holistic protections. This extra step creates another layer of management complexity and further complicates security integration, often requiring expertise not available in most internal IT organizations.

Third-party providers to the rescue

To fill in the gaps, companies are increasingly turning to third-party partners to address cloud security challenges and provide critical expertise, especially in areas such as security integration. Nearly all respondents to the survey (98%) said they would benefit from third-party expertise in at least one aspect of cloud security.

Fig. 1 **Security Challenges Drive the Need for Security Skills**



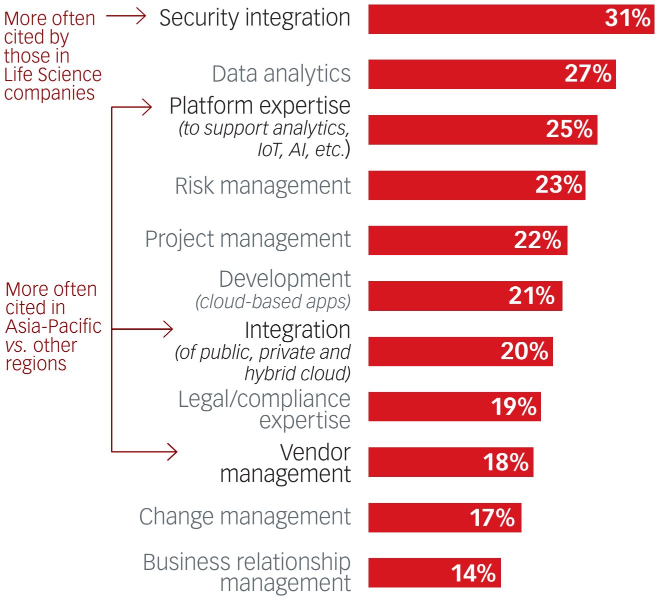
Source: IDG Research

Respondents are looking for help with issues such as educating IT and IT security staff on the intricacies of cloud security (41%), implementation of security solutions (39%), and proper usage and rollout of IT security metrics (39%). Once again, the need for security integration skills was a key driver for companies to develop these partnerships, cited by nearly one-third of survey respondents (31%).

Drilling deeper into the survey results, 67% of respondents plan to handle integration of data-security functions through a third-party partner or using a combination of in-house and third-party resources; and 68% plan to use partners to educate IT and IT security staffers and the general employee population about cloud security issues. Respondents with non-IT titles were much more likely to see third-party partners as a solution for countering security integration challenges: Thirty-one percent said the function would be completely handled by a third party, compared to only 15% of IT respondents. The latter group is closer to the work and therefore may be less likely to offload control.

"Cloud infrastructure and cloud security are the things that I outsource," notes one CIO respondent at a health, physics, and safety company. "I know my business, I know my app stack, and I need to be responsible for the deployment and maintenance of that app stack. The rest of it, I have a partner do."

Fig. 2 **Security Concerns Drive Third-Party Partner Alliances**



Source: IDG Research

Third-party partners can step in and fill the void in a variety of ways, especially in areas related to security integration. Potential services include:

- **Performing an initial assessment** to determine security and risk tolerance
- **Establishing** a comprehensive, holistic security strategy and architecture
- **Collaborating closely** with companies to identify a holistic set of security processes that can work across hybrid cloud, satisfy industry and regulatory requirements, and map to key business practices
- **Identifying the right portfolio** of applications to deploy in a public cloud by assessing security and risk tolerance
    - As part of this stage, a third-party partner can help establish identity and access management to streamline and control access to cloud and enterprise services and applications.
- **Making recommendations** for ease of orchestration across platforms

> **"The [head of security at my company] said that the companies that host applications and services in the cloud do a much better job at security than we do. This is what they do. They can't drop the ball on this."**
>
> *— Director of IT operations for an industrial products company*

- **Training IT and IT security teams** in the nuances of security and compliance in a public-cloud environment
- **Providing security training** for end users
- **Delivering managed services** in areas such as data protection, SIEM (security information and event management), incident management forensics, and managed operations, among other offerings

For many respondents, reliance on third-party partners for these emerging areas is critical as they try to do more with fewer internal IT resources. "I'm not getting done what I need to do with the compliance, risk management, security, and vendor management areas because I don't have enough skills to manage them," confirms one CIO survey respondent at an industrial products company. "Once you downsize your organization by two-thirds, the people who remain are very experienced, but they're just not experienced in this area."

Conclusion

As companies steer more of their infrastructure to the cloud, many find themselves confronting a similar scenario: They are confident in the security capabilities of public-cloud services, but they need help addressing some of the more complex challenges related to security integration and key talent acquisition. A specialized third-party provider can help close lingering security gaps, optimize and automate the cloud environment for peak performance, and ensure companies are successful as they migrate to and innovate in the cloud.

Click here to learn more.

For more information, please contact:

Christian Lachaux
Security Lead for the Accenture AWS Business Group

christian.lachaux@accenture.com

Accenture AWS Business Group
accentureaws@amazon.com