A TECHSTRONG RESEARCH WHITE PAPER

Balancing Velocity and Security in the Cloud

Research data confirms that innovative organizations build security into their cloud strategy

Daniel Kirsch
Managing Director
and Co-Founder

Judith Hurwitz
President
and Co-Founder

Techstrong Research

Sponsored by Lacework

Introduction

Businesses are in the midst of a digital transformation. Delivering online services and products as fast as possible is a strategic imperative. The cloud delivers the velocity businesses seek, but those making the transition are learning some di" cult truths: cloud security is di#erent, and capitalizing on cloud velocity (i.e., continuous and secure applications delivery) demands new approaches to security.

In the cloud, continuous integration practices shorten cycle times and improve e" ciency. When confronted by the cloud's increasingly complex and dynamic network environment, it is di" cult for security to keep pace. Why is security a challenge? Cloud security can't be approached as simply an o#-premises version of data center security. Security practices have to change if an organization is to bene! t from cloud velocity.

Cloud security can't be approached as simply an off-premises version of data center security. Security practices have to change if an organization is to benefit from cloud velocity.

Establishing the right balance between speed and security is an age-old IT con$ict. With the emergence of the cloud, two additional factors exacerbate the tension between speed and security:

1. **Cloud environments are rapidly evolving.** Unlike the traditional data center, cloud workloads change frequently, and are often spun up and down in order to respond to new opportunities.
2. **Gaining visibility is difficult when workloads are executed in the cloud.** Most security-relevant events never leave the cloud's virtual machines and containers which limits your ability to gain insight. If you do not capture and analyze logs at every level, including both the network and application layer, you may miss subtle abnormalities that indicate a potential vulnerability.

Illustrating the challenge of cloud security

Businesses are transforming the way they develop applications. Rather than building large, interconnected applications with many dependencies, developers are assembling applications with independent microservices. By chaining together pre-built, single-purpose components (often deployed in standalone virtual machines or containers), developers can deliver applications free from many of the issues associated with large, monolithic codebases. Microservices components automatically start and stop as needed, and they rapidly consume, abandon, and reuse network addresses. Traditional applications have predictable network patterns that give security o#erings the ability to track and alert administrators if there is an abnormality. However, because of the dynamic nature of microservices, network-oriented security solutions cannot establish a baseline of what "normal" looks like. These traditional security approaches were not designed with the cloud, microservices and containers in mind.

HURWITZ & ASSOCIATES
Insight to Action

Based on the quantitative research presented in this paper, as well as qualitative interviews with industry practitioners, Hurwitz & Associates sees clear evidence that IT leadership recognizes the complexity of this change and is ready to take action. To assess the state of cloud security, we surveyed IT leaders at primarily large companies across industries. The goal of the study was to better understand how organizations are approaching cloud security in this rapidly changing business environment. The results are clear, businesses are increasingly evolving their security strategy to advance their cloud strategy.

35% percent of the organizations are taking a cloud-first approach meaning that all new projects are done on the cloud.

Research Methodology

Hurwitz & Associates surveyed 85 IT leaders from the Americas and Europe. The participating companies ranged from mid-size organizations to large enterprises. Most participants (56%) worked at organizations with over 10,000 employees. A variety of industries are represented with most participants coming from:

- Financial services,
- Telecommunications & technology,
- Manufacturing, and
- Retail.

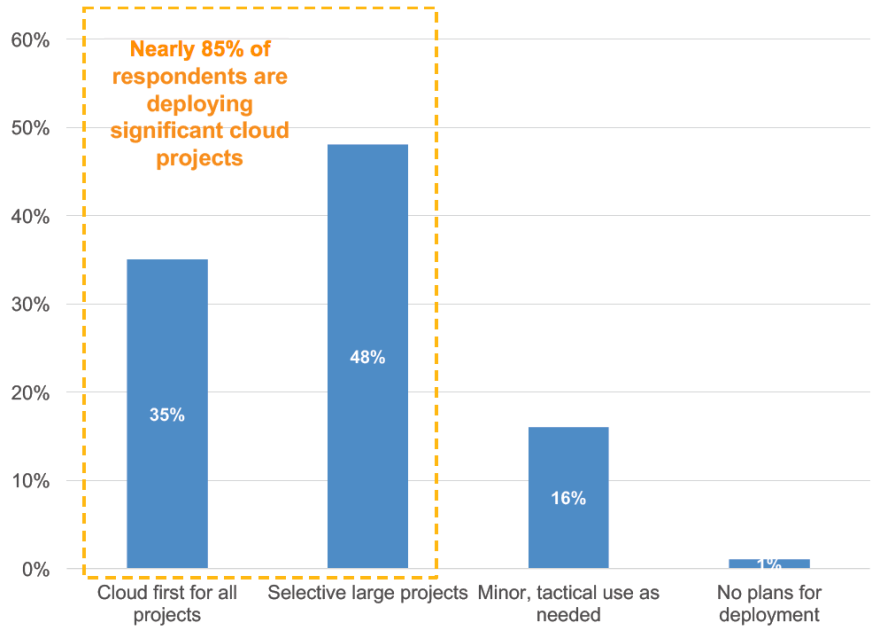
Respondents to the survey were questioned about:

