ARMOR™

BETWEEN YOU AND THE THREAT

How to Securely Move to Azure with Armor Anywhere

Microsoft Azure | Armor | Anywhere

Microsoft Azure

Many organizations want to take advantage of Microsoft Azure's Infrastructure as a Service (IaaS) offerings to host their data, applications and operating systems in the cloud. Azure provides incredible flexibility and scalability for its IaaS customers, who can increase or decrease their use of Azure processing, storage, networking and other resources immediately at any time.

There are always security concerns with migration to a new IT product or service. The concerns for cloud computing security are unique for two reasons. One is that your organization's software and data are being hosted on the same physical servers that other organizations are using. The other is that you must give some degree of control over your organization's software and data to the cloud service provider. This is true no matter which cloud service provider you use.

As with many other cloud providers, Microsoft Azure's philosophy is that in an IaaS environment, security responsibilities must be shared between Azure and your organization. While Azure takes care of those security controls that are part of its IaaS infrastructure, other responsibilities such as user access and application security fall onto your organization by default.

Armor | Anywhere

Fortunately, you don't have to handle all of those security controls on your own; you can utilize Armor's service, Armor Anywhere. Armor Anywhere is designed to offload many of your organization's Azure security responsibilities to Armor's battle-proven security controls and experts.

This white paper explains how Armor, Azure and your organization can work together to ensure that your organization's data, applications, and operating systems are securely deployed, monitored and maintained in Azure's IaaS environment.

Partners Sharing Security Responsibilities

The Armor Anywhere solution offers a shared responsibility model for Azure security. This model helps current and potential Azure customers ensure that each security responsibility is performed by the organization best suited for it and that no responsibilities are overlooked or duplicated. Armor, Azure and your organization become partners in securing your organization's use of Azure.

At a high level, the shared responsibility model assigns Azure all responsibilities that universally apply to all of its customers. Examples include restricting physical access to its facilities, restricting logical access to its cloud storage technologies, and safeguarding the hypervisor technologies that customers' virtual machine (VM) instances run on top of.

The division of the remaining responsibilities is simple. Your organization takes on all responsibilities that are specific to your organization. For example, only your organization would know which rights and privileges each of your employees should have for a particular application. No one else could make those decisions.

Also, only your organization should have access to your intellectual property and other sensitive proprietary information. Not only is this a sound security practice, but it's required by various security compliance initiatives and regulations.

This leaves Armor Anywhere to be responsible for security controls that aren't specific to your organization. For example, Armor Anywhere monitors your organization's VM instances to identify missing operating system patches and detect unauthorized changes to critical operating system files.

