imperva

WHITEPAPER

The Three Keys to Secure and Successful Cloud Migrations

Introduction

Most mid-sized to large enterprises have already moved some of their infrastructure, data, and workloads into the cloud for better agility, efficiency, and cost savings. Nearly three-quarters of businesses are running a hybrid and/or multi-cloud strategy today, according to Forrester Research.

Cloud migrations are often part of larger corporate digital transformations that include the adoption of DevOps strategies, microservices, APIs, containers, and more. Security is never the driver — though it may be the most important passenger. Numerous surveys of IT professionals show that security remains their biggest concern, and often an outright obstacle to their cloud adoption. Companies want to know:

- How can they ensure security and compliance controls are in place as they transition to the cloud, and are not a barrier to transformation?
- How can they ensure that security and compliance are consistent across cloud asset deployments as well as the assets that remain on-premises?
- How can they actually buy down the risk around their data with the right security investments as they move to the cloud?

To make cloud transformations as efficient and successful as possible, companies must remain secure and compliant throughout. And there are three keys to ensure secure and compliant cloud migrations, which every enterprise IT and security leader should know. They are:

- Standardize security practices across your cloud, hybrid, and Multi-Cloud assets
- Use modern security platforms built for the cloud automation era
- Use Defense-in-Depth to protect APIs, applications and data, wherever they reside

THE THREE KEYS

1. Standardize security practices across your cloud, hybrid, and Multi-Cloud assets.
2. Use modern security platforms built for the cloud automation era.
3. Use Defense-in-Depth to protect APIs, applications and data, wherever they reside.

Standardize security practices across your entire hybrid/multi-cloud infrastructure

Every company's business transformation is different, and performed at a different pace. Some companies jump in head-first, quickly moving all of their data and workloads off premises onto Infrastructure as a Service (IaaS) public cloud offerings. Others move more cautiously, keeping legacy applications and data on-premises, and surgically creating a limited number of new workloads and processes in private clouds. Most companies are somewhere in the middle, moving some data and workloads to a hybrid set of public and private clouds from a variety of providers, but keeping other data in place for unique strategic reasons.

Many companies choose a multi-cloud strategy in order to avoid overdependence on any one vendor. Statistics back that up, showing that companies on average are using almost 5 different public and private clouds today. With so many different cloud deployment and service models available today — read our in-depth Cloud Migration Guide to learn about them all — the number of different clouds used by companies is set to grow, not shrink. Flexibility, as you can see, is key.

However, this cloud diversity creates additional governance and security challenges. You still need to ensure that consistent compliance and security practices are followed. Without strong controls and best practices everywhere, your business is neither secure nor compliant. You don't want to protect against a threat in your legacy on-prem systems while leaving it undefended in the cloud.

The environment sometimes dictates your security tools. But when you have a choice, it can be quicker to achieve standardized controls through a comprehensive solution, as long as the footprint is broad enough. This way, you can achieve a single pane of glass that enables complete visibility across your enterprise.

Modern security platform for the cloud automation era

Today's cloud-enabled enterprises strive to be agile, collaborative, highly-automated, and efficient. Manually moving workloads and technologies to the cloud is a step backwards, being slow, labor-intensive, and error-prone. And that can ultimately lead to more security vulnerabilities, as well as wasted time and money.

That's why modern enterprises are rebuilding or refactoring business applications on microservices and cloud technology. They're investing heavily in cloud orchestration and automation to smooth and simplify every facet of their business IT infrastructure and lifecycle processes.

Take the modern agile development practice of Continuous Integration/Continuous Delivery, aka CI/CD. Here, developers strive to deliver features and application changes more quickly. Ensuring the code doesn't inadvertently create security vulnerabilities is key. However, manually combing through code to find potential vulnerabilities can slow down the CI/CD process to a crawl. What's needed is a solution that automatically spots vulnerabilities, or prevents exploits by default.

Organizations should adopt the same mindset where ever it must deliver security. Your security solution shouldn't just support the cloud, but actively enable and support efficient cloud workloads and workload migrations with rich automation, DevOps, and DevSecOps capabilities.

Modern enterprises also rely heavily on open APIs. On a technical level, APIs connect public and private clouds, and help orchestrate the management of the data and resources on them. On a business level, open APIs are key to building partner ecosystems and accelerating innovation.

To protect your cloud infrastructure, your security solutions must protect your critical APIs and manage access to them by applications and users, including privileged insiders.

Finally, your ability to rapidly deploy the protection your data needs at cloud speed can hinge as much on your security vendor's contract, as its technology itself. A software license that provides flexibility and agility is key to success, too.

