DEPLOYING SECURE HYBRID CLOUD:

SECURITY ASPECTS & CHALLENGES

LRS® IT SOLUTIONS

Everyone seems to have gotten the memo about the cloud. To achieve performance, reliability and cost-savings goals, enterprises are increasingly embracing the cloud for both software reliability and scalability. The move to the cloud alleviates the need to physically maintain servers and the network infrastructure surrounding them; however, it's important to note that with cloud environments, organizations won't be alleviated when it comes to security, rather they will need to continue to carry the responsibility of securing data and workloads both in the cloud and on-premises.

Even though a cloud service provider (CSP) may provide some level of security, hybrid cloud architecture can be complex and requires continuous management from enterprise security teams to ensure that data and workloads are kept safe and secure.

With increasing compliance requirements such as General Data Protection Regulation (GDPR), the growing number of advanced threats and the need to move at the speed of business, security teams need to provide a comprehensive security framework to protect cloud and on-premises environments.

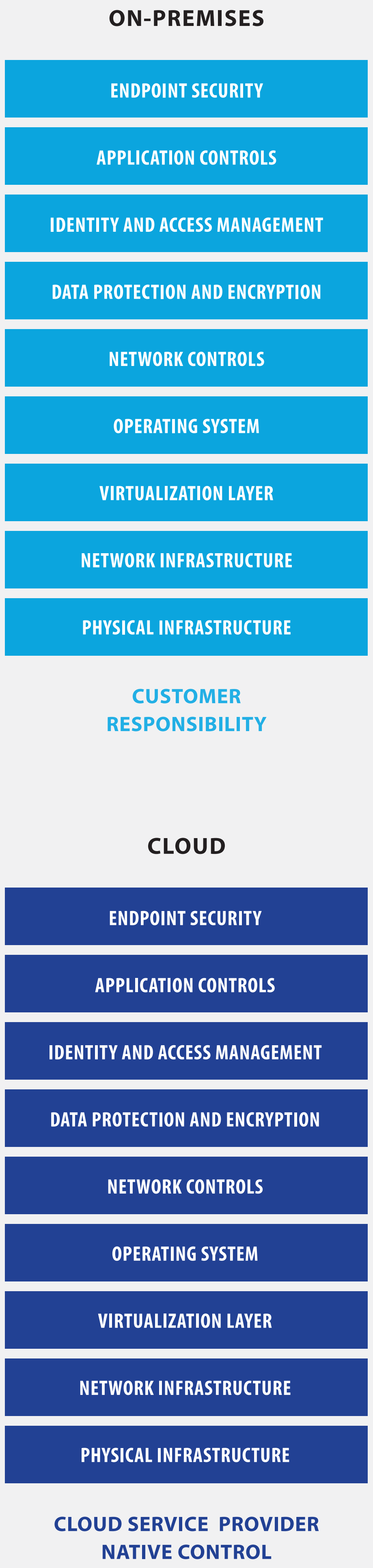
An essential step for a hybrid cloud security framework is to put security first. By enabling secure-by-design and integrating security controls into DevOps processes and cloud migration initiatives from the beginning, security can accelerate your business by not having to use valuable time and resources on reactive responses to threats and compliance issues.

The shift toward cloud and hybrid cloud environments has changed the mix of responsibilities that administrators of on-premises and cloud systems must address. Our findings have uncovered three main themes:

1. Increased Complexity and Scale of Hybrid Cloud Environments: Mainstream cloud adoption is leading to increasing hybrid cloud complexity and sprawl.

2. Lack of Automation and Third-Party Tool Integration: Manual processes and disparate tools leave security teams shorthanded in the race to innovation.

3. Limited Budgets and Staffing Shortages: Overstrained security teams are left to contend with limited staffing, reduced budgets and uncertain relationships with DevOps.



ON-PREMISES

ENDPOINT SECURITY

APPLICATION CONTROLS

IDENTITY AND ACCESS MANAGEMENT

DATA PROTECTION AND ENCRYPTION

NETWORK CONTROLS

OPERATING SYSTEM

VIRTUALIZATION LAYER

NETWORK INFRASTRUCTURE

PHYSICAL INFRASTRUCTURE

CUSTOMER RESPONSIBILITY

CLOUD

ENDPOINT SECURITY

APPLICATION CONTROLS

IDENTITY AND ACCESS MANAGEMENT

DATA PROTECTION AND ENCRYPTION

NETWORK CONTROLS

OPERATING SYSTEM

VIRTUALIZATION LAYER

NETWORK INFRASTRUCTURE

PHYSICAL INFRASTRUCTURE

CLOUD SERVICE PROVIDER NATIVE CONTROL

WHAT ARE SOME HYBRID CLOUD SECURITY CHALLENGES?

