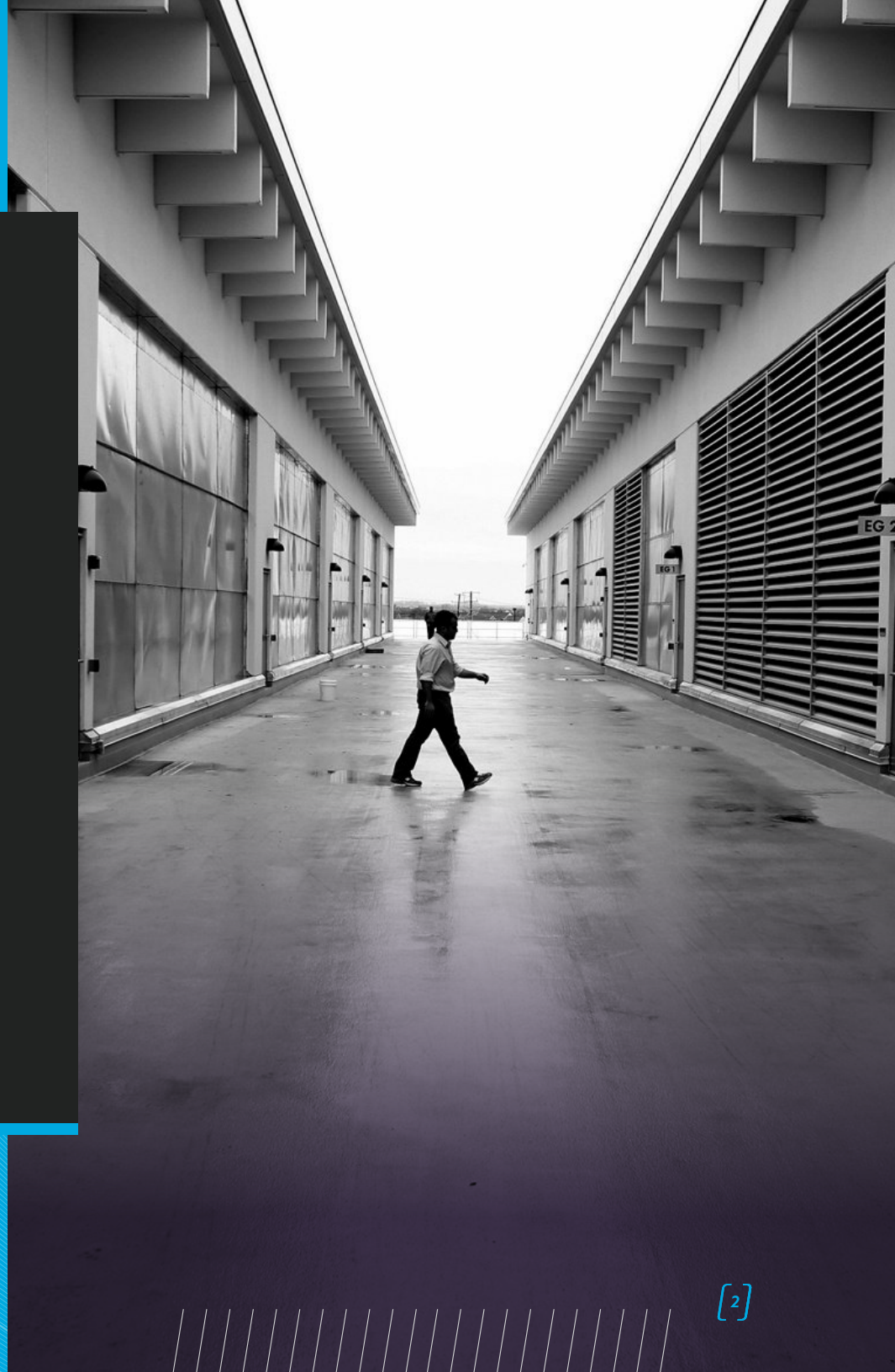
Why Companies Consider Leaving Public Cloud

SUMMIT

In recent years, cloud computing has been hailed as the ultimate solution for scalability, flexibility, and cost-efficiency. However, as the landscape matures, a growing number of organizations are reconsidering their cloud strategies and exploring cloud repatriation — the process of moving certain cloud workloads to on-premises infrastructure or colocation facilities.



