ARMOR™

BETWEEN YOU AND THE THREAT

I have multiple clouds ... Now what?

HOW TO IMPLEMENT SOUND SECURITY AT THE VM LEVEL

Best practices for VM-level security

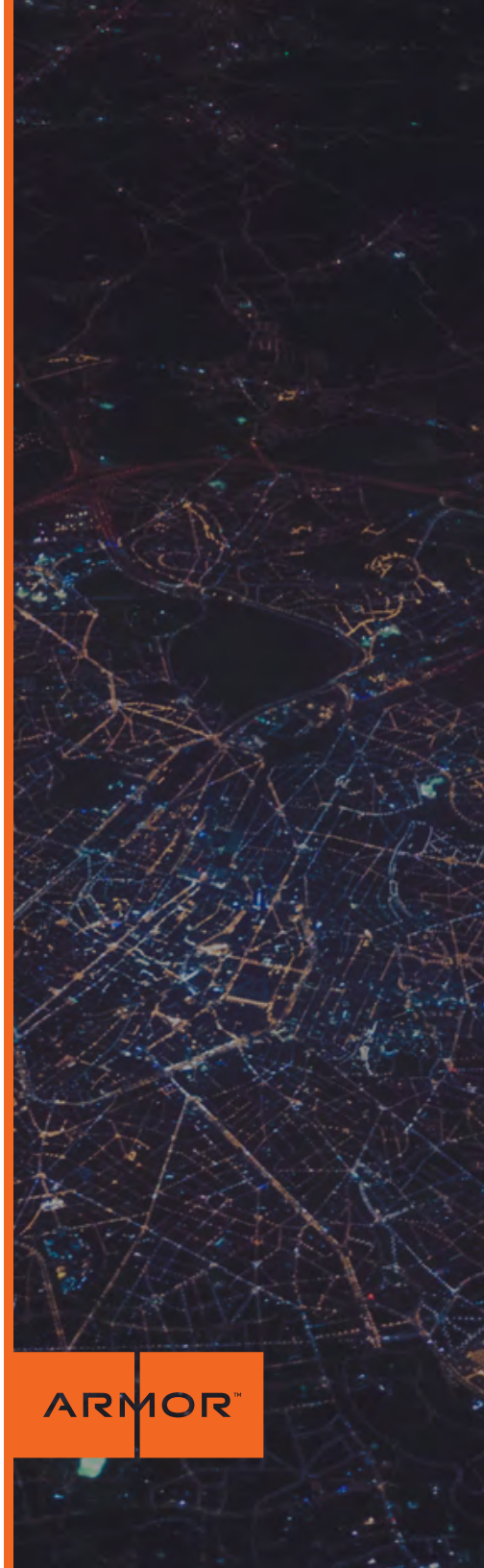
Once your organization is leveraging multiple clouds to power and scale data, services and applications, it may be time to evaluate your business's approach to instance/virtual machine (VM) security.

This paper explains the need to ensure each VM's contents are safeguarded through a combination of vulnerability mitigation and attack detection methods.

Explore the advantages of outsourcing some or most VM security control responsibilities to a cloud service provider or managed security service provider (MSSP).

The recent evolution in data security thinking is helping organizations improve the management of their security from the inside out.

"The recent evolution in data security thinking is helping organizations improve the management of their security from the inside out."



