CONNECT THE CLOUDS

WEAVING THE PERFECT MULTI-CLOUD ENVIRONMENT

Multi-cloud strategies are the norm among businesses, with the majority harnessing a hybrid cloud approach. But carrying out a successful multi-cloud strategy requires businesses to keep considerations in mind.

YOUR CLOUD OPTIONS

Typical cloud architecture is broken down into three main deployment models:

1. PUBLIC
2. PRIVATE
3. HYBRID

However, a fourth is also available:

4. VIRTUAL PRIVATE CLOUD

82 PERCENT of enterprises are actively harnessing a hybrid approach, making this the most popular deployment strategy.

The average business today stores **1.2 million files** in the cloud, a number that's grown tenfold over the previous year.

Business apps, services and processes are being designed with the cloud in mind.

THE THREAT ATMOSPHERE

Cybercrime costs global businesses more than **$300B EACH YEAR**

23 PERCENT INCREASE

From 2013 to 2015, the total cost of a data breach in the U.S. increased **23 percent.**

THE DATA TYPES

A **multi-cloud strategy** ensures the three main data levels receive the individualized data, security and performance attention that they require.

Public information

demands the lowest level of security, since it's data that is largely publicly available. This is the type of data that can typically be handled via popular public clouds like AWS or Azure without integrating additional security controls or threat intelligence.

Development workloads

involve private data — PII, early-stage development or company IP — that could be materially damaging in the event of a breach.

High-risk workloads

represent an organization's most sensitive information, such as PHI, PII, card data or key company IP — the kind that won't be adequately protected by a public cloud. This data calls for a security-focused virtual private cloud.

ANY ENVIRONMENT. TOTAL SECURITY.

No matter which environment you're using, partner with a cybersecurity expert that can secure each. **Seventy percent** of business security executives harbor anxiety about the cloud.

70%

If a managed cloud infrastructure isn't able to seamlessly integrate with your existing environment, it won't be able to deliver optimized security and performance.

Look for security expertise, around-the-clock support, self-service resources and other signs of experience from a provider.

A FUTURE-FOCUSED CYBERSECURITY PARTNER WILL BE ABLE TO:

- Identify & Protect the Most Valuable Data
- Share Risk & Simplify Audits
- Save Money & Increase Efficiency

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™

armor.com | 1.844.682.2858 | @armor

Sources:
Armor, "The cloud crossover: 10 reasons you're ready for a managed cloud"
Armor, "A cloud for every workload: Reimagining multi-cloud strategies through persistent data classification"
Armor, Page on Shared Responsibility
Armor, Page on Security Solutions
ponemon.org/library/2015-cost-of-cyber-crime-united-states
rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey
searchcloudapplications.techtarget.com/definition/multi-cloud-strategy
cloudlock.com/company/news-and-press/press-releases/cloudlock-reports-that-one-in-four-employees-exposes-enterprises-to-cloud-cyberattacks/
image.slidesharecdn.com/dss-cloudandrisks-2015-rigabusinessschool-150201143546-conversion-gate02/95/2015-the-cloud-for-managers-riga-business-school-dss-cloud-risks-and-some-thoughts-6-638.jpg
computerweekly.com/news/2240219265/Cyber-attacks-move-to-cloud-with-adoption-report-shows
grantthornton.global/en/insights/articles/cyber-attacks-cost-global-business-over-$300bn-a-year/