- The level of use of cloud computing within their company,
- Their company's approach to developing a security team,
- The Role of security in managing cloud services, and
- How security is handled in the development, execution, and operations of projects.

It's important to note, that nearly all of the study participants are using the cloud. Approximately 35% percent of the organizations are taking a cloud-! rst approach meaning that all new projects are done on the cloud. In addition, almost 50% of participants are taking a selective approach to the cloud, where signi! cant and large projects are being developed or migrated to the cloud while others will continue to remain on premises.

HURWITZ & ASSOCIATES
Insight to Action

Figure 1: What is Your Organization's Current Plan for Cloud Deployment now and in the next 6 Months?



Source: Hurwitz & Associates, 2018

Customers' Key Cloud Security Requirements

Based on this survey data and 1-on-1 conversations with security executives, these cloud security features surfaced as requirements to ensure a secure cloud. We believe that choosing solutions that o#er these capabilities will make the journey to the cloud safer and more productive.

- **Container Aware –** As containers become the backbone of cloud applications, security teams need to track, identify, and manage containers along with monitoring contain-to-container tra" c within the cloud, not just from and to the cloud.
- **Integrate Existing Security Investments –** Rather than creating security silos, the cloud security products should integrate into existing security investments such as SIEM. In addition, cloud security products should work with capabilities that your cloud service provider o#ers, for example, Amazon Web Service's governance, compliance, risk auditing and other security services.
- **Automation –** It's no secret that there is a shortage of security professionals. It is important that security o#erings incorporate automation to allow security teams to address more events and to give junior analysts the ability to handle issues that are typically left for more senior analysts.
- **Correlate Data to Identify Abnormalities –** Cloud security o#erings should be able to ingest relevant data and understand what the environment looks like under normal conditions. The solution should then alert administrators to anomalies in the environment. Without capable anomaly detection, security administrators face a complex set of rules and policies, which will

It's no secret that there is a shortage of security professionals. It is important that security offerings incorporate automation to allow security teams to address more events and to give junior analysts the ability to handle issues that are typically left for more senior analysts.

slow down your company's ability to innovate while adding signi! cant overhead.

- **Documentation –** Cloud security products should fully document security events. This documentation is critical for investigations and also ensures that the environment can be quickly audited.

Key Study Findings & Recommendations

Security Continues to Keep Cloud Professionals Up at Night

Survey respondents agreed that security is a top priority for their cloud solution. Asked to rank-order seven possible cloud solution characteristics, "safe and secure" topped over half of the lists (53%). The next most mentioned priority - "deliver new services and updates faster" - topped only 13% of the lists.

Our interviews with cloud security leaders con! rm these ! ndings. We spoke to an IT executive at a large US-based insurance company. Her company's data center is at capacity, and rather than investing in a data center buildout, all new services will be developed on the cloud. The insurance company's applications often include customer data. When we asked this executive about her top three concerns regarding the cloud, she emphatically said "security, security, security."

We asked all of the survey respondents to agree or disagree with the following statement: "we catch every cyberattack and data breach of our cloud," only 2 in 5 (41%) survey respondents agreed. We suspect that the problem is much more serious than the level of con! dence suggests. It is simply not evident that security leaders are actually identifying all security threats.

Only 2 in 5 (41%) survey respondents agreed with the statement: "we catch every cyberattack and data breach of our cloud." We suspect that the problem is much more serious than the level of confidence suggests. It is simply not evident that security leaders are actually identifying all security threats.