Your security solution should support efficient cloud workloads and workload migrations with rich automation, DevOps, and DevSecOps capabilities.

Defense-in-depth for applications, APIs and data, wherever they reside

One of the benefits of an on-premises-only infrastructure is the ability for security teams to lock it down and minimize the attack surface. There is a massive cost to your business, though, as you greatly hamper your employees' productivity, and their ability to innovate, partner, and quickly grab business opportunities.

If not executed securely, migrating to the cloud can cause your organizations' threat surface to balloon, exposing you to a potential explosion of attacks and leading to breaches whose financial damage outweighs all of your cloud-earned gains. To stay ahead of threats while protecting cloud migration, you need a multi-layered security architecture that provides autonomic defense-in-depth.

Start with application security. Web application and API firewalls can be your first line of defense, creating a hard-to-penetrate barrier against malware and hackers. Complement that with DDoS protection to ensure your websites and applications remain up, even when facing the most ferocious packet firehoses. Bot management can also quickly identify and automatically prevent automated attacks, while Account takeover protection leverages AI to block botnet traffic as well as attackers using stolen user logins.

Moreover, security shouldn't just guard the walls and perimeters of their clouds. For best protection, it should reside adjacent or within the cloud applications and data. This will protect your business's crown jewels against insider threats such as careless handling, compromised accounts, or privileged users that are malicious.

Such data security should also include protection and oversight for data that is increasingly stored in born-in-the-cloud databases, aka Databases-as-a-Service (DBaaS), such as Amazon RDS, Azure SQL, and others.

To stay ahead of threats while protecting cloud migration, you need a multi-layered security architecture that provides autonomic defense-in-depth.

Buying your risk down

And remember: when implementing a defense-in-depth strategy, businesses are best guided by a thorough threat assessment that takes a risk buydown approach. Creating a comprehensive inventory of threats is a great first step. However, technology should always serve business risk and outcomes. So the next step is even more key: calculating the potential financial losses if each of those vulnerabilities is exploited. Financial damage can result from lost sales, regulatory penalties, brand reputation damage, and more.

Using such an outcome-led methodology enables security teams to weight risk properly, and invest rationally. Rather than buying impressive-sounding technologies simply for their own sake, IT and security leaders can now put their dollars into security layers that offer the greatest ROI in terms of reducing financial risk. In this way, a risk buydown mindset works perfectly with a defense-in-depth approach.

What Imperva offers

As a cybersecurity leader championing the fight to secure data and applications wherever they reside, Imperva offers a full defense-in-depth portfolio of application and data security solutions. Built on a full-stack architecture and deployed across a global network, Imperva protects applications, websites, business-critical APIs, legacy systems and applications based on open source, and much more. Our DDoS Protection service mitigates attacks in 3 seconds or less, while our WAF, RASP, and Bot Protection capabilities are recognized as leaders by analysts such as Gartner and Forrester Research. Our AI-infused analytics capabilities deliver actionable insights to IT and security professionals to save them time, effort, and cost. Companies can also bake in our Runtime Application Self-Protection (RASP) technology, which sits within application code to autonomously prevent exploits against known and zero-day vulnerabilities. RASP also provides precise data on what code is targeted. That allows your internal security teams to focus resources and better manage the risks.

For example, enterprises can add RASP to the developers repository, making it easy for teams to integrate it into the CI/CD pipeline. In this way, RASP is automatically installed whenever Jenkins is used to build a Docker base container, or whenever applications are deployed to a server. RASP can also be swiftly and automatically updated by CD technologies whenever applications, containers, or servers are reconfigured. That's effortless, built-in protection and compliance.

Finally, our stack of Data Security solutions, including the new Cloud Data Service, provide the most-targeted protection of your most valuable asset — your data — wherever you choose to host it. Imperva Data Security can tell you whether you have sensitive data in the cloud and help you classify it. It can discover any known database vulnerabilities that could expose the data, and constantly monitor data access, so that you always know who is accessing your data and what they are doing with it. All of the above solutions provide informative analytic dashboards that rely on machine learning and AI on the back-end to distill the thousands of daily security events harvested from all of your clouds into several holistic, easy-to-understand narratives that your team can then quickly investigate and take action on. This enables complete visibility, and helps in singling out enterprise-wide attack campaigns.

MORE RESOURCES

eBook:
Cloud migration guide

Webinar:
Migrating to the cloud safely and securely

Webinar:
Security in the age of hybrid cloud

Gartner Report:
Defining cloud web application and API (WAAP) services

White Paper:
Secure your data to effectively reduce business risk

Datasheet:
Imperva cloud web application firewall

Free Trial:
Imperva cloud data security

Learn more:
Visit imperva.com

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com