Cloud Infrastructure Security

It's Time to Rethink Your Strategy

CloudPassage

iSMG
INFORMATION SECURITY
MEDIA GROUP

Cloud Infrastructure Security

It's Time to Rethink Your Strategy

Infrastructure security used to be easier. Now, it is dramatically more complex, owing to a broad range of factors. At the top of the list: how the virtualization of infrastructure removes the ability to use control of the physical IT environment as a security defense.

It takes a new mindset to manage cloud infrastructure. And to truly reap the benefits from the cloud means that leaders must rethink their approach to infrastructure security.

"You suddenly are in a situation where you don't control the physical environment; you don't control the operational environments," says Carson Sweet, CEO and co-founder of CloudPassage, a software-defined security provider for cloud infrastructure.

"You're really limited to the virtual machines or workloads themselves in terms of what you can touch and make security modifications to. Previously, responsibility for the infrastructure flowed to being responsible for the workloads. Security is now complicated, and organizations are struggling."

The degree to which one gives up control of IT infrastructure varies based on the adoption of private, public or hybrid platforms. But to ensure cloud infrastructure security, organizations cannot apply their traditional set of IT tools and techniques.

For example: One can focus on the elements of the cloud ecosystem that they do control. But tasks such as implementing endpoint security are resource-intensive and difficult to manage across cloud computing deployment models.

"With BYOD, companies are already losing control of the endpoints," says Jim Reavis, chief executive officer of the Cloud Security Alliance. "Companies often don't see the entire communication taking place with the cloud server. You can't deploy endpoint controls in an effective way."

With those ideas as context, please read on for:

- Lessons learned from cloud infrastructure pioneers;
- How regulators view cloud infrastructure security;
- How to assess cloud infrastructure risk;
- The business benefits of a software-defined approach to cloud infrastructure security.

Lessons Learned from the Pioneers

The reality is that security has to be cautious; they have limited resources and time to evaluate changes. It can seem like change is the enemy, yet progressive security leaders cannot stop the organization from utilizing cloud infrastructure. The benefits are just far too compelling.

"They are no longer able to stand in front of the cloud train and say, 'No, we're not going to do it,'" Sweet says. "The benefits of cloud infrastructure are just too great. The flexibility, the ability to get to market faster, to use op ex dollars instead of cap ex dollars - all of these things are extremely compelling to the businesses."

Although the adoption of cloud computing is a relatively recent development, organizations already can learn a great deal from pioneers. To start, in order to capture the most benefit from the cloud, organizations must re-architect applications.

This, in turn, opens the door for security to align with operations regarding the goals and expectations of the cloud. This alignment allows for the removal of friction points that otherwise could affect the overall value derived from the cloud.

Among the lessons learned:

1. Adapt to the Pace of Change

With the proliferation of cloud platforms and environments that business wants to leverage, the security landscape continues to shift. The rate of change is far higher today than it was even five years ago. Consequently, an elongated change control process is no longer defensible. Rather than attempting to slow the process down using antiquated approaches that do not readily apply to the cloud environment, security functions must adapt to the higher rate of change.

The automation and integration of security seamlessly with every new cloud platform must become the norm, not the exception. To achieve continuous oversight, the security

"[Security leaders] are no longer able to stand in front of the cloud train and say, 'No, we're not going to do it.' The benefits of cloud infrastructure are just too great."

Carson Sweet, CEO, CloudPassage

Carson Sweet, CEO, CloudPassage

department must have access to centralized solutions with visibility across distant and diverse cloud environments.

2. Expect Regulatory Scrutiny

The cloud is a disruptive force for companies and regulators alike. Not surprisingly, the adoption of the cloud amplifies regulators' interest and scrutiny. "Pain points are proportionate to regulatory oversight. Extra layers and audit trails exist for more highly regulated industries," notes Reavis of the Cloud Security Alliance.

In fact, with application deployment models driven by agile development supporting Software as a Service (SaaS), the explosion in mobile applications, and business transformation taking place at a blistering pace, the only thing that security departments and regulators can count on is that change is a constant. With the continued adoption of cloud computing, slowly but surely, regulators will increase the compliance burdens on companies, particularly for heavily-regulated financial institutions. It is best to plan for increased scrutiny now, rather than be surprised by it later.

Since regulators often struggle to stay current with the latest developments within cloud computing, they also struggle in regulating activities relating to infrastructure. "When auditors see a major disruption like cloud infrastructure, they put themselves on red alerts," says Sweet. "So the fear, uncertainty and doubts that the regulators and auditors come in with, which translates into scrutiny and the amount of attention that those environments get, is amplified dramatically."