Protecting your data

Limit data exposure for your organization through encryption. The same data will be either in transit or at rest at different moments in time. You need a variety of security to limit data exposure during either of these states.

Compliance and governance

If you work in a highly regulated sector like healthcare, finances, or government, hybrid cloud infrastructure may present additional considerations. Know how to check your distributed environments to make sure that they are compliant; how to implement custom or regulatory security baselines; and how to prepare for security audits.

Security in the supply chain

Hybrid cloud environments often include products and software from multiple vendors in a complicated ecosystem. Know how your vendors test and manage their software and products. Understand when and how your vendors have inspected source code, how and which implementation guidelines they follow, and how and when vendors can provide updates and patches.

Physical controls for hybrid cloud security

Hybrid clouds can span multiple locations, which makes physical security a special challenge. You can't build a perimeter around all your machines and lock the door.

In the case of shared resources like a public cloud, you may have Service Level Agreements (SLAs) with your cloud provider that define which physical security standards will be met. For example, some public cloud providers have arrangements with government clients to restrict which personnel have access to the physical hardware.

But even with good SLAs, you're giving up some level of control when you're relying on a public cloud provider. This means other security controls become even more important.

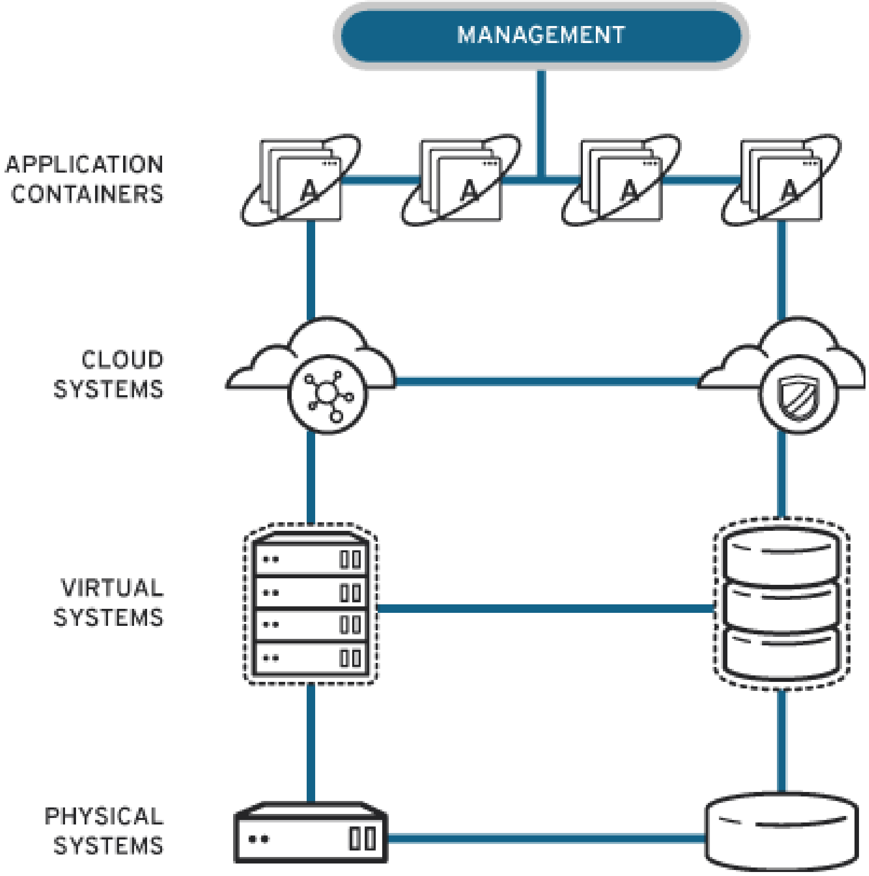
The components of hybrid cloud security

Hybrid cloud security, like computer security in general, consists of three components: physical, technical, and administrative.

Physical controls are for securing your actual hardware. Examples include locks, guards, and security cameras.

Technical controls are protections designed into IT systems themselves, such as encryption, network authentication, and management software. Many of the strongest security tools for hybrid cloud are technical controls.

