ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™

The complexities of the secure DIY cloud

BALANCING COST, COMPLIANCE & OPTIMIZATION

So you're considering a DIY cloud?

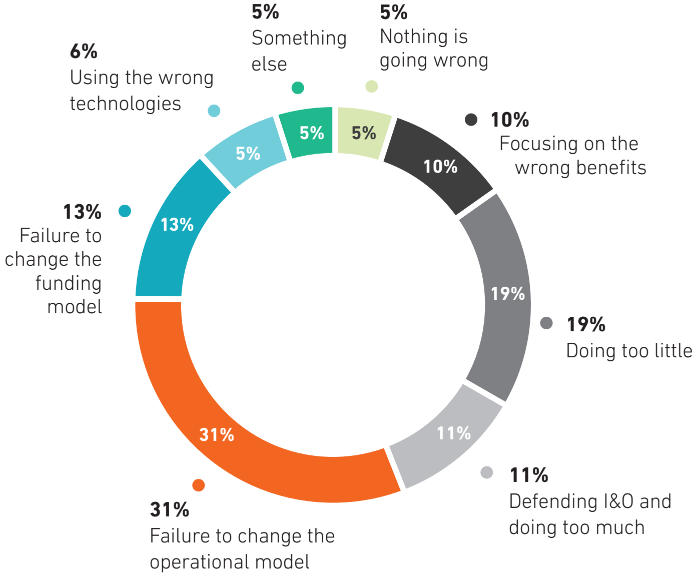
Cloud computing has become a necessary component of IT services across many organizations. For businesses that prefer to maintain complete control over their infrastructure and IT environments, private cloud solutions can be built to a company's precise needs.

Private and do-it-yourself clouds have the potential to add considerable value to the organizations adopting them, but they also present challenges from implementation and management perspectives — particularly when they need to be secure.

As a result of security missteps and other issues, many of these deployments fail to meet organizations' expectations. In fact, according to Gartner analyst Tom Bittman, 95 percent of private clouds will fail to deliver across at least one key metric.

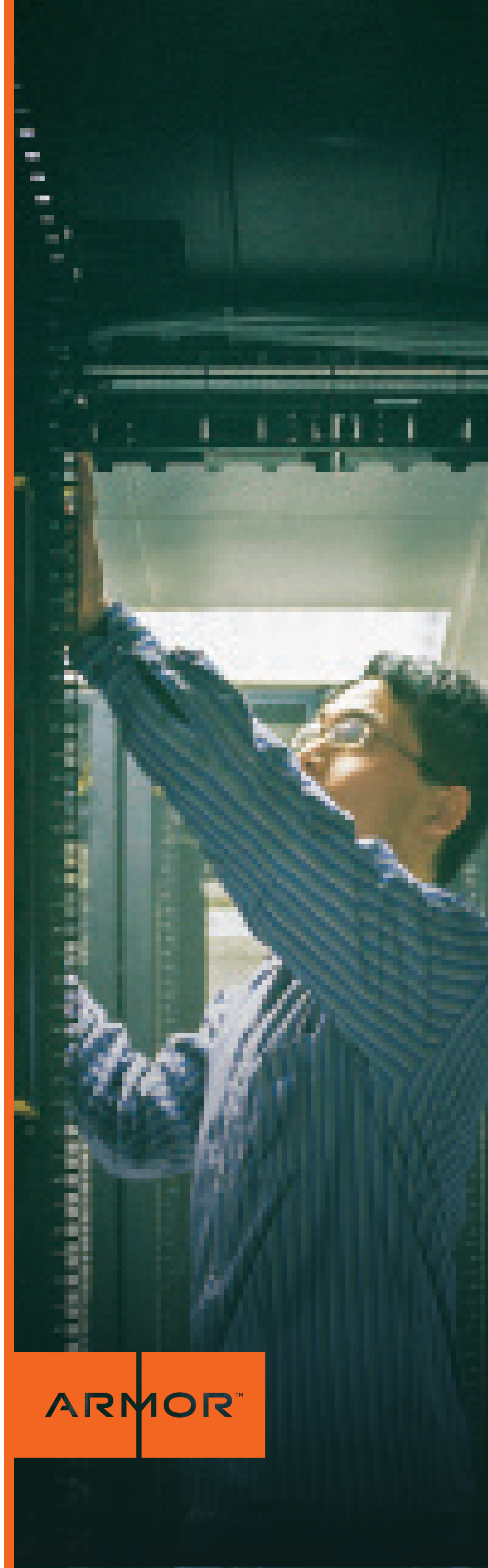
As organizations evaluate their options for building or procuring secure and managed cloud environments, it is important to first understand the complexity, which often emerges from security, compliance and other related concerns, that they may run into as they deploy new solutions.

What is going wrong with your private cloud?



