Predicts 2017: Cloud Security

Published: 11 November 2016    ID: G00296116

Analyst(s): Jay Heiser, Steve Riley, Greg Young, Neil MacDonald

With the security implications of cloud computing still not fully understood, security and risk management leaders must carefully guide their organizations through evolving areas of implementation and purchasing best practices.

Key Findings

- No useful level of consensus exists on what constitutes best practices for cloud security, and as a result, organizations struggle to determine which cloud control processes and products they should apply.

- The state of cloud security practice and the fitness of the associated technologies continue to mature, building awareness among IT leaders around the appropriate use cases for cloud computing, but further development is necessary.

- Excessive focus on IaaS security draws energy and attention from SaaS control, a crucial responsibility for organizations relying on cloud applications.

Recommendations

Security and risk management leaders managing cloud security and emerging technology security should:

- Develop a security and control organizational model that emphasizes the three key cloud security functions, with different individuals managing the security of virtualized environments, the control over the utilization of SaaS, and the risk and compliance concerns inherent in a multitenant environment.

- Utilize the growing variety of cloud control tools, including CWPP for virtualization security and CASB for SaaS governance, to enhance visibility into cloud-based activities and to ensure reliable compliance with policies.

- Implement additional control mechanisms to augment the native capabilities of public cloud services.
Strategic Planning Assumptions

Through 2020, 70% of cloud security, compliance, and risk-control time and resources will address SaaS provider and activity management.

Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.

By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

In 2017, dissatisfaction with security features will encourage over half of new IaaS customers to add third-party security products within 12 months.

Analysis

Cloud computing remains hyped and widely misunderstood. Ambiguity about what cloud computing actually delivers to an organization is compounded by a variety of real and imagined concerns about the security and control implications of different cloud models. In practice, most of the concerns that chief information security officers (CISOs) and security teams have around cloud computing fall into one of three areas (see Figure 1):

1. The security of virtualized environments, including private clouds and IaaS
2. The control over the utilization of SaaS and the data located within such models
3. The risk and compliance responsibilities inherent in a multitenant environment
Each one of these three areas of cloud security carries unique challenges. Each is managed by different corporate staff. As cloud models evolve, business units must master a succession of new processes and products. For IT security and risk leaders, attention to some of the evolving practices in cloud control will assist in identifying how to achieve security over these separate but linked areas.

What You Need to Know

Despite many concerns, cloud computing has turned out to be a secure practice. Significant doubts remain, though, about the particular use cases that are appropriate for the various forms of cloud computing. Relatively little consensus exists among security leaders and IT professionals around the policies and technologies that are best used for security and control.

Fortunately, there are a growing number of useful security and control practices. Given the highly complex and distributed nature of cloud computing, these new security and control practices are often practical only with new technologies that provide visibility into activities and the status of data. Increasingly, IT departments are applying policy through tools that use the cloud to secure the cloud, overcoming the scalability challenges of complexity, volume and distribution.

Orchestration platforms, such as cloud workload protection platforms (CWPP) and cloud access security brokers (CASB), represent an increasingly significant form of a tool, enabling the organizational control of complex and distributed activities within different cloud computing environments.
Strategic Planning Assumptions

Strategic Planning Assumption: Through 2020, 70% of cloud security, compliance, and risk-control time and resources will address SaaS provider and activity management.

Analysis by: Jay Heiser

Key Findings:

- The SaaS market is 55% bigger than the IaaS market, estimated at $38.6 billion versus $24.9 billion (see "Forecast: Public Cloud Services, Worldwide, 2014-2020, 3Q16 Update").
- SaaS products can be easily purchased by non-IT business units and used without the knowledge of the IT department.
- The nature of the prevailing SaaS model means that the enterprise has relatively less ability to exert control over user privileges and activities.

Market Implications:

As the usage rate of SaaS increases, organizations regularly express impressions of SaaS as an uncontrollable model. This lack of control could be quite costly, as CASB vendors report huge amounts of sensitive data stored inappropriately in SaaS. The lack of agreement on which corporate role is responsible for SaaS governance, and the relative lack of policy requiring more specificity around SaaS "ownership," has helped to mask urgency over SaaS control. Yet with over 1,000 SaaS apps reportedly in use in client organizations, pressure builds among security and IT teams to manage such resources with something more than the limited control mechanisms offered by these systems.

