



## Inside the 6 principal layers of the cloud security stack





## The cloud is critical, complex

Establishing a secure cloud infrastructure has become incredibly important for most organizations. Use of cloud services for hosting sensitive data and applications is at an all-time high because of the benefits that cloud infrastructures can provide, but many still consider the money, resources, staffing and importance placed on cloud security to be insufficient.

Only 33 percent of IT professionals recently surveyed by the Ponemon Institute believe that their organizations are achieving their objectives for cloud security.<sup>1</sup> With the cost of a single data breach often reaching millions of dollars, organizations are increasingly realizing the need to make greater efforts toward securing the cloud infrastructures that serve as the foundations of their business.

Unfortunately, achieving a secure cloud posture can be incredibly complex. It involves procuring, integrating and managing dozens of point security products, as well as making all the necessary changes to processes, staff training and resource utilization. And once achieved, the secure cloud posture must be maintained through constant monitoring, periodic risk reassessments and other means.

Organizations are encouraged to approach cloud infrastructure security through a tiered cloud security stack approach that divides the security technologies into various layers: physical, network, guest system, application, hypervisor and orchestration.

These technologies are then used by people and processes through a set of cross-cutting security controls that wrap around the technologies. These controls include risk management, security architecture, incident handling, threat management, vulnerability management, change control and data security lifecycle support.

By establishing and maintaining a secure cloud infrastructure, an organization can reduce the number of data breaches that occur and minimize the impact of breaches that cannot be stopped, while also enabling greater use of cloud technologies to improve the organization's flexibility and scalability and to potentially lower costs for the organization.

“By establishing and maintaining a secure cloud infrastructure, an organization can reduce the number of data breaches that occur and minimize the impact of breaches that cannot be stopped.”

1. “Cloud Security: Getting It Right,” Ponemon Institute, July 2015.

## Understanding cloud objectives

Organizations are continuing to migrate their data workloads and applications to public and private cloud-based solutions for greater flexibility, scalability and lower costs. Much of the initial reluctance to use clouds stemmed from security concerns, particularly of cloud infrastructures being inherently less secure than standard IT infrastructures.

New approaches for securing cloud-based data and applications are available and regarded as being quite secure, but these approaches have not yet been widely adopted for securing public and private cloud infrastructures.

Often, end organizations assume that the cloud provider is fully responsible for security, but that is rarely true, even in private clouds. In most situations, at least some of the security responsibility falls on the user. And increasingly, organizations are acquiring and using cloud services without involving the IT department.

According to the Ponemon study, fewer than one-fourth of those surveyed report that their organization's security team is regularly involved in evaluating the security of cloud services for use by their organization.<sup>2</sup> The repercussions of failing to properly secure sensitive data in the cloud are obvious: an increase in data breaches and failures to meet security compliance requirements.

Organizations may greatly improve this situation by being proactive in establishing and vetting secure cloud infrastructures to store their data workloads, applications and assets. This may involve both public and private clouds, and it necessitates either being wholly responsible for planning, implementing, monitoring and maintaining the security of the clouds' infrastructures, or acquiring services from a third party that helps offset some, or most, of these security responsibilities.

Regardless of the mechanism chosen to achieve a secure cloud, an organization should confirm they meet the following objectives:

- Ensure complete security and visibility within the cloud environment.
- Minimize dwell time from weeks or months to days or even hours. Dwell time is the amount of time that a threat actor remains undiscovered and unmitigated within an environment.
- Automatically block lesser threat actors so that the security controls — including people — may focus on finding and stopping the most sophisticated threats.

2. "Cloud Security: Getting It Right," Ponemon Institute, July 2015.

## 3 standard secure cloud models

There are three basic models for securing a cloud environment:

### 1 An in-house model

Where the organization establishes its own dedicated servers or cloud and is fully responsible for its security.