Consequently, addressing perceived or real cloud-security related concerns may involve educating regulators on basic cloud dynamics and the company's adoption of cloud-based solutions - without creating additional areas of concern during the process.

3. Mind the Security Gaps

With regulatory standards changing slowly, core security needs such as preventing data compromise, exposure management, security event management and access control still apply to the cloud infrastructure. In fact, given the existence of public, private, community and hybrid cloud models, and the resulting inability to control access and security of the cloud infrastructure, organizations must ensure that the basic "blocking and tackling" of

security is in place. “Understand your shared responsibilities,” says Reavis. “Depending on the cloud service, responsibility for the audit and assurance of controls, for example, varies. Know your provider and know your responsibilities.”

While basic security tactics still apply, the delivery parameters must change to accommodate the cloud environment. Organizations cannot enforce control if they do not have visibility across the enterprise. They cannot rely on an old tool set or deploy security solutions that fail to deliver the appropriate level of protection for each type of cloud the company utilizes.

Without the capabilities to ensure cloud infrastructure security, regardless of the deployment model, the security department may artificially limit the company’s options to leverage the cloud.

This, in turn, affects the security department’s ability to play an active role in the company’s efforts to adopt the cloud. In fact, the inability to secure cloud infrastructure may result in a concerted effort to exclude the security department from the decision-making process regarding the adoption of additional cloud-based platforms. It may also reaffirm or enforce the operation’s view of the security department as an impediment to progress.

4. Legacy Approaches Will Not Work

Migrating “tried and tested” approaches, such as next-generation firewalls, which are far less effective in virtual environments, will often cause bottlenecks that affect the cloud solution’s performance.

In addition, legacy approaches to security are often incompatible with cloud environments, as they rely on a degree of control that the company no longer possesses. Even as legacy solutions begin to create work-arounds, the growing changes and choices in cloud infrastructure environments become difficult to ubiquitously support.

Forcing such tactics to apply causes friction with operations, hinders growth with costly licensing models, and subjects the

To truly reap the benefits from the cloud means that leaders must rethink their approach to infrastructure security.

business to many varied security-related threats.

5. Big Data Experience Needed

There are additional internal pressures facing security organizations relating to how they staff their security function. Sweet sees security organizations struggling to hire professionals with relevant cloud experience and the ability to apply security analytics.

Given the volume of data in the cloud, Sweet sees a rush to hire staff with big data skills. "The amount of data that's got to be considered and analyzed for threat analytics, vulnerability scanning, all the things you think about in a relatively slow-moving environment, those are really becoming big data problems," says Sweet. "The ability for security organizations to pry big data analysts away from the big data companies out there, it's very difficult to do. So that's probably the single biggest skill area that we see sort of some challenge in."

How to Assess Cloud Infrastructure Risk

To minimize gaps, security departments must analyze risk and compliance factors for every cloud environment. This includes assessing the ability to apply continuous integrity and data extrusion monitoring of data within the cloud.

In order to assess the risk they face, organizations must analyze their overall infrastructure security strategy.

Key questions to answer during the assessment include:

- What will the new infrastructure model look like?
- How will it operate? Which elements of the company's current strategy will need to change?
- What are the limitations of current approaches; a.k.a. where do security gaps currently exist?

The idea behind the assessment is to identify gaps to close within the existing IT security strategy. Documenting the gaps forms the basis of the plan to support the evolution of strategy. To help the security department plan and further justify the effort, the assessment should also include steps to uncover plans to adopt additional cloud solutions in the near future.

Assessing IT security strategy should also include meeting with auditors - internal and external - as well as the primary regulators. Such discussions can help uncover general and specific security concerns regarding public, private, and hybrid cloud models. It can also help organizations gather information regarding the tools and tactics that regulators deem appropriate to secure cloud infrastructure.

It might also unearth approaches employed by other organizations that have withstood regulatory scrutiny. Finally, meeting with regulators can reveal which function(s) typically own cloud security, and help the organization align its approach with the prevailing industry wisdom.

Legacy approaches to security are often incompatible with cloud environments.

The Benefits of Software-Defined Security

When an organization's infrastructure changes dramatically, the security function, rarely, if ever, receives additional resources. CISOs, then, must ensure security with existing personnel and resources.

