IBM Virtual Server Protection for VMware technical overview

Transcript

IBM Virtual Server Protection for VMware technical overview

Introduction

Virtualization brings enormous benefits to the data center: Energy efficiency, performance, and flexibility just to name a few. However, the ultimate success of virtualization is not simply dependent on these factors. Virtualization must also provide these benefits without compromising the overall security of the IT infrastructure. As data centers evolve to dynamic infrastructures, so do the security challenges that IT managers face.

Solving the problem of security in a virtual environment requires a new way of thinking about security, which is why we are introducing IBM Virtual Server Protection for VMware, an integrated threat mitigation solution for your virtual environment.

IBM Virtual Server Protection, or VSP for short, integrates with VMware's VMsafe security framework API to leverage the hypervisor to deliver integrated and optimized security for virtual environments. VMsafe gives IBM VSP complete visibility into your VMs. That means VSP can inspect and block network traffic like an IPS or firewall and also look inside the memory of a running VM to detect more sophisticated attacks like rootkit hooks.

In this technical video, we are going to take a closer look at VSP. We'll show you how it is installed and some of its capabilities. Towards the end of the demo, we'll see VSP actively protecting VMs.

Installation

The VSP VM is packaged and distributed in Open Virtualization Format. The Open Virtualization Format encapsulates the network, memory and hard disk settings for the VM. Installation is a simple matter of deploying the IBM VSP virtual machine into the ESX server you want to protect.

After deployment is complete, the VM is powered on. The first time you login, you will be taken through a configuration wizard to set up the VM. The wizard steps you through setting new passwords, hostname, networking and ESX information required for communication between VSP and the hypervisor.

The last step of the installation is registering VSP with SiteProtector. SiteProtector enables centralized policy management, monitoring, event analysis and reporting. Designed for simplicity and flexibility, SiteProtector provides centralized management for VSP and the full suite of IBM Internet Security System products.

Policies

Let's use SiteProtector to take a look at some of the capabilities of VSP.

When we first login to SiteProtector, we are presented with a security dashboard summary that shows the health of our devices as well as summary information about events. We'll switch to the policy tab to take a closer look at the policies that define the behavior for VSP.

We'll start with the **Asset Settings** policy - it specifies which VMs you want to protect with VSP. When a VM comes online that is within the protection scope, VSP automatically discovers the VM and begins protecting it.

This is also where the global Network monitoring and intrusion response settings are set.

The **Firewall** policy in VSP works like most firewalls: you define what traffic you want to permit, block or monitor. We only have a few rules defined here for simplicities sake. Let's look at one of the active rules. The firewall rule takes advantage of a powerful feature unique to VSP called Virtual Objects. Virtual Objects allow you to define arbitrary groupings of machines to simplify policy creation. Once you're defined a virtual object, you can use it in any of your policies. For example, here we are using the “Web Servers” virtual object as a shortcut to explicitly specifying each web server individually. We'll see Virtual Object used throughout our policies.

Network Access Control defines which VMs get access to the virtual network. Here we've defined four groups of machines (using virtual objects) that have access to the network. Machines that are not explicitly permitted access to the network can still be given some access using the “access control for quarantined assets” tab. Network Access Control can be used to combat virtual server sprawl by acting as a gatekeeper to the network while the security group verifies the security posture of a new virtual machine.

Using the **VM Events** policy, you can closely monitor VM infrastructure events such as VM creation, power on, power off, registration and removal. This feature provides important oversight of virtual machine lifecycle events that can negatively impact the security posture of the virtual network.
The **Anti-Rootkit** introduces a new concept in security, pioneered by IBM research. The anti-rootkit policy allows inspection of critical guest operating system data structures using memory introspection. If the monitored data structures are modified by known rootkits, VSP will generate an event. This feature augments existing host-based anti-virus software by watching for rootkit behavior at a higher privilege level – outside of the guest OS. This makes the anti-rootkit feature resistant to a common malware technique of disabling host-based anti-virus agents upon execution.

Lastly, we'll take a look at the **Security Events** policy. This policy is used to configure VSP's intrusion prevention engine, known as the Protocol Analysis Module or PAM for short. PAM is backed by the world-renowned X-Force research and development team. The X-Force team is one of the of the oldest and best-known commercial security research groups in the world.
This security policy is composed of thousands of signatures that detect and optionally block security threats.

Analysis
Now let's switch to the analysis tab and look at a sampling of some security events.
This view is already set up to just show us events detected by VSP. The filtering and sorting capabilities of the analysis view make it easy to focus in on the specific events you are interested in.
The Tag Name column shows a short description of the event and the status column shows us how VSP responded to the event. This sampling of events shows some SQL injection attacks, some Cross site scripting attacks, and a variety of other interesting events. Let's look at a few of these more closely.
This event from the anti-rootkit engine has detected an attempt to modify the System Service Dispatch Table on the Win-XP-CHI VM. The System Service Dispatch Table is a critical Operating System structure and its integrity is paramount to a secure system. There is a good chance that this VM has been compromised so before it causes any trouble, we will power it off. We could also use the Network Access Control policy to ban the VM from the network in case it gets powered on again.
Going back to the events list, we see a couple of events that show some potentially sensitive personal information has been sent through the network. VSP can detect sensitive data like credit card numbers, addresses, and phone numbers. The event details show that the sensitive data was sent out in a file via email.
Our event list also shows a few events that report status changes in our monitored VMs. These are mainly informational but can be quite helpful when investigating an incident. Also, as with all events in SiteProtector, you can configure a response rule to send an email or an SNMP trap if you want to monitor the event more closely.
Here we have a couple of SQL injection attacks. Looking at the details of the event, we can see that the target of the attacks was 10.155.0.22, which is our web server. Drilling down even further shows us that someone tried to use one of the classic SQL injection attacks.

Let's use the filter capabilities to see what other events have targeted our Web server.

The **Encrypted Session Policy Abuse** event is an interesting one. It alerts us to encrypted traffic on a non-standard port. In this case port 2222 is being used as an SSH target on our web server. This is suspicious because port 2222 should not be open or used on this server and the event could be an indication of a malicious backdoor. Since this is our web server, we can't shut down it down right now so we'll create a firewall rule to block access to port 2222 on our web servers until the security team can do further analysis.
Once the new rule is created, we deploy it. The deployment affects all of the individual VSP appliances to ensure that the same policy is used everywhere. This is important when the environment allows VMs to be migrated between ESX servers. Maintaining consistent policies across the VSPs keeps a virtual machine's security policy persistent as it moves.

Summary/ Conclusion
IBM encourages clients to take a defense-in-depth approach to enterprise security. The Virtual Server Protection for VMware solution provides dynamic protection for every layer of your virtual infrastructure

and helps you meet regulatory compliance by providing customized security reporting for your Virtual Infrastructure.

For more information, please visit **ibm.com/security**