Why Companies Consider Leaving Public Cloud

Cost Management

While the cloud offers dynamic scalability, the costs associated with data transfer, storage, and compute can spiral out of control if not managed effectively. Predictable, fixed costs of on-premises infrastructure can offer better financial control.

Performance and Latency

Applications requiring low latency or high throughput can suffer from performance issues in a cloud environment, especially when data is geographically dispersed. On-premises solutions can provide faster, more consistent performance due to physical proximity.

Security and Compliance

Some industries face stringent regulatory requirements that are more easily managed within a high-visibility data center environment. Additionally, concerns over data sovereignty and transparency drive the need to keep sensitive data on-premises.

Customization and Control

On-premises infrastructure allows for greater customization and control over the hardware and software stack, which is crucial for specialized workloads that require specific configurations.

Strategic Long-Term Planning

For some organizations, the cloud was a stepping stone towards modernization, but the long-term strategy may involve leveraging existing on-premises investments and expertise, leading to a hybrid or fully on-premises approach.

The Reality Check: Cloud Repatriation is Complex and Requires Careful Planning

Despite its allure, cloud repatriation is not a straightforward process.
It involves multiple complex steps and considerations:

1

Data Migration

Transferring large volumes of data back on-premises is logistically challenging and requires careful planning to ensure data integrity and minimal downtime.

2

Infrastructure Readiness

On-premises infrastructure must be assessed and potentially upgraded to handle repatriated workloads. This includes ensuring sufficient capacity and resilience.

3

Application Refactoring

Cloud-native applications may need significant modifications to run efficiently on-premises. This process can be resource-intensive and time-consuming.

4

Security Overhaul

Security practices in the cloud differ from those on-premises. Repatriation requires rebuilding security frameworks to protect against new threat vectors and ensure compliance.

5

Operational Expertise

On-premises management requires a different skill set compared to cloud operations. Organizations need to ensure their teams possess the necessary expertise or partner with managed service providers.

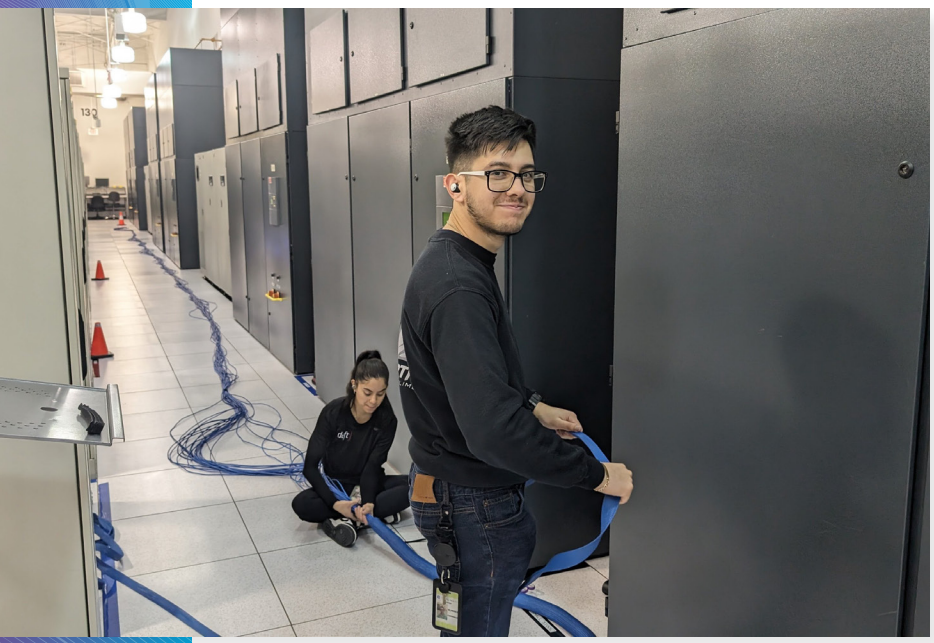
Common Misconceptions about Cloud Repatriation

FORRESTER REPORT

Almost seven out of 10 IT leaders are experiencing difficulties creating transparencyabout their cloud costs with main problem areas being data management and fees for data imports and exports. The effort required to develop and operate integration scenarios is also difficult to calculate and track.[1]

MYTH 1

The Cloud is Always to Blame for High Costs



REALITY

Poor migration strategies and management are often the culprits.

