Optimizing the Cloud

The 5 Tenets of Continuous Improvement

TABLE OF CONTENTS

Overview

The 5 Tenets of Continuous Improvement

For enterprise business, the question of the cloud is no longer when to make the move, but instead how to implement it exceptionally. As explained in the 2019 Gartner Hype-Scale Report, "the focus has shifted from the unrealistic promises that cloud will transform everything and the pessimistic view that it didn't deliver, to a pragmatic approach that views cloud as inevitable."

Put quite simply: "The focus is now on how to do it well versus on whether to do it at all."

The cloud may be the next undeniable step to be future-ready, yet a simple "lift and shift" does all any company to unlock its full potential. With cloud adoption always rising and more complex strategies being applied, optimization is the key for sustainable success in the cloud.

For many, digital transformation has already brought business to the cloud.

94% of respondents of a recent survey from RightScale report using the cloud with 84% of enterprises using a multi-cloud approach.[1]

With significant portions of enterprise workloads running in the cloud, central IT teams face the expanding needs and concerns of cloud management. Optimizing costs ranks as the highest priority, but is also directly connected to the other top tenets for cloud optimization:

To reach the optimal business agility for today's competitive enterprise, organizations must do more than cut costs. Continuous improvements over each of the tenets is necessary to be secure, compliant, agile, and effective in the industry.
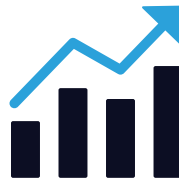
Digital transformation is not complete by simply moving to the cloud. Through strategic optimization, businesses can tackle the mounting challenges and harness what the cloud truly has to offer.

Security   **Availability**   **Performance**

84%

of enterprises
use a multi-cloud
approach[1]

Cost   **Risk**

Security

As opportunities within the cloud landscape grow, so do the number of vulnerabilities. The Cloud Security Alliance (CSA) defines the top 11 cloud security threats as follows:[2]

1. Data breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and
5. key management
6. Account hijacking
7. Malicious insiders
8. Insecure interfaces and APIs
9. Weak control plane
10. Metastructure and applistructure failures
11. Limited cloud usage visibility
12. Abuse and nefarious use of cloud services

When reviewing this daunting list, it comes as no surprise that 91% of businesses are concerned about cloud security.[3] From data breaches to account hijacking to insufficient access management internally, enterprise IT teams can quickly find themselves struggling to stay on top of such a broad range of security threats.
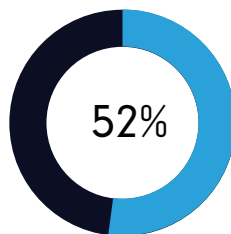
While outsider threats make big headlines, internal issues are also causing major headaches:[3]
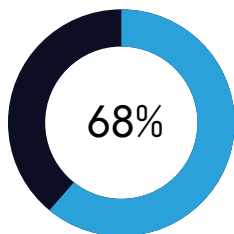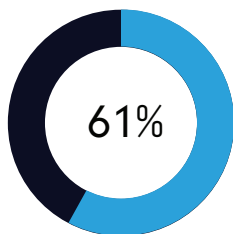
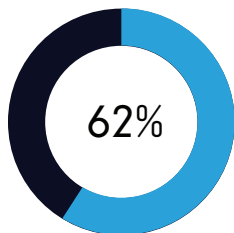| 68%	61%	52%
Data Loss/Leakage	Data Privacy	Confidentiality

91%

of businesses are concerned about cloud security[3]

Public cloud users have even more specific security concerns:[3]

62%	55%	52%
Misconfiguration of the AWS cloud platform	Misuse of employee credentials and improper access controls	Insecure interfaces/APIs
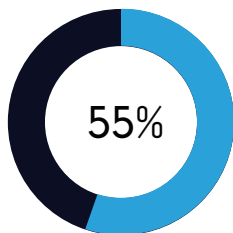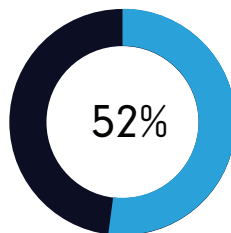
Compliance standards compound the internal security issues.

