KASPERSKY lab ENTERPRISE

Borderless security engineered for your elastic hybrid cloud

Kaspersky Hybrid Cloud Security

www.kaspersky.com
#truecybersecurity

Borderless security engineered for your hybrid cloud environment

Data has become increasingly fluid, travelling constantly beyond the corporate IT perimeter on mobile devices as well as being processed on virtual as well as physical machines. And, with the uptake of public clouds and managed infrastructures, data is flowing off-premise and back as never before.

The growing adoption of an elastic cloud services model, where private data center resources expand instantaneously on demand and as needed into external clouds, delivers unprecedented flexibility, agility and clear economic benefits. There is no upfront investment in infrastructure, no waste and no delay in meeting immediate resourcing requirements while maintaining manageability.

Public clouds provide another great benefit – business continuity. If your data center suffers disruption or damage, off-premise resources can keep the show on the road until the issue is remedied. Public cloud providers themselves have invested heavily in their own business continuity and cybersecurity, creating safe, resilient environments for your business workloads. But that's not the end of the story...

Top Security Challeges for cloud adopters

- Malware and ransomware attacking physical, virtual and cloud-based workloads
- Data breaches as a result of a reactive and un-coordinated security approach
- Decreased transparency due to growing infrastructure complexity
- Administrative challenges because of disparate controls and tools
- Systems resources squandered by heavyweight traditional solutions.
- Insufficient protection for data stored inside private data centers
- DoS attacks disrupting operational continuity or preventing data exchange

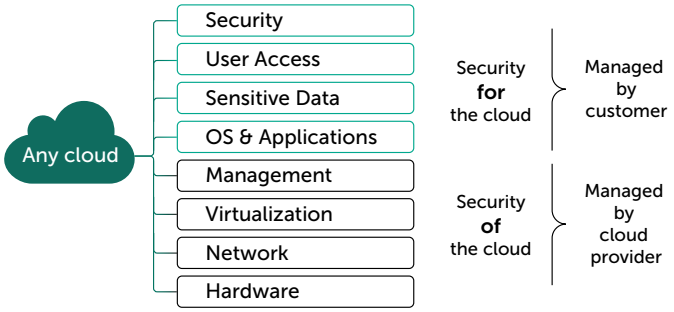
How secure is your data in public clouds?

The answer to this question is not as straightforward as it may seem.

Public clouds, as they currently stand, are very secure places. Great attention is paid to continuously ensuring that your data stays absolutely contained in the hosted environment and that there is no danger of leakage, within or beyond the external cloud.

But the fact that data is securely contained doesn't necessarily mean it's safe. Data leakage is just one aspect of security. Data exposed ransomware may, for example, remain fully and securely contained but may also be corrupted and thus absolutely useless. And any data which interacts with people, which is after all its main function as an organizational asset, is exposed to the effects of human error, and potentially of human malefactors.

Shared Security Responsibility Model

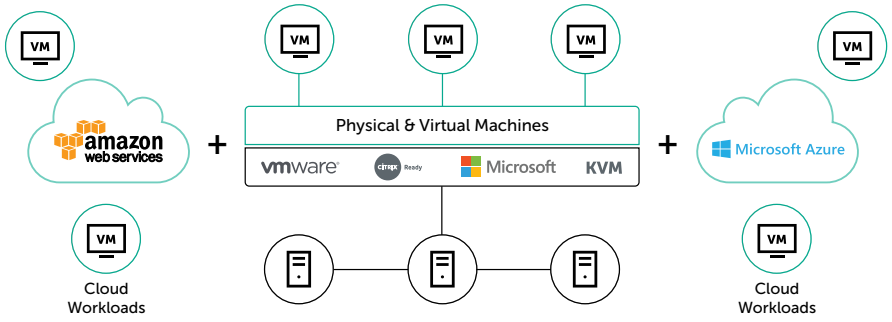


Hosted cloud service providers are responsible for the security of the environment they provide, but responsibility for the internal security of each workload, wherever it sits, remains firmly with you. This is what's known as the 'Shared Security Responsibility' model, where you and your service provider are responsible for different security aspects of your working relationship, and of your data assets.