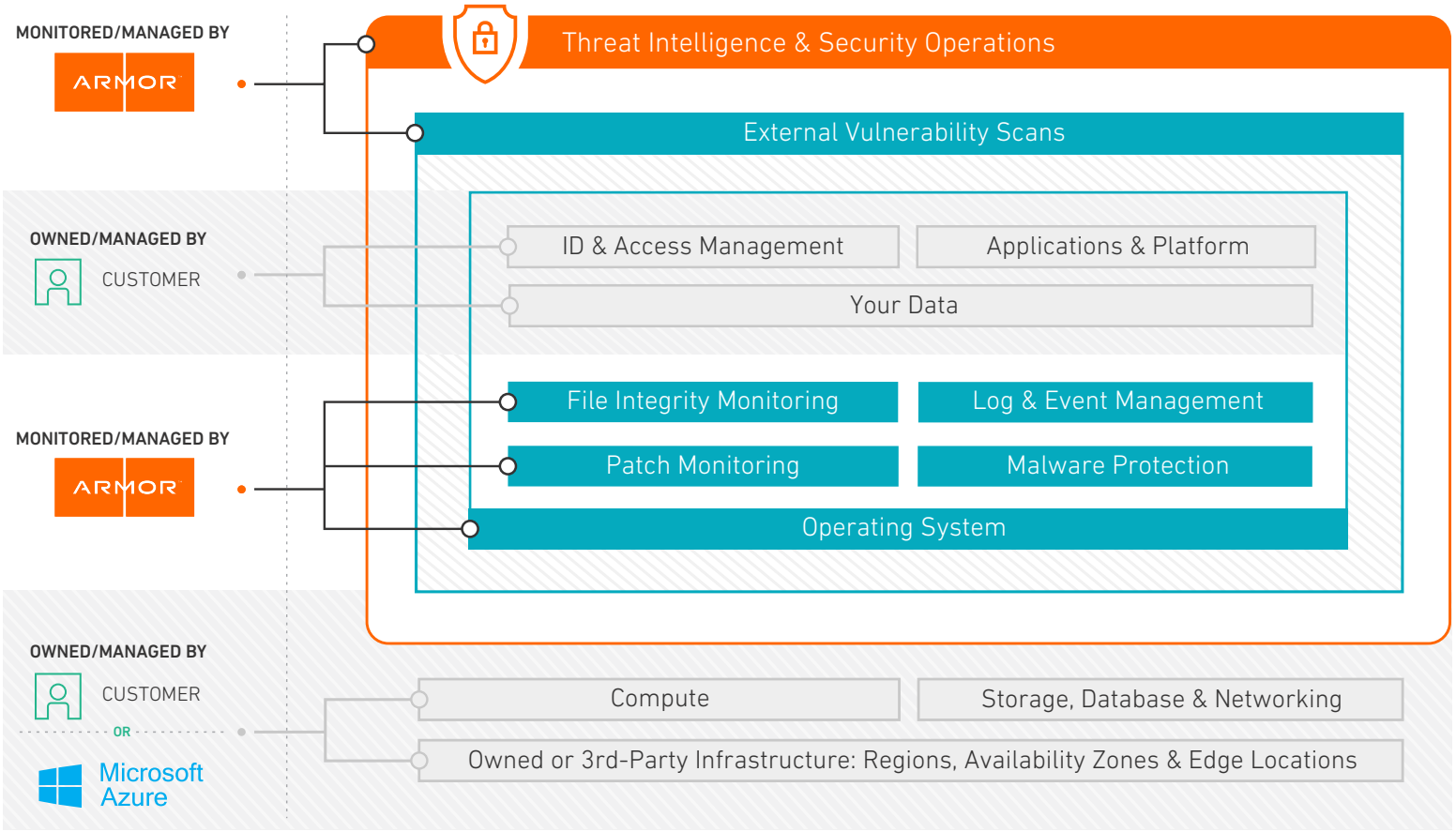
Deploying Armor Anywhere into a new or existing Azure VM instance is easy: all you have to do is install the Armor Anywhere agent. The agent does the rest of the work for you, including the installation and configuration of embedded security services. It fulfills its responsibilities within the operating system, and it securely communicates with Armor's security operations center around the clock. The Armor Management Portal (AMP) provides a single interface for you to monitor the data from the Armor Anywhere agents across all of your Azure VM instances. Using Armor Anywhere as part of your Azure security solution offloads a considerable burden from your organization.

One of the biggest advantages of using Armor Anywhere is that you will know that it is helping to reduce your burden by streamlining management of your security program. This is so important because the alternative could be disastrous. If your organization doesn't notice that critical operating system files have been tampered with, for example, an attacker may have unauthorized access to your Azure VM instance for an extended period of time. That could be the start of a major data breach.

Every organization must practice due diligence when it comes to securing its data, applications, and operating systems. Today organizations are expected to follow sound risk management practices, including the identification and characterization of vulnerabilities and threats, the assessment of the risk posed by those vulnerabilities and threats, and the mitigation of that risk to acceptable levels. Using Armor Anywhere for securing Azure VM instances strongly supports due diligence.

A Closer Look at the Shared Responsibility Model

The graphic shows Armor Anywhere's shared responsibility model for Azure security. It groups the responsibilities into four layers, with the responsible party identified on the left side for each layer. Let's walk through those layers from bottom (cloud infrastructure) to top (security operations center).



Azure Responsibilities

Azure responsibilities for security fall into three categories:

- Physical security. Azure provides a wide range of physical security controls for its facilities, everything from monitoring facility premises with guards, cameras and sensors to restricting who can access the facilities and what each person can access within each facility.
- Network security. Azure enforces a small number of network security controls, but each control is important. One example is the detection and mitigation of distributed denial of service (DDoS attacks, whether these attacks originate from external locations or from an Azure customer's VM instance.
- Virtual infrastructure security. Azure ensures that its virtual infrastructure is strongly secured, because a breach of that infrastructure could allow an attacker to compromise many customer VM instances at once. Responsibilities in this category include managing hypervisor security, such as applying hypervisor patches and maintaining a secure hypervisor configuration, and periodically releasing updated VM images that incorporate the latest patches.

