ARMOR™

The cloud crossover

10 REASONS YOU'RE READY FOR A MANAGED CLOUD

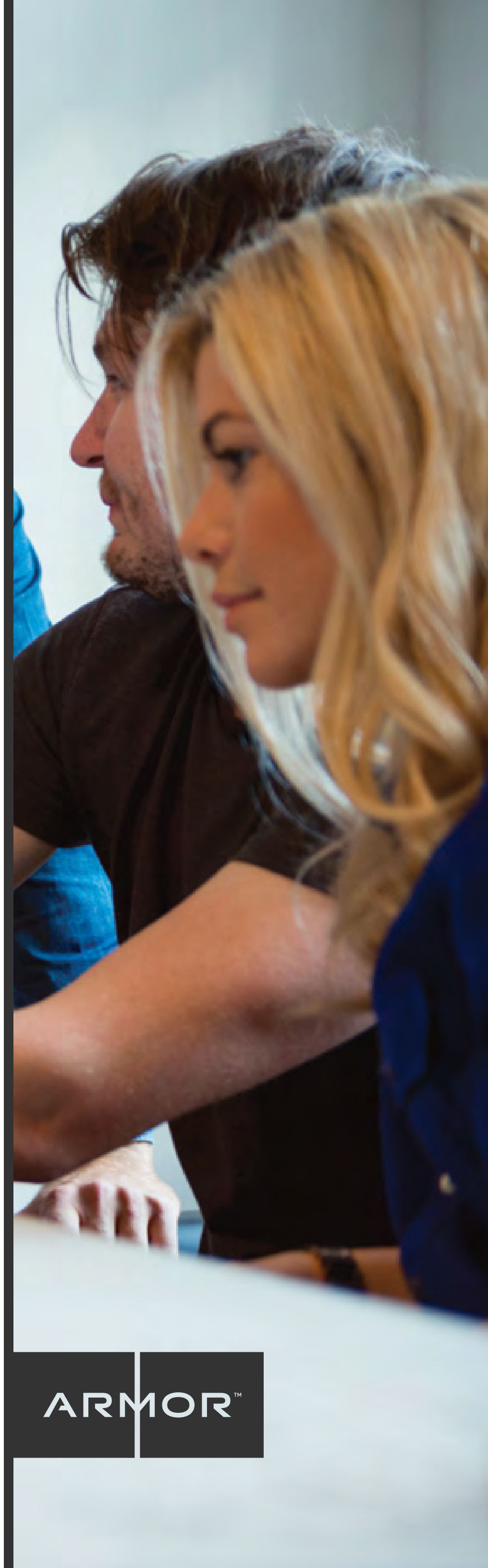
Executive summary

There are many managed cloud services available, but only a small subset of those emphasize security and are, therefore, known as secure managed cloud services. Even among these services, there is a great deal of differentiation from one service to another.

The best secure managed cloud services, besides promoting optimal security, are also active (i.e., proactively identifying emerging problems and responding to them rapidly) and customized (i.e., taking each customer or workload's security needs, operational characteristics and other specific requirements into account).

The best secure managed cloud services provide several benefits to their customers, including the ability to:

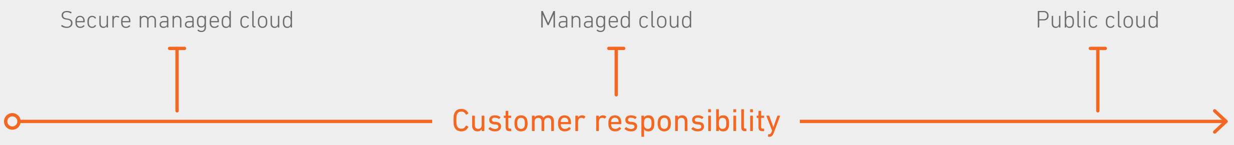
- Alleviate the need to have staff provide 24-hour monitoring and maintenance for cloud workloads
- Reduce the cost of ownership through lower infrastructure and labor expenses
- Speed the time to market for new IT deployments (from months to hours)
- Provide unique capabilities that each customer does not have the resources to provide themselves directly
- Reduce risk by optimizing security controls and offering superior response times when problems occur
- Respond to emerging threats and attacks, preventing both impact and success
- Enable more efficient paths to government or industry compliance, such as HIPAA, SOX and PCI DSS



What is a managed cloud?

