LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.
The patch management issues listed in this cloud security primer continue to weaken enterprise security. In a 2012 security survey, over half perceive their patch managements’ success as only “fair” or “minimal.”

This security challenge is further compounded by the increasing volume of significant attacks in organizations. In the first quarter of 2013, multiple zero-day exploits plagued widely used applications, such as Java, Internet Explorer, Adobe Reader, Acrobat, and Flash Player.

To mitigate patching issues and prevent potential high-impact attacks, organizations must deploy security solutions with effective virtual patching feature. It is then mandatory to understand how virtual patching works.

**COMMON PATCH MANAGEMENT ISSUES:**

- No available patch
- Out-of-support and unpatchable systems and applications
- Frequent patch cycles and emergency patching
- Business continuity interruptions
- Rollbacks and intentional delays

**What is Virtual Patching?**

Virtual patching or vulnerability shielding provides the functionality of a software patch by creating protective network policies based on internal and external resources.

This is done to “virtually” mend a discovered vulnerability and prevent it from being exploited while waiting for the vendor’s patch to be released.

It works on the premise that exploits take an identifiable network path to and from an application to use vulnerabilities, making it possible to manipulate and protect the network through rules.

---

An effective virtual patching solution controls communications in targeted software through the following technologies:

**Intrusion Detection and Prevention (IDS/IPS)**

To protect unpatched network-facing system resources and enterprise applications and servers, this technology leverages smart rules and out-of-the-box vulnerability protection.

Self-learning rules and comprehensive network behavior analysis makes it possible to:

- Provide zero-day protection for known vulnerabilities that have not been issued a patch
- Block unknown vulnerabilities by examining all incoming and outgoing traffic for protocol deviations, policy violations, and attack signals
- Defend against SQL injection, cross-site scripting, and other web application vulnerabilities

**Multilayered Firewall**

To detect threats deep in a network and prevent denial-of-service attacks, virtual patching leverages an enterprise-grade, bi-directional stateful firewall that does the following:

- Decrease attacks in the physical, cloud, and virtual servers with fine-grained filtering, design policies per network, and location awareness for all IP-based protocols and frame types
- Detect reconnaissance scans

**Recommendation Scanning**

This tool automatically recommends which rules need to be deployed to optimize protection based on the OS version, service pack, patch level, and installed applications as well as which rules can be removed to minimize resource utilization.

Virtual patching can either be integrated to traditional patch management solutions to protect critical systems until a patch can be deployed, or be a permanent shield for out-of-support and unpatchable systems.
Virtual Patching Responsiveness

One of the major issues with patching is the significant delay between the time when a patch is released and when a patch is deployed across pertinent systems. Virtual patching protects an organization during this vulnerable period. It prevents possible exploits while waiting for the patch to be deployed in affected systems.

The table and figure below shows how solutions with virtual patching capability, such as Trend Micro™ Deep Security, protects an organization against possible exploits and known vulnerabilities:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Impact</th>
<th>Date discovered</th>
<th>Deep Security rule release</th>
<th>Vendor patch</th>
<th>Number of days customers are protected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Critical Vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2012-1889: XML Core Services</td>
<td>CVSS Severity: 9.3 (HIGH)</td>
<td>06/12/2012</td>
<td>06/12/2012.Rule Identifier: 1005061</td>
<td>07/10/2012</td>
<td>29</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>System level access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Oracle Critical Vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-0422: Oracle Java 7 Vulnerability</td>
<td>CVSS Severity: 10.0 (HIGH)</td>
<td>01/10/2013</td>
<td>01/11/2013. Rule Identifier: 1004711</td>
<td>01/13/2013</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Used in Blackhole Exploit Kit (BHEK) and Cool Exploit Kit (CEK)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ruby on Rails Critical Vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-0156: Ruby on Rails Vulnerability</td>
<td>CVSS Severity: 7.5 (HIGH)</td>
<td>01/09/2013</td>
<td>01/09/2013. Rule identifiers: 1005326, 1005331, and 1005332</td>
<td>01/13/2013</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>- Data breach</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Denial of service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Access privilege elevation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ATTACKER

New vulnerability is discovered; security researchers publish exploit codes.

Solutions with virtual patching block target ports to bypass exploits.

PORTS

Solutions with virtual patching automatically apply protective network rules to prevent exploits to known vulnerability while waiting for the vendor’s patch to be released.

**VIRTUAL PATCHING IN MIXED ENVIRONMENTS: HOW IT WORKS TO PROTECT YOU**
Maximizing the Benefits of Virtual Patching

Virtual patching enables organizations to manage complex patch and vulnerability challenges despite on-going infrastructure changes brought by virtualization and cloud adoption. It also addresses the challenge of having a continuous influx of high-profile vulnerabilities and critical updates week after week.

A virtual patching system may be optimized by including additional protection to the following:

- Network resources
- Cloud components
- Virtual and physical servers
- Endpoints

By utilizing virtual patching as a complement to standard patching, organizations can not only mitigate exploits but also deal with operational and financial problems related to standard patching.
TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years’ experience, we deliver top-ranked client, server and cloud-based security that fits our customers’ and partners’ needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.