High costs in the cloud are often attributed to the cloud itself, but the reality is that ineffective migration strategies and management practices are usually at fault. Common pitfalls include:

1. **Lift-and-Shift Migrations:** Moving applications to the cloud without modification can lead to inefficiencies and higher costs due to lack of optimization for the cloud environment.
2. **Lack of Governance:** Without proper governance, cloud resources can be mismanaged, leading to wasted resources and inflated costs.
3. **Underutilization of Cloud Features:** Failure to leverage cloud-native features such as auto-scaling and reserved instances can result in suboptimal performance and higher expenses.

1. A Forrester Consulting Thought Leadership Paper Commissioned by BOOMI, February 2024

MYTH 2

On-Premises is Inherently More Secure

REALITY

Security depends on proper setup, maintenance, and expertise.

While owning hardware might seem to offer greater control and security, the reality is that security is determined by how well the environment is managed. Key considerations include:

1. **Configuration Errors:** Both cloud and on-premises environments are vulnerable to misconfigurations, which can lead to security breaches.
2. **Expertise Requirements:** Ensuring robust security requires skilled personnel who are knowledgeable in the latest security practices and technologies.
3. **Physical Security:** On-premises data centers require strong physical security measures, which can be costly and complex to implement.
4. **Regular Updates and Patching:** Timely updates and patching are crucial for maintaining security. In an on-premises environment, this responsibility falls entirely on the organization.

FORRESTER REPORT

About 40% of respondents complained they weren't able to establish effective cost governance within their cloud architectures, so they were essentially unable to get to grips with the causes of money being wasted in the cloud.[1]

MYTH 3

Public Cloud Providers Offer Superior Support

REALITY

Some data center providers can be equally unresponsive.