### 2 A split model

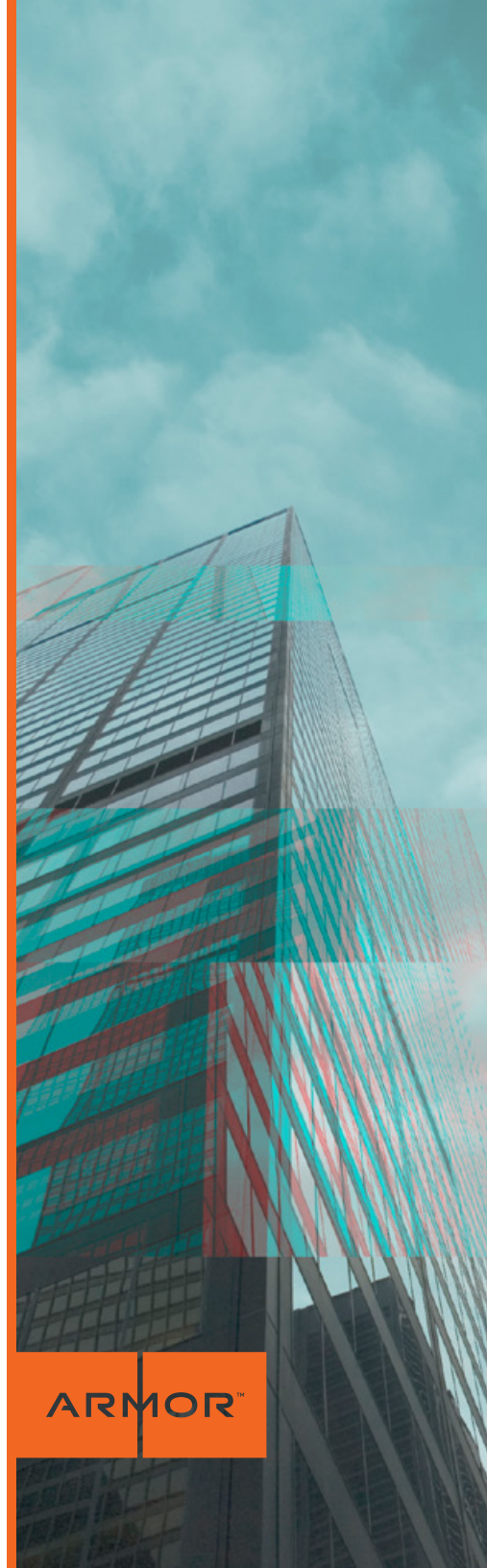
Where different parties are responsible for securing different layers of the cloud environment. The cloud vendor secures the cloud infrastructure itself, including the hypervisors, the cloud's internal network and the physical facilities where the cloud is hosted. Securing the higher layers of the cloud environment, such as the guest operating systems and the applications and data they contain, is either done by the organization (the customer) or by a third party, such as a cloud security vendor, on behalf of the organization.

### 3 An external model

Where the cloud security vendor employs nearly all the appropriate security measures at all layers, leaving few responsibilities in the hands of the organization.

Regardless of the model selected, it is ultimately the organization's responsibility to ensure that all of the necessary security controls are in place and working correctly. Whether this is achieved by the organization deploying its own security controls, acquiring services from a cloud security provider, or employing a combination of these is somewhat irrelevant.