Polled attendees at Gartner's Datacenter Conference in Las Vegas in December 2014

Source: "Problems Encountered by 95% of Private Clouds"
Tom Bittman, VP Distinguished Analyst, Gartner
February 5, 2015



Setting the stage for the cloud: business objectives

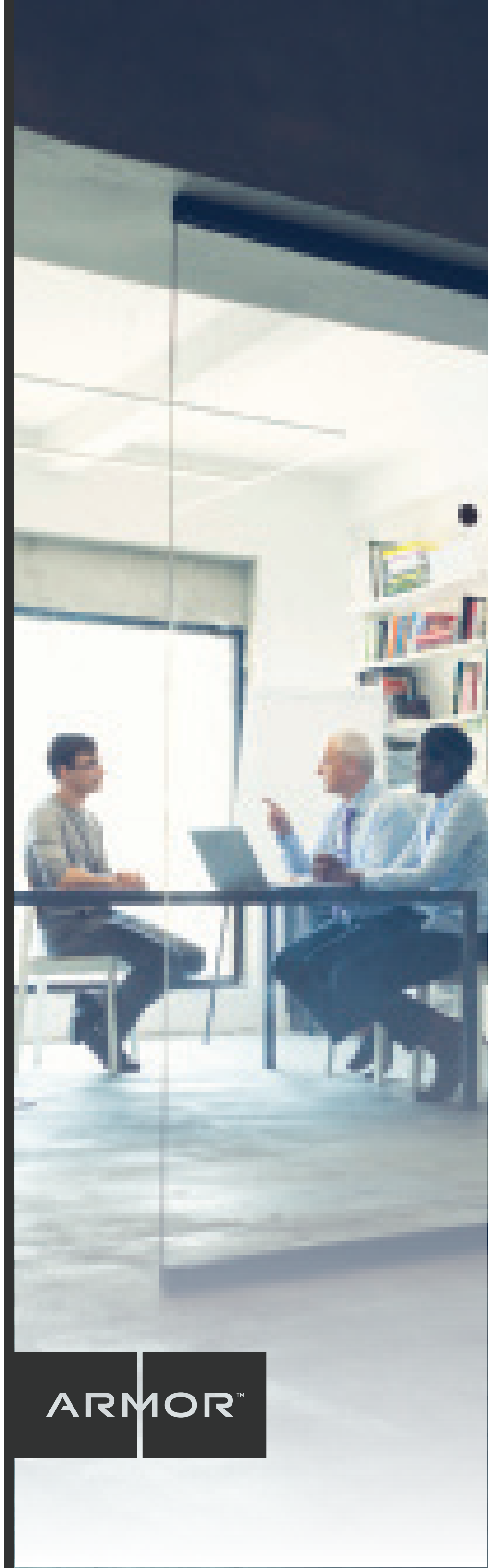
Complexity can emerge from the onset of secure cloud deployments, so the first step to implementing cloud technology is to outline clear objectives for the infrastructure

These will vary by individual use cases, but even goals that are seemingly simple can have multiple layers of complexity, especially when security is not properly considered.

For example, businesses that want to expand the scalability of payment processing would have to also consider how new solutions transfer and store payment data, which then necessitates a further evaluation of compliance (e.g., PCI).

Laying the foundation for a successful secure cloud requires a keen understanding of business objectives, risk management and control, and IT requirements. Otherwise, organizations run the risk of investing in the wrong technologies or coming up short in regard to a key business need like compliance.

> "Complexity can emerge from the onset of secure cloud deployments, so the first step to implementing cloud technology is to outline clear objectives for the infrastructure."



Very few cost calculations are apples-to-apples

One of the first components frequently considered when deciding between building a secure private cloud internally or leveraging a third-party provider is the issue of cost. Traditional cost estimation models for the cloud consider the basic element of shifting IT costs from capital expenditures (CapEx) to operational expenditures (OpEx).

While it is true that leveraging a third-party provider lowers upfront investments, this basic model does not provide a true comparison of the different routes for deploying secure cloud infrastructure.

The DIY cloud is typically considered to be heaviest on the CapEx side of the spectrum. However, maintaining a private cloud environment still produces ongoing expenses in the form of additional power and cooling, plus other costs associated with maintaining on-premises IT infrastructure (e.g., staffing, facilities, physical access control and security).

This issue is further compounded by the fact that it's difficult for many companies to calculate return-on-investment (ROI) for new cloud deployments.

CapEx vs. OpEx for Cloud Infrastructure

Capital expenditures, or CapEx, are purchases of tangible assets like servers and routers. For organizations creating their own private cloud infrastructure, for example, the CapEx would include all costs associated with getting physical equipment procured.

In contrast, operational expenditures, or OpEx, are costs related to keeping that cloud infrastructure up and running. Using the on-premise cloud infrastructure model, the OpEx there would be all of the costs associated with labor and system upkeep. All of the costs associated with third-party cloud infrastructure usage would fall under the OpEx category, not CapEx, since the monthly or annual subscription fee is for the operational maintenance and oversight of outsourced cloud infrastructure.