Single points of control, such as identity governance and administration (IGA) tools and CASB, are increasingly important for security teams, which can now maintain governance over what would be an otherwise unmanageable SaaS environment.

While clear product categories have yet to fully solidify, it is now obvious that third-party mechanisms to manage policy, privileges and activity will grow in use within midsize to large enterprises, and within highly regulated organizations of all sizes.

Recommendations:

Security and risk management leaders managing cloud security should:

- Recognize the relative risks associated with the poor visibility of SaaS activity, and the relatively weak control features typical of SaaS offerings.
- Develop a plan for the effective utilization and governance of SaaS.
- Identify opportunities to consolidate control across multiple clouds through IGA tools and CASBs.
Select the situations where the organization can reasonably expect better SaaS control — across the business, you can’t do everything to the same degree of rigor.

Related Research:

- "Cloud Procurement Skills and Guidelines Optimize Results and Minimize Risk"
- "Everything You Know About SaaS Security Is Wrong"
- "Developing Your SaaS Governance Framework"

Strategic Planning Assumption: Through 2020, public cloud IaaS workloads will suffer at least 60% fewer security incidents than those in traditional data centers.

Analysis by: Neil MacDonald

Key Findings:

Gartner has concluded that the security posture of major cloud providers is as good as or better than most enterprise data centers, and that security should no longer be considered a primary inhibitor to the adoption of public cloud services. However, simply moving on-premises workloads to a public cloud doesn’t automatically make these workloads more secure.

New approaches are needed that exploit the programmatic infrastructure of public cloud IaaS providers. If these capabilities are properly leveraged, the workloads will be better protected than those in most traditional enterprise data centers. Successful attacks typically result from misconfiguration, mismanagement, missing patches and mistakes; thus, the more we can use automation to remove and reduce human error (and to tackle the patching problem), the more secure our services will be. Changes to security and management processes to adopt high levels of automation could be applied in enterprise data centers, but such changes require a fully software-defined, programmatic infrastructure that most enterprise data centers simply do not have.

Finally, not all IaaS providers have equivalent security and automation capabilities. Amazon Web Services (AWS) is ahead of Microsoft Azure, which is ahead of Google Cloud Platform (GCP) at this point, and these three hyperscale cloud providers are well ahead of the rest of the market.

Market Implications:

- Properly exploiting the programmatic infrastructure of IaaS providers to improve security will require changes to security culture, knowledge and processes, thus slowing adoption.
- Not all security vendors support public cloud IaaS, so enterprises may be required to use different vendors and consoles than those used in their own on-premises data centers.
- The best security solutions will be those that integrate natively into the IaaS environment.
The built-in security capabilities of leading IaaS providers will encroach on parts of the information security market, such as basic firewalling, web application firewall (WAF) and application delivery controller (ADC).

**Recommendations:**

Security and risk management leaders managing cloud security should:

- Utilize the cloud IaaS provider's native security capabilities, in conjunction with secure DevOps (DevSecOps) practices and tools, to automate security controls throughout the application life cycle.
- Require security vendors to fully API-enable their capabilities for orchestration and automation to fill gaps in IaaS-native capabilities, or if consistent policy is desired in hybrid scenarios.
- Integrate application security testing and other vulnerability scanning capabilities into the deployment cycle, including scanning containers if they are used.
- Use immutable infrastructure to ensure automated uniformity of deployments, and prevent administrative access to infrastructure once deployed.
- Architect similar automated security and management capabilities in private cloud deployments, whether internally developed, hosted or outsourced.