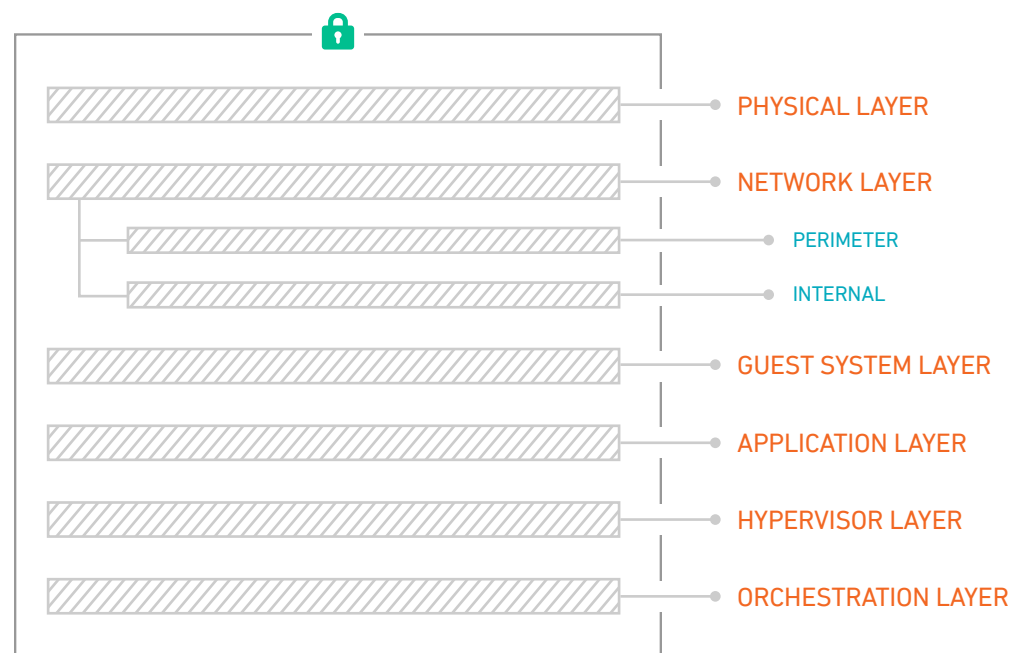
What really matters is the strength of the security achieved, the costs of the security controls, and the money saved by preventing data breaches and other incidents that would have otherwise occurred.





## Inside the tech stack

The sheer number of individual security technologies that need to be selected, deployed, configured, maintained and monitored for a truly secure cloud infrastructure is daunting. To better understand the scope of effort involved, consider the technologies in the context of a cloud security stack. A common stack has several layers, listed from lowest to highest, and may include dozens or more security technology tools.



The types of technologies needed for securing a particular cloud infrastructure will vary somewhat based on deployment models, data sensitivities, compliance regulations, and other organizational and environmental concerns.

## Physical

Security at the physical layer includes many technical and non-technical concerns. Many of these controls require large capital expenditures, such as building space, HVAC, power, redundancy and disaster recovery, cages, dedicated drops, 24-7 CCTV, not to mention the physical servers themselves, and any associated maintenance and costs with replacing failed hardware.

Outsourcing infrastructure to cloud environments greatly reduces the overhead and operational expenses involved with building and maintaining distributed data centers.