Finally, administrative controls are programs to help people act in ways that enhance security, such as training and disaster planning.



Technical controls for hybrid cloud security

Technical controls are the heart of hybrid cloud security. The centralized management of a hybrid cloud makes technical controls easier to implement.

Some of the most powerful technical controls in your hybrid cloud toolbox are encryption, automation, orchestration, access control, and endpoint security.

ADMINISTRATIVE CONTROLS FOR HYBRID CLOUD SECURITY

Lastly, administrative controls in hybrid cloud security are implemented to account for human factors. Because hybrid cloud environments are highly connected, security is every user's responsibility.

Disaster preparedness and recovery are an example of an administrative control. If part of your hybrid cloud is knocked offline, who's responsible for what actions? Do you have protocols in place for data recovery?

Hybrid architecture offers significant advantages for administrative security. With your resources potentially distributed among on-site and off-site hardware, you have options for backups and redundancies. In hybrid clouds that involve public and private clouds, you can fail over to the public cloud if a system on your private data center cloud fails.

The LRS Security approach to securing your hybrid cloud

While offering certain protections from zero-day exploits and insider attacks, the cloud alone does not provide the enterprise security controls you'd expect and need for a business leveraging the cloud. In one study, 42 percent of organizations reported an attack in their hybrid cloud environments, and more than half of the organizations surveyed had easily remediable network vulnerabilities from using outdated browsers and legacy or unpatched operating systems.

Much like on-premises IT environments, a hybrid cloud environment has similar security concerns and requirements such as protecting data, securing systems and ensuring regulatory compliance. However, a hybrid cloud environment carries an additional challenge, which is to apply the same speed and attention to securing data on both cloud as well as on-premises environments.

The LRS security approach to securing hybrid cloud environments addresses the critical needs of enterprise-wide security with a focus to protect data, enhance productivity, and ensure compliance.

Protect Data
Data is one of the most valuable and critical assets entrusted to or created by a company. In a hybrid cloud environment, data lives both on-premises and in the cloud as well as moves between where it's stored and the endpoints and devices where it's accessed. For a hybrid cloud environment, you need to bring your own security controls to complement the security of your cloud service provider to keep your data safe and secure.

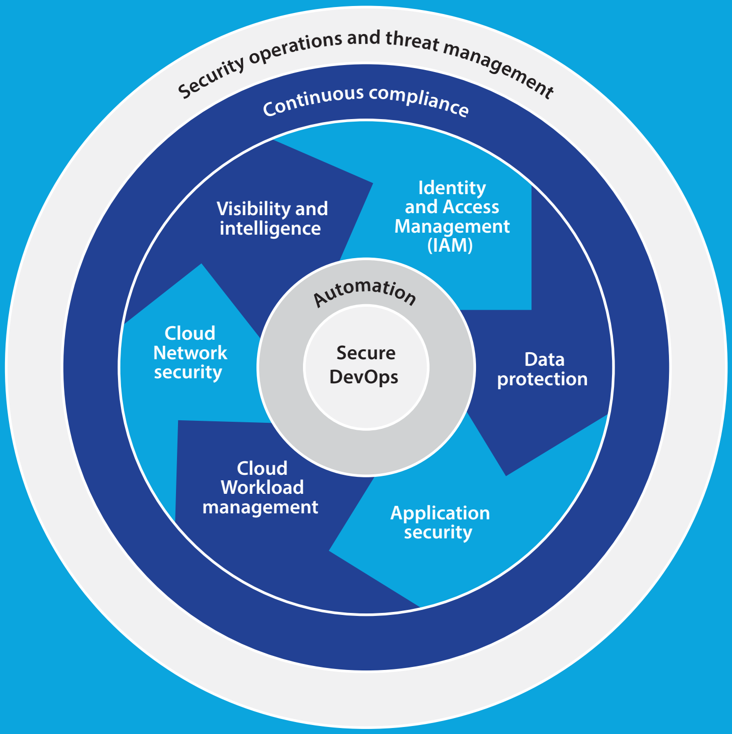
Enhance Productivity
For any business, productive time and resources are essential to maintaining success. Therefore, time and resources used in attending to preventable security incidents may not be the most efficient path for continued business growth. However, by working closely with DevOps to provide a security framework and the necessary tools to incorporate security controls from the beginning, productivity is not lost in having to go back and incorporate it later.