**Related Research:**

- "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center"
- "Market Guide for Cloud Workload Protection Platforms"

**Strategic Planning Assumption:** By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

**Analysis by:** Steve Riley

**Key Findings:**

- Properly instrumented workloads can benefit from greater visibility and control in the cloud than on-premises.
- Most IT departments aren't yet ready for the default IaaS paradigm in which developers have responsibility for everything.
- Mapping cloud security controls to IT security and operations teams requires investing in new tools from new vendors.
- Attacks against cloud deployments succeed because customers, not providers, fail to fully address their portions of the shared-responsibility model.
Market Implications:

The common perception that placing workloads in public clouds requires visibility and control trade-offs is simply not true. IaaS cloud providers offer two important capabilities that provide the necessary control and visibility into the cloud. An identity and access management (IAM) feature helps enterprises design an authentication and authorization scheme that empowers users to get work done. At the same time, the feature ensures that they have only the necessary privileges required for their roles. An instrumentation and logging feature tracks the "who, what, when, where" details associated with all cloud resources — valuable data for security monitoring, performance tracing, budgeting and auditing.

The default IaaS paradigm expects developers to write code, of course. It also expects developers to manage operations functions — such as instance configuration and patching — and to configure security controls, like packet filtering. Many enterprises struggle to adapt to this paradigm. In response, providers have extended their IAM features, enabling IT departments to define functional groups that align with typical IT work roles. An emerging product category extends this further to establish security and operational control planes that span multiple clouds and even on-premises components (see "Market Guide for Cloud Workload Protection Platforms" for more information). These tools automate security at scale and mitigate configuration vulnerabilities that could allow attacks, such as accidentally exposing a database server to the public internet.

Enterprises benefit from the security built into the cloud. With IaaS, for example, the provider is responsible from the concrete to the hypervisor, and the customer is responsible from the virtual machine to the applications, data and users. So while the public cloud reduces overall security scope, it doesn’t completely eliminate the need for customers to manage the top end of the computing stack. On-premises security habits and designs are a poor fit for the cloud. To properly address the customer portions of the shared responsibility model, leaders should plan to make full use of the cloud’s native visibility and control capabilities, and augment with third-party tools when appropriate.

Recommendations:

Security and risk management leaders managing cloud security should:

- Educate security and infrastructure and operations (I&O) teams about the full breadth of native visibility and control features offered by cloud providers.
- Evaluate and deploy new cloud-aware tools to improve visibility and control across multiple cloud services, to involve security and I&O teams in day-to-day cloud activities, and to relieve developers from distractions not related to writing code.
- Treat the cloud as an opportunity to apply some fresh thinking and to adopt new methods for defending information from attack.

Related Research:

- "Staying Secure in the Cloud Is a Shared Responsibility"
**Strategic Planning Assumption:** In 2017, dissatisfaction with security features will encourage over half of new IaaS customers to add third-party security products within 12 months.

*Analysis by:* Greg Young

**Key Findings:**

- The built in or native IaaS security option can be a good starting point for single cloud enterprises.
- Not all security safeguards are available within the portfolio of native IaaS security offerings.
- Correlating and rationalizing security policy and security operations between multiple noninteroperable security mechanisms, as well as satisfying compliance requirements, adds difficulty and complexity.

**Market Implications:**

Security within IaaS is a quickly shifting landscape. IaaS vendors are offering security features, but they are usually not as fully featured or easily integrated with third-party solutions. As IaaS adoption increases, so too do the numbers of enterprises sourcing IaaS from multiple vendors; such native solutions are not interchangeable. The ability for third-party security solutions to integrate with native controls is still emerging.

Firewall policy management (FPM) vendors are the first movers in this space, although their emphasis is mostly on policy and reporting. Gartner believes supporting heterogeneity is the emerging dominant success factor for third-party security controls, a capability in which most FPM vendors excel. However, if an enterprise is almost exclusively with a single IaaS vendor and does not need multi-environment support, the savings for using native security controls can be spectacular.

**Recommendations:**

Security and risk management leaders managing cloud security should:

- Determine whether your enterprise has or will adopt multiple IaaS providers, and factor this into the native versus third-party security decision. Native security controls from different IaaS providers are not likely to be interoperable at present or in the midterm.
- Communicate your granular requirements to existing and potential vendors. If the native security features meet requirements, then they are contenders on a shortlist.

**Related Research:**

- "Best Practices in Network Segmentation for Security"
A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

This topic area is too new to have on-target or missed predictions.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Clouds Are Secure: Are You Using Them Securely?"

"How to Evaluate Cloud Service Provider Security"

"How to Enhance the Security of Office 365"

More on This Topic

This is part of an in-depth collection of research. See the collection:

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNited KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp