AGENTLESS VIRTUAL PATCHING

Optimizing Protection and Performance with VMware and Trend Micro

The Patch Management Challenge

Today's enterprises are bombarded with a constant stream of vulnerabilities with nearly seven critical patches are released every day. This seemingly never-ending cycle of patching consumes excessive time and IT budget. And still it is virtually impossible to stay current with patches. One third of enterprises revealed in a recent survey that they devote an inordinate amount of time and staff resources to patch management—the highest across all IT security tasks listed. Yet only 22% found their patch management to be very effective[1].

Worse yet, virtualization only compounds your security challenges: using traditional approaches to patch in virtual environments can impact both protection and performance. However, using agentless security for virtual patching will complement existing patch management processes by shielding known and potential vulnerabilities without negatively impacting the performance of virtual environments.

Where are you most vulnerable?

Enterprises need to shield known and unknown vulnerabilities in a broad range of critical applications and systems.

- Enterprise Applications: Each year thousands of critical software flaw vulnerabilities are reported in operating systems, databases, servers, and other applications. Patching these vulnerabilities can be disruptive. And even when a patch is available, it can take weeks or even months before the patch can be fully deployed.
- Legacy Web Applications: The majority of records that are breached are the result of SQL Injection attacks on web applications, which are inherently open and accessible to attackers Perimeter security won't shield these systems and it can be difficult to locate and assign the custom development resources necessary to fix the code.
- Unsupported Operating Systems and Applications: Patches are no longer developed or issued for older operating systems and applications that have reached their end-of-life. Often, virtual patching is the only cost-effective way to ensure continued protection for these and other unsupported systems.
- Locked-down Systems: Mission critical systems involved in day-to-day operations requiring 24x7 up time cannot be patched due to company revenue impact or productivity loss.

Why this impacts virtual environments?

Virtualized desktops and data centers should be shielded by the same levels of virtual patching as their physical counterparts. However, traditional agent-based solutions that are not architected for virtualization can result in a number of significant operational security issues.

- Resource consumption: Even when idle, traditional security agents for security such as virtual patching occupy a significant amount of memory in each virtual machine (VM), especially when multiple security agents are installed on each machine to provide a range of protection. This reduces consolidation ratios and increases CAPEX and OPEX.
- Network degradation: Traditional security products are inefficient in virtual environments, since all inter-VM traffic must be piped to a central appliance to scan. This redirection of network traffic creates potential compliance issues, network performance, and overall congestion.
- Instant-on gaps: When VMs are activated and inactivated in rapid cycles, it is difficult to consistently patch those virtual machines and keep them up to date. Dormant VMs that have not been patched can introduce massive security vulnerabilities when powered on.
- Operational overhead: Administrators need to ensure that new VMs have received all the latest patches. Maintaining consistent patching as VMs move around or change state can be extremely time consuming and still result in security gaps.

Agentless Virtual Patching Benefits

Together VMware and Trend Micro provide agentless vulnerability shielding for virtualized data centers, while delivering:

- Higher consolidation by offloading virtual patching from individual VMs to a single security virtual appliance on each vSphere host.
- Faster performance by neutralizing security storms and resource contention from simultaneous patching.
- Better manageability by eliminating agents for virtual patching and the need to configure and update each one.
- Stronger security by providing instant-on protection for new VMs coordinated by the dedicated security appliance.

Agentless virtual patching shields vulnerabilities without impacting performance

VMware and Trend Micro have partnered to deliver agentless security that enables virtual patching on virtualized desktops and data centers. The joint solution minimizes impact on VM performance and reduces contention issues by leveraging two mutually dependent solutions:

- **VMware vSphere** optimizes security by offloading traditional per VM agent-based security processing to dedicated, per host, security-hardened virtual machines delivered by VMware partners.
- **Trend Micro™ Deep Security** provides a security-hardened virtual machine that integrates with VMware APIs to offer agentless virtual patching (and additional agentless security capabilities) for VMware virtual machines.