The Speed vs. Security Debate Rages On

Software developers have been isolated from their security and operations teams for decades. Now those silos are breaking down as new business models and stake holders demand more agility and faster time to market. Organizations are responding with DevOps practices designed to support accelerated software release cycles - sometimes leading to several releases each week.

The rapid speed of development has created a challenging environment for security: the drive for velocity makes is easy to overlook foundational security requirements. However, if the development team doesn't take cloud security into account, the company will likely encounter a breach. It's a di" cult challenge -- aligning security with the speed of DevOps to ensure secure applications and a secure cloud strategy.

The tension between speed of development and ensuring a secure environment has existed for years. Cloud practitioners paint a rosier-than-expected picture of this perennial debate. Only 35% of respondents felt that "Security limits our ability to maximize the bene! ts of DevOps and operations automation," and 78% agreed that "we ! x security vulnerabilities fast enough to avoid signi! cant

HURWITZ & ASSOCIATES
Insight to Action

business risk." However, there is always tension between the security team and the DevOps organization. A CSO at a large retail company remarked, "I am tired of being Mr. No," re$ecting the lingering perception that security brings speed and innovation to a halt.

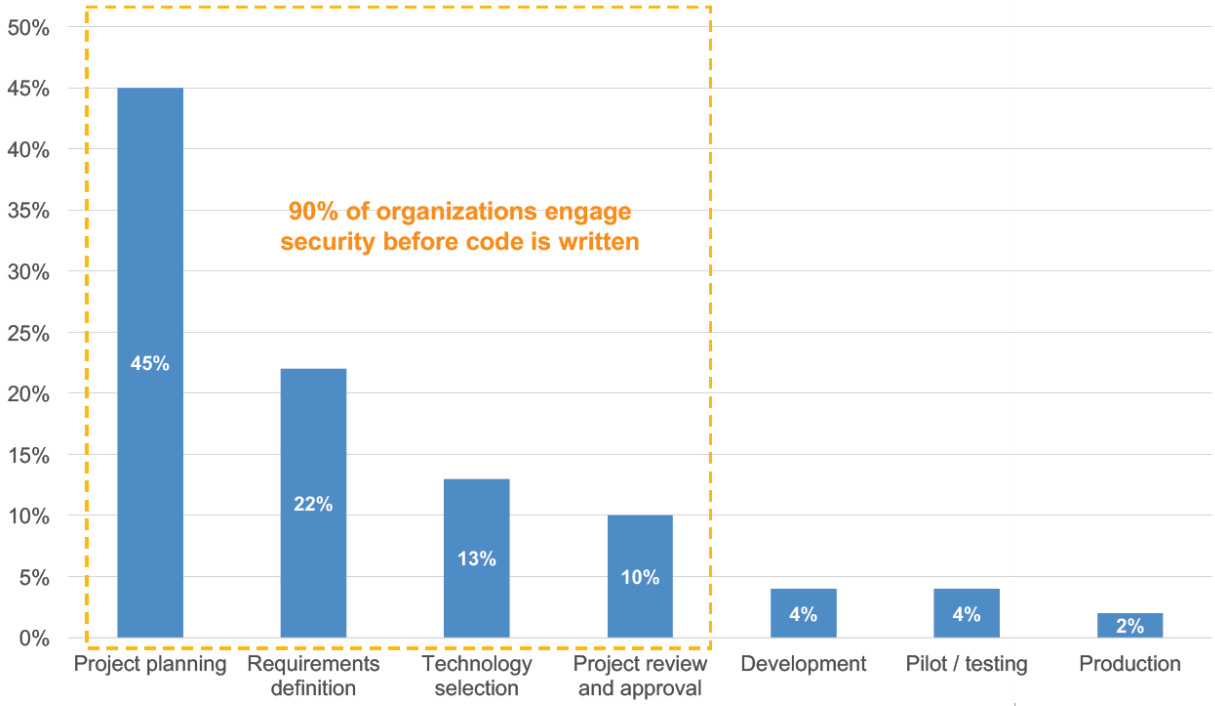
Over the last several years, DevOps has emerged as a strategy and culture shift. DevOps is the strategy of bringing together development teams with operations teams. More recently, we have seen security being more tightly integrated into DevOps. Some organizations have begun building what they call DevSecOps teams.

As organizations begin to prioritize security, the adversarial relationships between security and IT Operations is beginning to diminish.