Increasing pressure from cybersecurity

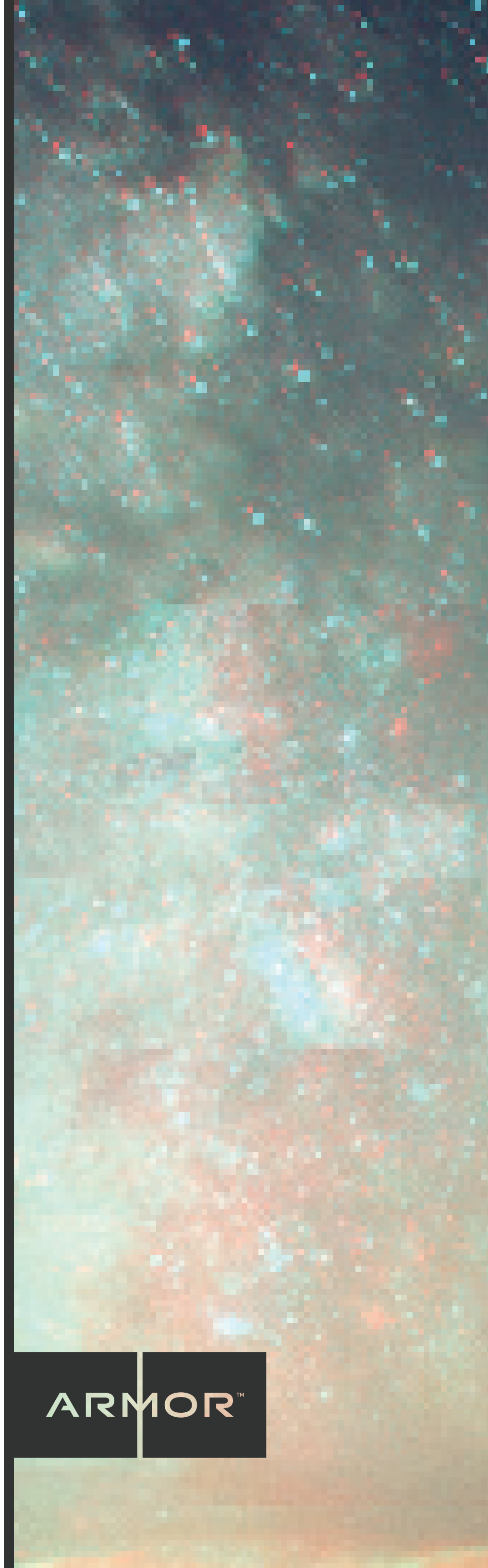
In just the first six months of 2015, close to 246 million records have been stolen or lost, meaning that over 1.3 million records are affected every day. The threat of data breach will never end. It is becoming easier for cybercriminals — even for those who aren't particularly knowledgeable about IT — to develop and distribute malware and hacking tools.

In addition to increasing pressure from a technical perspective, the threat of data breaches is likely to become increasingly prominent in public consciousness.

For context, as Verizon's 2015 Data Breach Investigation report noted, The *New York Times* published more than 700 articles related to data breaches in 2014, compared to fewer than 125 in 2013. This indicates that organizations experiencing data breaches are at a greater risk of reputation damage as well as traditional risks such as regulatory fines, lost sales and reparation.

Verizon also tracked a significant increase in attacks, such as phishing, that target individuals in order to gain access credentials, meaning that every employee could become a target of those looking for sensitive data. According to numbers from APWG, malicious outsiders were the cause of 62 percent of all stolen or lost records from the first half of 2015.

> "Organizations experiencing data breaches are at a greater risk of reputation damage as well as traditional risks such as regulatory fines, lost sales and reparation."



How important is your data?

Data has always been a critical component of successful organizations, but it is important to realize that not all data can be treated the same way — doing so is unnecessarily expensive and likely to leave gaps in a company's cybersecurity strategy.

Especially when migrating data from multiple sources into a cloud environment, classification is a central component to protecting it. This doesn't apply to just corporate data, as additional information sources like healthcare records and customer credit card data also needs consideration.

The data classification process should start with information that is likely to be high risk. For example, reviewing data and assigning attributes based on compliance mandates will help in determining what security safeguards, at minimum, will need to be in place to avoid fines and damaged brand reputation.

A comprehensive strategy also considers information that presents a moderate risk as well as low-risk data. This framework not only saves organizations money, it gives them a better understanding of their data ecosystem.

This understanding is essential for maximizing the value of cloud services, whether utilizing a private DIY cloud platform, managed services or another third-party provider. Organizations will be able to select exactly the right cloud solution for the needs of specific information.

DATA CLASSIFICATION

SEVERE — High-Risk and/or High-Availability Production Workloads

DATA & PERFORMANCE NEEDS

- "Tier 0" applications data with PII that require high-level access
- Data and application security
- Requires compliance with industry (PCI) or regulatory (HIPAA) mandates
- Intellectual property
- High-availability architecture
- Low-latency performance requirements

