How to seamlessly and securely transition to hybrid cloud

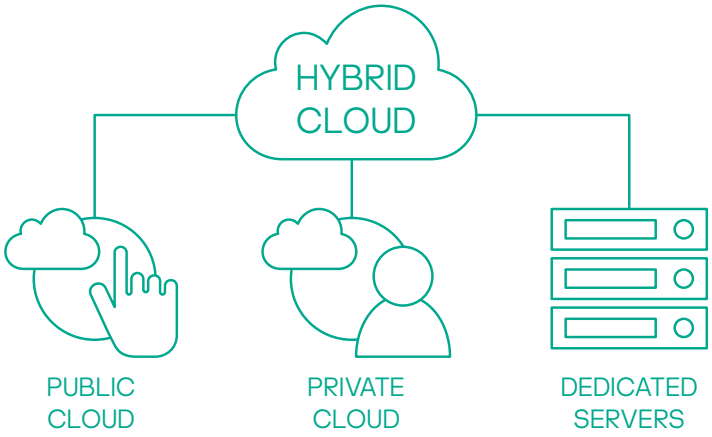
A vital enabler of your digital transformation

kaspersky

#bringonthefuture

A vital enabler of your digital transformation

Digital transformation is a never-ending story. Many businesses that five years ago hadn't even considered migration to the cloud are now operating complex infrastructure requiring them to manage diverse workloads across multiple public and private clouds, in addition to their on-premises systems.



The attraction of this 'hybrid cloud' strategy for digital transformation is compelling. Not only does it dramatically increase an enterprise's agility, flexibility and reduce its costs; according to a 2019 survey by IDG Research[1], a hybrid cloud strategy 'appears to accelerate the IT transformation journey, with 63% of respondents reporting the most progress using a hybrid cloud approach.'

So it's maybe unsurprising that among the results of Flexera's 2019 survey[2] of cloud computing trends, 84% of enterprises had a multi-cloud strategy, 69% were using hybrid cloud, and on average they were running applications in 3.4 public and private clouds, and experimenting with 1.5 more.

The same survey found 67% of respondents had adopted Amazon Web Services (AWS) and 60% were using Microsoft Azure. A further 15% and 14% respectively were experimenting with them, and 4% and 9% planned to do so. So if you're using or planning to use a public cloud solution, it's almost certain to involve AWS and/or Azure.

5 elements of digital transformation

Enterprise computing has moved beyond data storage and reporting to a strategic function that introduces new ways of working internally and with external partners and customers.

1. **IT is a force for innovation and collaboration**
2. **Modern IT leverages existing assets and investments, integrating the power of flexible cloud technologies**
3. **Hybrid cloud enables faster data processing, application development and implementation**
4. **Enterprises can quickly scale and respond to evolving business needs**
5. **Managing all data resources from a unified platform allows businesses to unlock new opportunities and position emerging/next gen technologies, such as AI, machine learning and the Internet of Things (IoT)**

Microsoft – Accelerate your digital transformation: the enterprise guide to hybrid cloud

1 IDG Research – The Challenge of Change: IT in Transition (2019)

2 Flexera (RightScale) – Cloud Computing Trends: 2019 State of the Cloud Survey

Research shows the security of this rapidly evolving infrastructure to be a top priority. So if you want your transition to hybrid cloud - as well as your broader digital transformation – to be successful, the security of your environment is a vital place to start.

Why is hybrid cloud security such a major issue?

Research by analysts such as Forrester, IDC, PwC and others has highlighted the diverse challenges faced by enterprises in securing their workloads within a hybrid cloud environment.

Back in 2015, IDC[3] warned that 'The primary barrier to the adoption and increased usage of public cloud services is security. Typically, an organization's concerns about security are multifaceted, touching data security, regulatory compliance, external threats to the service provider's cloud infrastructure and datacenter environments, shadow/rogue IT usage, and issues related to the lack of visibility into the cloud service provider's infrastructure.'

These concerns were echoed in a 2017 Forrester survey of IT executives[4]. When asked 'What challenges have you faced deploying/using multiple cloud platforms/environments?' the #1 answer was 'Security concerns'. And in reply to the question 'Which features of a hybrid cloud infrastructure platform are most important to you?' the #1 reply was 'Consistent security across public and private infrastructure'.