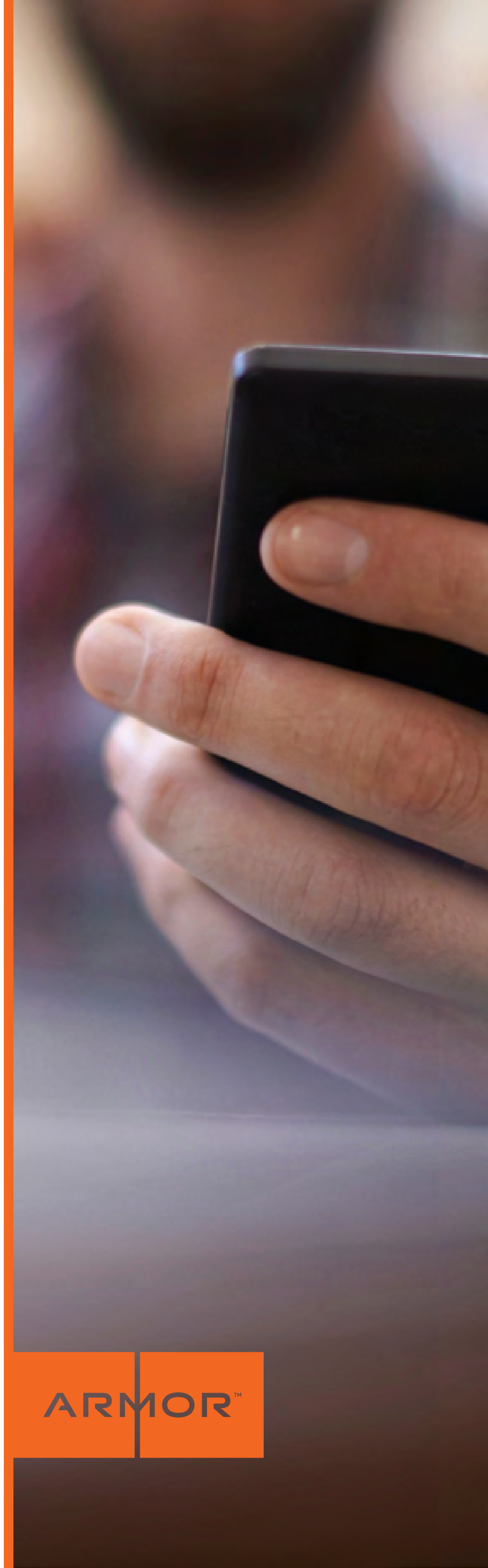
First, let's define the differences between the various clouds.

A managed cloud service involves a third-party service provider managing the delivery of network-based services, applications and equipment on behalf of cloud customers.



Although managed cloud services are often assumed to be for public clouds only, they can be leveraged for any type of cloud, including private and hybrid.

The idea behind managed cloud services is for an organization to transfer some or most of its cloud-related responsibilities to a third party. The basic characteristics of typical managed cloud services can be grouped into three categories: security, infrastructure and experience.



Security

Security management is often rather minimal for a basic managed cloud service provider. The provider takes care of all security considerations related to the physical infrastructure itself, such as data center security and periodically scanning the infrastructure's software components for vulnerabilities and ensuring that those vulnerabilities are effectively mitigated.

The provider is also responsible for enforcing basic physical security principles (e.g., restricting local access to the cloud servers and the facilities that house them).

Most or all other security-related duties, including compliance efforts, are the responsibility of the cloud customer with a typical public cloud or managed cloud service.