ELEVATED — QA, Testing, Staging or Production Workloads

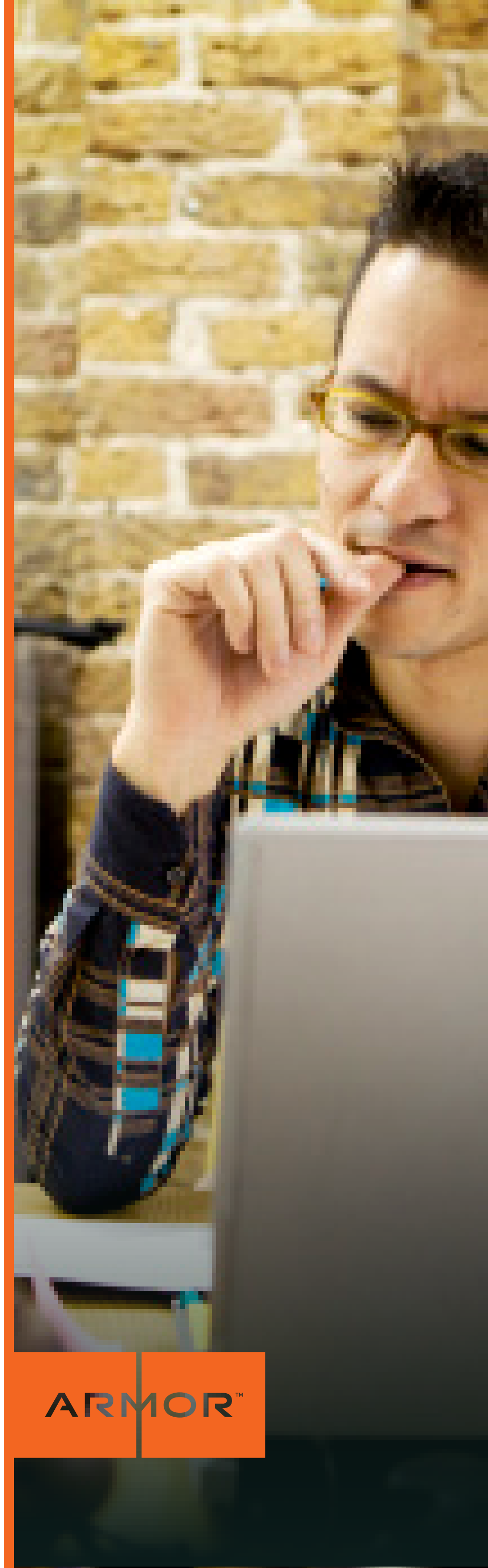
DATA & PERFORMANCE NEEDS

- Non-production data
- No personally identifiable information (PII) or company IP
- Risk-based level of security performance and availability
- Early-stage development

LOW — Public Workloads

DATA & PERFORMANCE NEEDS

- Data that's already publicly available
- Non-sensitive files



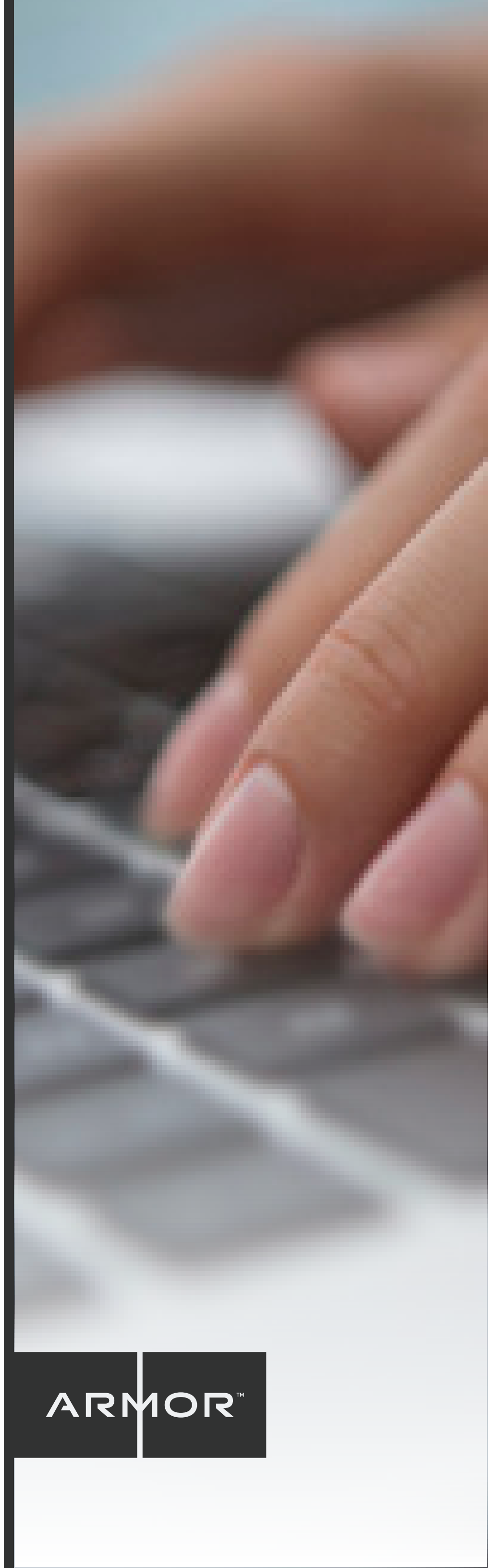
The complexity of cloud migration

One of the key benefits of the secure cloud — virtual access to protected computing resources — is also a factor that can make deployments more difficult. Making the transition from legacy IT environments to cloud technology requires existing systems to be migrated.

A 2015 study from NTT Communications found that there is also a great deal of confusion regarding which cloud delivery model works best for different application types, data workloads and business objectives.

This issue becomes an even more dominant theme when considering the best choice will be different based an organization's existing systems and goals for the secure cloud. For instance, depending on compliance requirements, some applications may need a much higher degree of security than others.