Over half of the report's respondents are challenged to monitor complex and frequently updated policies, and to pass audits and risk assessments. While all compliance measures are put in place to protect sensitive data, fulfilling the requirements strains internal IT, driving 69% of enterprise executives to consider hiring an outside technology firm for compliance support.[4]

Security is a constantly evolving component to cloud optimization and one that organizations can't afford to lag in. Optimizing without cutting corners on protection is a finely tuned skill that requires expert attention, yet only 50% of organizations are satisfied with their cloud security vendor.[3]

Optimize and strategize for stronger security.

With constantly updated policies and evolving best practices, companies can easily lose track of the necessary changes and fall prey to preventable risk with weak access management, encryption standards, and governance.

Filling the gaps for better cloud security requires detailed knowledge of all the ins and outs of an organization's systems and infrastructure—sometimes an overwhelming feat even for internal teams as they are often tasked with a multitude of additional responsibilities. Through close collaboration with cybersecurity experts, enterprise IT teams can hand off the painstaking details of data protection policies and procedures to cloud partners, not just for immediate protection but for long term safety and compliance.

Availability

The availability of workloads is extremely important when it comes to keeping your business up and running. While it is critical for enterprises in the cloud, not all cloud providers are upfront about the amount of downtime and availability an organization can expect with their service. Even the most well-researched cloud provider can prove undependable for mission-critical uptime and end up costing businesses.
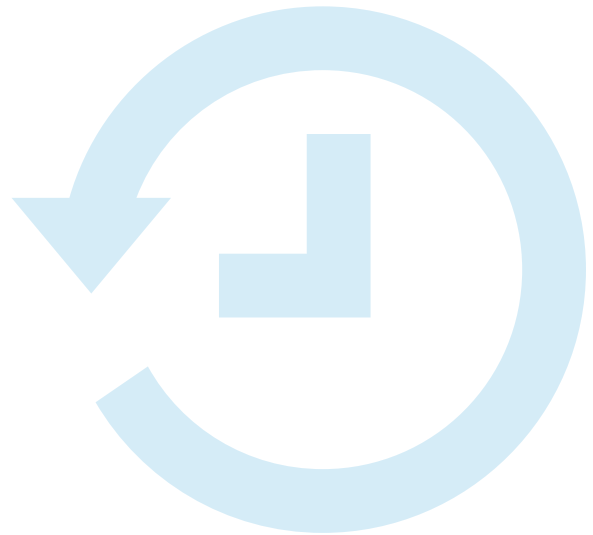
In fact, companies reporting frequent outages and brownouts experience up to 16x higher costs than companies with fewer instances of downtime.[5]

The real numbers behind 100% are less than comforting.

A common misconception with cloud providers revolves around the correlation between service level agreements (SLAs) and downtime.

While details in a provider's SLA may go so far as to claim 100% uptime, it only means the provider will reimburse the organization when downtime occurs—a much different expectation of availability than the SLA conveys.[6]

Dubious SLAs leave organizations vulnerable to unexpected downtime with costly consequences, even requiring some businesses to brace for inconsistent availability by expanding internal IT departments. Companies that report frequent downtime on average require nearly twice the number of team members to troubleshoot problems.[5]

69%
of enterprises have considered hiring an outside partner for compliance support[4]

50%
of organizations are dissatisfied with their cloud security vendor[3]

16x
higher costs for companies with frequent outages[5]

High availability requires a step up from SLAs.

Ensuring high availability demands a more proactive approach from cloud service providers and chosen technology partners. Better commitments beyond SLAs are needed to monitor, mediate, and optimize for availability. Maintaining availability beyond the status quo is possible with the right level of guidance.