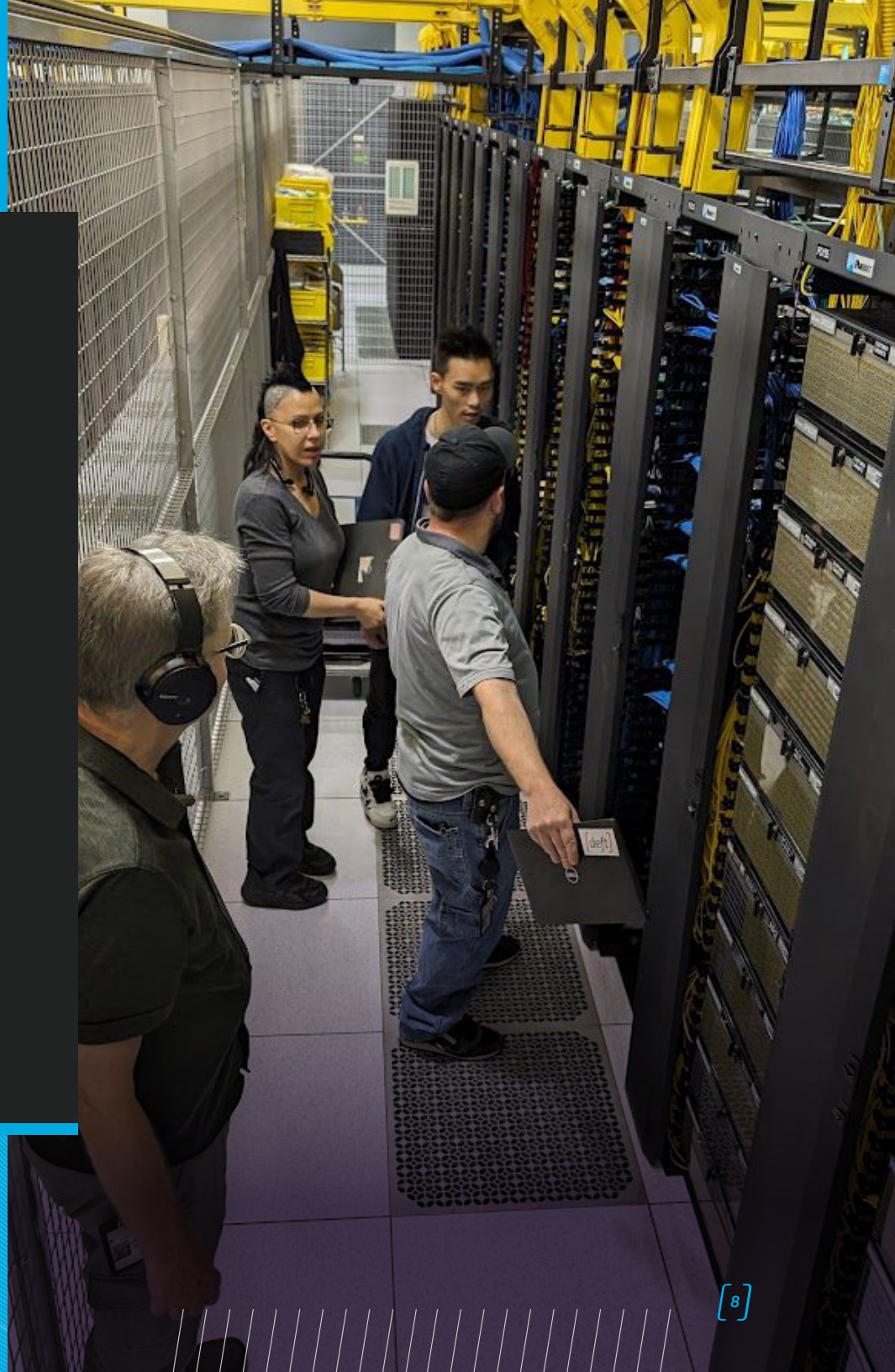
There is a common belief that public cloud providers offer superior support due to their scale and resources. However, the support experience can vary:

1. **Scalability Issues:** Large cloud providers often have standardized support processes that can be impersonal and slow, particularly for smaller customers.
2. **Tiered Support Models:** Accessing expert support often requires navigating multiple tiers of customer service, leading to delays in resolving critical issues.
3. **Boutique Providers:** Smaller, boutique data center providers may offer more personalized and responsive support. These providers can often resolve issues more swiftly and tailor their services to meet specific customer needs.

1. A Forrester Consulting Thought Leadership Paper Commissioned by BOOMI, February 2024

Technical Challenges of Cloud Repatriation

Cloud repatriation involves several technical hurdles, including replicating cloud configurations on-premises, securely transferring data, re-architecting applications, and implementing robust security measures. Each step requires careful planning and precise execution to ensure a smooth transition and maintain operational performance.



Rebuilding Infrastructure: Replicating Cloud Configurations On-Premises

Repatriating workloads necessitates replicating the sophisticated configurations of a cloud environment within an on-premises infrastructure. Key challenges include:

1. **Resource Allocation:** Cloud environments dynamically allocate resources based on demand, while on-premises infrastructure requires careful capacity planning.

2. **Network Architecture:** Replicating cloud networking capabilities, such as virtual private clouds (VPCs) and global load balancing, requires robust networking hardware and expertise.

3. **Service Integration:** Integrating services on-premises often involves selecting and configuring compatible hardware and software solutions.

Data Repatriation: Securely Transferring Data from the Cloud

Securely transferring data from the cloud involves logistical and security challenges:

1. **Data Volume and Bandwidth:** Moving large volumes of data can strain network bandwidth and take considerable time.
2. **Data Integrity:** Ensuring data integrity during transfer is crucial, requiring robust verification processes.
3. **Minimizing Downtime:** Data migrations should be planned to minimize operational downtime.