To do so, security leaders must develop a robust strategy, as well as secure the necessary resources to implement, maintain, and scale as the business continues to embrace the cloud for solutions. Industry-leading companies often turn to a purpose-built, software-defined approach to securing their cloud infrastructure.

What is software-defined security? It's an approach that overcomes the limitations of traditional solutions, as it is not server- or device-centric. Software-defined security better equips security functions to respond to the changes taking place in the threat landscape because it provides immediate security coverage; it is fast to implement through abstraction, virtualization and automation; and it supports robust policy orchestration - a cornerstone of cloud security.

Ultimately, software-defined security provides organizations with the ability to capture and analyze security data on an ad-hoc basis. Through an API, it provides seamless integration with existing security solutions such as Security Information and Event Management (SIEM), enhanced proactive management of governance risk and compliance solutions, and the adoption and maintenance of identity and access solutions.

Software-defined security also scales quickly, across any cloud environment, making it portable and easily adaptable to business needs. By only paying for services utilized, it delivers an economic approach to security that is consistent with the lower cost, higher utility cloud environment. It enhances a company's visibility of their business compute workloads and their network communications. Increased visibility translates to more timely and actionable threat intelligence.

A software-defined security platform provider - with experience in managing for dynamically scaling environments and security best practices - can help organizations ensure security in a highly efficient and cost-effective manner. Automating and integrating software-defined security delivers an enhanced view of security for the business, security and compliance functions, and potentially facilitates better security and risk-related decisions by the line of business managers.

Bottom Line: Be an Enabler

Ultimately, cloud infrastructure security brings with it a unique opportunity. Security leaders now can reinvent their image and be seen as a true business enabler. No more heading up "the office of just-say-no," security leaders can be seen as true business partners, helping other senior leaders to identify, capture, and benefit from the full range of cloud initiatives. But to reap that benefit, security leaders must assert themselves boldly in the adoption, deployment, and risk management of the cloud platform.

"Change is fundamentally the enemy of security and compliance, but it's not going to stop," says CloudPassage's Sweet. "The security practitioners who will be leaders in the fields are those who recognize and then embrace this reality."

About CloudPassage

CloudPassage® is the leading software-defined security provider for cloud infrastructure. Enterprises trust Halo®, a purpose-built, Software-Defined Security platform, to deliver seamless, scalable security and compliance across any mix of private cloud, public IaaS and hybrid/multi-cloud environments. Founded in 2010 and headquartered in San Francisco, CloudPassage partners with top cloud technology companies such as Amazon Web Services, BitNami, Datapipe, GoGrid, HP Cloud, Rackspace, RightScale and OneLogin.

CloudPassage currently protects more than 400 production application deployments in the cloud, including a number of Fortune 1000 enterprises, and automates security for more than 10,000 new cloud workload instances each month.

About Halo: Purpose-Built to Secure Cloud Infrastructure

The Halo cloud security platform is purpose-built to provide organizations with the critical protection, visibility, and control needed to assure cloud security - without the fixed perimeters of legacy security. It provides companies with consistent security and compliance controls across clouds and data centers alike. Halo automates security and compliance in an easily integrated and scalable platform. Halo is platform and provider agnostic and easily integrates with a company's existing infrastructure. It typically takes less than an hour to deploy Halo.

Halo's architecture combines a cloud-based security analytics engine, lightweight agents and a secure asynchronous messaging protocol for continuous command-and-control and monitoring. This architecture enables the Halo platform to deliver a wide range of software-defined security and compliance capabilities for application workloads.

Halo's quick deployment, broad control consolidation, legacy solution enablement, and deep automation free security personnel from mundane technical tasks - allowing security staff to focus on more strategic needs.

Resources:

Cloud Infrastructure Security: How to Secure Buy-in and Budget

Business and security leaders often fail to understand that adopting a cloud infrastructure changes the dynamics of IT security and regulatory compliance. Learn how the security department can obtain the buy-in and budget to secure cloud infrastructure.
http://www.bankinfosecurity.com/cloud-security-how-to-secure-buy-in-budget-a-7338

How to Tackle Cloud Infrastructure Security

Listen to Carson Sweet, CEO of CloudPassage, as he shares insight and strategies to improve cloud infrastructure security, including the lessons learned from cloud pioneers, the biggest security gaps companies must overcome, and the benefits of deploying a third-party cloud infrastructure security service.
http://www.bankinfosecurity.com/interviews/how-to-tackle-cloud-infrastructure-security-i-2350

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY® (Prevention. Response. Notification.)

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com