RS

Rimini Protect™

Rimini Protect™ for VMware

> *"To put it simply—yes. We have seen anywhere between 3X to 8X to 10X changes in pricing,"* Woo told CRN. *"The per-core charging is another way of masking that you are also responsible for paying for a lot of shelfware given their product SKU simplification."*
>
> ———
>
> TRACEY WOO
> Forrester Principal Analyst[2]

Many organizations rely on VMware software as a crucial component of their infrastructure. However, recent changes in Broadcom's licensing model to subscriptions have led to significant increases in associated annual fees[1].

As a result, organizations are turning to Rimini Street for industry-leading support and proactive security services and solutions, regardless of their VMware version.

The Business Challenge

On April 15, 2024, Broadcom announced that VMware will complete its transition from a perpetual license owned by a client to a subscription-based VMware license model, providing access to the most recent version and support for a fixed term. Broadcom also confirmed in their announcement:

> "It is important to emphasize that nothing about the transition to subscription pricing affects our customers' ability to use their existing perpetual licenses."[3]

For those customers choosing not to sign up for subscription support offerings from Broadcom, the company has announced free access to "zero-day" security patches for supported versions of vSphere (7.x and 8.x). Broadcom defines zero-day security patches as. "…a patch or workaround for Critical Severity Security Alerts with a Common Vulnerability Scoring System (CVSS) score greater than or equal to 9.0."[4] While the availability of some security patches provides some reassurance for clients, patches for "high" severity levels (CVSS score 7.0-8.9) may not be available.[5]

[1]ComputerWeekly.com <u>"What are the options when migrating from VMware?"</u>

[2]CRN <u>"Broadcom Price Hikes And Partner Snubs Fueling Scale Computing's Record Growth, CEO Jeff Ready Says"</u>

[3]Broadcom <u>"A changing market landscape requires constant evolution: our mission for VMware customers"</u>

[4]Broadcom <u>"Zero Day (i.e., Critical) Security Patches for vSphere (7.x and 8.x) Perpetual License Customers with Expired Support Contracts"</u>

[5]First.org <u>"Common Vulnerability Scoring System v3.1: Specification Document (Section 5)"</u>

Rimini Street®

The Rimini Street Solution

Our proactive solutions allow us to mitigate vulnerabilities and weaknesses both within and beyond Broadcom's scope.

**Security Advisory Services and Threat Intelligence Services
(Included with Rimini Support™)**

Our services include conducting a security assessment for the client to analyze the security risk posture of the client's unique enterprise ecosystem. Threat intelligence reports and hardening guidance are then leveraged to help improve a client's security posture. We also publish off-cycle zero-day advisories which include mitigation strategies, direct mitigations, and information regarding our security solutions' ability to provide protection against exploits.

Note: Occasionally, Broadcom may suggest from their perspective that there are no workarounds for a given vulnerability as a part of their security advisory. As an example, in Broadcom Advisory VMSA-2024-0012, it was reported that there were no workarounds for vulnerability CVE-2024-37081. However, Rimini Street issued a threat intelligence report with mitigation options, including configuration changes that fully mitigate this vulnerability and others as well.

Our clients also benefit from the ability to raise security cases with our team using the same industry-leading support process and SLAs as Rimini Support, including:

› 10-minute guaranteed response time for P1 critical issues

› Frequent cadence of update communications for every case

› Root-cause analysis to help prevent future issues

Rimini Protect™ Security Solutions

Our security team is continuously assessing new techniques and solutions to help enhance our clients' security postures, specifically ecosystems that include VMware. Our solutions can protect against weaknesses in databases, applications, and network connections. Solutions securing hypervisors are also available through our innovative vendor-network.

Depending on the client's environment, Rimini Street's security solutions may be recommended to help address remaining or residual risks including:

RIMINI PROTECT™ APPLICATION RUNTIME SECURITY
Embedded into the runtime of applications and middleware, our application runtime security solution provides security at the Common Weakness Enumeration level within the application code, protecting against entire classes/ categories of vulnerabilities such as request forgery, cross-site scripting, and even remote code execution flaws such as insecure deserialization, even in custom code.

RIMINI PROTECT™ APPLICATION RISK MITIGATION
Fully managed service providing shields that mitigate your applications' vulnerabilities (Advanced WAF and Shielding) at speed without touching a line of code, which helps protect your environment from sophisticated attacks.

ADVANCED DATABASE SECURITY
Interactive zero-day and virtual patching security solution that works through in-memory database activity monitoring, protecting commonly used open-source and commercial databases that are not fully supported.

HYPERVISORS
We engage an innovative vendor that can help provide our clients with zero-day security protection specifically designed to defend against ransomware and other common malware-based attacks targeting Linux-based hypervisors. Lockdown rules employed with this zero-day security protection are designed to prevent the exploitation of "Escape to Host" attacks and known existing categories of weaknesses commonly found in hypervisor technology.

Rimini Street's security solutions can also be offered as fully managed services, providing Rimini Street clients with **optimal protection and cost-effective solutions.**

Rimini Street®