Infrastructure

Infrastructure refers to the architecting and management of the cloud infrastructure itself. These are largely the types of services that you would expect any managed cloud provider to offer.

At the most fundamental level, virtually all infrastructure services include providing power, climate control, Internet connectivity, and managing the deployment and migration of cloud workloads among servers.

A cloud management offering includes performance oversight, such as monitoring the resource utilization of all cloud workloads and planning for long-term expansion

Finally, infrastructure management can also involve a degree of assembly related to various tools and services that enhance the performance and security of the solution. It also helps keep cloud infrastructure software up-to-date, which has not only operational implications but also serious security ramifications. of the cloud infrastructure to handle increasing needs.

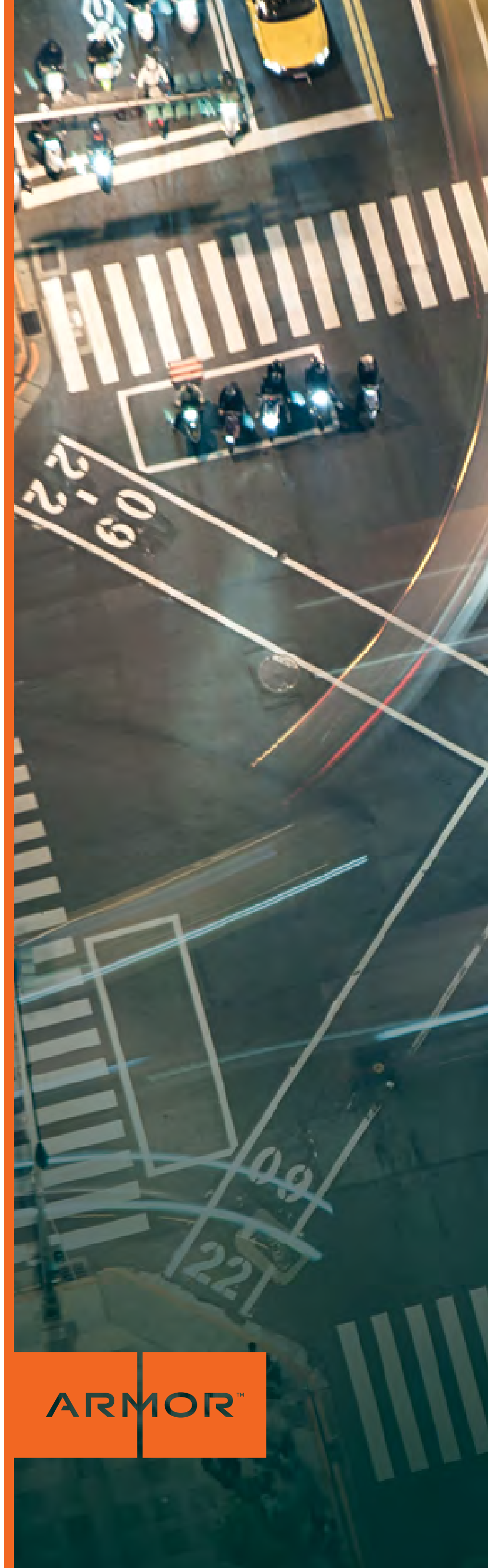
Experience

In terms of managed cloud services, experience can be divided into two types. One refers to the experience that a cloud provider's staff has with the cloud infrastructure itself — basically, their knowledge and familiarity with the cloud infrastructure's operations and security.

The other type of experience refers to the specialized knowledge that the cloud customer has with their own data, applications, controls and services that they have migrated to the cloud.

In a managed cloud service arrangement, the cloud customer often has to work closely with the cloud provider when a problem arises.

In most scenarios, the cloud provider lacks experience and direct knowledge of the customer's cloud deployment, configuration, security needs and compliance requirements.