Armor Anywhere Responsibilities inside the VM Instance

In the shared responsibility model, Armor Anywhere takes care of two layers, one supporting security inside the VM and the other supporting security outside the VM. In this particular layer, inside the VM, Armor Anywhere responsibilities are as follows:

- File integrity monitoring. Armor Anywhere monitors the operating system's critical files to identify any changes to those files. Armor uses its data on these changes as one of many sources of information to help draw broader conclusions about the security of your environment.
- Log and event management. Another important responsibility handled by Armor Anywhere is log and event management. Armor Anywhere collects security-related operating system event information from logs, then makes that log information available to your organization through AMP. AMP enables you to view and query the log information for all your Azure VM instances. Armor Anywhere also takes care of log retention duties to ensure that the necessary information is available to support compliance initiative reporting.
- Patch monitoring. Armor Anywhere frequently checks each of your organization's Azure VM instances to identify any missing operating system patches. Your organization is immediately notified of any missing patches, and your staff can use AMP to view the information on missing patches, including which patches are missing for each VM instance and what actions are required for each patch, such as rebooting the operating system after patch installation.
- Managed malware protection. Another feature of Armor Anywhere is that it provides managed malware protection within each of your organization's Azure VM instances. This protection looks for a range of malware attempting to infect the operating systems within the Azure VM instances. If Armor Anywhere finds malware, it will notify Armor experts for follow up with your organization.

Your Organization's Responsibilities

The next layer in the shared responsibility model is your organization's responsibilities. The details of these will be unique for each organization, but at a high level they usually include the following:

- Identity and access management. This involves managing the identities used to authenticate users, administrators, services, devices, and any other entity. In addition, you also need to manage the authentication mechanisms used to verify claimed identities, as well as to use access control lists and other methods of specifying the rights and privileges for each identity.
- Application and platform security. Application and platform security encompasses several security controls, including change management processes for software patches and configuration settings, software vulnerability assessment, and application-specific protection, such as Web application firewalls. Additionally, your organization may need to ensure that only the necessary network connectivity is permitted between your organization's own VM instances, as well as between your organization's VM instances and other organizations' VM instances and systems. The overall goals for application and platform security are to minimize vulnerabilities in the operating system and applications, and to detect and potentially stop attacks attempted against the operating system and applications.
- Data security. The importance of data security is wholly dependent on the sensitivity of the data being stored or processed within your organization's VM instances. If sensitive data is present, examples of possible security controls include storage encryption technologies to safeguard the confidentiality of the data, and data loss prevention (DLP) technologies to identify attempts to inadvertently or intentionally exfiltrate the data. However, even if sensitive data is not present in the traditional sense, there still may be passwords, cryptographic keys, or other system security data that your organization must protect.

Armor Anywhere Responsibilities outside the VM Instance

The outermost layer in the shared responsibility model is handled by Armor Anywhere. Not to be confused with traditional perimeter security, the security controls in this layer essentially wrap around the other security controls sitting on top of the Azure cloud infrastructure. This layer includes the following:

- External vulnerability scans. To complement the vulnerability scans your organization performs from within each VM instance, Armor Anywhere can perform external vulnerability scans. They show you which vulnerabilities are readily visible to external attackers, making them more likely to be targeted, and help your team identify targetable attack vectors and potential mitigations for your environment.
- Managed security operation center services. Armor experts provide security operation services for Armor Anywhere customers around the clock. When they see a major security problem involving your organization that requires a rapid response, they notify you immediately.
- Threat intelligence. Because Armor Anywhere is used to monitor security operations for customers around the world, Armor is always seeing the latest threats and gathering information on them. This threat intelligence, along with threat intelligence collected from many other sources, is then utilized for all Armor Anywhere customers to improve protection and detection capabilities.

Advantages of an Armor-Azure Approach

There are four main advantages of using Armor Anywhere to help secure your organization's new and existing Azure VM instances:

1. You can leverage Azure's capabilities, including its flexibility and scalability, while ensuring that the security of your organization's data, applications, and operating systems are maintained.
2. You can save a great deal of time and effort by using Armor Anywhere agents to handle numerous security monitoring functions, such as log management and malware protection, instead of having to evaluate, select, acquire, deploy, configure, monitor and maintain all of those security controls yourself.
3. When Armor detects a potentially serious security event within one of your Azure VM instances, Armor Anywhere experts quickly analyze the information and contact you if immediate action is needed to safeguard your organization.
4. Armor Anywhere helps your organization achieve a lower total cost of ownership for IaaS cloud usage compared to do-it-yourself security solutions and even other managed security services.

For more information on Armor Anywhere and its partnership with Azure, visit https://www.armor.com/azure/.