Based on these responses, Forrester found 'The top challenges inhibiting further expansion of hybrid cloud are security/privacy concerns, lack of cloud platform and management skill sets, and lack of consistent monitoring and management tools across platforms. Without consistent platforms and security, current staff skills

3 IDC whitepaper – Journey to the Hybrid Cloud – September 2015

4 Forrester – Unlock the value of cloud: a spotlight on IT executives – November 2017

will be stretched, limiting how much more hybrid companies can safely adopt cloud solutions. These concerns will continue to hold companies back from becoming more hybrid.'

The consultancy also noted that 'Companies turn to trusted vendors to help them expand hybrid cloud capabilities with consistent security and performance. Decision makers strongly prefer integrated solutions from vendors they trust. Security concerns top the list of hybrid cloud challenges. Starting with a strong security foundation built on known and trusted technologies is the best way for companies to safely expand their hybrid cloud with confidence.' And 'The more that companies can prioritize platforms that leverage the components they already know and trust, the less variation they will introduce with each new cloud platform.'

PwC made more wide-reaching recommendations[5], suggesting that 'Companies should realize the cloud is unique, a place where distributed data dictates a new way of thinking about security.

'Companies should have a cloud architecture that is designed with security in mind. Robust processes focused on protecting data loss are also vital. Further, safeguarding cloud-based data from attacks requires not only strong security capabilities, but also routine monitoring and updating.

'It is also increasingly important for companies to embrace automation of the cloud and especially security automation. When combined with the principles outlined above, automation can greatly reduce the risk of human error while keeping pace with the velocity and elasticity of the cloud. With these steps, organizations can not only improve their cloud security, but help create a more resilient data system that can create competitive advantages in an increasingly digital world.'

5 PwC – Cloud security: How to manage six common pitfalls – July 2017

Where are these concerns coming from, and how can you address them?

If you're an IT leader tasked with integrating public cloud workloads into your existing environment, there are a number of security issues that are going to be a cause for concern. In its 2019 Cloud Security Survey[6], for example, the SANS Institute found the top 4 major concerns reported by organizations in relation to the use of public cloud for business apps were:

- Unauthorized access by outsiders (55.6%)
- Inability to respond to incidents traversing our cloud apps and data (52.3%)
- Unauthorized access to sensitive data from other cloud tenants (52.3%)
- Lack of visibility into what data is being processed in the public cloud and where (51.4%)

Other significant security concerns included poorly configured or insecure interfaces or APIs, poor configuration and security of quickly spun-up application components, unauthorized (rogue) application components or compute instances, misconfiguration or vulnerability of hypervisors and other virtualization platforms, inability to audit, and inability to meet compliance requirements.

Put simply, in order to realize the benefits of public cloud within your hybrid cloud and/or digital transformation strategy, you're going to want your workloads to be more secure, and in particular to have no security gaps. This in turn means addressing common threats such as the following.

6 SANS 2019 Cloud Security Survey

	The threat	The solution
Data breaches or leakage	Elastic digital environments can compromise infrastructure visibility, and lead to a fragmented approach to cybersecurity. This makes corporate hybrid clouds a sweet spot for cybercriminals, particularly as the same tools can generally be used to penetrate traditional and cloud infrastructures.	Maintain reliable cyber-defenses for each individual workload in your hybrid cloud environment. The visibility and transparency of both IT and security layers is also essential – ensuring you can see every workload and provision automated cybersecurity capabilities to every corner of your rapidly changing cloud environment.
Data loss or non-integrity	Multiple scenarios can make your data inaccessible or damaged due to unintentional actions by your own end users, as well as malicious activity. Backing up or replicating data doesn't mean you won't find issues when restoring it.	Implement cybersecurity tools providing powerful runtime protection capabilities featuring behavioral analytics empowered by machine learning. This enables the identification of the most advanced yet hidden threats or sophisticated ransomware.
Unwanted or unknown applications	Because you can't always control what's installed on your on-premises or cloud servers, it's vital to have solutions that control what's running on them – right from application startup.	The most successful cyber-defense strategies are based on a combination of application startup control (whitelisting, default deny) and exploit prevention capabilities.
Resource-hungry security	Most hybrid clouds are a mixture of software-defined private data centers and elastic public cloud services. Both require protection, but adopting a 'traditional antivirus everywhere' approach to hybrid cloud security is a massively inefficient utilization of cloud resources.	You need to have a clear picture of all aspects of your hybrid cloud and its constituent parts, and implement cybersecurity capabilities delivering the most efficient combination of protection and resource-efficiency, avoiding unnecessary costs.
Security and infrastructure misalignment	Hybrid cloud requires the constant provisioning of cybersecurity to newly-deployed cloud workloads. But if your IT and security layers don't interact effectively, your security teams won't be able to safeguard what they cannot see.	Working with public cloud APIs and extensions allows a reliable connection between IT and security layers to be established. Both can then work in harmony, empowering each other's capabilities and simplifying security provisioning.
'Shared responsibility'	While hosted cloud service providers are responsible for the security of the environment they provide, responsibility for the internal security of each workload remains with the customer.	It's your responsibility to monitor, control and protect all of your workloads, wherever they happen to be. This means taking control of three key layers of security responsibility – prevention, detection and response.