## Network

### Perimeter

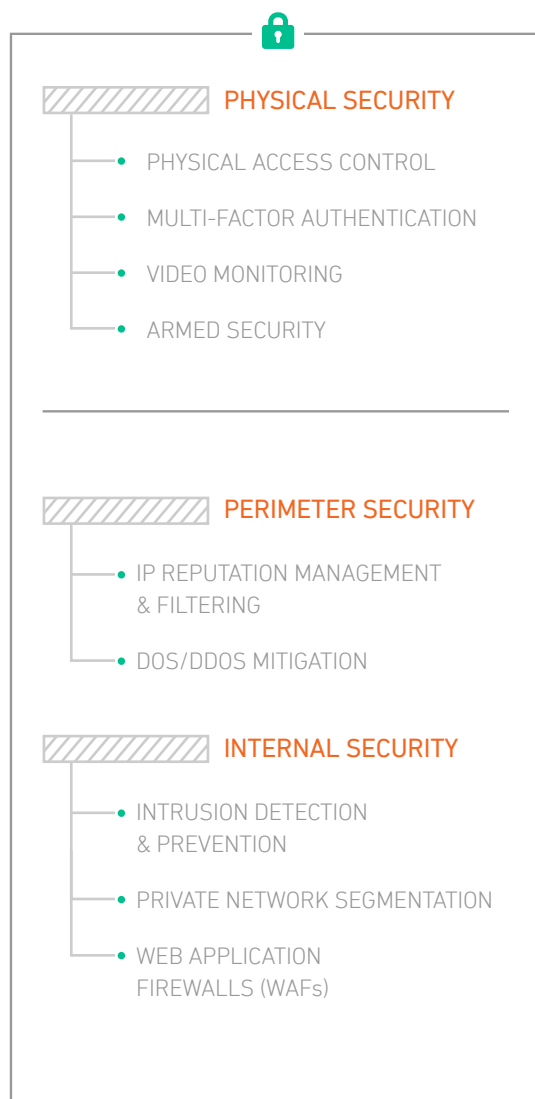
Perimeter security is focused on narrowing the attack surface area by forcing traffic through critical inspection points. As your first line of defense, this is where organizations can begin to eliminate or funnel malicious traffic, thus reducing the amount of traffic that needs to be inspected and proven valid. It is more effective to stop attacks at the furthestmost network layer possible to provide a lower total volume of unproven traffic needing to be inspected by subsequent security appliances. These controls are most effective if deployed to inspect not only inbound but also outbound communications from the guest system.

Security technologies often utilized at the perimeter layer include the use of firewalls, dynamic access control lists, implementing threat intelligence to block newly malicious communications, IP reputation management and DDoS mitigation.

### Internal

The network layer is home to communications that are sent and received by cloud servers. It is where micro-network segmentation occurs, and where isolated security zones can be established, typically by hypervisor-based firewalls.

This layer can also encrypt and decrypt network communications. As the lowest layer with access to unencrypted network traffic, it is typically where network-based intrusion detection (NIDS) or intrusion prevention systems (NIPS) as well as Web application firewalls (WAFs) are deployed to look for malicious network activity.



## Guest System

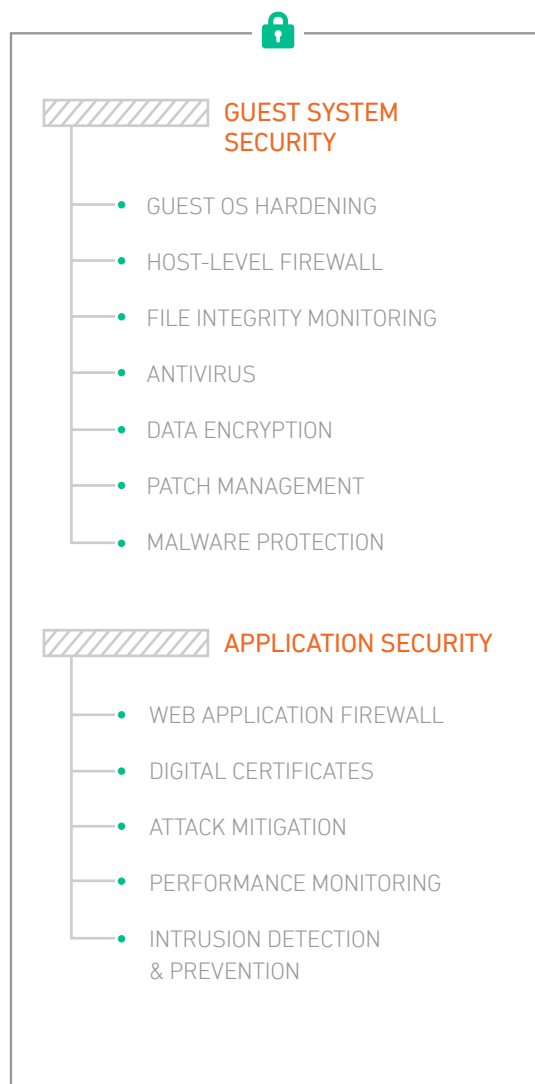
It is important that the guest operating system is hardened before an application is installed and configured. Guest systems need rapid testing and subsequent application of patches, especially critical security-related fixes, to minimize the time a system is vulnerable to exploitation. A vulnerable guest system can provide opportunity for a threat actor to establish a foothold in your organization.