Ensure Compliance
Achieving and maintaining compliance can be complex, especially in a hybrid cloud environment where there are unique compliance challenges across heterogeneous environments. Therefore, in order to meet and maintain compliance in a hybrid cloud environment, it is essential to have visibility and reporting into both the cloud and on-premises systems.

Hybrid Cloud Security:

Areas of focus and capabilities

For a more detailed look at what's needed to make sure you're safe and secure on both your cloud and on-premises environments, the wheel graphic organizes the 10 areas of focus and capabilities for establishing a comprehensive security framework.



Security operations and threat management
Continuous compliance
Visibility and intelligence
Identity and Access Management (IAM)
Cloud Network security
Automation
Secure DevOps
Data protection
Cloud Workload management
Application security

Secure DevOps
It all starts with a focus on Secure DevOps. Line-of-business leaders apply pressure on DevOps teams to deliver value to cloud initiatives at speed and scale. These teams need to be supported by being given security policies and architectures to develop applications and workloads on the cloud with security in mind from the beginning, not as an afterthought. According to 2020 security predictions for hybrid cloud, vulnerabilities in container components are one of the top security concerns for DevOps teams.

Automation
By integrating automated provisioning of security policies, security technologies and vulnerability scanning in your hybrid cloud environments and workloads, you are able to save valuable time and resources otherwise spent on reactive responses to threats.

Security operations and threat management
To be effective with security operations and threat management, it is essential to have central policy management and visibility across both your on-premises and cloud workloads, enabled through a single unified security framework. Your security operations center (SOC) and team will need to continue to detect known and unknown threats, go beyond individual alerts to identify and prioritize potential incidents, and apply AI to accelerate investigation processes.

Continuous compliance
Achieving and maintaining continuous compliance across regulatory and industry mandates is a tough task for most organizations — and especially so for DevOps teams. Your business can get ahead of compliance with AI-based software to stay on top of regulatory trends, dynamic monitoring tools to track compliance risk across your organizations, automation to streamline auditing and reporting, and services to deliver invaluable expertise and insight.

Identity and Access Management (IAM)

Hybrid cloud architectures inherently multiply the places where an attacker might seek valuable data. With security software that can span multiple systems, administrators can apply uniform identity and access policies, view access logs and other records while delivering a seamless user experience.

Data protection

In a hybrid cloud environment, security controls must be consistent across multiple systems so that data is protected against internal and external threats. Protect your data inside or outside your on-premises perimeter — including across multiple clouds.

Application security

The future of applications is cloud-based. To maximize your enterprise-security value, developers need tools that automatically address application security risk and intelligently report vulnerabilities in code before it is put into production. For open-source components, cloud security depends on automated security testing that reviews adopted code.

Cloud workload management

Administrators" time to deal with security issues in a hybrid environment is limited. With constrained resources, they must prioritize. Security software and service solutions that leverage automation to efficiently scan for vulnerabilities and apply policies and security fixes across hybrid cloud ecosystems are ultimately a necessity at scale.

Attackers rely on the inattention and time lag that can plague security administrators. Effectively securing hybrid cloud systems requires an emphasis on consolidated, up-to-date views of logs and other security data so IT staffers and security analysts can quickly spot anomalies and react to them with a consistent approach for each CSP.

Visibility and intelligence

Hybrid cloud environments can be diverse and complex. Therefore, it is essential to have visibility into threats and vulnerabilities within your organization, so that any security incidents are responded to quickly and accurately.

Cloud network security

Because cloud systems may be challenging, securing them requires flexibility, speed, automation, and alignment with on-premises systems. An ideal system should ensure that applications work securely across multiple CSPs' cloud environments and on-premises systems.

Hybrid cloud security solutions from LRS IT Solutions

No matter where you are on the cloud spectrum, products and services from LRS can help address all areas of focus and capabilities for a comprehensive hybrid cloud security framework.

- **Assessments - Cloud Maturity, Cloud Strategy Design/Validation**
- **Roadmaps - Prescriptive, Multi-stage, Aligned to your business Objectives**
- **Migration - Data Migration, Cloud enablement, Cloud PoC/PoT**
- **Backup & Recovery**
- **Disaster Recovery**
- **Secure DevOps**
- **Security operations and threat management**
- **Identity and Access Management (IAM)**
- **Application security**
- **Visibility and intelligence**
- **Cloud network security**

LRS® SECURITY SOLUTIONS

IBM Platinum Business Partner

To learn more about our offerings, visit www.lrsitsolutions.com or call (217) 793-3800 and schedule a consultation with an expert from the **LRS® Team.**