Optimizing security for hybrid cloud workloads

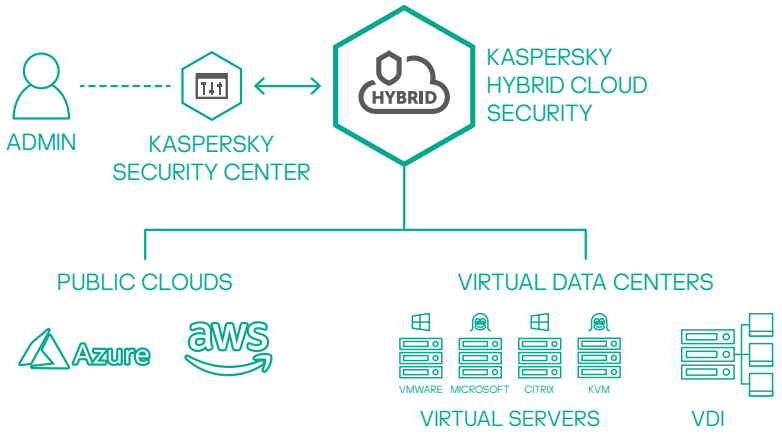
To address these kinds of issues, you're going to want a workload protection solution that prevents threats through systems hardening, patching etc.; detects incidents when they occur; and responds effectively, through active defense and mitigation, quarantining, blocking ports, killing infected data streams and severing affected connections.

But you'll also want a solution that achieves this without compromising performance, maintains your agility, ensures compliance and keeps you audit-ready. An ideal hybrid cloud workload protection solution is therefore one that:

- Provides the necessary level of protection for all the different types of workloads running on your various hybrid cloud platforms.
- Delivers an essential set of technologies including system hardening, exploit prevention, antivirus, firewall and file integrity monitoring.
- Is structured as a comprehensive, multi-layered solution focused on maximizing security and minimizing risk.
- Does not cause performance degradation for services or users, or impose any unnecessary overheads on servers or resources.
- Supports compliance by satisfying a broad range of regulatory requirements related to how baseline technologies are deployed, configured, updated and continuously monitored.
- Enforces consistent security policies throughout all parts of the hybrid infrastructure – maintaining visibility and control.
- Enables 'ongoing' audit by integrating state of security reports into daily/weekly/monthly IT reporting, and providing the means for this.
- Takes account of continuous infrastructure changes, through broad and timely support for platforms and operating systems, and integration with native APIs, third-party technologies such as SIEM, etc.

So how does Kaspersky help to secure your hybrid cloud environment

Kaspersky Hybrid Cloud Security provides an adaptive workload security solution to protect your entire hybrid cloud from the most sophisticated threats. Integrations with AWS, Azure and virtualization platforms via native APIs enable infrastructure discovery, consistent visibility, auto-scaling and the deployment of automated security agents. A single pane of glass management console also enables policy-based management – closing security gaps, reducing management burden, and supporting auditing and compliance.