Security is Getting a Seat at the Table

As organizations begin to prioritize security, the adversarial relationships between security and IT Operations is beginning to diminish. Nearly 90% of survey respondents said "our security and cloud operations teams work closely together." As shown in the ! gure below, the vast majority of organizations engage the security team before developers begin to code. Only 6% waited until the project was in testing, pilot, or production.

Figure 2: When evaluating an ideal cloud solution, what is your most important priority?

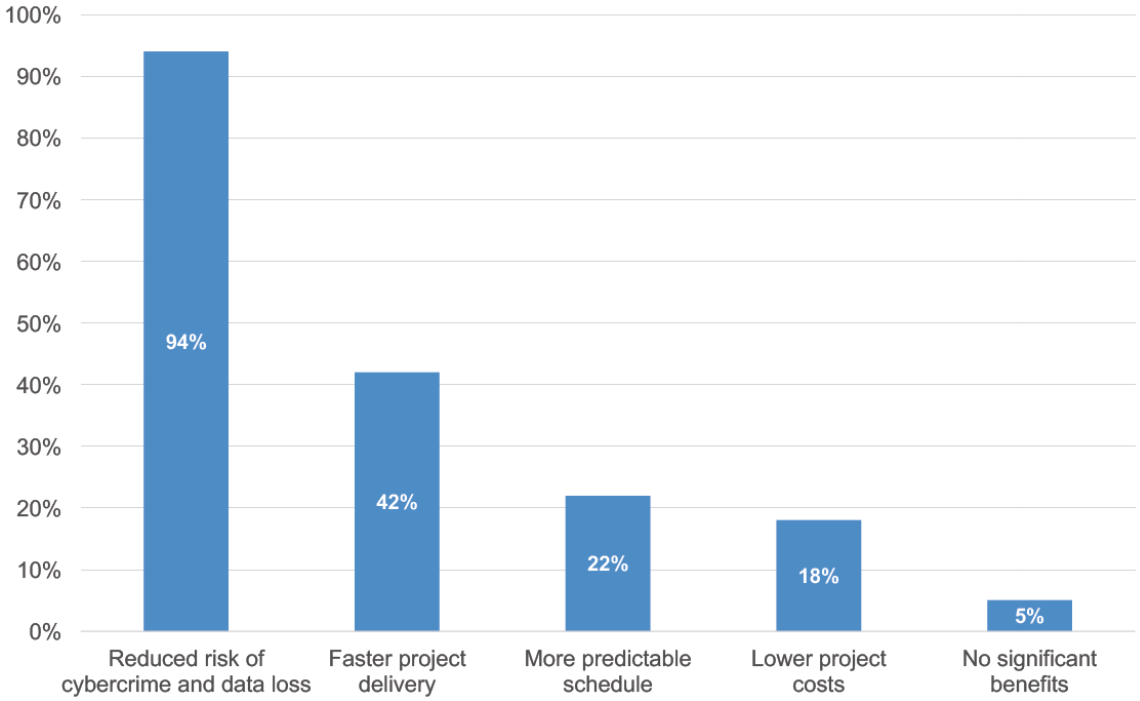


Source: Hurwitz & Associates, 2018

Attitudes towards early security engagement re$ect a recognition of the positive bene! ts that the security team can add to a project. Unsurprisingly, nearly all of the participants believe that early security engagement results in "reduced risk of cybercrime and data loss." Contrary to what some people might assume,

the other top bene! ts of early engagement focused on faster delivery time and reducing project costs.

Figure 3: What are the top benefits of early engagement by the security team in a Cloud project? (Choose up to 2 statements)



Source: Hurwitz & Associates, 2018

In addition, involving the security team earlier in a project, you can ensure that a project meets compliance goals. Early engagement allows the security team to integrate security throughout an o#ering and often prevents costly delays. The ultimate result of engaging security early in a project is that you can provide safe and secure applications and services that don't put your organization or your customers at risk.

Only 35% of participants felt "SIEM tools give us all the security visibility we need."

Available Cloud Security Tools Are Maturing

Attitudes towards existing cloud security tools varied, but in general study participants felt that they were not getting the security protection that they need. In addition, respondents agreed that securing the cloud requires a new approach when compared to securing the data center. Below are some of the conclusions made in the study:

- Challenge of unpatched software - Nearly 75% agreed that "controlling vulnerabilities related to unpatched or downrev software is a challenge."
- Failure of existing security tools - Only 35% felt "SIEM tools give us all the security visibility we need."