> "There is a great deal of confusion regarding which cloud delivery model works best for different application types, data workloads and business objectives."



Why ROI doesn't tell the whole story

According to a 2014 Information Week survey, only 23 percent of companies are "highly likely" to calculate the ROI of their cloud solutions. One of the challenges that emerged in Information Week's report is the prominent usage of multiple cloud environments.

Businesses such as General Electric use multiple cloud service providers to ensure their software environments can meet specific usage needs. While this has the advantage of fine-tuning cloud technology to specific applications, it adds to the complexity of modern cloud strategies and in determining the value of each cloud environment.

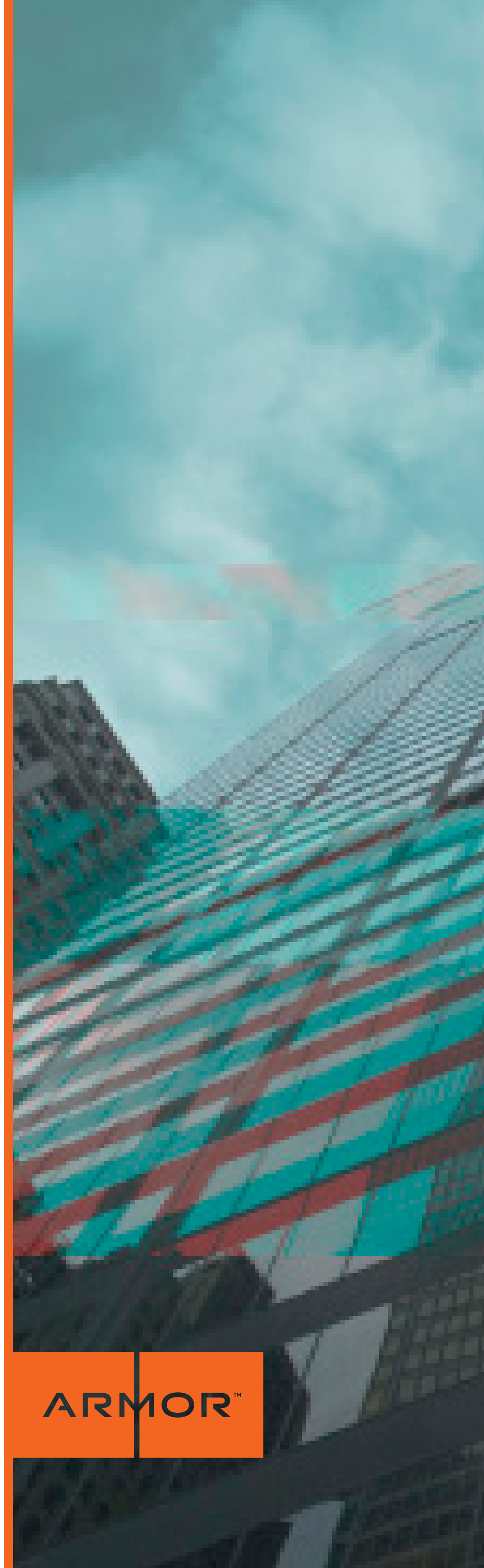
Traditional ROI calculations, which focus heavily on direct, quantifiable increases, also miss some of the less quantifiable value of the cloud. Features such as scalability and security can save companies from experiencing IT downtime during periods where productivity matters most.

This perspective also overlooks how security, performance and compliance mix into the strategies for different industries. Commodity clouds are readily scalable and provide adequate performance, but security-conscious organizations will realize they aren't designed for highly sensitive data workloads, intellectual property or compliance-based information.

Yet consumers still demand cloud-based solutions that require access to this sensitive data, even though they're on the hook by the customer and any government or industry regulations should a breach occur.

That's when organizations began to look into private clouds or dedicated options as a DIY approach — an expensive, complex and highly demanding undertaking.

> "Commodity clouds are readily scalable and provide adequate performance, but security-conscious organizations will realize they aren't designed for highly sensitive data workloads, intellectual property or compliance-based information."



Organizations are not just in the cloud, they're in the clouds

Another common strategy is to utilize a hybrid approach of on-premise and third-party cloud infrastructure, so even companies that do support their own clouds often develop increasingly complex IT ecosystems. NTT Communications' research also found that IT decision-makers run an average of four different cloud environments, and about 14 percent are managing more than seven.

With so many moving parts and separate ecosystems, the cloud management burden grows exponentially. This is why new cloud deployments must be customized to business needs — the considerations that must be made change dramatically depending on whether the organization plans to utilize one cloud environment or whether it will eventually utilize seven unique environments.

The cloud skills gap

Staffing has also become an issue in light of the cloud's explosive growth. According to research firm International Data Corporation (IDC), 7 million cloud-related jobs will be vacant by the end of this year.

The cloud skills gap is especially problematic because it can exacerbate complexities in virtually all areas of an organization's cloud solution, from the choice of which technologies to invest in to configuring and managing cloud deployments appropriately, as well as building an appropriately secure cloud.

When considering the complexities associated with both cybersecurity and the cloud, the skills gap becomes even more prominent. As showcased in Cisco's 2014 Annual Security Report, there is a shortage of around 1 million information security employees and managers.

