Private and Public Clouds – your Hybrid Environment

Securing your private cloud is a relatively straightforward business. The use of virtualization to create a software-enabled data center is a comparatively established practice, and Kaspersky Lab has responded with specialist software offering the lightest footprint on the virtual machine (or, in the case of VMware, no discernable footprint at all) to optimize the efficiencies and protect the resource savings and flexibility that virtualization technology delivers.

But moving out of the private to the public cloud arena, and in particular straddling the two, has introduced new issues. Where does your security responsibility begin and end, and how do you orchestrate and protect workloads as they move between clouds, on- and off-premise?

Security Threats and Their Mitigation

There are multiple risks faced by elastic cloud environments regardless of size. Virtualization platforms used in the software-defined private data center or cloud platform chosen to run business-critical apps. Cloud services providers, like Amazon, do a lot to make sure that public clouds remain a safe harbor for cloud-adopters of any scale. AWS provides a range of highly effective cloud-native security tools for building borderless enterprise-level environments. Nevertheless, the risk will always remain. At Kaspersky Lab, we see a number of serious threats (and not just in terms of cybersecurity) that could negatively influence your cloud adoption strategies and slow your digital transformation journey.
Kaspersky Lab’s recommendation for preventing data breaches is to maintain reliable cyber-defenses for each individual workload in your hybrid cloud environment. The visibility and transparency of both IT and security layers are also essential here, ensuring that you can see every workload you need to protect and provision automated cybersecurity capabilities to every corner of your rapidly changing elastic cloud environment.

Data Breaches or Leakage
Infrastructure visibility is an issue in today’s elastic digital environments – and your cybersecurity itself may also have become less transparent, so you can’t always pinpoint exactly where you’re at risk, and when. And, even if you do know, it may be too late. This fragmented security approach makes corporate hybrid clouds a sweet spot for cybercriminals, particularly as the same tools can generally be used to penetrate traditional and cloud infrastructures. A serious data breach can expose sensitive customer or business-partner information, intellectual property, and trade secrets, all of which can lead to serious consequences.

Data Loss or Non-integrity
While data breaches generally remain a result of malicious activity, there are multiple scenarios when your data may become inaccessible or damaged due to even quite unintentional actions of your own end-users, as well as malicious activity. Most organizations feature data recovery strategies to ensure the least possible RTO (Recovery Time Objective) and shortest RPO (Recovery Point Objective). However, backing up or replicating your data does not necessarily mean you may find some unwelcome surprises when you restore later on. Fast growing statistics of successful and very damaging ransomware attacks against organizations of all kinds show that maintaining data integrity is quite a hard mission. No matter how old the data or where it’s located – as a physical, virtual or cloud workload – data loss or non-integrity is at your own risk.

Unwanted or Vulnerable Applications
Corporate end-users install and work with a wide range systems and applications for many reasons and you can’t always control what’s installed on end-user devices or even on business-critical servers. The broader the corporate environment, the harder it is to keep everything under control. Even business-critical applications you’re entirely familiar with may not be resistant to zero-day vulnerabilities and exploits but require immediate remediation against potential cyber-risks.

Resource-Hungry Security
Most hybrid clouds operate as a mixture of software-defined private data centers and elastic public cloud services. Both require protection, while combining technologies delivering different integration capabilities. Adopting an old-school “traditional antivirus everywhere” approach to hybrid cloud security is a massively inefficient utilization of your cloud resources, compromising the effectiveness of business-critical systems and significantly reducing the return on your investment in digital transformation.