Vulnerability mitigation and attack detection inside the VM

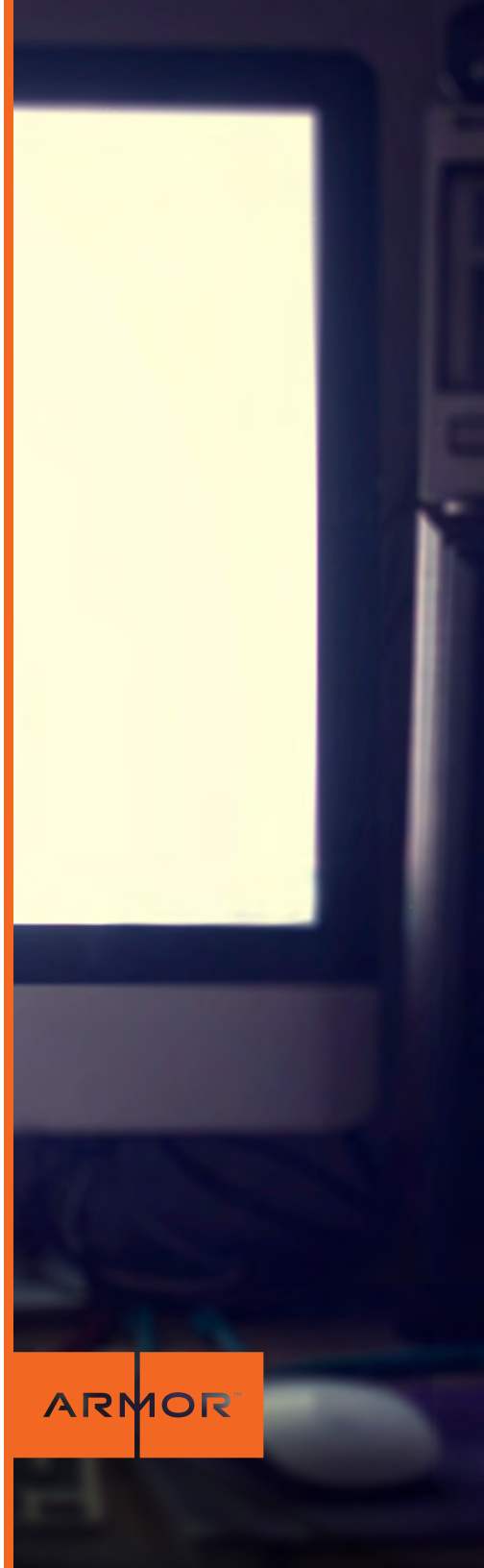
Before an organization migrates its data and applications to public clouds, it's important to understand the wide range of security controls that are necessary to safeguard each VM's contents — the guest operating system, applications and data — so that the organization can estimate the costs associated with each control.

Cloud service providers are responsible for the infrastructure of their cloud, including physical security for the data centers, network security for the back-end networks and securing the hypervisor.

The organization is ultimately responsible for its own security in the cloud. This includes auditing the cloud service provider's security practices, as well as the security controls inside each VM.

These security controls for the VM fall into three groups: guest operating system security, application security and access control.

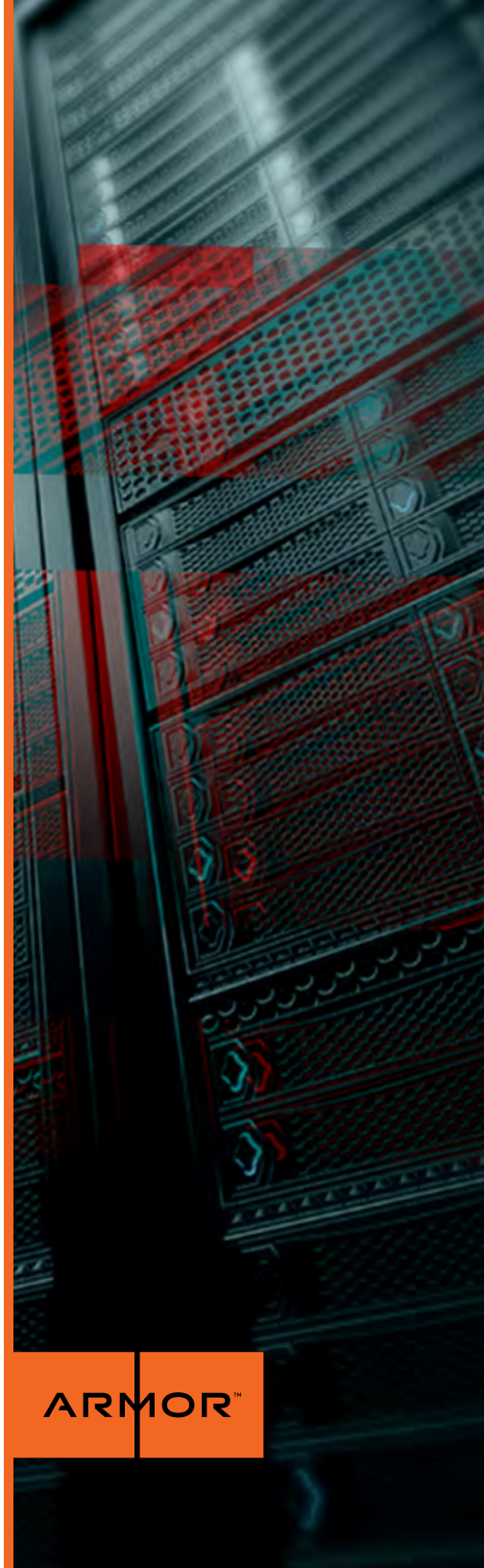
> "The organization is ultimately responsible for its own security in the cloud."