Application Re-Architecting: Adapting Applications for On-Premises Environments

Cloud-native applications often require significant modifications to function efficiently on-premises:

1. **Dependency Management:** Identifying and replacing dependencies on cloud services with on-premises solutions.
2. **Scalability and Performance:** Adjusting applications optimized for cloud scalability to perform efficiently in a fixed-capacity on-premises environment.
3. **Configuration and Deployment:** Replicating streamlined cloud deployment processes on-premises.

Security Configurations: Implementing In-House Security Measures

Repatriation requires rebuilding security configurations from scratch:

1. **Access Control:** Implementing robust access control mechanisms.
2. **Network Security:** Establishing perimeter defenses like firewalls and intrusion detection systems.
3. **Data Encryption:** Ensuring strong encryption for data at rest and in transit.
4. **Compliance:** Adhering to regulatory requirements through regular audits and best practices.

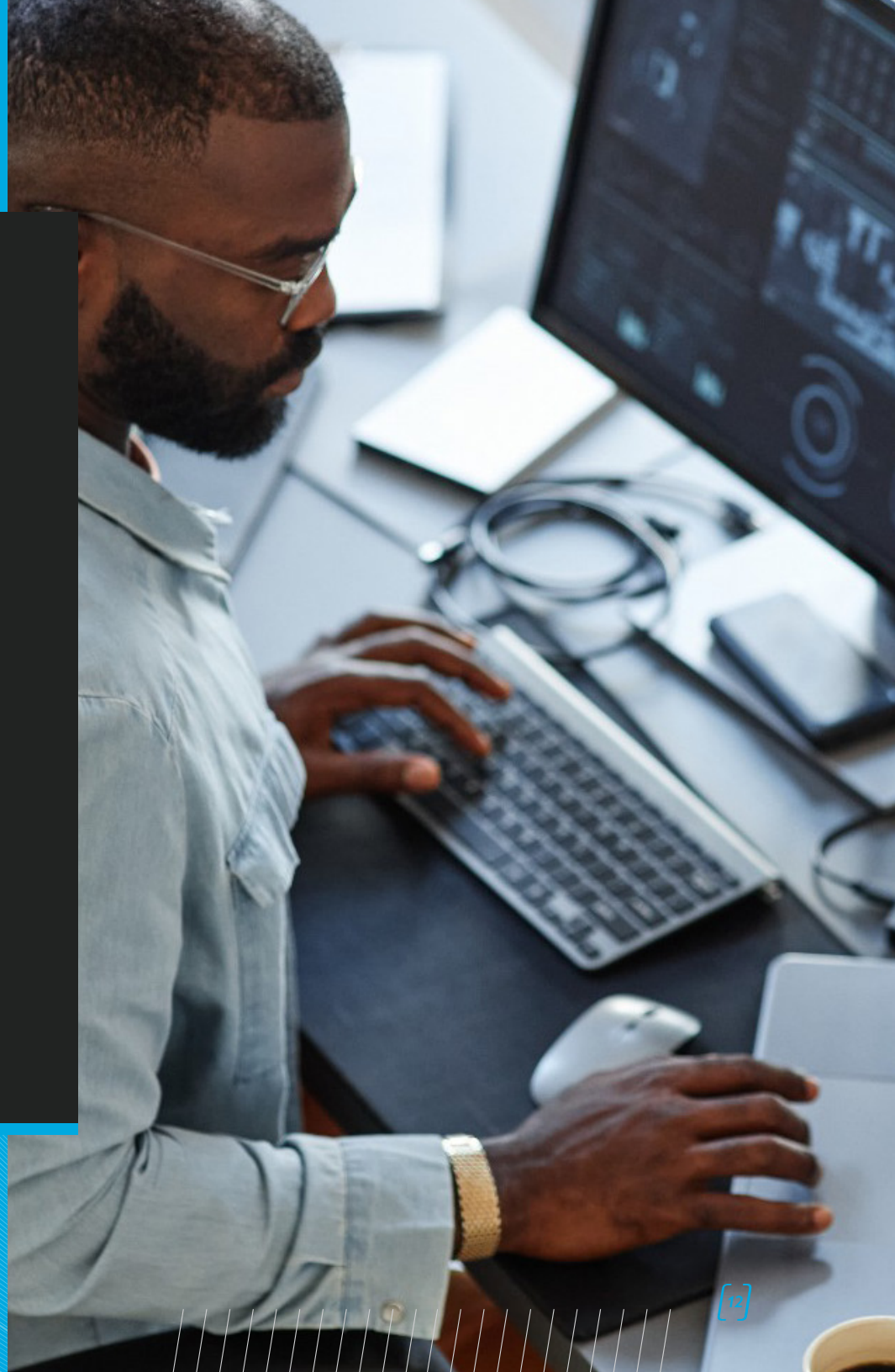
Backup Strategy: Redesigning Backup for On-Premises

