kaspersky BRING ON THE FUTURE

Safeguarding Your Microsoft Azure Cloud Estate

Kaspersky Hybrid Cloud Security

Public and managed clouds are now a part of the enterprise IT landscape. What's new is an increasing recognition that public clouds like Microsoft Azure have matured to the point that they are ready to handle even business-critical workloads.

These capabilities will have an impact on the security vision of enterprise organizations, and the construction of their IT strategies. How will your IT infrastructure scale and evolve over the next three to five years? How can the best use be made of the capabilities of public and managed clouds, while ensuring that the resulting hybridized infrastructure remains reliable and, above all, safe?

Cybersecurity incidents continue to be a huge concern, with increasing numbers large organizations suffering the financial, reputational, and sometimes legal consequences. Corporate security must be agile and intelligent enough to fight against current and future threats, and must also have the scalability and the flexibility to adapt and evolve alongside your hybridized cloud environment, incorporating both public and private cloud estates.

51%

of businesses admit that IT infrastructure complexity directly affects their ability to maintain appropriate levels of cybersecurity

Up to

80%

of data losses in hybrid clouds are due to outdated or reactive cybersecurity

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 designed to offer 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 into the public cloud arena, and in particular straddling both private and public clouds, has introduced new issues. Where does your security responsibility begin and end, and how do you orchestrate and protect workloads as they move on- and off-premise?

Know Before You Go

There are multiple risks faced by elastic cloud environments regardless of size, virtualization platforms used in the software-defined private data center or the cloud platform chosen to run business-critical apps. Cloud services providers, like Microsoft Azure, do a lot to make sure that public clouds remain a safe harbor for cloud-adopters of any scale. Azure 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.

Data Breaches or Leakage

Our 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.

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, an 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

The most efficient way to maintain data integrity is to implement cybersecurity tools that provide powerful runtime protection capabilities featuring behavior analytics empowered by machine learning. This enables the identification of the most advanced yet hidden menaces or sophisticated ransomware.

While data breaches generally remain a result of malicious activity, there are multiple scenarios when your data may become inaccessible or damaged due to or 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 (Recovering 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 and 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

The most successful cyberdefense strategies are based on a combination of application startup control (whitelisting, default deny) and exploit prevention capabilities.

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 fully resistant to zero-day vulnerabilities and exploits but require immediate remediation against potential cyber-risks.

Resource-Hungry Security

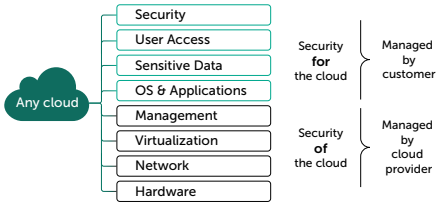
It's important to understand that it is your own responsibility to have a very clear picture all aspects of your hybrid cloud and its constituent parts, and to implement the cybersecurity capabilities which will deliver the most efficient combination of protection and resource-efficiency.

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

Working with public cloud APIs and extensions allows a reliable connection between IT and Security layers to be established, so that both can work in harness, empowering each another's capabilities and simplifying security provisioning, regardless of the size of your hybrid cloud environment

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 rapidlly 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 the security of your workloads, applications and data in public clouds remain your responsibility. And when these workloads are business-critical, this responsibility becomes even more important. Microsoft Azure is a leading public cloud service, offering a highly advanced cloud environment incorporating outstanding reliability and scalability.

However, shared security responsibility dictates the need for additional capabilities, enabling an elastic cybersecurity layer that covers your entire cloud environment, public and private, fully protecting the data you hold on your Azure-based workloads. You need to be fully aware of the risks, and how to remediate such risk throughout your cloud ecosystem, including your public cloud presence.

Cybersecurity Extensions To Defend Azure Cloud

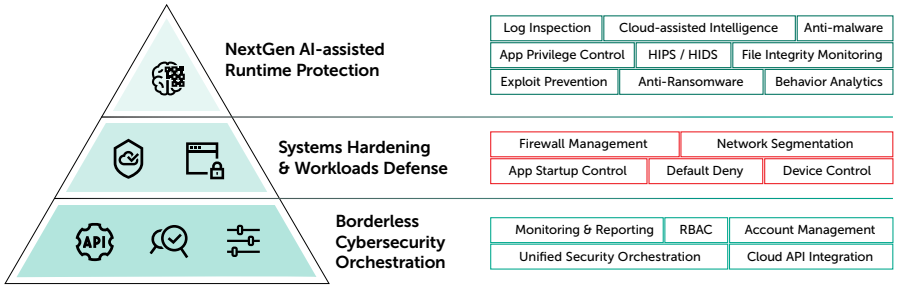
Kaspersky Lab's approach is to work with Microsoft Azure Extensions, not just applying next generation AI-assisted protection for your cloud workloads, but also enabling straightforward, flawless security monitoring and provisioning. This administrative ease and simplicity means that workloads running in your Azure estate can be brought under protection in a matter of seconds, fully safeguarding your cloud-based assets and your users.

We start by bringing to the table our leading edge 'next generation' capabilities – based around the most tested, most awarded[1] and most appreciated[2] 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 and your integrated cloud-based security to detect and respond to the most advanced cyberthreats.