Guest operating system security

The guest operating system security group includes all the security controls that eliminate or mitigate vulnerabilities of the guest operating system (OS) within each VM, as well as the detection and mitigation of attacks against each guest OS. The controls that are generally most important for accomplishing this are as follows:

Configuration Management	Configuration management ensures that the guest OS is secured properly (i.e., hardened) before deployment and, once deployed, detects and reverses any unauthorized changes to the secure configuration throughout the life of each guest OS instance. Configuration management is also useful for adjusting the OS to take into account significant changes in risk — for example, temporarily mitigating a critical new vulnerability until a patch is available.
Patch Monitoring or Management	As needed or on a regular schedule, vendors release patches for their products to fix security flaws, address unforeseen problems or add new features. Patch management is the process of identifying new patches that need to be deployed, prioritizing and scheduling their deployment, testing them before deployment if appropriate and feasible, and installing them onto production systems along with any other necessary changes.
Vulnerability Scanning	Vulnerability scanners are used to identify missing patches and security configuration issues and to estimate the relative severity of each discovered vulnerability so that remediation efforts can be prioritized. Vulnerability scanning is an important complement to configuration and patch management because it emphasizes any gaps in those processes.
Attack Detection Technologies	Attack detection is a broad term for a wide variety of tools that are dedicated to detecting malicious activity and, in many cases, stopping it as well. Some attack detection technologies reside outside of the guest OS, such as hypervisor-based firewalls and intrusion prevention systems (IPS). Other attack detection technologies are specific agents to be managed on the guest OS — for example, antivirus software, rootkit detectors, log aggregation agents or host intrusion detection systems (HIDS).



File Integrity Monitoring (FIM)

FIM tools monitor critical files, such as system binaries or configuration files, to detect and alert on any unauthorized changes, typically file modification or replacement. Such changes often occur because an attacker is establishing persistence within the VM.

Some FIM tools (known as file integrity management tools) can intercept and block unauthorized attempts to change monitored files, while others just report changes after they have occurred. This is still helpful, though, because these tools can help identify other malicious indicators based on correlating events, as well as provides narrative for an attacker's behavior.

Log & Event Management

Log and event management is the process of auditing security-related activities and monitoring and analyzing those audit records to identify incidents and other events that necessitate a response.