Several other security technologies, which are also leveraged at the hypervisor layer to protect the guest system include event logging, time synchronization, file integrity monitoring, encryption of stored data, resource availability monitoring, further segmentation and enhanced malware protection. Many of these controls aid in the overall security posture by removing local agents from the view of threat actors and enforcing policies at the hypervisor layer.

## Application

Web applications, including software-as-a-service (SaaS) offerings and third-party services, naturally reside at the application layer. Security technologies specifically designed to protect Web applications reside in this layer. Some examples include Web application firewalls (WAF) and next-generation firewalls, which sit between applications and threats.

They can support a variety of different cryptographic methods. These technologies require man-in-the-middle positioning to successfully decrypt, inspect and re-encrypt (if needed). Management of supported ciphers, key lengths and certificates are required to inspect encrypted traffic.





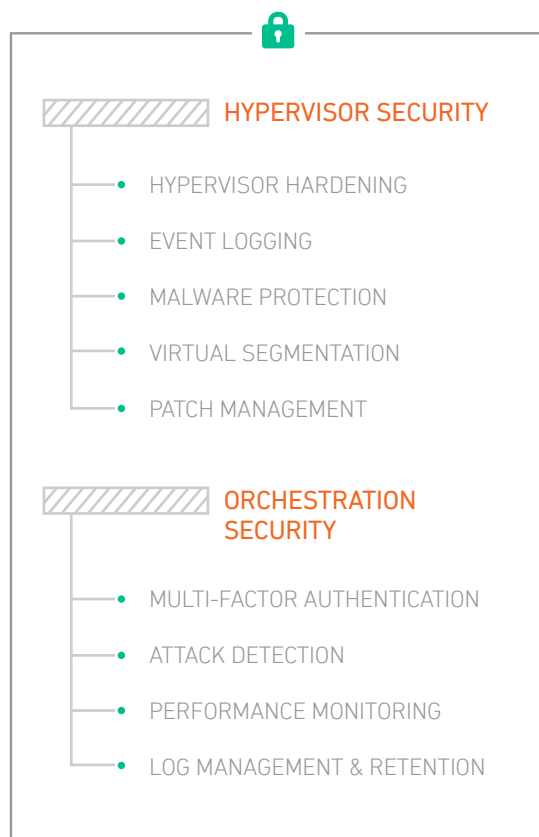
## Hypervisor

The hypervisor layer encompasses the cloud server's virtualization environment where guest operating systems and virtual networking reside. The hypervisor needs to be hardened as much as possible while still enabling the required functionality.

This hardening should include the rapid application of patches — particularly security-related fixes — to minimize the time a system is vulnerable to exploitation.

## Orchestration

The orchestration layer is the most difficult to accomplish and fully operationalize. These frameworks, which are typically custom-built service buses, leverage security technologies throughout the cloud environment and are used for the unification, oversight and dynamic defense of the organization's guest systems

