IDC

TECHNOLOGY ASSESSMENT GUIDE

Sponsored by: Lacework

Use this guide to help navigate the cloud security vendor selection process to capitalize on digital-first efficiency gains using build time and runtime solutions to protect your distributed workforce.

Vendor Assessments Are Key to Unlocking Cloud Security Benefits

August 2022

Written by: Philip Bues, Research Manager, Cloud Security

Introduction

Most organizations expect that inflationary pressures, supply chain disruptions, or staffing/labor shortages will have the greatest impact on their IT spending plans for the remainder of 2022, according to IDC's May 2022 *Future Enterprise Resiliency and Spending Survey, Wave 4*. These organizations also recognize that cloud services can offset these challenges because they offer a pay-as-you-grow (PAYG) model, have resources that can be deployed quickly in response to changing business conditions, and have trained and certified third-party security staff available 24 x 7. Recent IDC estimates show the public cloud services market grew 29% in 2021. However, a bigger target is painted on the digital-first organizations as their cloud usage scales.

AT A GLANCE

KEY STATS

- The Russia-Ukraine war and follow-on actions by governments around the world have organizations investing in their cyber-readiness and cyberdefenses.
- According to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 4* (May 2022), the security services receiving the greatest funding increases are security training (32.7%), vulnerability assessments (25.8%), and ransomware assessments (22.5%).

The cloud is open to the internet by default, making it completely dynamic, so security must be provisioned differently. Cloud security in and of itself is complex, yet it is widely acknowledged that complexity is the worst enemy of security. Herein lies a classic security paradox. Now add to it the accelerated digital transformation driven by the pandemic, which left a trail of misconfigurations and vulnerabilities, and a series of high-profile ransomware and supply chain incidents. Organizations need to ask the right questions and understand the differentiation between cloud security vendors and their solutions. IDC offers this technology assessment to help organizations sort through the options.

Understanding Hybrid Cloud and Multicloud Security Solutions

On-premises security models that were designed to protect monolithic applications are simply not intended or optimized for the cloud. Today's emphasis is on agile operations. Cloud security tools protect assets in software-defined compute infrastructure, regardless of when the virtualization happens in the datacenter or IaaS. The key is to have a singular set of unified security tools across all infrastructure — one set to rule them all. This consolidation trend has continued and extends to functionality by reducing the number of point products and choosing security solutions that provide hybrid cloud and multicloud visibility from a single pane of glass.

Where to start?

Depending on the maturity of an organization's security program, a typical cloud journey will include defining a cloud environment, determining a deployment model, partnering with the right cloud provider, and engaging with a third-party security vendor directly, either through a channel partner or with a managed security service provider, to prepare a security audit road map. The road map is part of an initial vendor assessment. It provides recommendations for the following areas:

- **Visibility.** Start with level setting on your organization's cloud assets: How many? Where are they? As your security program matures, you need solutions that can gain additional visibility into asset utilization, licenses, security incidents and associated impacts, real-time risk analysis of both known and unknown threats (aka zero-day threats such as Log4j), and regulatory and compliance reporting. IDC recommends that organizations start by taking advantage of a "free" strategic risk assessment across multicloud and noncloud environments offered by third-party security vendors.
- **Insights.** Once you have the visibility, you can start monitoring and gaining insights. Insights into cloud asset relationships not only reveal how assets correlate to one another but also form the basis for the protection of those entities. Ephemeral workloads, Kubernetes/containers, and serverless functions make this a difficult proposition. They are added and removed often without the knowledge of the security teams, which creates opportunities for bad actors and causes the attack surface to grow. Continuous monitoring of workloads for both known and unknown threats is required to answer questions about what's happening in the environment, how to quickly identify and shut down threats, and whether something anomalous is taking place. The application of behavioral analytics makes continuous anomaly-based detection possible, a requirement for digital-first organizations that wish to compete long term.
- **Action.** Multiple lines of business will be involved to act on issues discovered in the environment. As a result, organizational friction is a by-product that will have to be mitigated, as most security and nonsecurity teams are overwhelmed. Look internally at the cloud security skills and expertise on hand. Is there a match between the challenges that you have discovered and your current security talent, training, and tools? A talent gap makes it difficult to perform these operations at scale in-house. The lack of cloud security staff, training, and tools is one of the issues that keep most CISOs up at night.