Three pillars of the secure managed cloud infrastructure

Security

- World-class security operations center (SOC)
- Real-time threat identification & mitigation
- Proactive vulnerability scanning
- Dedicated compliance expertise
- Advanced penetration testing

Infrastructure

- Seamless integration
- Continuous patching & updating
- Demonstrated performance management
- Diligent onboarding & implementation
- Proven security architecture

Experience

- Standard around-the-clock support
- Protection by highly-trained cybersecurity professionals
- Self-service tools
- Secure portal dashboard

Many clouds, many differences

Managed cloud services should not be thought of as a simple commodity to be purchased from any provider; indeed, there are major differentiators that separate one such service from another.

These relate primarily to the division of responsibilities between the managed cloud service provider and the customer, as well as the managed cloud service provider's general philosophy.

These differences are mapped to the following collection of differentiators and benefits.

1 You need built-in security

The biggest differentiator between providers is security. Some providers put such emphasis on security that they are actually known as secure managed cloud service providers.

These providers take on much of the security responsibility that would otherwise be shouldered by customers. But not all secure clouds offer the same levels or types of security. First, consider how and where a cloud vendors security controls are integrated. Some providers focus on perimeter security, such as IP reputation filtering, Web application firewalls (WAF) and antivirus solutions.

Other secure managed cloud provides go a step further with advanced infrastructure protection. How these are architected and integrated vary from vendor to vendor, but it's important to consider the following technology: intrusion detection, log management, vulnerability monitoring, malware protection, patch management and file integrity monitoring.

Likewise, progressive secure cloud vendors — those with dedicated and experienced security engineering and operations teams — have a wide variety of additional services that other providers do not.

Such an offering may include compliance expertise or consultation to help features to help customers achieve, document and maintain compliance with various laws and regulations, including HIPAA and PCI.

Another example of the increased focus on security is the secure cloud provider's responsibilities for identifying vulnerabilities within customer cloud implementations, at the individual virtual machine (VM) level, and mitigating threats against those vulnerabilities.

When conducting a comparative evaluation of true secure managed cloud vendors, execute an in-depth analysis to any security claims. How, where and what type of security technology used is critical; the manner in which a cloud vendor manages and oversees the technology matters even more.

Vendors that are able to provide — and demonstrate — all the aforementioned security capabilities should go to the top of the list.

> "Progressive secure cloud vendors — those with dedicated and experienced security engineering and operations teams — have a wide variety of additional services that other providers do not."

2 You value customized service

Also consider the customization options for different managed cloud services. Some service providers are not equipped to understand each customer's unique deployment and business realities.

If a customer of one of these providers needs technical support in the case of operational problems, security incidents or other issues, the customer would contact the provider and be assigned a random technical support agent to provide assistance.

This agent would likely have little to no information about the specifics of the customer's cloud implementation and usage, security environment or other aspects particular to that customer.

Contrast that with a provider that emphasizes customized services. Such providers offer a dedicated person or team that knows the customer's policies and needs, infrastructure usage, environment configuration and business objectives.

This level of service typically includes "run books," with extremely detailed logs of all changes, and provides the ability to respond much more rapidly and effectively to emerging problems than other providers.

3 You want a proactive partner

A final differentiator is how proactive the provider is in terms of managing the cloud service.

A provider that is more proactive will identify emerging problems with performance, security and other aspects of the cloud more rapidly and act decisively to correct those problems before they become disruptive.

For example, a reactive provider might scan the cloud infrastructure software occasionally (e.g., monthly) for vulnerabilities, whereas a proactive provider might implement a continuous monitoring program that frequently scans for vulnerabilities.

A proactive provider will mitigate most threats and vulnerabilities before its customers are ever affected. In contrast, a reactive provider will take action only after a problem has occurred and notify the customer accordingly — after the damage is done.

Are you a candidate for a managed secure cloud?

- Need to augment size and/or capabilities of current IT team
- Want the ability to focus on core business activities
- Desire a partner to help you mitigate risk
- Prefer not to architect a solution in-house

"How, where and what type of security technology used is critical; the manner in which a cloud vendor manages and oversees the technology matters even more."