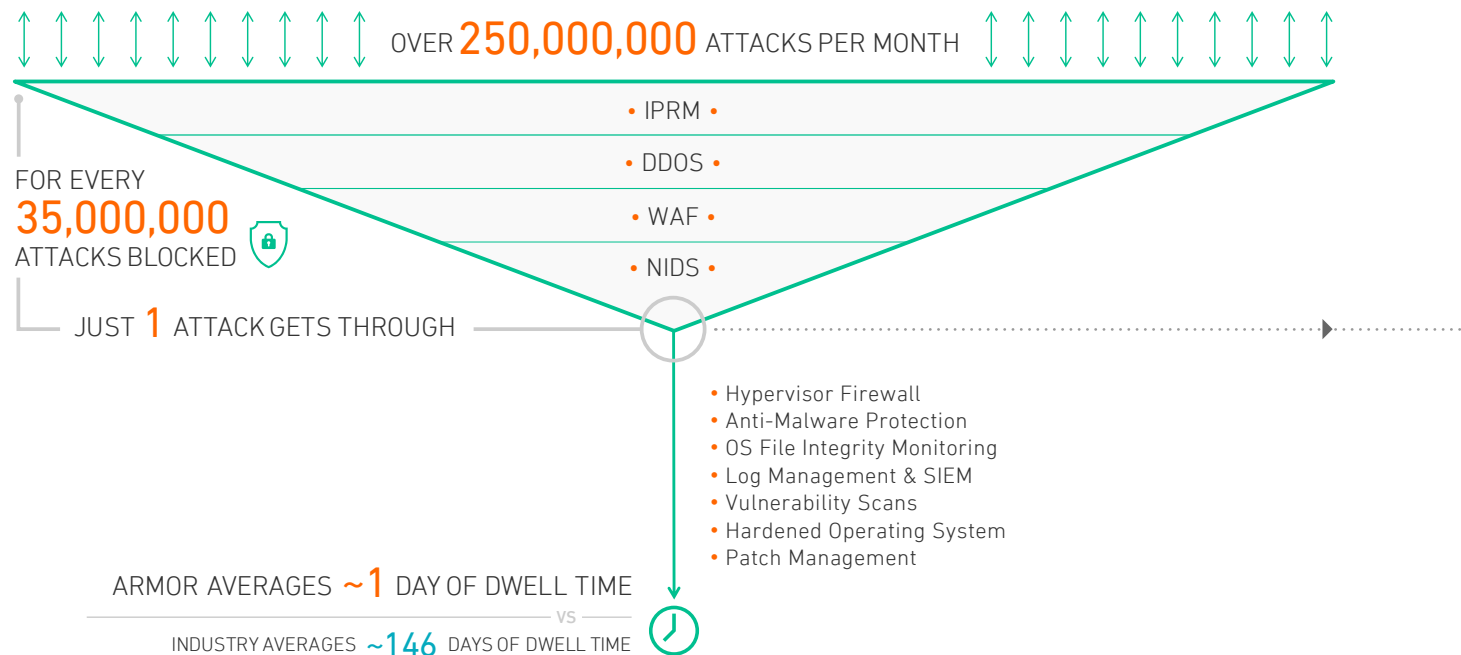




## The secure cloud in action

How does this strategy work in the real world? Armor cybersecurity experts and engineers integrate these security controls as core components of a proprietary active cyber defense approach. Everything Armor has learned over years of fighting — and winning — the cyber wars has gone into this framework, which are monitored and fine-tuned.

Leveraging this solution, Armor blocks more than 250,000,000 targeted attacks each month. With a dwell time 100 times shorter than the industry average, Armor is able to quickly identify and mitigate remaining risks.



### MISSION THREAT INTELLIGENCE

Reduce noise with Armor's proprietary threat intelligence platform, talented teams and layered edge defenses.

### MISSION SECURITY OPERATIONS

Reduce dwell time utilizing secure architecture and forged-in-battle techniques managed by Armor's proactive and relentless security operations center (SOC).

**ARMOR™**

## Cross-cutting security controls

As if the numerous security technologies required aren't enough, consider that they are simply the tools needed to begin building a secure infrastructure. They are of little or no value without the people and processes in place to take advantage of their capabilities and to react when failures, breaches or other security events occur.

Some security controls that are heavily reliant on people and processes are cross-cutting, each applying to several of the cloud security layers. These cross-cutting controls can be thought of as "wrapping around" the individual security technologies.