Security and Infrastructure Misalignment
Hybrid cloud adoption promotes a new dynamism and effective inventory, as well as the constant provisioning of cybersecurity to hundreds of newly-deployed cloud workloads at a time, which can end up feeling like an ongoing IT security nightmare. As a security professional, you have limited or delayed visibility of the cloud machines your IT colleagues are proliferating, so those machines will remain vulnerable until next time you scan the corporate network. But automated tools used by generalist IT staff to perform administrative tasks like network segmentation, isolation and topology reconfiguration can be very helpful in responding rapidly to emerging cyberthreats, and in helping to perform a proper due diligence. If your IT and Security layers don’t interact, security teams will never be able to safeguard what they can’t see, and IT generalists won’t able to help them enable a truly secure and adaptive ecosystem throughout your hybrid cloud.
Shared Responsibility in Public Clouds

Public clouds come with their own built-in security. But the Shared Responsibility Model dictates that your workloads, applications and data in public clouds remain your responsibility. And when these workloads are business-critical, this responsibility becomes even more important.

AWS is the leading public cloud provider, offering the most advanced environment on the market, incorporating outstanding reliability and scalability, and providing a range of cloud-native security tools for borderless enterprise-level environments.

However, shared security responsibility dictates the need for additional security capabilities, enabling an elastic cybersecurity layer that covers your entire cloud environment. public and private and fully protecting the data you hold on your AWS estate.

Integrated Security for AWS Cloud

Kaspersky Lab's philosophy has been to create a perfectly balanced blend of best-of-breed protection, resource-efficient cybersecurity and enterprise-level orchestration capabilities for your AWS environment. Thanks partly to integration via AWS API, we do this better than anyone else.

Working in harness with AWS, we start by bringing to the table the latest edge ‘Next Generation’ cybersecurity capabilities – based around the most tested, most awarded1 and most appreciated2 protection engine in the industry today. Next generation cybersecurity means people and machines working together to build an elastic adaptive cloud security environment. This is what we offer, enabling you to detect and respond to the most advanced cyberthreats.

---

1. Engineerered for physical, virtual & cloud workloads
2. Multi-layered integrated security for any private data center
3. Seamless, automated and agile security for AWS and Azure public clouds
4. Helps to meet shared responsibility with a full set of security tools
5. Enterprise-level security orchestration across your entire hybrid cloud

Best in class protection, visibility and manageability

Tightly integrating our advanced cyber-security capabilities with those of AWS through their API brings further benefits:

- Systems Efficiency
  Cloud infrastructure inventory becomes far more straightforward, as does the automated security provisioning of your AWS EC2 instances regardless of their location. Such systems efficiencies can generate significant savings in terms of time and resources.

- Full Visibility
  Visibility can become a major headache in hybrid cloud environments, and here again close integration pays dividends. Integration via AWS API means you can see into every corner, understand how your cloud is organized and be confident that you are protecting all your cloud workloads.

- Smooth Orchestration
  AWS API integration allows for the unified management of all your IT assets, on-premise and in the cloud, through a single console, providing full transparency and enabling smooth and efficient orchestration and administration.

- Security ‘for’ and ‘from’ the Cloud
  Our industry-leading protection for your AWS EC2 instances is also available in AWS MarketPlace, helping to make your cloud migration smooth, straightforward and safe. What can be better than best security for the cloud, available from the cloud?

- Flexible licensing
  Multiple licensing and pricing options, including BYOL (Bring-Your-Own-License) and PPU (Pay-Per-Use) helps optimize your investment in IT and digital transformation and maintain a high ROI in your cloudization project.

---

1. https://www.kaspersky.com/top3
2. Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms
Edge-to-Edge Security Capabilities

By deploying these capabilities and applying this quality and scope of multi-layered security right across your private and public cloud infrastructure, you have the reassurance of knowing that all your data, processes and applications are protected by all-encompassing ‘edge to edge’ security.

Securing the Future of Corporate IT

Amazon Web Services is changing the face of corporate IT. At Kaspersky Lab, we help ensure the security, visibility and manageability of your every workload, across both your AWS cloud estate and your private cloud environment, now and in future. Kaspersky Hybrid Cloud Security delivers multiple industry-recognized security technologies to support and simplify your IT environment transformation, securing your migration from physical to virtual, and to the cloud, while visibility and transparency guarantees a flawless security orchestration experience.