On-premises environments necessitate a redesigned backup strategy:

1. **Backup Infrastructure:** Investing in backup hardware, such as storage systems and tape drives.
2. **Backup Software:** Selecting and configuring software that supports the organization's data protection requirements.
3. **Frequency and Retention:** Defining backup schedules and retention policies.
4. **Disaster Recovery:** Developing and testing comprehensive disaster recovery plans.

Best Practices for Successful Cloud Repatriation

Successful cloud repatriation relies on best practices such as thorough planning, engaging expert consultants, considering managed migration services, and ensuring ongoing post-migration support. These strategies help mitigate risks and ensure a smooth, efficient transition back to on-premises infrastructure.



Thorough Planning: Mapping Out the Migration Process in Detail

Successful repatriation requires meticulous planning:

1. **Assessment:** Conducting a thorough assessment of current cloud usage and requirements.
2. **Roadmap:** Developing a detailed roadmap outlining each step of the migration process.
3. **Timeline:** Establishing a realistic timeline with milestones and checkpoints.

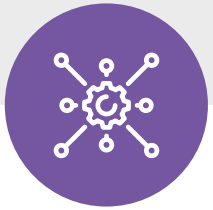
37SIGNALS RESULTS

37signals left the cloud for Summit. Now, they save over $1 mil/year.

Expert Guidance: Engaging Consultants Experienced in Cloud Repatriation

Consultants with cloud repatriation experience can provide valuable insights:

1. **Assessment and Strategy:** Helping assess current infrastructure and develop a repatriation strategy.
2. **Implementation:** Assisting with the technical aspects of migration and infrastructure setup.
3. **Optimization:** Offering post-migration support to optimize on-premises operations.



Managed Migration: Consider Outsourcing the Migration for a Smoother Transition

Outsourcing the migration can mitigate risks and ensure a smoother transition:

1. **Managed Service Providers:** Engaging providers that specialize in cloud repatriation.
2. **Turnkey Solutions:** Considering turnkey migration solutions that handle all aspects of the process.
3. **Ongoing Management:** Ensuring ongoing management and support post-migration.

Post-Migration Support: Ongoing Maintenance and Optimization of On-Premises Infrastructure

Post-migration, continuous support and optimization are essential:

1. **Regular Maintenance:** Implementing regular maintenance schedules to ensure infrastructure health.
2. **Performance Monitoring:** Continuously monitoring performance and making necessary adjustments.
3. **Security Updates:** Keeping security measures up-to-date to protect against emerging threats.

Feeling like the public cloud isn't the perfect fit anymore?

Cloud repatriation can be a great option, but it's important to plan it out well. At Summit, we've been managing complex IT systems for over 24 years, so we know the ins and outs of this process.

Here's how we can help:

Smooth transition
We'll guide you through the whole process, making sure everything that should live on-prem makes it there smoothly.

Expert help
Need a hand? Our engineers are available 24/7 by phone or Slack to answer any questions. We even have a 15-minute support ticket response time SLA.

Flexible options
We can mix and match Summit's shared/private VMware Cloud, third-party clouds, managed services, and colocation gear to create the perfect hybrid solution.

Reliable infrastructure
Our facilities are top-notch with 100% uptime on network and power.

Cost-effective solutions
We're all about finding the most efficient and budget-friendly way to get you back on track.

We're your repatriation dream team! Let's chat and see if bringing things back on-premises is the right move for you.

summithosting.com

SUMMIT