Trend Micro Deep Security

Trend Micro Deep Security shields vulnerabilities in critical systems until a patch is available and deployed or in place of a future patch that may never materialize. Deep Security can be deployed as a single virtual appliance on a VMware ESX server to provide agentless protection for guest VMs. With agentless virtual patching for VMware VMs, you get a timely, cost-effective complement to traditional patching processes that can significantly lower costs, reduce disruptions, and give you greater control over the scheduling of patches. Plus your mission-critical enterprise systems and applications stay better protected against data breaches and you reduce compliance costs.

VMware vSphere

VMware vSphere helps to offload key security functions such as virtual patching to a dedicated security appliance, eliminating the security agent footprint in virtual machines. This advanced architecture frees up system resources, improves performance, and eliminates the risk of security "storms".

With a hardened tamperproof security virtual appliance provided by Trend Micro, vSphere uses robust and secure hypervisor introspection capabilities to prevent compromise of the protection capabilities. Demonstrating compliance and satisfying auditor requirements are enabled through detailed logging of activity from the security service.

How agentless virtual patching works

1. VMware vCloud Networking and Security enables agentless VM introspection, monitoring current, new, and reactivated VMs to ensure up-to-date security from the latest vulnerabilities.
2. VMware vCloud Networking and Security enables Trend Micro Deep Security to communicate with the guest VMs to implement virtual patches.
3. Trend Micro Deep Security uses a dedicated, security-hardened virtual appliance that integrates with the VMware vShield APIs to provide agentless security.
4. Together, this approach allows vulnerabilities to be shielded without deploying in-guest security agents.

> "Deep Security protects our healthcare system by proactively shielding vulnerabilities in Electronic Health Record web applications and operating systems from targeted attacks until patches can be deployed."

Bill Gillis,
Beth Israel Deaconess Medical Center

Agentless Virtual Patching Features

- Intrusion Detection and Prevention (IDS/IPS) rules shield known vulnerabilities—for example those disclosed on Microsoft Tuesday—from being exploited, with out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. In addition, IDS/IPS rules also provide zero-day protection for known vulnerabilities that have not been issued a patch, and unknown vulnerabilities.
- Recommendation Scanning streamlines security update management and makes patching even easier by automatically recommending which rules need to be deployed to protect a given system. Deep Security scans the system to identify which IDS/IPS rules need to be deployed to optimize protection—based on the OS version, service pack, patch level, and installed applications. In addition, as the server environment changes and patches are deployed, Deep Security automatically recommends which rules can be removed to minimize resource impact.
- Enterprise-grade, bi-directional, and stateful firewall allows communications over ports and protocols necessary for correct server operation, and blocks all other ports and protocols. This reduces the risk of unauthorized access to the server.
- Web application protection rules defend against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities, shielding these vulnerabilities until code fixes are completed.
- Inter-VM protection leverages a single virtual appliance to provide host-based based protection to multiple VMs. This gives you the ability to monitor inter-VM traffic without losing the ability to specify policies per VM.
- Security updates from a dedicated team of security experts ensure the latest protection by continuously monitoring multiple sources of vulnerability disclosure information to identify and correlate new relevant threats and vulnerabilities. Trend Micro also participates in the Microsoft Active Protections Program to anticipate emerging threats and provide more timely protection.
- Protection for physical, virtualized and cloud computing environments ensures that vulnerabilities are shielded, no matter how the hosts are deployed. In addition to providing guest-based protection, Deep Security leverages VMware APIs to provide virtualization-aware protection, maximizing deployment flexibility.

Choose the Right Solution for Vulnerability Shielding

VMware has developed strong APIs to improve security. And Trend Micro is a leader providing virtual patching solutions. With a leading virtualization platform and security that fits your enterprise, VMware and Trend Micro have partnered to help you maximize protection while minimizing complexity. For more information, please visit www.trendmicro.com/virtualpatching

TREND MICRO™

Securing Your Journey to the Cloud