Performance

The overall performance of an organization's chosen cloud platform is another major tenant in optimization. While customers and partners rely on businesses to consistently deliver at today's lightning-fast pace, each company's performance hangs on their cloud provider.

Performance hinges on cloud reliability. Even for today's titans of industry, finding continuous, highly available services with predictable costs is a challenge when vetting cloud providers.

The biggest cloud providers still suffer big missteps.

Azure admittedly struggled between 2018 and 2019 with CTO Mark Russinovich citing "three unique and significant incidents that impacted customers during this time period," but assured that Microsoft is taking steps to address it.[7] Despite his confidence, Gartner Research VP Sid Nag still believes Azure reliability "is becoming a major issue" due to the recent "outages with their networking and another issue related to the availability of [Azure] Active Directory which they rely on for their cloud services to work."[9]

Even the "most reliable in the business," Google cloud services has met scrutiny over their claims for superior uptime over Azure and AWS. Depending on the source, Google wins the performance title with only 208 minutes downtime in 2018, while AWS was down for 312 minutes within the same timeframe—statistics Google claims are from "two leading third-party research firms." However, research from Gartner shows that AWS is reliable 99.9987% of the time, taking the title of most reliable being available. The same research has Google trailing with an uptime score of 99.9982%.

Poor performance and downtime have real consequences for business.

Making strides to optimize performance requires a company to look back. Using specialized tools and in-depth knowledge of industry best practices, organizations can map usage and issues over time to create a holistic picture of what works and, more importantly, what happens when their strategy doesn't work. By consistently examining and reexamining performance over time, organizations can predict potential issues and continuously adjust to improve reliability. Dedication to this practice can save businesses undue costs and headaches, as well as their reputations.

2x
the team members are needed to troubleshoot issues for companies with frequent downtime[5]

Cost

While each of the five tenets have a crucial role in cloud optimization, controlling costs is at the top of almost every enterprises priority list. From the Rightscale 2019 State of the Cloud Report, 68% of respondents cited managing and optimizing cloud services costs as the top responsibility for central IT teams.[1] Yet, managing, much less optimizing, costs is an overwhelming task, leading cloud users to underestimate their wasted cloud spend.

Customers could not overlook the outrageous overcharges from an invoice error.

Billing from cloud providers is notoriously complex, yet an unfortunate sect of AWS customers reported double to triple their normal charges from a billing error in September 2019. Affected customers took to Twitter expressing surprise and outrage as Amazon scrambled to rectify the situation, with one customer even pointing out that his company was charged for services that accumulated to more than 950 hours in one month.[9]

> **"I can go back and see my instances run for 744 hours (what I'd expect in a month) in previous months," the customer tweeted. "Amazon invented more hours than actually exist in a month for billing purposes."**

Amazon refunded the overcharges, granting relief to customers who just "couldn't figure it out" when they saw triple their normal charges, but it doesn't take an egregious error to leave cloud customers puzzled.

A reputation for baffling billing.

AWS isn't the only public cloud service to deliver confusing bills. Microsoft's Azure billing is also famous for its lack of simplicity. Charges become muddled between AWS's 500,000 SKUs and Azure's unnecessarily messy spreadsheets. Depending on whether the customer is viewing their PDF invoices versus their CSV-file detailed usage data reports, Azure users will be presented with different terminology for the same line item, making cost versus usage comparisons confounding.

Between different formats and billing breakdowns, actual resource usage can quickly get lost, begging the question: How can you control your costs if you can't understand how you accrued them in the first place? On average for 2019, organizations estimate waste at 27%, but actual measured waste comes in at 35%.[1]

Companies can cut costs without cutting corners.