So the answer to 'How secure is your data in public clouds?' is, at best, 'As secure as it is anywhere else'. The same security considerations apply to data wherever it travels. You can't protect data by simply securing the place where it's sitting at any one time. Recognizing this fact is becoming increasingly important as more and more business-critical data travels more and more widely beyond the controlled environment of the corporate IT perimeter.

Protect your data, not just its surroundings

Every package of data needs to be protected from the inside, wherever it happens to be at any one time, and while it's in transit. This is your corporate responsibility, which can't be outsourced or delegated.



To secure your workflow, you must be able to orchestrate it

So, first question, do you know exactly where every single data package is sitting, or travelling to, at any one time, and who's interacting with it?

Access control and monitoring is an ongoing security issue. The larger and more complex your IT infrastructure, the more solutions are needed to optimize efficiency and systems performance, and the harder it is to keep track of each workload, and every application. The expansion of data center infrastructures to incorporate external resources adds a further dimension to this issue. Ensuring that you can pinpoint what's being accessed and processed, on and off-premise, and how, is critical.

To secure your workloads, you must be able to harden them

What's happening? What applications are running where, and is every application behaving as it should? Vulnerabilities in applications remain the primary means of penetration and infection used by cybercriminals. Systems hardening is achieved through providing layers of technology to stop this happening. From banning or restricting certain applications to monitoring the ongoing behavior of every application at work in your organization and shielding vulnerabilities against exploitation – all these critical threat prevention and detection controls and interventions are your responsibility.

To secure your organization, you must be able to protect your data

To protect your runtime data, you need to be able to recognize when it's under potential or actual attack, and by what. From APTs (Advanced Persistent Threats) specifically targeting your business to opportunist ransomware, from data theft and financial fraud to random human error, threats to your data come in all shapes and sizes. And, cybercrime being a highly lucrative and sophisticated industry, new attack methods are constantly being developed and applied.

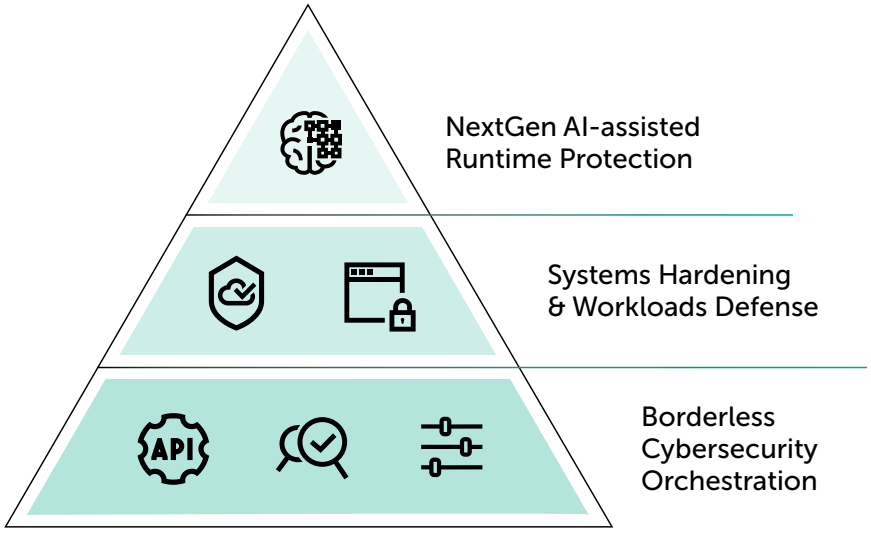
What's true of data in clouds remains true of all data – the quality of threat intelligence your security system relies upon, and the timeliness and accuracy of its application, will dictate the effectiveness of your ongoing protection. Your IT security system must be able to spot, block and remediate a potential threat before it reaches your data and impacts your operations. And it must do this without compromising systems performance and, importantly, without generating 'false positives' – causing disruption and wasting resources with false alarms.

Again, all this is your responsibility. Your cloud services provider can only secure your data so far: the rest us up to you.