ARMOR™

The choice is yours

Choosing a secure managed cloud service over a typical cloud service can provide significant benefits to a customer. Some secure managed cloud service providers are also active in their cloud service management and offer customized services for their customers. This combination — secure, proactive and customized — is highly desirable for many reasons.

4 You demand around-the-clock protection

It's obvious to state that using a secure managed cloud service should provide a reasonably secure solution. What makes security so challenging is the need to constantly monitor and maintain those security controls to take into account new vulnerabilities, threats, attack vectors and other aspects of the constantly changing security environment.

It's also critically important to take into account the individual needs of each customer, and often even different needs for different workloads from a single customer.

All of these challenges can be met by taking an active and customized approach to security, ensuring that continuous monitoring and prompt maintenance is occurring.

Elite cloud vendors can customize security controls, as needed for particular workloads, and ensure their staffs have all the necessary information about the characteristics of each customer workload.

This allows quick responses to emerging threats and attacks, helping to prevent many attacks from succeeding and strictly limiting the impact of those attacks that might succeed.

Perimeter security

- DoS/DDoS mitigation
- IP reputation filtering
- Web application firewalls

Infrastructure security

- Intrusion detection
- Log management
- Patch management
- Vulnerability monitoring
- Malware protection
- Integrity monitoring
- Antivirus solution

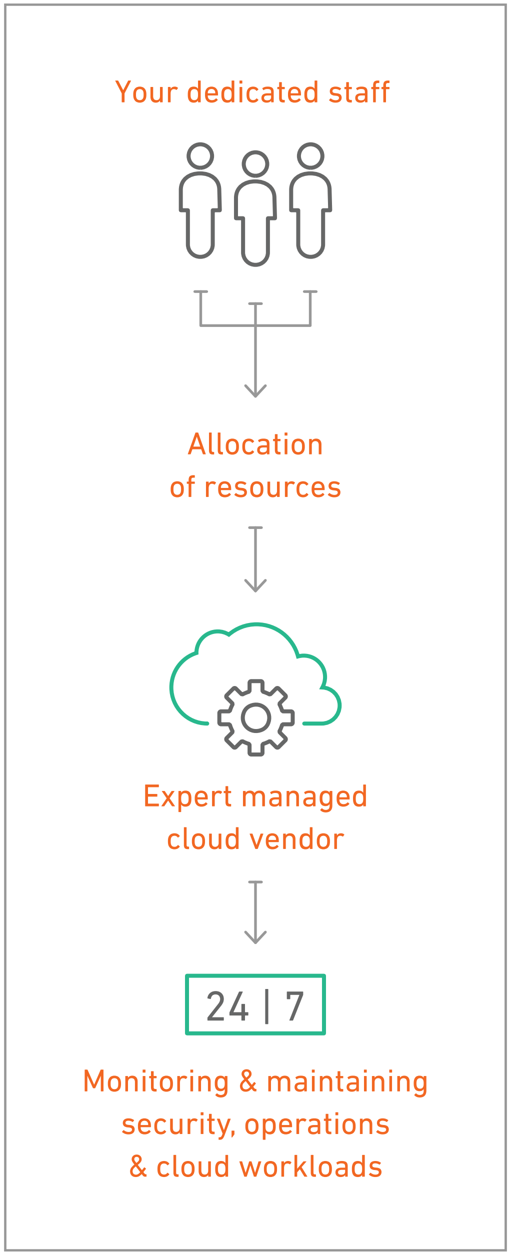
5 You want to smartly allocate resources

Using a secure managed cloud service gives an organization much greater flexibility in terms of allocating staff time. For example, instead of having to dedicate staff for around-the-clock monitoring and maintaining the security and operations of the cloud workloads, the organization can outsource these responsibilities to a secure managed cloud service provider.

This is often much more cost-effective for the organization, as well as a popular decision for the organization's employees. Employees may then be assigned to other, potentially more valuable, tasks or business objectives.

Resource allocation is a particularly important consideration for smaller organizations and, more generally, any organization that may lack the necessary cloud security and operational expertise.