Although potential waste may be accumulating around every corner, companies have just as many opportunities to optimize. While erroneously billing may inflate invoices, so does over-allocation of resources can add equally unnecessary amounts to an enterprise's bill. Right-sizing instances and setting more appropriate power schedules allow for more cost-effective infrastructures.[10]

Just like measures to improve performance, dedicating time to thoroughly analyze usage every month is a core component of long-term cost optimization. Yet understanding where exactly overspending occurs on an invoice or where workloads can be streamlined can still be baffling for internal teams. Organizations can greatly benefit from a partner with experienced cloud experts to decipher bills and provide insights for long-term savings.
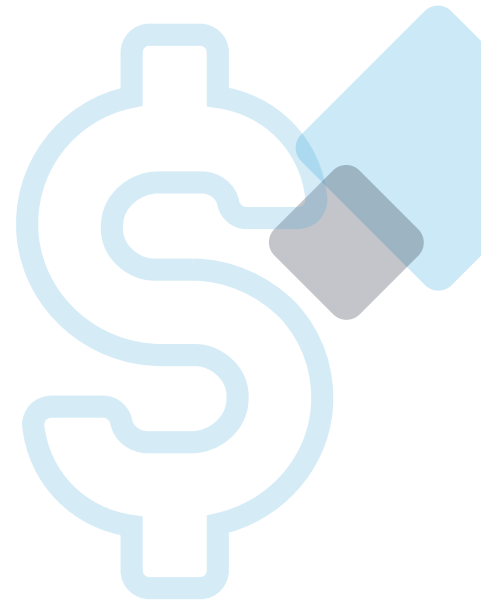
68%
of businesses report cloud service costs as a top responsibility for central IT teams[1]

950
hours erroneously billed in one month[9]

500k
SKUs in AWS's billing spreadsheets

35%
of IT spend is wasted[1]

Risk

Availability, performance, security, cost—all of these cornerstone tenets involve various forms of risk. Risk can manifest dire consequences from inaction and equally spur hesitation to try new technologies or strategies. While risk may be a common excuse for organizations to avoid challenging the status quo, optimization is the key to mitigating risk in each of these areas.

The risk of downtime costs more than dollars and cents—but it costs a lot of that too.

Often, the first risk associated with inconsistent availability is the impact that it will have on revenue. According to Gartner, the average cost of IT downtime is $5,600 per minute.[11] But thi is merely the tip of the risk iceberg when it comes to availability: lost productivity with employees scrambling to troubleshoot, compliance failure, and damage to company reputation.

Reputation damage is tied directly to performance.

Outages and faltering service can hit a company's image hard, especially with slow updates during the incident, and customers make sure their frustration over disruptions are heard loud and clear. For instance, when telecommunications enterprise Mitel Networks experienced an outage in 2019, the company faced a chorus of outrage:[12]

- "No phones, intermittent network outages. Lost a whole day's work, and it still not resolved with NO ETA!"
- "No amount of credit on my bill will make up for the business I lost today."
- "Mitel site doesn't show any outages. We are looking to leave Mitel in the next 12 months."

No business wants to be seen as unreliable and suffer the cost of damage control.

Running the risk of never recovering.

Risks to security are seen at every level of business IT, from insufficient employee passwords to malicious cyberattacks. But the deep reaching implications of these risks can be enough to shutter a business' doors for good.[13]

The global average cost of a breach in 2019 was $3.92 million, a 1.5 % increase from 2018, with the time it takes for an organization to identify and contain a breach lasting up to 279 days.[14] Downtime, reputation damage, revenue loss—all of these risks connect back to security.

Wasted cloud spend is a silent—and terribly common—killer for enterprise business.

Waste often goes unnoticed, making it one of the most dangerous risks to a company. Resources billed by the hour often run idly while not in use and will be invoiced regardless of efficiency. Oversized infrastructures run just as high a risk of bloating billing—a recent survey found 40% of instances were at least one size larger than needed for their workloads.[15] Between idle and oversized resources, wasted cloud spend is predicted to exceed $14.1 billion in 2019.[16]

Risk permeates across all four of the other tenets and paralyzes an enterprise from becoming a future-ready business. But through optimization, companies can reduce risk and manage IT costs to increase their agility in the market.