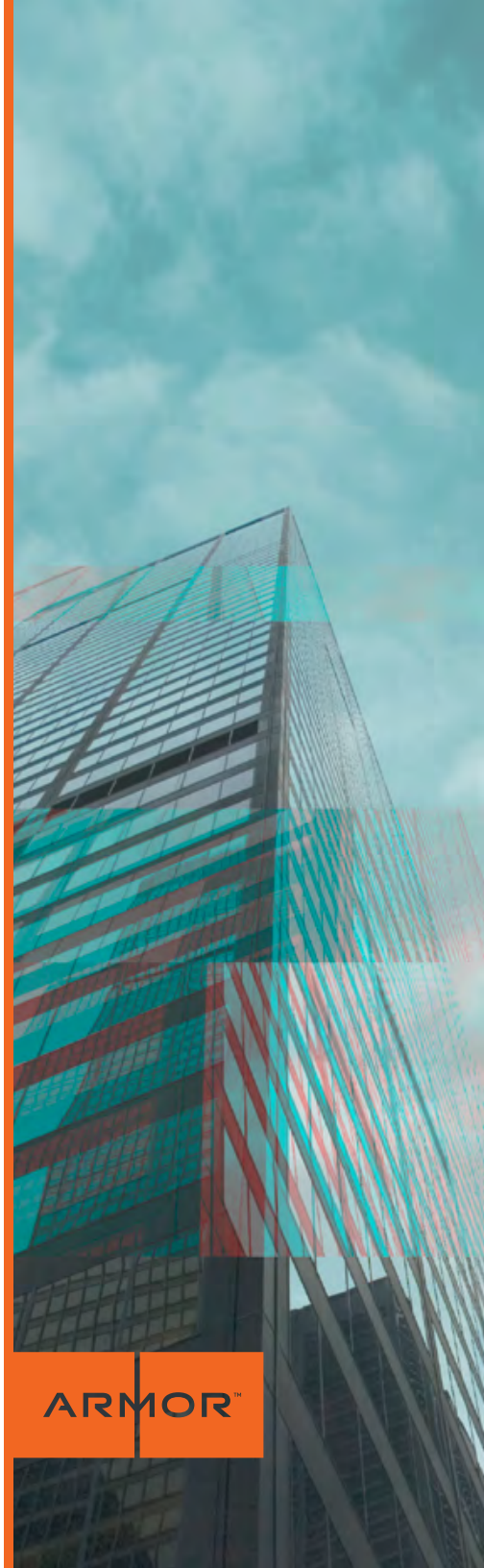
Log and event management — typically achieved via a security information and event management (SIEM) system — can monitor all types of security-related events, including those involving both guest OS logs and non-guest OS logs. This approach consolidates various outputs from all security controls to provide more accurate and complete dashboards and/or events.

The SIEM performs constant monitoring of guest OS security events, identifies significant security concerns and alerts appropriately to prevent compromises or minimize the impact of a compromise in progress. For example, a SIEM may alert administrators of a new incident, or it may automatically reconfigure other security controls to stop malicious activity.

Where is Threat Intelligence?

Strictly speaking, threat intelligence isn't a security control. Threat intelligence is a term that encompasses a variety of methods for gathering and presenting information on observed and potential threats against the organization.

If packaged in a machine-readable format, this information can automatically be used by certain security controls (e.g., SIEMs, IPS and firewalls) to improve attack detection and blocking capabilities. In a human-readable format, threat intelligence can be used to educate security analysts about current threats, which in turn may drive changes to the organization's short- and long-term security posture.



Application security

Application security is the next segment of security controls an organization must responsibly implement. This layer helps eliminate or mitigate application vulnerabilities within each VM, and detect and attempt to stop attacks against the applications.

The security controls that support guest OS security also support application security by safeguarding files and configuration settings, applying patches to applications, monitoring log entries, and identifying and stopping certain types of attacks. In addition, there are controls that are completely or mostly dedicated to application security. Here are three of the most important solution types:

Identity & Access Management (IAM)

IAM technologies identify and authenticate each user (human or process) before granting it the requested access to an application. IAM technologies can also restrict what each user can do with the application, such as what features are available to each user and what rights each user has to read and write information using the application.

An IAM solution helps ensure that only the authorized people and systems can access a particular cloud-based application and that each user can perform only the permissible actions using the application.

Data Security

In the context of security for cloud-based applications, data security refers to technologies specifically designed to protect sensitive data that is or can be accessed using those applications.

Data security encompasses data at rest (e.g., stored in the cloud), data in transit (e.g., traveling across virtual or physical networks) and data in use (e.g., held in memory, being processed, etc.), all of which require different cryptographic solutions that are either built into the application or that are utilized by or with the application.

Web Application Firewall

A Web application firewall (WAF) is a specialized attack detection technology that identifies and stops attacks against Web applications and the servers interacting with the Web applications behind the scenes, especially database servers. Other attack detection technologies, even intrusion prevention systems, typically lack the breadth and depth of Web application understanding and attack recognition that WAFs offer.