Instead of attempting to train all the staff necessary to achieve around-the-clock cloud management, an organization may outsource infrastructure efforts to more qualified and experienced professionals.



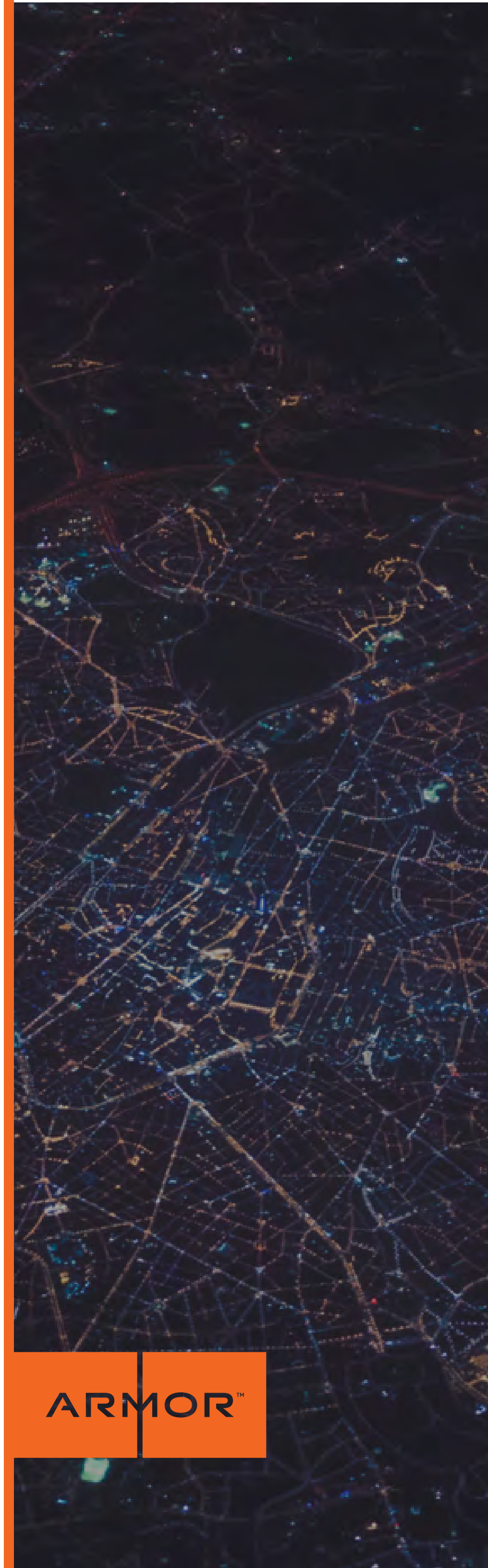
Your dedicated staff

Allocation of resources

Expert managed cloud vendor

24 | 7

Monitoring & maintaining security, operations & cloud workloads



6 You want to reduce total cost of operation

In general, migrating from traditional data center infrastructure to cloud architectures can produce cost savings. This is a result of the flexible and scalable nature of cloud architectures; cloud customers pay for the resources that they use or have reserved in case they are needed. Migrating to the cloud can be quite favorable in financial terms, such as the organization incurring operating costs instead of capital costs.

Cloud migration is ideal for organizations that have rapidly changing needs or only need cloud resources for a short period of time, removing the need to build in-house computing infrastructure sized to handle maximum expected usage.

Cost of ownership is also improved because of the reduced overhead in having a cloud provider maintain the security of all its cloud servers instead of having each customer maintain security for its own servers.

Ultimately, the total cost for using a secure managed cloud service provider can be less than comparable solutions that provide equivalent security and compliance levels.

> "Migrating to the cloud can be quite favorable in financial terms, such as the organization incurring operating costs instead of capital costs."

7 You want to go to market faster

For many IT deployments, speed is increasingly critical. It can take several weeks or months to execute an IT deployment in traditional environments.

In this scenario, the time required to research, architect, procure, assemble, integrate, test, train, deploy, optimize and run the solutions, not to mention securing all included data, applications and environments, is considerably long.