Integrated Security for Microsoft Azure

We complement Azure's own cloud-native tools with proactive AI-assisted systems and runtime protection, including:

- **Our award-winning anti-malware engine**, providing automatic, real-time file level protection for every cloud workload – on-access and on-demand.
- **Cloud-assisted Intelligence** rapidly identifying new threats and provides automatic updates.
- **Behavior Detection** monitoring applications and processes, protecting against advanced threats and even bodiless malware and rolling back any malicious changes made inside cloud workloads if needed.
- **Exploit Prevention** controlling systems operation processes and applications behavior, helping block advanced threats including ransomware.
- **Anti-Ransomware** protecting cloud workloads and their shared networks against attacks, rolling back any affected files to their pre-encrypted state.
- **HIPS / HIDS** detecting and preventing network-based intrusions into cloud-based assets.
- **Application Controls**, enabling you to lock down all your hybrid cloud workloads in Default Deny mode for optimum systems hardening, as well as dictating what applications can run where, and what they can access.
- **Device Control**, specifying which virtualized devices can access individual cloud workloads, while Web Control protects against internet-based cyberthreats.
- **Network Segmentation** providing visibility and automated protection of hybrid cloud infrastructure networks.
- **Vulnerability Shielding**, preventing advanced malware and zero-day threats from exploiting unpatched vulnerabilities.
- **Mail Security** including Anti-Spam - protecting email traffic in cloud workloads.
- **Web Security** including Anti-Phishing - protecting against threats from potentially dangerous websites and scripts.
- **File Integrity Monitoring** protecting critical and system files, while Log Inspection scans internal log files to ensure operational hygiene.



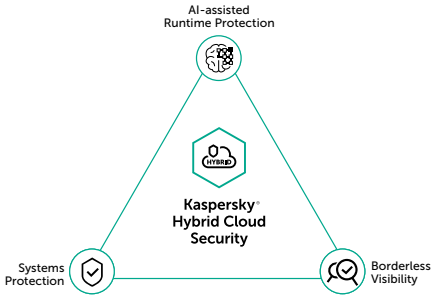
All these capabilities, covering your physical server environment as well as virtual and Azure cloud-based resources, are provided in a single Kaspersky Lab product, orchestrated through a single unified security console.

1 https://www.kaspersky.com/top3

2 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms

Why Kaspersky Hybrid Cloud Security?

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



Integrated Protection, Visibility and Orchestration

Edge-to-Edge Security

By deploying this quality and scope of multi-layered security right across your private and public cloud infrastructure, you have the reassurance of knowing that every workload, in no matter what location, operates in a fully secure 'edge-to-edge' hybrid cloud ecosystem.

Cloud-friendly Provisioning

Thanks to Azure Extensions, you can provision all these cybersecurity capabilities right inside your cloud workloads, keeping your always-on business apps safe and secure.

Compliance

Our integrated security approach means you can be confident that the security of everything you put into your Azure cloud adheres to your corporate standards, and that your assets and users are safeguarded at all times.

Unified Orchestration

Cybersecurity becomes a natural part of your cloud ecosystem thanks to integration into Azure Security Center.

Simplifies Security Provisioning

You can deploy real-time multi-layered protection for Azure cloud workloads straight from the Azure MarketPlace,

Flexible Licensing

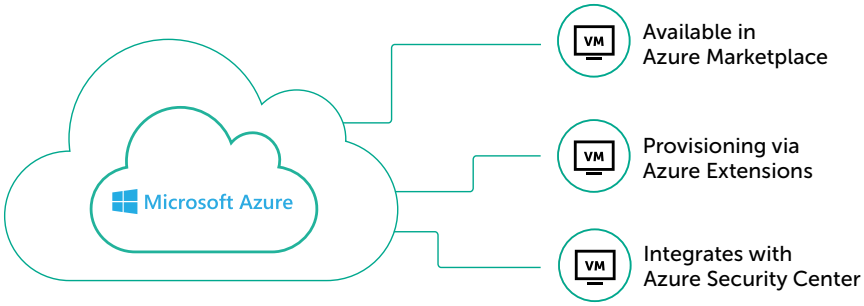
Multiple licensing and pricing options, including BYOL (Bring-Your-Own-License) and PPU (Pay-Per-Use) helps optimize your investment in IT and digital transformation and maintain a high ROI in your cloudization project.

Cloud Security That Just Works

The overall result is a perfectly orchestrated and adaptive cybersecurity ecosystem that delivers precisely the capabilities your hybrid cloud workloads require, while resource efficiency and seamless orchestration remain paramount.

Securing the Future of Corporate IT

Microsoft Azure is helping to change the face of corporate IT. At Kaspersky Lab, we help ensure the security, visibility and manageability of your every workload, across both your Azure cloud estate and your private cloud environment, now and in future.



www.kaspersky.com

Kaspersky Hybrid Cloud Security for Azure: kaspersky.com/azure
Kaspersky Hybrid Cloud Security for AWS: kaspersky.com/aws
Kaspersky Hybrid Cloud Security: kaspersky.com/hybrid

#hybrid
#aws_instance_security
#azure_vm_security