What to look for when securing your hybrid cloud data center

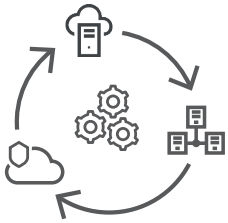
In summary, you can look to external data hosting software providers to deliver a secure, fully contained environment for your workloads to operate in. But it's your responsibility to monitor, control and protect of every piece of your data, wherever it happens to be.

At Kaspersky Lab, we refer to these three aspects of security responsibility as Cybersecurity Orchestration, Systems Hardening and Runtime Protection. We implement each of these security layers through a number of complementary and interlocking technologies – as shown below.



When specifying a solution to secure your hybrid cloud environment, we recommend you make a point of including a requirement for, in particular:

Borderless Orchestration



Cloud API – Integration with public clouds (such as Amazon AWS and Microsoft Azure) via native API. This allows for infrastructure discovery, the deployment of automated security agents, and policy-based management.

Account Management – Locking down cloud-based machines and increasing operational hygiene by ensuring that security operators and administrators have the correct permissions to access specific areas of the cybersecurity console

Role-based Access Control – Your infrastructure and security teams can have different levels of access and control over the cybersecurity layer of your hybrid cloud environment, based on the operational roles you assign to them.

Systems Hardening

Applications Control and Whitelisting – Banning or controlling what applications can run, where and when, reduces your attack surface. (Kaspersky Lab remains unique in operating its own Whitelisting Lab, specifying which applications can run safely by our customer at any one time, enabling the implementation of a highly secure 'default deny' policy if required)

Vulnerability Shielding – Techniques like exploit prevention, vulnerability assessment and automated patch management (all of which are of course included in Kaspersky Security for Hybrid Clouds) which prevent attackers from penetrating your systems via vulnerabilities in the popular applications your users rely on.

Run-time Protection

Anti-ransomware – Ransomware penetration prevention, including mail and web anti-malware. Kaspersky Security for Hybrid Clouds also incorporates 'automatic roll-back', so that any corrupted files are automatically returned to their previous, unencrypted status.

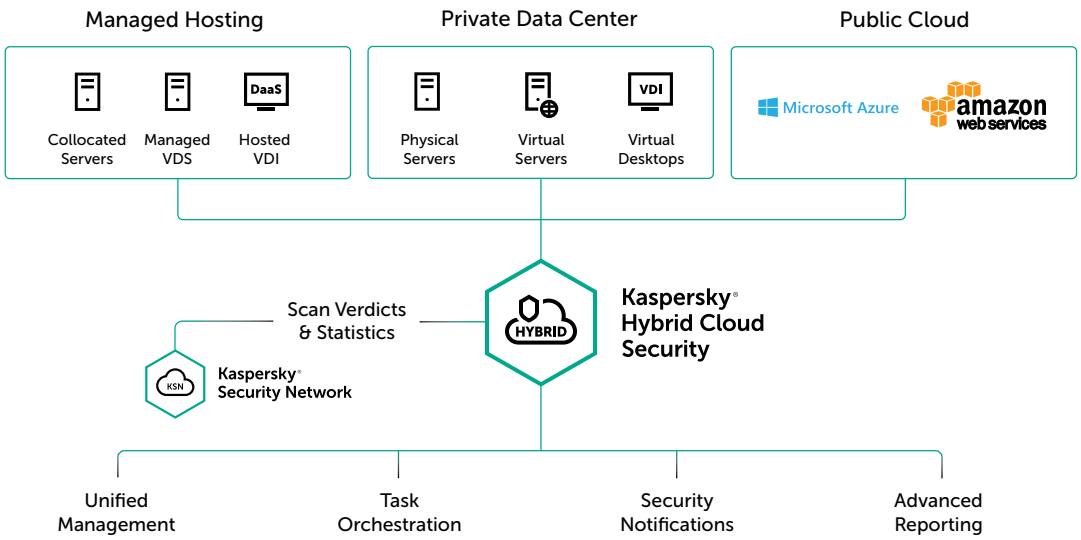
Advanced Threat Intelligence – access to and the ability to apply high quality real-time threat intelligence to your systems and data protection mechanisms.