- The need to protect again insider and external threats - About half thought their "cloud defenses are equally e#ective against insiders and external threats."
- Cloud requires a new approach. An overwhelming 85% of respondents recognized that "cloud security is di#erent than traditional data center security."
- Automation is critical. Almost all respondents agreed (95%) that "cloud automation is increasingly important to meeting our business goals."
- Security's does not hinder DevOps - Only 35% felt "security limits our ability to maximize the bene! ts of DevOps and operations automation."
- Flexibility of cloud security o#erings – Approximately 40% felt "our security solutions aren't as $exible and scalable as the rest of our cloud."

85% of respondents recognized that "cloud security is different than traditional data center security."

One executive we interviewed was evaluating new o#erings that integrate cloud security into existing solutions, explaining that "as we began to prototype the cloud we had 50-plus security products from over a dozen vendors in our data center, but none of them give us full insight into every level of the cloud." Survey respondents con! rmed this executive's desire for cloud visibility. When asked to identify the most important characteristic of a cloud security solution, "immediate incident detection and alerting" was the clear front runner, appearing as the number one choice on 34% of wish lists and making a top 3 appearance for nearly 3 out of 4 respondents (73%). The second most sought-after characteristic was, not surprisingly, "automated installation and operation."

One executive we interviewed was evaluating new offerings that integrate cloud security into existing solutions, explaining that "as we began to prototype the cloud we had 50-plus security products from over a dozen vendors in our data center, but none of them give us full insight into every level of the cloud."

Best Practices to Ensure a Safe Cloud Environment

No one needs a survey to know businesses are moving to the cloud. The challenge for organizations navigating the transition is to protect the business without losing the agility they seek. Based on the survey results and our interactions with front-line practitioners, we o#er the following ! ve best practices:

1. **Software development teams must collaborate closely with security teams when projects are being planned.** If they don't, they'll face one of two consequences: projects will slow to a crawl as required security measures are bolted on, or the schedule will be met at the expense of adequate security. Cloud security tools that deliver insights into operations can do double duty, helping the security team protect the business while also giving developers and operations sta# a clearer picture of what's going on. Basically, the earlier security problems are removed during development, the less expensive it is to ! x them.
2. **Use cloud-specific security tools.** There are signi! cant di#erences between data center and cloud security that must be taken into account (e.g., container visibility and security). Indeed, more businesses are beginning to understand that data center and cloud security are not the same. Many successful companies are creating cloud security teams that understand how to work in collaboration with the DevOps teams to protect the integrity of the business.

HURWITZ & ASSOCIATES
Insight to Action

3. **Automate cloud security.** With so many changes to applications and services in the cloud, it's easy for mistakes to happen. Centralized incident and event management systems look for anomalous data and processes to safeguard the company IT assets. Automation is everywhere, from con! guration management and patching tools to ! le integrity monitoring and insider threat detection. It's the only way to prevent unintended breaches from happening in the ! rst place.

4. **Maximize visibility into your cloud.** It's the only way to ensure your cloud services are up to data and secure. A good solution will provide insights into both short-cycle events (e.g. intrusions, breaches, suspicious insider behavior) as well as longer-cycle items (e.g. S3 bucket con! guration hygiene, CIS benchmark compliance). Ideally, dashboards and reports will provide information relevant for a variety of use cases beyond just security.

5. **Make a good plan.** A comprehensive security strategy and plan will ensure you make a successful digital transformation while managing cyber risk. As we've heard through this survey and from Hurwitz clients, security is a part of the entire product lifecycle. So your plan needs to tackle topics ranging from the culture of your DevSecOps e#orts to the tools you use to the responses you'll make to security incidents.

A comprehensive security strategy and plan will ensure you make a successful digital transformation while managing cyber risk.

HURWITZ & ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a strategy consulting, research and analyst ! rm that focuses on how technology solutions solve real world customer problems. Hurwitz research concentrates on disruptive technologies, such as Big Data and Analytics, Cognitive Computing, Security, Cloud Computing, Service Management, Information Management, Application Development and Deployment, and Collaborative Computing. Their experienced team merges deep technical and business expertise to deliver the actionable, strategic advice clients demand. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

35 Highland Circle • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com