

Enterprise Vulnerability Management (Retina CS and Retina Network Security Scanner) End of Life Announcement

Notification Date: December 31, 2019
Reminder Dates: January 31, 2020 & March 31, 2020

This document serves as the official announcement for the end-of-sale and end-of-life for BeyondTrust Enterprise Vulnerability Management formerly Retina CS and Retina Network Security Scanner (all versions). This statement discontinues the software availability, and supportable usage of the products as of the dates indicated. Please read this document carefully, as it contains important information on future support.

Summary

Effective **December 31, 2019**, BeyondTrust will not accept new orders for BeyondTrust Enterprise Vulnerability Management formerly Retina CS and Retina Network Security Scanner (all versions).

Effective **December 31, 2020**, BeyondTrust will no longer provide upgrades, enhancements, maintenance or support for BeyondTrust Enterprise Vulnerability Management formerly Retina CS and Retina Network Security Scanner (all versions).

Key Dates

End of Sale Date:	December 31, 2019
Last Date to Renew:	June 30, 2020*
End of Life Date:	December 31, 2020 for existing customers under current maintenance contracts.

* Maintenance renewals can only be extended until December 31, 2020.

Intended Audience(s)

This announcement is intended for customers with:

- Retina CS (RCS)
- Retina Network Security Scanner (RNSS)
- Retina Host Security Scanner (RHSS)
- Retina Standalone Security Scanner (RSSS)
- BeyondTrust Network Security Scanner (BNSS)
- BeyondTrust Enterprise Vulnerability Management (EVM)
- BeyondTrust Host Security Scanner (BHSS)

Replacement Product(s)

BeyondTrust will not offer a replacement product for Enterprise Vulnerability Management and Retina products. However, we are recommending customers work with our strategic partner Tenable, Inc. (www.tenable.com) to acquire vulnerability management services as described below.

Renewals

BeyondTrust will offer pro-rated maintenance renewals until the end of life date: December 31, 2020. (Last date to renew is June 30, 2020.)

Migration

After careful consideration, we have selected Tenable to be our exclusive, strategic partner for customers currently using BeyondTrust's Vulnerability Management Suite. Tenable was recently named the market leader in the 2019 Forrester Wave for Vulnerability Risk Management, ranking highest in both Strategy and Current Offerings.

Tenable has a proven track record of product innovation in vulnerability management and extensive investment in vulnerability research. We are confident Tenable is the best go-forward partner for BeyondTrust Vulnerability Management Suite customers. Tenable has also created attractive incentives for transitioning BeyondTrust customers.

For more information, please contact Tenable directly at beyondtrust@tenable.com or go to <https://www.tenable.com/try> to start your 30-day free trial today. You can also view a recorded Tenable-BeyondTrust webinar for VM customers here:

<https://lookbook.tenable.com/beyondtrust-to-tenable-transition-resources/od-webinar-tenable-for-beyondtrust-customers>

Support

Standard BeyondTrust Support End of Life policy applies. BeyondTrust will support the Vulnerability Management (Retina) products until December 31, 2020 for customers under active maintenance contracts. Extended support past that date is not available for this product.

FREQUENTLY ASKED QUESTIONS (FAQs) – Updated Jan 31, 2020

1. Why is BeyondTrust making this decision?

As all product companies in dynamic markets do, BeyondTrust regularly reviews its product portfolio to ensure strategic, market, and business alignment. Our Vulnerability Management offering is not core to our leadership in the Privileged Access Management (PAM) segment; therefore, we are exiting the business and

recommending customers take advantage of an attractive alternative through our strategic partnership with Tenable.

2. What do I need to do now?

Customers whose maintenance contracts renew prior to April 1, 2020 should consider renewing or extending their maintenance agreement with BeyondTrust to ensure continued support, unless you are able to quickly acquire and deploy an appropriate solution from Tenable. All interested customers should contact Tenable directly to discuss solution alternatives.

3. What if I don't do anything?

BeyondTrust licenses are perpetual, and existing environments will continue to operate beyond the end of life period. However, BeyondTrust will not provide updated vulnerability audit signatures, support or maintenance for any BeyondTrust products operating after the end of life date, so the value of the product will decline quickly once it is unsupported. It's critical that customers move to an alternative platform to avoid an interruption in vulnerability scanning.

4. Can I still renew my maintenance and support?

BeyondTrust will accept maintenance renewal orders through June 30, 2020, but not after that point. Maintenance contracts must end by December 31, 2020.

5. Is it possible to extend support beyond the end of life date?

No. Extended support cannot be offered beyond the end of life date.

6. I purchased maintenance and support for a period extending after 12/31/2020, can I get a refund or credit for that period?

Yes, you may request a refund for the period of maintenance and support for which you have pre-paid, which extends beyond 12/31/2020. Alternatively BeyondTrust will provide a credit for the purchase of other BeyondTrust products or services, or for Tenable's vulnerability management solutions. Please contact your account representative in either case.

7. Will Tenable provide any migration support or tools to help me move to their solutions?

Yes – Tenable is offering their QuickStart professional services package to assist BeyondTrust EVM/Retina customers at a discount of 35% off of their list price. In addition, BeyondTrust is supporting Tenable in the development of a migration tool for scan job configurations; please stay tuned for more information as it becomes available.

8. Is Tenable offering special discounts for BeyondTrust customers?

Yes – Tenable is offering discounts on their products based on each customer's particular situation. In addition, they are offering discounts off of professional services (see above) and 75% discounts off of instructor-led training.

9. How can I get more detailed information about this EOL and Tenable's solutions?

Please watch the recording of the joint Tenable-BeyondTrust webinar delivered on January 28, 2020, here:

<https://lookbook.tenable.com/beyondtrust-to-tenable-transition-resources/od-webinar-tenable-for-beyondtrust-customers>

10. What happens to EVM/Retina on January 1, 2021? Will it stop working?

No – the product will continue to operate (scan, generate reports, etc.). However, we will no longer be providing new vulnerability audit checks, bug fixes, or new features, so the value of the solution will diminish rapidly at that point.

11. How does the EVM/Retina EOL affect the discovery scanning feature in Password Safe?

There will be no change to our discovery capabilities. While BeyondTrust is exiting the VMS business, we are not EOL'ing the discovery scanning capabilities used in our PAM products. BeyondTrust is maintaining ownership and use (for discovery) of our VMS intellectual property.

12. What if I am a PowerBroker for Windows (PBW) customer using Vulnerability Based Application Management (VBAM) rules?

Due to BeyondTrust exiting the Vulnerability Management business, the VBAM feature in PBW will no longer be supported with the EOL of EVM/Retina. While the feature will still exist within the product, the vulnerability audits (signatures) will no longer be updated after December 31, 2020.

13. Whom do I contact with questions?

Please contact your sales representative or sales@beyondtrust.com for any questions. For support related inquiries, please contact [BeyondTrust Support](#). For any questions about Tenable's offerings or pricing, contact Tenable at: Beyondtrust@tenable.com or visit <https://www.tenable.com/beyondtrust>.