The cloud's emphasis on self-service has also put pressure on traditional IT roles in that IT professionals have to be more cognizant of how non-technical teams interact and use technology. This is an area in which service providers can be especially beneficial, since they not only have a firm grasp of the technology, but of how to deploy and use it across numerous use cases and industries.

Integrating, managing and securing

To get a DIY cloud off the ground, businesses will need to think about and plan for all staff, processes and tools necessary for these three core elements:

INTEGRATION

A DIY cloud is far from a plug-and-play situation, as a lot goes into just deployment. Once a strategy is in place, you have to figure out what hardware to purchase, the physical hosting location and how resources will be accessed and shared. Then comes installation and setup, which can be tricky when integrating cloud with legacy tools and workflows. These challenges are why implementations can easily run months or years behind schedule.

MANAGEMENT

Of course, once a DIY cloud is finally up and running, likely some level of support and oversight is needed to keep it operational. This often means that your IT department — which may be overburdened as it is — is tasked with adding another key element to their already long to-do list. Additional training may be needed to ensure constant and consistent maintenance from internal teams, and often new workflows and assets are required for upkeep.

SECURITY

Last is security, the most crucial component. It's the most critical consideration businesses need to keep in mind with a DIY cloud. A breached system is catastrophic, and can lead to immense monetary losses and a severely damaged reputation, in addition to fines or even the end of the business in some instances.

Security in the cloud is a far different beast than security with legacy systems, so old solutions don't cut it. Ideally, businesses should implement multiple layers of security to protect the cloud from both all known issues and from zero-day threats.

Changing expectations of accountability

The pressure on companies is also growing because of shifting expectations related to accountability. As Experian Marketing Services predicts, accountability for cybersecurity will expand outside of the IT department in 2015 and beyond. Business leaders will increasingly be expected to ensure smart decisions are being made to protect customer data.

This means that complex technology deployments will face ever-growing scrutiny, especially when considering the other myriad issues discussed. As a result, cloud deployments need to be more collaborative than ever, in order to bring together both the requisite business and IT expertise.

Even though IT teams will still take the lead on these projects, the business side of organizations will be expected to understand and validate the security of their organization's technology choices.

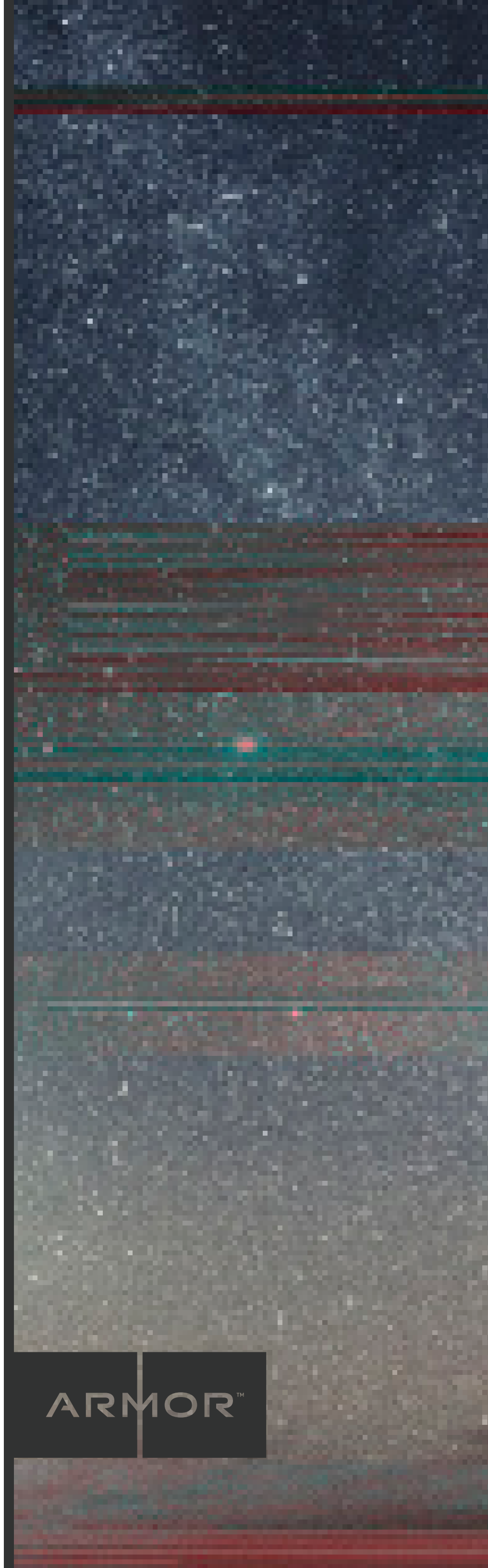
What's the best way to deploy secure cloud technology in a safe, efficient manner? You do have options.

Managed secure cloud services: The best of both worlds

Despite the complexities associated with building a secure cloud in-house, there are still options for companies that don't want to trust public cloud resources. Although managed cloud services are often associated with the public cloud, they can be leveraged to deliver any kind of cloud services, including the major delivery models as well as private clouds.

This does not mean that there aren't critical decisions to be made when leveraging a managed cloud. The major element that must be considered is how to properly choose providers and what level of responsibility the organization wants to share. This process should begin with the first phase of consideration, when businesses are initially exploring their objectives and goals for cloud solutions.