Changing Buyer Considerations

Depending on how your organization is structured, it may encompass development teams, platform teams, and security teams. These teams may have different priorities and incentives, driven by your buyer persona expectations and your organizational internal targets. The desired outcomes for these teams will continue to evolve as your organization grows. It's necessary to break down any silos that may exist and take a step back while considering the ideal approach and differentiation offered by security vendors for an end-to-end, "build time to runtime" holistic security solution.

Digital-first vendor solutions will typically incorporate shift-left approaches such as infrastructure as code (IaC) to secure the build and runtime visibility, detection, and response capabilities to secure the workload. Today, many more intrusion points need to be tracked and secured, leaving potential gaps. For example, you may have one tool of distinctive competency for addressing vulnerabilities in code inclusive of open source dependencies and another tool with runtime detection and response. Utilizing both agent and agentless solutions helps close those gaps.

When conducting cloud security vendor assessments, organizations need to pay attention to certain checkbox items. The following list provides an overview of the build time and runtime phases:

- **Build time.** Cloud security vendors have made advancements that bring security into the software development life cycle (SDLC) earlier with solutions such as IaC. This automated, immutable infrastructure approach eliminates configuration drift, scans for vulnerabilities/compliance issues, and ensures consistency across environments.
    - Capabilities such as continuous monitoring and prioritization of vulnerabilities, cloud security posture management, asset relationship mapping, and machine learning to model for risk reduction should be key considerations.
- **Agent/agentless.** Depending on your environment (i.e., IaaS, SaaS), you may be considering an agent or agentless solution. An agent-based solution provides workload protection and runtime insights for deeper inspection and continuous monitoring, enabling organizations to detect threats in real time or near real time. Advancements in this technology have reduced latency concerns over time, but there will always be some resource consumption in order to gain rich context visibility into the workload. In the event an agent-based solution is not feasible and an environment needs to be spun up quickly, an agentless solution that provides workload scanning is also a good fit.
    - If vendors advise you to choose one option over the other, then it's time for a new conversation. While there may be pros and cons depending on your environment, and certain regulated industries may allow only one or the other, the technologies can be used together.
- **Runtime.** To reduce false positive alerts and uncover known and unknown threats such as escalation privileges and malware, look to vendors that offer a cloud workload protection platform (CWPP) for automated security across all layers of the technology stack, either on premises or in the cloud. Among the many benefits is deep visibility into process logs, which remain even after container destruction, making even the most challenging ephemeral workload triage possible. If a breach occurs, dwell time and lateral movement attacks should be continuously evaluated.
    - Partnering with vendors that use machine learning and behavioral analytics for anomaly detection in your environment is a modern-day necessity just as enforcing a zero trust approach should be part of your security fabric.

During the vendor selection process, the lines between buyer personas are blurring. In the past, the C-suite may have driven the process, but the voice of the developer and the voice of the security practitioner are becoming more influential. It's important to engage these different internal audiences during a vendor assessment. Doing so may also help with talent retention efforts.

Industry

Depending on the clients you serve, or seek to serve, it's important to recognize the unique challenges certain industries face to engage with the appropriate security vendor. According to the FBI's 2021 IC3 study, the top infrastructure sectors victimized by ransomware include healthcare, financial services, and government:

- **Healthcare.** Unique challenges faced by provider/payer/life sciences companies include M&A activities, government regulations, and the proliferation of structured and unstructured data that creates an ever-expanding attack surface. Most attractive to hackers may be the value of protected health information (PHI) on the dark web. To keep patient data safe, secure, and private, look for a security vendor that streamlines compliance and takes into account the full life cycle of PHI.
- **Financial services.** Cybercriminals see financial services and fintech as fertile ground for sensitive information — both public and nonpublic. It's no longer just about protecting against a cyberheist (most of the time) or ransomware; it's the way in which security models capture the attack data and operationalize it that creates value. In this field, where it's a race to zero latency, information technology decision makers (ITDMs) should look to work with vendors that provide "always on" security monitoring, visibility, and validation across their environments and activities.
- **Government.** Nation-state attackers are causing disruptions to global supply chains and critical infrastructure. In response, the U.S. government has mandated that federal agencies and their suppliers must adopt a zero trust architecture strategy by the end of fiscal year 2024 and has issued an executive order aimed at removing barriers to sharing threat intelligence with private businesses. These directives, which include the ever elusive implementation of multifactor authentication for many organizations, will result in increased remote secure access spending. Aligning with vendors that have certifications such as being FedRAMP authorized helps maintain compliance and speeds up the onboarding process.