$5.6K
Cost of IT downtime per minute[11]

$3M
The global average cost of a data breach in 2019[14]

40%
of instances are at least one size larger than needed[15]

$14B
of cloud spend was expected to be wasted in 2019[16]

Successfully Covering All Five Tenets

Migrating to the cloud is a mandatory step for the enterprise business to stay competitive, but digital transformation cannot stop there if an organization intends to stay ahead of the pack. True optimization requires careful exploration of the five tenets explored throughout this eBook: Security, Availability, Performance, Cost, and Risk.

Cloud optimization is much more than products or deliverables in a service package. It is a unique strategy for each individual organization, requiring a partner that thoroughly understands current states and desired business outcomes. Digital transformations don't happen overnight, and optimization can't occur using only a single product or by signing up for a siloed service. Comprehensive guidance on the united tenets is needed for continuous improvement.

While most cloud service providers can offer support at a tertiary level, evidence shows that the basic Service Level Agreement misses the mark. To achieve true optimization, service agreements must turn providers into client advocates, and providers must take a forward-thinking approach.

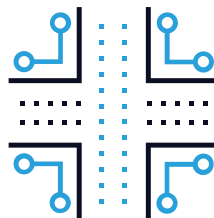## Proactive optimization with Guidance Level Agreements.

Ntirety offers the industry's first and only Guidance Level Agreements (GLAs), offering enterprise organizations real direction and better opportunities to reduce risk, optimize IT spend, and improve business agility. While SLAs are the basic requirements a service provider should offer, GLAs are the difference makers for companies ready to take the next step:

| Contractually committed | Aligned and accountable to business outcomes | Covers all your hybrid and multi-cloud infrastructure | Reports on a monthly basis |

Analyze and predict performance requirements to design more cost-effective and reliable environments.

Ntirety's cloud experts utilize the latest tools and follow industry best practices to create secure, highly available environments—all with a proactive perspective on all elements. From overspending to being under-provisioned, Ntirety reviews and analyzes to right-size instances and resolve the most common challenges, including unclear costs, wasted IT spend, and fickle availability. GLAs even go so far as to predict future needs for reliable performance with anticipated costs included.

Increase security and reduce risk with better management of your entire infrastructure.

Using Monitoring Insights™, Ntirety delivers a better grasp on infrastructure needs and how to manage—even forecast. Identifying risks and vulnerabilities for a right—sized environment makes it easier to incorporate the right products and services needed to

protect systems and data. Cloud security and all the risks involved touch every tenant, making its optimization an overall boost to your organization's confidence.

Balance your IT ecosystem for cloud optimization.

Security, Availability, Performance, Cost, and Risk—optimizing each of these components is directly connected to the progression of the others. For enterprise organizations trying to achieve an agile, future-ready outlook, utilizing the guidance and expertise of trusted cloud service providers takes the burden off internal IT teams and present real direction to achieve these goals. Ntirety's Guidance Level Agreements provides enterprises with a true commitment to consistently deliver expert recommendations to reduce risk, better manage costs, and create a more proactive and competitive business.

▶ Is your enterprise prepared for the opportunities—and threats—that are possible?
Schedule a consultation by visiting ntirety.com/getstarted today.

Sources:

1. RightScale 2019 State of the Cloud Report
2. CSO Online, 2019.
3. 2019 AWS Cloud Security Report
4. PWC Pulse Survey, 2017.
5. Logic Monitor IT Outage Impact Study
6. Networld World, 2019.
7. Microsoft Azure, 2019.
8. The Register, 2019.
9. CRN, 2019.
10. Embotics Cloud Cost Optimization, 2017.
11. Gartner, 2014
12. Downdector, 2019.
13. TechRepublic, 2017
14. SecurityIntelligence, 2019.
15. RightScale 2017 State of the Cloud Report
16. ParkMyCloud, 2019