Providers can then be vetted by the security features, level of customer support, compliance offerings, performance benchmarks, business continuity and disaster recovery controls, and type of clouds they offer to narrow the field.



Secure cloud services are not created equal

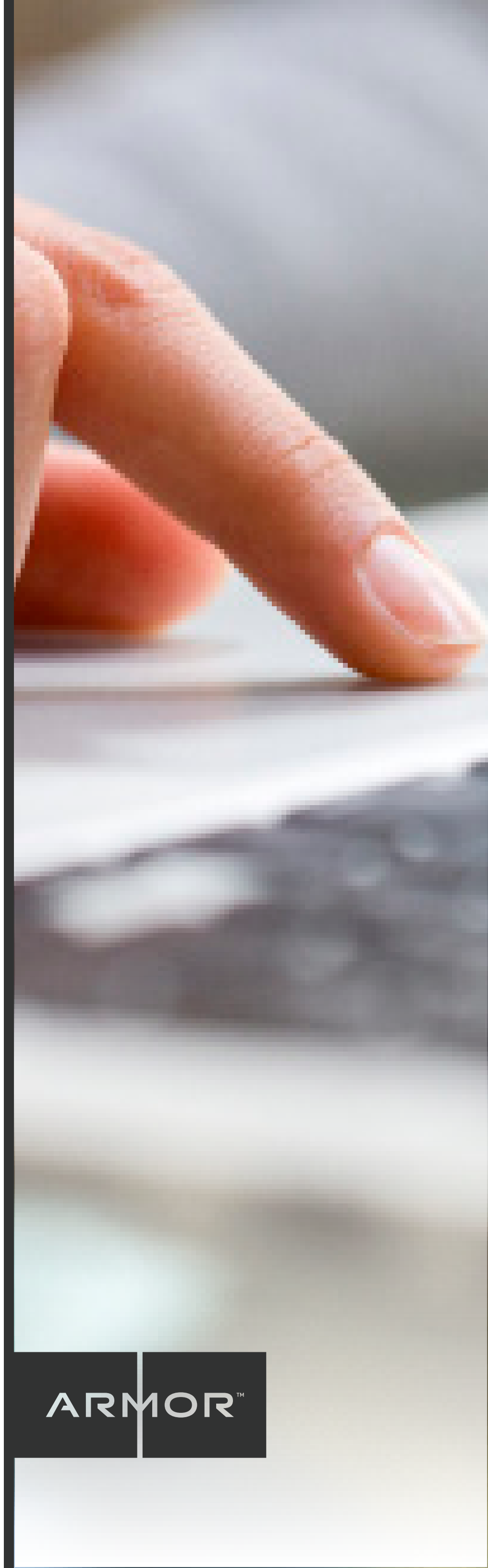
Most organizations today understand the potential value that cloud infrastructure can offer. As a result, it is rarely a question of whether to adopt the cloud, but how and to what extent.

Most organizations face a number of complexities, stemming from the challenges associated with selecting the right technology and the right providers — all while ensuring data remains safe.

However, deploying a highly secure and available cloud environment is only the first step. Where differentiation occurs is how these environments are managed, integrated and protected. For example, some may only conduct monthly software scans while a highly secure service will incorporate threat intelligence and continuous monitoring into an environment.

This is where managed and secured cloud infrastructures offer a considerable degree of value. They bring the expertise that is necessary to maintain a secure cloud even in the face of ever-evolving cybersecurity threats. Because security is built into their businesses, every employee that manages their cloud infrastructure understands best practices and ensures that critical organizational data is not only always available, but always protected.

> "Most organizations face a number of complexities, stemming from the challenges associated with selecting the right technology and the right providers — all while ensuring data remains safe."