This last feature is the most critical. Here, we are talking about artificial intelligence – the ability of a system to spot software or behavioral anomalies and so to recognize and identify threats it has never come across before. This is achieved through a combination of techniques including machine learning and behavioral analytics, through drawing directly on cloud-based intelligence databases and through the interventions of human experts.

This ability to identify and defend against unknown threats is absolutely fundamental to data security. Without this level of what we refer to as 'HuMachine® intelligence' – experts and expert systems working in unison – your data will be vulnerable to future attacks, no matter how many other security technologies are applied. Kaspersky Lab solutions are built around this combination of machine intelligence (we've been implementing machine learning in our technologies for over a decade now) and our unequalled expertise, enabling us to detect, identify and block tomorrow's threats as well as today's.

Cloud security as elegant as it is essential

Kaspersky Lab's Hybrid Cloud Security solution delivers all the above, and more, providing an adaptive security landscape to protect your entire hybrid cloud from the most sophisticated threats.



For Elastic and Secure Clouds

Hybrid environments are highly dynamic - your security must rapidly adapt to your changing operational landscape as it evolves and scales.

- Accelerate visibility across cloud environments for superior edge-to-edge protection.
- Detect and respond to advanced cyberthreats by harnessing the combined power of people and machines.
- Secure any cloud workload, system, network, or data with multiple controls.

One Product, Any Cloud

A solution engineered to deliver next generation cybersecurity for enterprise-grade hybrid cloud environments.

- Proven security for physical and virtual servers, VDI, storage, and even data channels in your private cloud.
- Advanced security controls for workloads in public clouds, including AWS and Azure.
- Meets ongoing enterprise Service Level Objectives (SLOs) by minimizing cyber-risk.

A Seamless Security Experience

The transparency and cross-integration of your IT and Security dictates your security status against known, unknown and emerging threats.

- Integration between core technologies of your cloud and its security layer via native API
- Automated security provisioning, for secure and uncompromised cloud migration
- A seamless enterprise-level security orchestration experience for any cloud

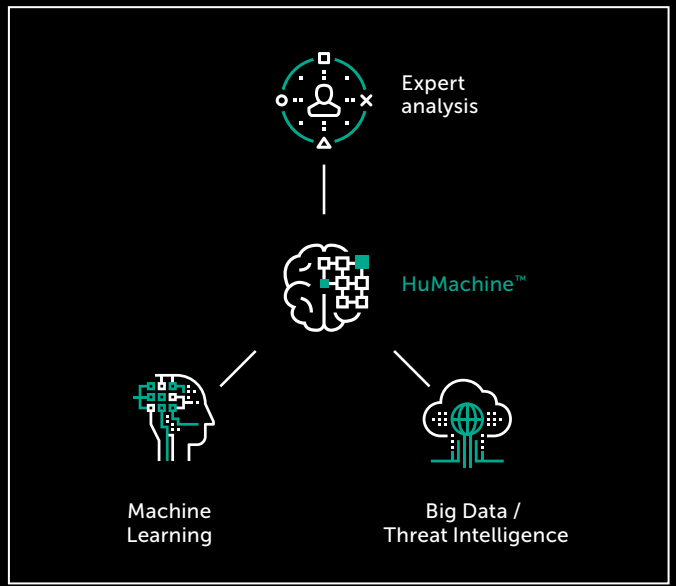
Thanks to state of the art capabilities implemented in our Hybrid Cloud Security solution, infrastructure and security layers integrate and interoperate, combining strengths to create a safe and efficient environment, allowing for the borderless migration of workloads between private and public clouds. The result is continuous, elastic, transparent and manageable security, so you can go as hybrid as business needs dictate.

In short...

Externally managed cloud based hosting services offer considerable business benefits and provide secure environments where organizational data can safely be stored and processed. But responsibility for the security of your work packages remains with you. By ensuring that you at all times retain full visibility and control of your data, processes and applications, and by applying 'HuMachine'® based advanced threat intelligence to data protection, you ensure the security of all aspects of your hybrid cloud data center.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**
Our unique approach: **www.kaspersky.com/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.