Access control

A third control, focused on safeguarding virtual access, applies to an organization's remote administration of VM contents. A common form of access control is a virtual private network (VPN) configured between an organization's facilities and each cloud the organization uses.

A VPN provides secure connections to the cloud servers so that the organization's administrators can manage and maintain VMs and associated content.

Because a VPN could also provide a route for attackers to use to access administrative utilities and privileges, the VPN must strongly authenticate each administrator before granting access. Organizations should use multifactor authentication for this purpose, such as requiring that each administrator have an organization-issued smartcard and know the password protecting it.

Privileged session monitoring and auditing, in comparison, monitors all commands or actions performed by the organization's administrators within each VM.

This allows privileged actions to be audited and suspicious activity to be handled quickly (e.g., alerting administrators of compromise or disabling a misused administrative account). It makes administrators more accountable for their actions by linking each action to the responsible person and, in turn, deters insider threats.

This technology is also helpful at detecting the use of stolen administrator accounts, such as those compromised by external attackers. This helps identify unusual activity patterns, such as an account being used from an unexpected part of the world at a time of the day when the person associated with the administrator account is usually not working.

Responsibilities for Securing the Application Layer

Securing the application layer is a tough responsibility. There can be numerous vulnerabilities within the application layer, depending on how customized the applications are and how they are configured. These vulnerabilities may be readily exploitable by attackers to breach sensitive data and perform other highly damaging compromises.

Because of the organization-specific composition and configuration of many applications, as well as the highly sensitive nature of the data accessible through these applications, the responsibilities for securing the application layer typically have to be retained by the organization and cannot be handed off to the cloud provider or an MSSP. This is reflected in models of typical public cloud responsibilities, such as the Amazon Web Services (AWS) model.

Consequently, organizations should make sure that the guest OS and access control security controls are well taken care of — either on their own or through qualified partners — so that they can focus their resources on securing the application layer.

Sharing VM security control responsibilities

Each of the three controls are necessary to properly secure the contents of an organization's VMs. Organizations must consider both the initial and ongoing costs associated with selecting, procuring, deploying, integrating, managing and maintaining security controls in each of their VMs across their entire multi-cloud environment.

Many organizations find that the expected savings from moving to the cloud are largely nullified by the cost of establishing and managing a consistent security posture in complex cloud environments.

Fortunately, there is an alternative: the organization can outsource the responsibility for some or most of the VM security controls to cloud providers or MSSPs.

It is often cost-effective for an organization to outsource much of its VM security control management and monitoring.

"Many organizations find that the expected savings from moving to the cloud are largely nullified by the cost of establishing and managing a consistent security posture in complex cloud environments."

24|7 Economies of Scale

These savings are realized due to the economies of scale that cloud providers and MSSPs can achieve, such as having security administrators and analysts monitoring and maintaining all customer VMs on a 24-7 basis and immediately initiating incident response processes when a successful compromise or other critical problem is detected.

Shared Intelligence

Proven secure cloud providers are also extremely knowledgeable about security controls and practices, so they may offer expertise that customer organizations simply do not have.

They can also apply lessons learned from one customer to the entire customer base. One such use case would be identifying a compromise of one VM and using threat intelligence about that compromise to reconfigure VM security controls to prevent similar compromises against other VMs.

Business Objectives

Before outsourcing VM security controls, consider security, business and compliance requirements and objectives. These help define the extent to which the organization can shift its VM security responsibilities through outsourcing and the requirements that the outsourcers must meet, such as how quickly an outsourcer must deploy a critical patch versus a minor patch, respond to security alerts, update threat intelligence feeds, etc.

The organization can then perform evaluations and identify the cloud providers and/or MSSPs that are the best fit for taking over designated VM security responsibilities.