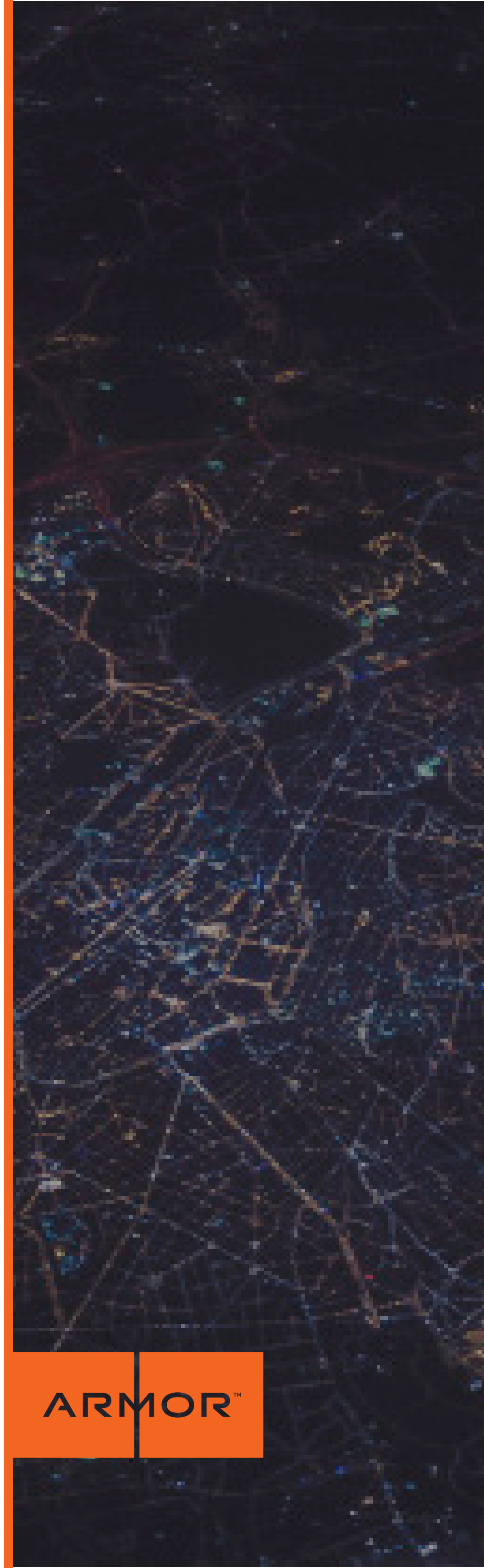
Conclusion

Many organizations are adopting the cloud and are investigating DIY approaches in an attempt to maintain control while also leveraging the flexibility and scalability inherent of the technology. But, unless they are implemented and maintained properly, such an investment will not yield ROI.

Securing the cloud is no easy feat. Trying to guarantee security, privacy and compliance often proves far too difficult for many firms. Unfortunately, many organizations discover this shortfall when it's too late.

The key, then, is to turn to a managed service provider with deep knowledge of and experience with cloud security. This should be a vendor that delivers true security outcomes, not just cloud infrastructure.

An expert third party has the skills, experience and knowledge necessary to ensure compliance, privacy and security — and often at a cost far lower than what it could take if done in-house. With such a team helping out, an organization can focus on core business needs while not having to worry about security, cloud infrastructure, management and other inherent complexities.



Sources cited

http://blogs.gartner.com/thomas_bittman/2015/02/05/why-are-95-of-private-clouds-failing/

https://www.gfi.com/whitepapers/Hybrid_Technology.pdf

https://news.microsoft.com/download/presskits/learning/docs/idc.pdf

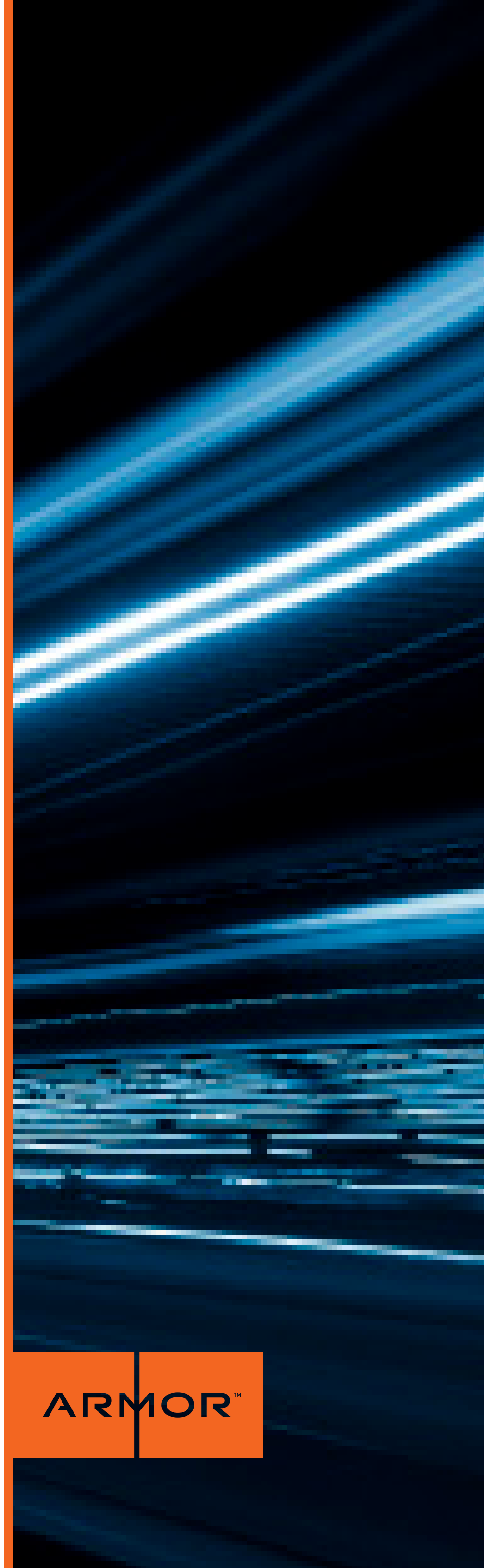
http://www.symantec.com/connect/blogs/2013-internet-security-threat-report-year-mega-data-breach

http://research.zscaler.com/2015/04/malvertising-exploit-kits-clickfraud.html

http://info.us.ntt.com/rs/nttamericainc/images/WP-Cloud-Reality-Check.pdf

http://www.informationweek.com/cloud/infrastructure-as-a-service/cloud-roi-why-its-still-hard-to-measure/d/d-id/1297746

http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™