ePlus Solution Brief

Securing Multi-Cloud Workloads

Protecting critical assets, no matter their location.

As organizations increasingly move towards a multi-cloud strategy for managing their data, it is critical to mitigate the risks associated with this diversification. While the benefits of adopting a multi-cloud strategy are clear, security cannot take a back seat. The key to implementing a resilient multi-cloud strategy is to incorporate security into each component from day-one when it is easiest and less costly to implement and enforce.

Why Multi-Cloud?

Today's reality is that almost every industry has moved some type of data or workload to the cloud or to an as-a-service model. Progressively, more workloads are moving between clouds as organizations mature their capabilities. Also, more enterprises are connecting from the data center to a public cloud. This diversification helps enterprises mitigate the risks associated with vendor lock-in and may help address other business critical areas or functions, such as business continuity.

The move to a multi-cloud enterprise requires consistent, automated protections across deployments that prevent data loss and business downtime.

How ePlus Can Help

ePlus provides our clients with tailored solutions focused on achieving outcomes that address the specific needs of their organization. Our comprehensive approach couples leading technology with valued services to help navigate the sea of solutions and software to provide you an efficient, integrated and affordable solution.

We work with your organization and understand the skills, processes and technology you have made investments in and will tailor our approach to ensure your organization is best positioned to mitigate critical risks.

How Does ePlus Secure Multi-Cloud Workloads?

ePlus leverages partnerships with leading technology providers and couples that with our deep technical knowledge and experience to provide a comprehensive approach to help secure your multi-cloud workloads and ensure a strong security posture.

Our approach incorporates Data Protection, Infrastructure and Application Protection, Scalable Identity and Access Management, Automation and Orchestration. FLIP TO LEARN MORE →

According to industry reports, corporate users have on average **27 ID/PASSWORDS EACH**.

A Forrester study showed that **86% OF CLOUD** strategy and application management decisions makers described their cloud strategy as multi-cloud.

The 2018 State of the Cloud report states that **FOUR IS THE MEDIAN** number of clouds in use by organizations.

A report published on Application Delivery states that **56% OF ORGANIZATIONS** choose their cloud platform on a per-app basis.

According to Gartner, multi-cloud strategies will be common for **70% OF ENTERPRISES** by 2019.

CONTACT US

Contact us today to learn more about how the ePlus approach to Securing Multi-Cloud Workloads can be implemented for your environment.

@ eplus-security@eplus.com
☎ 1-888-482-1122
www.eplus.com/security

e+

Where Technology
Means More®

THE EPLUS APPROACH TO SECURING MULTI-CLOUD WORKLOADS

DATA PROTECTION

Traditional models of data management and security no longer hold true for multi-cloud environments. Authenticated and authorized employees must have access to corporate data from any trusted location, on any trusted device, at any time. As more cloud services are adopted, monitoring these data flows can become a significant challenge. Enterprises must have a thorough understanding of their data – what it is, where it goes, and who can access it. This means security teams must safeguard sensitive data wherever it resides. To do this effectively and provide a full range of data protection capabilities in a multi-cloud enterprise, your security team will need to perform many tasks including data discovery and classification, data and file activity monitoring, data masking, encryption and more.

INFRASTRUCTURE AND APPLICATION PROTECTION

Visibility and policy enforcement on server and container workloads, cloud connectors and APIs is critical in the as-a-service model. Exposed services can leave enterprises vulnerable to breaches. For your security team to quickly detect anomalous behavior and respond to threats, having visibility across all multi-cloud instances is key. The telemetry from **policy enforcement** and control points give your security team **real-time visibility** into what is happening in your multi-cloud environment. They will be able to setup prioritized alerts so when policies are breached action can be taken. This may also help your organization meet or exceed any compliance requirements. It is also critical that the shared responsibility model for each specific cloud provider or as-a-service instance is fully understood. While you can count on the provider to secure the cloud itself, it is up to you to secure everything in that cloud. Human error is generally the biggest risk factor in security. DevOps plays a key role in automating routine, repeatable tasks, and is a good way to ensure your security posture in a multi-cloud enterprise. When **governance rules** are built for your multi-cloud enterprise and married to an **automation platform**, your corporate standards and policies are managed efficiently and with minimal margin for error.

SCALABLE IDENTITY AND ACCESS MANAGEMENT

With every cloud service comes a new user account (and password and controls) to manage. The typical enterprise employee has dozens, perhaps hundreds of applications that span multiple clouds, mobile and on-premise solutions, and all can hold confidential, sensitive and regulated information. Because of this, security per single service does not scale. Poor password management also accounts for a large majority of breaches. By implementing **an identity and access management framework** (which is comprised of multiple components, including but not limited to identification (authentication), federation, access monitoring and access control (authorization)) you will help reduce risk and ease the burden of multi-cloud management in your enterprise. At its most fundamental level, identity and access management is the discipline that seeks to ensure the right people have access to the right resources at the right time for the right reason.

AUTOMATION AND ORCHESTRATION IS A PRIORITY

In the past, administrators needed expertise in multi-tiered or monolithic architectures. With cloud usage, especially multi-cloud, orchestration tools become critical. The process to spin up an environment to host a new application or service container, or create an auto scaling event, may contain hundreds of individual manual tasks. To maintain data integrity and security of the environment, the required steps generally need to be performed in a specific order, using **privileged permissions**, and may need to occur multiple times on any given day. Advanced orchestration capabilities are key, especially for multi-cloud management, where there is the need to oversee applications across different cloud platforms. Your DevOps team can create templates that orchestrate these processes into a single workflow. Critical tasks then become a single API call. **Cloud orchestration tools** have the potential to lower overall IT costs, free up engineering time, improve delivery times, and reduce friction between teams.

Cyber Security Frameworks

ePlus provides advisory services to help companies pursue alignment to leading industry frameworks such as CIS and NIST.

🟩 *Indicates control is either fully or partially addressed by this ePlus solution.*

CIS CONTROLS ADDRESSED

1	2	3	🟩 4	5	🟩 6	7	8	9	🟩 10	11	12	🟩 13	🟩 14	15	🟩 16	1	18	19	20

NIST CYBERSECURITY FRAMEWORK ALIGNMENT

IDENTIFY

ID.AM	ID.BE	🟩 ID.GV	ID.RA	ID.RM	ID.SC

PROTECT

🟩 PR.AC	PR.AT	🟩 PR.DS	🟩 PR.IP	PR.MA	🟩 PR.PT

DETECT

🟩 DE.AE	🟩 DE.CM	🟩 DE.DP

RESPOND

RS.RP	RS.CO	RS.AN	🟩 RS.MI	RS.IM

RECOVER

RC.RP	RC.IM	RC.CO

Corporate Headquarters:
13595 Dulles Technology Drive
Herndon, VA 20171-3413

Nasdaq: PLUS