Risk Assessment

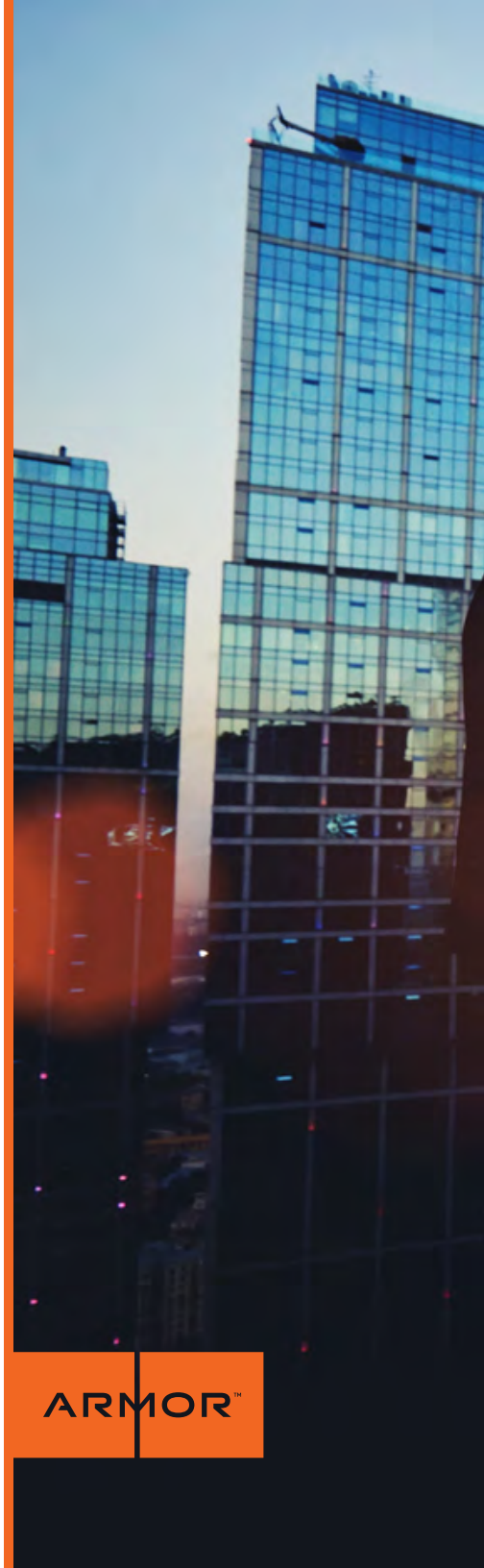
Before outsourcing VM security controls, an organization should do a risk assessment to determine which controls will bring unacceptable risk to the organization if outsourced.

A common example is cryptographic key management. It is generally recommended that encryption keys be stored separately from the data that they encrypt, which means that organizations should avoid storing their encryption keys in the cloud.

Another common control that should be managed on-premise is IAM. Many organizations want to rely on existing enterprise IAM solutions for their cloud applications instead of establishing and maintaining more IAM implementations.

For these reasons, many organizations perform key management and IAM functions in-house, even if they outsource most other VM security controls. Other organizations use their cloud provider or MSSP for key management purposes after establishing clear agreements that define the consequences of unauthorized key usage and specify minimum security controls for protecting access to their keys.

Such an agreement can be an effective form of risk transference. Similar agreements are prudent if an organization is outsourcing IAM to prevent unauthorized use of credentials.



An evolution in data security

As organizations better understand the risks of migrating data and applications to public clouds and the best ways to mitigate those risks, overall reluctance to use cloud technologies continues to decline.

The ever-growing use of clouds indicates that organizations have evolved their data security strategies. It no longer matters where your data, applications and operating systems are located.

What matters is that you implement, manage and maintain the necessary security controls, often with a focus on protecting the confidentiality of sensitive data, across all of your physical and virtual platforms.

Security needs will vary based on platform type, location and function. For example, some VMs may need stronger security than others because the sensitive data they contain is at particularly high risk of compromise and there would be a significant negative impact to the organization should the data be stolen or held for ransom.

Organizations should ensure that the cumulative effect of security controls for each physical or virtual platform is sufficient to reduce risk to an acceptable level.