Secure managed cloud services, however, typically offer superior onboarding services allowing any organization to acquire and start using secure cloud services in a matter of hours.

8 You need unique capabilities

A secure managed cloud service provider may provide unique capabilities that an organization simply cannot provide for itself.

These capabilities may include intellectual property, tools, skills and collective intelligence. It may be difficult or even impossible for an individual organization to replicate these capabilities at a reasonable level of effort or cost.

For example, a secure managed cloud service provider may be able to afford subscriptions to threat intelligence services that its customers individually could not otherwise justify. Secure managed cloud service providers also offer dedicated security operations and information security engineering teams with deep expertise.

Through collaborative learning, secure managed cloud service provider also can uniquely see a threat against one of its customers and leverage this information to protect its other customers from the same threat.

9 You want to reduce risk

The best secure managed cloud service providers are experts in risk reduction. They understand which security controls are needed to maintain compliance with requirements and to effectively reduce business, technical and/or operational risk to acceptable levels for their customers.

More importantly, they implement, monitor and maintain these controls on behalf of their customers, helping them achieve compliance as a natural outcome of having such a secure infrastructure.

Along with this, the best secure managed cloud service providers can offer superior response times when problems occur. While many providers only guarantee how quickly a response to a problem will begin, the best providers talk in terms of how quickly a problem will be resolved.

> "The best secure managed cloud service providers are experts in risk reduction."

(10) You have compliance requirements

Complementary of the risk-reduction demands, most organizations are also subject to one or more compliance initiatives regarding the security of their sensitive data. Examples of these initiatives include HIPAA, PCI DSS and SOX.

Secure managed cloud service providers are quite experienced with achieving compliance through their offerings, so this can greatly reduce the amount of effort that customers expend to achieve compliance.

Organizations should be cautioned, however, to carefully evaluate how prospective service providers actually comply with requirements. Many providers claim they meet compliance requirements, but these requirements can be achieved on different levels. And many providers are actually compliant only at the physical level, not at logical levels above that.

In such a case, each customer must still put forth extensive effort to achieve compliance at logical levels above the compliant physical level. Elite secure managed cloud service providers offer rigorous compliance at all levels to minimize their customers' burdens.

Another benefit of using services from a secure managed cloud service provider is that these providers have relationships with compliance auditors. An example is Qualified Security Assessors (QSAs) for PCI DSS compliance.

These auditors have already reviewed the provider's PCI DSS compliance efforts and certified that the provider meets the PCI DSS requirements. This means that a customer of the provider only needs to display compliance with those requirements that may only be met by the customer directly. This speeds the audit process and reduces costs for the customer.

> "Secure managed cloud service providers can greatly reduce the amount of effort that customers expend to achieve compliance."

More power, more value

Secure managed cloud service providers offer a high-quality solution at an excellent value to any organization that is considering a migration to the cloud or is concerned about the security of their existing cloud deployments.

The best secure managed cloud service providers endeavor to deliver a highly secure environment for their customers through a variety of security capabilities via a cloud management style that is both proactive and customized.

Reasons for adopting such a secure managed cloud service include resource allocation, cost of ownership, speed to market, unique capabilities, risk reduction and optimal security.

When compared to public clouds and typical managed clouds, secure managed clouds offer major benefits in terms of customer responsibility and monthly cost.

Generally speaking, public clouds involve the most customer responsibility, followed by managed clouds; secure managed clouds involve the least customer responsibility, taking a burden off organization management and staff.

Likewise, public clouds often involve the highest total cost as compared to managed clouds and secure managed clouds, which are the most cost-effective.

This may be surprising. However, it can be quite expensive for an organization to design and deploy a secure in-house solution with the equivalent security controls, compliance tools and staffing offered by a secure managed cloud.

> "The best secure managed cloud service providers endeavor to deliver a highly secure environment for their customers ... "

Discover which Armor solution best matches your data workloads with our 30-second online tool.

START NOW

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™