Unparalleled security at the core

Kaspersky is best known for our security expertise and innovative protection technologies. Multi-layered security provides consistent high levels of threat prevention, detection and mitigation.
Our solutions are the most tested and absolute leader of the Top3 aggregate metric; and in 2018 Kaspersky has once again been named a Gartner Peer Insights Customers' Choice for Endpoint Protection Platforms, having received a high customer satisfaction rating of 4.6 out of 5 as of May 28, 2019.[7]

7 Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its afliates.

Protection for datacenters and private clouds

Kaspersky Hybrid Cloud Security is designed to minimize impact on virtualized infrastructure while delivering the highest level of security. Thanks to centralized file-level threat analysis, the solution eliminates redundant data and operations, dramatically reducing IOPS, CPU cycles, memory and storage footprints. As a result, up to 30% of virtualization resources are returned back to the pool, allowing more virtual machines (VMs) to be run on the same hardware – boosting the consolidation ratio, or enabling the resources to be used for increased infrastructure reliability.

Protection for public cloud (IaaS)

Kaspersky Hybrid Cloud Security leverages native API integrations with AWS and Azure to provide consistent visibility, reduce the attack surface, minimize dwell time and lateral movement, preserve business-critical data, and support compliance in public cloud environments.

Unified security orchestration

Kaspersky Security Center takes the complexity out of security administration and IT systems management. Fully scalable, the console enables digital transformation and facilitates comprehensive security management, with easy separation and delegation of administrator responsibilities.

Compliance

Application control, file integrity monitoring and log inspection can help enterprises comply with system and data security requirements such as PCI DSS (V3.21 ref# 10.5, 11.5), ISO/IEC 27001 (A10.10.1, A10.10.3, A.12.4.2), FedRAMP (CM-7, RA-5, AU-2, AU-5, AU-6, AU-9), Common Criteria (CC 3.2-3.4, 4.2, 5.1, 5.2, 6.1, 7.2, 7.3) and others.

Breadth of solution

- **Our award-winning anti-malware engine** provides automatic, real-time file level protection for every cloud workload – on-access and on-demand.
- **Cloud-assisted intelligence** rapidly identifies new threats and provides automatic updates.
- **Exploit prevention** controls systems operation processes and applications behavior, helping to block advanced threats including ransomware.
- **Anti-ransomware** protects data shared by cloud workloads.
- **Application controls** enable you to lock down all your hybrid cloud workloads in default deny mode for optimum systems hardening, as well as dictating which applications can run where, and what they can access.
- **Device control** specifies which virtualized devices can access individual cloud workloads, while **web control** protects against internet-based cyber threats.
- **Network threat protection** provides visibility and automated protection of hybrid cloud infrastructure networks.
- **Vulnerability shielding** prevents advanced malware and zero-day threats from exploiting unpatched vulnerabilities.
- **Mail security** including **anti-spam** protects email traffic in cloud workloads.
- **Web security** including **anti-phishing** protects against threats from potentially dangerous websites and scripts.
- **File integrity monitoring** protects critical and system files, while log inspection scans internal log files to ensure operational hygiene.

Kaspersky Hybrid Cloud Security therefore complements AWS and Azure's own cloud-native tools, and provides an edge-to-edge workload protection solution for your public cloud resources, as well as your physical and virtual server environments – all orchestrated through a single unified console.

Where to start?

- If you're already using one or more Kaspersky solutions, you can find out more about how to organically and seamlessly extend your existing security into your hybrid cloud – a strategy recommended by analysts such as Forrester – **here**.
- Or, if you've yet to benefit from the industry's most tested, most awarded security[1], you can find out more about us **here**, and more about Kaspersky Hybrid Cloud Security **here**.
- You can find more specific information on the benefits of Kaspersky Hybrid Cloud Security for **AWS** and **Azure** via these links.
- Or, if you want to start using and benefiting from Kaspersky Hybrid Cloud Security immediately:
- For Amazon Web Services, visit **the AWS Marketplace** where you can also take advantage of a free 30-day trial.
- For Microsoft Azure, visit the **Azure Marketplace**.

1 In 2018 Kaspersky products participated in 88 independent tests and reviews. Our products were awarded 73 firsts and achieved 77 top-three finishes. You can learn more about the tests here.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky BRING ON THE FUTURE