"The ever-growing use of clouds indicates that organizations have evolved their data security strategies."

Partner with a cloud security expert

Organizations have evolved outsourcing security functions. Many organizations have resisted outsourcing for many reasons, including reluctance to trust an external party with critical operations, sensitive data and other aspects of IT, and concerns over a loss of control over IT.

This attitude has changed, in large part because organizations are striving to streamline their IT operations, save money and focus on their core business. The combination of migrating data and applications to the cloud, and having cloud providers and/or MSSPs manage most aspects of the VMs and respective contents, is now understood to be extremely beneficial in many cases.

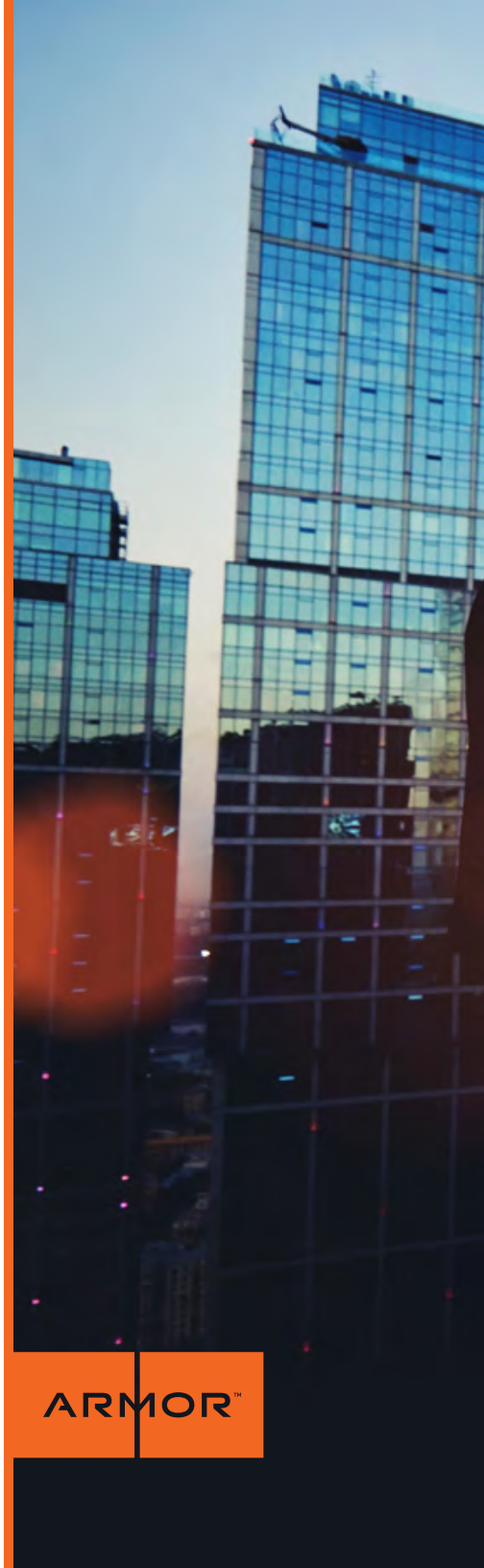
The most efficient arrangement is for an organization to select a single secure cloud provider to manage all of its public cloud VMs, regardless of where each VM is located. Consolidating VM security management across clouds is incredibly helpful at improving efficiency, and it enables the cloud provider to create and maintain a uniform security posture based on consistent sets of security tools across all of the organization's VMs.

It also allows the cloud provider to monitor security across and between VMs, correlating events to detect potential attacks in progress and stopping them quickly to prevent or minimize damage.

Comparing Cloud Vendors

When selecting a cloud provider or MSSP for VM management outsourcing, look for a company that offers the following functions, at a minimum:

- Configuration management
- Patch management or patch monitoring
- Vulnerability scanning
- Hypervisor-level firewall (micro-segmentation)
- Anti-malware (included)
- File integrity monitoring and/or management
- Log and event management
- Privileged session monitoring and auditing
- Threat intelligence
- 24/7 security management



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™
BETWEEN YOU AND THE THREAT