Security hygiene must be exercised at every level, from the C-suite to the individual practitioner. Organizations need continuous education on the importance of designing, building, embedding, and implementing cloud security. It's a cloud journey, so you need to be thinking long term. Best practices include the following:

- Avoid traditional security solutions that are not built for the cloud, which can drain your resources. Choose only cloud-native solutions.
- Assess your security posture and identify gaps to build a holistic cloud security strategy.
- Look for modern solutions based on machine learning and automation for data collection, analysis, and detection of anomalies and threats at scale. It is not practical to deal with the security challenges in the cloud without automation and self-learning models.
- Integrate DevOps and operations workflows and include scanning and reporting capabilities throughout the software life cycle.
- Use a platform approach to iteratively add more layers to meet your evolving needs and stay current with newly developed features and security mechanisms.

Worksheet Section

TABLE 1: *Vetting Initial Vendor Fit*

	Yes/No
Does the vendor provide a free strategic cloud risk and threat assessment?	
Is the vendor knowledgeable about applicable regulations and laws that affect our company?	
Does the vendor offer free early access programs for new releases and product line extensions?	
Does the vendor have a track record of quickly identifying and responding to zero-day vulnerabilities such as Log4j?	
Will the vendor and its partners provide the level of technical and customer support necessary for our organization?	
Depending on the maturity level of our organization, can the vendor cater its cloud security solutions to meet us where we are?	
Do the use cases/case studies presented by the vendor match our organization's desired outcomes and build trust?	

Source: IDC, 2022

TABLE 2: *Key Required Capabilities*

	Yes/No
Does the vendor provide cloud security posture management?	
Does the vendor provide cloud workload protection for virtual machines and containerized environments, including those that use Kubernetes?	
Does the vendor provide DevSecOps with shift-left approaches securing our organization from build time to runtime?	
Can the vendor integrate with our organization's other IT systems (such as change control systems and ticketing/alert channels)?	
To identify risks such as misconfigurations and vulnerabilities earlier, does the vendor use infrastructure-as-code scanning along with vulnerability scanning during CI/CD?	
To prioritize vulnerabilities, does the vendor use proprietary and commercially available risk feeds plus correlation with runtime data?	

Does the vendor support multicloud, including Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes? Is the vendor's solution available on online marketplaces?	
In multicloud, does the vendor have behavior-based anomaly detection capabilities for users and cloud resources?	
Can the vendor baseline activity against our organization's unique environment versus what it thinks is standard behavior?	
Can the vendor provide a single platform to inventory cloud assets, track configuration changes, and find vulnerabilities?	
Does the vendor provide both agent-based workload protection and agentless workload scanning?	
Is there vendor support for ongoing compliance monitoring and reporting for audits?	
Is the pricing competitive and offered with variable terms or periods?	

Source: IDC, 2022

TABLE 3: ***Long-Term Vendor Compatibility***

	Yes/No
Does the vendor use the latest AI/ML technology for detection of known/unknown and continuous response?	
Does the vendor use the latest AI/ML technology to continuously self-learn in a cloud environment and automatically correlate the various pieces to build behavior-based analytics?	
Has the vendor consistently been ahead of the market trends?	
Has the vendor demonstrated multiple customer engagement touch points, such as user groups, feedback surveys, and training?	
Are the solutions/products updated frequently?	
Has the vendor shared its road map, and does it align with our organization's future success?	
Does the vendor have sufficient investment funding to ensure it will be an effective long-term partner?	

Source: IDC, 2022

About the Analyst

Philip Bues, *Research Manager, Cloud Security*

Phil Bues is the Research Manager for IDC's Cloud Security practice. In this role, Phil drives research, provides thought leadership, and advises clients on complex issues including cybersecurity of the cloud and in the cloud. His commentary addresses the benefits and challenges to what's been called the shared responsibility model and how that line may change going forward.

MESSAGE FROM THE SPONSOR

About Lacework

The dynamic nature of the cloud requires a new approach to security. The Lacework Polygraph® Data Platform uses your own data and automation to protect your cloud environment and prioritize risks with accuracy. Customers depend on Lacework to increase productivity, consolidate tools, and meet compliance goals.

The Polygraph Data Platform learns and understands behaviors that introduce risk across your cloud environment, so you can innovate with speed and safety. With visibility from build time to runtime and automated insights into unusual activity, threats, vulnerabilities, and misconfigurations, you gain the context to prioritize and act faster.

Using patented cloud behavioral analytics, the platform automatically learns how your environment is supposed to run and tells you when it deviates — providing the right alert, with the right context.

Whether you operate in one cloud or multiple, have a hybrid environment, or use Kubernetes and containers, Lacework has you covered with one platform to protect it all.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com