Examples of cross-cutting security controls include the following:



### RISK MANAGEMENT

Risk management should be at the center of any secure cloud infrastructure's design and maintenance. For example, a formal risk assessment should be conducted of the proposed design before it is ever implemented.

Periodic risk assessments should be performed after deployment to take into account changes in security technologies, vulnerabilities, threats and risk tolerance, as well as to identify any deviations from the organization's requirements.



### SECURITY ARCHITECTURE

The organization's security architecture is the implementation of its risk management findings and security compliance requirements in terms of security controls (e.g., people, processes and technologies).

The security architecture is how the organization actually fulfills its security requirements. Because each organization has a unique set of security requirements, sensitive data sets and applications to protect, the security architecture for each organization should also be unique.



### INCIDENT HANDLING

Incident handling is typically an entire program dedicated to supporting the incident response lifecycle, ranging from preparation and detection through containment, eradication and recovery, and ending with studying and applying lessons learned from previous incidents.





## THREAT MANAGEMENT

Threat management refers to the organization's practices for identifying potential threats and preventing them from successfully compromising the organization's IT resources. The most common form of threat management is the use of automated threat intelligence feeds by technologies that detect attacks, such as IDSs, and security information and event management (SIEM) solutions.

A threat intelligence feed subscription could be used by several technologies at different layers of the cloud security stack to automatically block activities that have been labeled as highly suspicious. In addition, threat intelligence can be leveraged by cybersecurity experts responding to incidents or otherwise investigating suspicious activity.



## VULNERABILITY MANAGEMENT

Vulnerability management practices strive to identify and remediate exploitable flaws and configuration errors in software. To identify vulnerabilities, a variety of automated vulnerability-scanning techniques may be used at several layers of the cloud security stack, as well as periodic code reviews, penetration testing, ethical hacking and other methods.

The other major aspect of vulnerability management is mitigation, such as patch management and configuration management.



## CHANGE CONTROL

Change control involves tracking any additions, alterations and removals that might affect an organization's security architecture, including configuration management and patch management activities; incident containment, eradication and recovery actions; and routine maintenance activities.

Change control enables faster diagnosis of many operational problems and promotes accountability and compliance with the organization's security policies.



## DATA SECURITY LIFECYCLE SUPPORT

Although there are individual encryption technologies to protect data in transit and data at rest, there is also a need to support other parts of the data security lifecycle. Most notable are having secure data backup, restore and deletion capabilities.

## Achieve security & compliance in the cloud

To establish a secure cloud infrastructure, an organization must first ensure that dozens of point security products — from multiple vendors — are in place and properly configured, monitored and maintained.

These responsibilities may be performed by the organization itself, a third party (e.g., an advanced cybersecurity organization or secure cloud provider,) or a combination of these. The organization must also implement and continually execute the numerous cross-cutting security controls (e.g., people and processes) that wrap around the individual security technologies.

Following this structured approach to securing cloud infrastructures makes it easier, faster and less resource-intensive to achieve the main objectives of a secure cloud infrastructure:

By meeting these objectives, an organization can significantly reduce the number of attacks that result in successful compromises, as well as minimize the impact caused by the compromises that still occur because they are detected more quickly.

Gaining full security and visibility into the cloud infrastructure also helps an organization achieve its security compliance requirements by facilitating audits, event logging and monitoring, and other common compliance needs.

All organizations — even those extremely reluctant to embrace cloud technologies — may find that they substantially benefit from reevaluating their cloud migration strategies to take into account the full benefits of following a structured approach to securing cloud infrastructures.

- ④ Ensure complete security and visibility within the cloud environment.

---

- ④ Minimize dwell time from weeks or months to days or even hours. Dwell time is the amount of time that a threat actor remains undiscovered and unmitigated within an environment.

---

- ④ Automatically block lesser threat actors so that the security controls — including people — may focus on finding and stopping the most sophisticated threats.



---

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 2016. All rights reserved.

