



# RSA NETWITNESS® PLATFORM CUSTOMER NEWSLETTER



April 2019: Issue 1

Latest RSA NetWitness Version:

[V11.2.1.1](#)

V11.1 Latest Version:

[V11.1.0.3](#)

V10.6 Latest Version:

[V10.6.6](#)



[NW Community](#)



[NW Working  
Groups](#)



[RSA Ready](#)



[NW Knowledge  
Base](#)



[RSA University](#)



[Customer Sup-  
port](#)



[RSA Ideas  
\(Enhancements\)](#)

## Recent RSA Link Content

### Recent Blogs:

- [RSA NetWitness Packet Meta in ELK](#)
- [Using RSA NetWitness to Detect Command and Control: PoshC2 Hex Encoded Executables](#)
- [What's on your wire: The curious case of ICMP Tunneling](#)
- [Custom TCP Shell and Mobile Messaging Apps](#)
- [Web Shells and RSA NetWitness Part 3](#)
- [RSA NetWitness Storage Retention Script](#)

View more blogs [here](#).

### Recent KB Articles:

- [000037185 - RSA NetWitness 11.x /var/log mount is full...](#)
- [000035892 - Requesting updates to the Geo IP data...](#)
- [000035088 - How to Uninstall Windows Legacy...](#)

### Recent RSA NetWitness Ideas:

- [Dynamic or drop-down list value in Edit Event Group...](#)
- [Add to Investigation Timeline](#)
- [EPS Report](#)

## RSA NetWitness Product Support Lifecycle

Going forward, RSA NetWitness will follow an N-1 product support methodology where N represents the current major software release. The RSA NetWitness product lifecycle support chart found [here](#) contains all of the version information, upgrade paths, hardware support, and more.

Please be aware of the following End of Primary Support (EOPS) dates:

Product	Version	EOPS Date
RSA NetWitness Logs & Network	11.2	TBD
RSA NetWitness Logs & Network	11.1	Jul 2019
RSA NetWitness Logs & Network	11.0	Dec 2018
RSA Security Analytics	10.6	Oct 2019

There are many reasons to upgrade from v10.6.x to v11. [This infographic](#) shares a few of those highlights.

## RSA NetWitness Version 11.3 Was Announced at RSA Conference! GA is Planned for the 2nd Week of April!

RSA NetWitness v11.3 brings many new capabilities and enhancements. Below are the [top 3](#).

- RSA NetWitness Endpoint is fully integrated into the platform!** RSA NetWitness is the only fully native endpoint detection and response solution within an evolved SIEM, to equip security analysts with industry-leading detection, investigation, and incident response capabilities.
- RSA NetWitness UEBA models based on deep endpoint process data** collected by RSA's EDR Solution, RSA NetWitness Endpoint. This advanced analytics capability can rapidly detect anomalies in user's behavior and uncover unknown, abnormal, and complex evolving threats that will be otherwise missed by analyzing logs alone.
- RSA NetWitness Platform now fuels **threat-aware authentication** to enable continuous authentication and the ability to block insider threats and malicious actors in the act of an attack while reducing the time and effort by overworked security operations teams.

## Please Do Not Open a Case Using Email

Your experience with our products and services are important to us and we want you to have the best experience possible. One area where you can help us help you is by not opening up a support case via email. Data shows us that cases opened through email, on average, take significantly longer to resolve. Cases opened through phone calls are able to be resolved quicker, but cases opened through RSA Link have, by far, the fastest resolution times. The preferred method of creating a case is through [RSA Link](#).

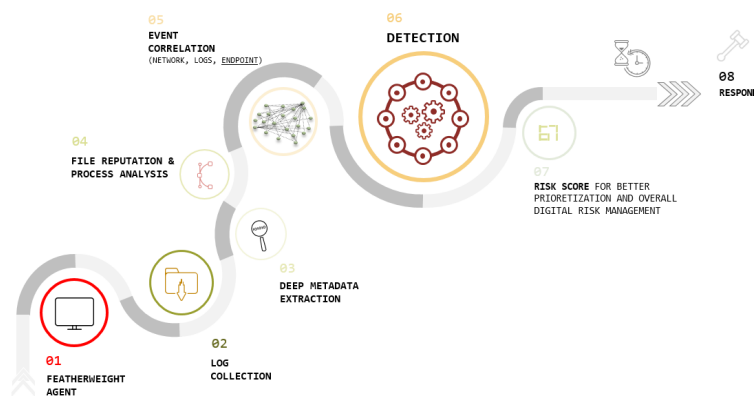
## Sneak Peek Into V11.3—Fully Integrated Endpoint Detection & Response

Here's a preview of a new feature coming in version 11.3.

**Endpoint Detection and Response** is now **fully integrated** with the rest of the RSA NetWitness Platform to provide one complete security analytics platform which provides unparalleled visibility and a seamless security analyst hunting experience.

This feature provides:

- Enhanced visibility across hosts and user interactions
- Forensics-enabled metadata gathering to inspect the entire compromise chain
- Defense in-depth on the endpoint



## 3 Month Trial Designated Support Engineer (DSE)

Did you know about the new 3 month trial DSE premium service offering from Customer Support? A Designated Support Engineer is a highly technical support engineer who gets assigned to you and becomes your single point of contact for all RSA NetWitness problem resolution. Instead of creating a case and working with a randomly assigned technical support engineer, you will work with the same engineer on every single case you open. This will save you time and effort because in only a short amount of time, your DSE will become intimately familiar with your RSA NetWitness environment and you won't have to spend nearly as much time providing background information and other details for each case. Historically, RSA has only sold a 1 year DSE offering. We recently introduced this 3 month paid trial to let customers experience this premium service offering and decide whether or not it's something they would like to invest in. If you have any questions or would like to discuss further, please contact your account manager.



## Upcoming Events

The events below are a sample of events we're hosting in the month of April. If you happen to be in the area, please feel free to join us.

Event Name	Location	Date	Registration Link
International Privacy & Security Forum	Washington DC	April 4-5	<a href="#">Register Here</a>
Bsides Oklahoma City	Oklahoma City	April 12th	<a href="https://www.bsidesok.com/">https://www.bsidesok.com/</a>
International Cyber Risk Management Conference	Toronto, Canada	April 15-16	<a href="https://register.icrmc.com/">https://register.icrmc.com/</a>
Arrow, RSA and Dell Technologies Event	Chicago, IL	April 18th	<a href="#">Register Here</a>
Threat Hunting with RSA—Heads Up and Heads On	Seattle, WA	April 25	<a href="#">Register Here</a>

## Please Share Your Feedback

This is our first edition of this monthly newsletter and we welcome your thoughts and feedback on ways to improve. Please take 1-2 minutes of your time to complete this four question survey: <https://www.surveymonkey.com/r/ZLXQB3Y>

# RSA NetWitness Training Addendum



## Upcoming RSA NetWitness Training Classes

Training Course Name	Theater	Start Date	End Date	Delivery Location
Certified Ethical Hacking	Americas	6/3/2019	6/7/2019	Reston, VA
RSA CISSP Certification Bootcamp	Americas	6/10/2019	6/14/2019	Overland Park, KS
RSA NetWitness Logs and Network Administration and Operations	EMEA	5/1/2019	5/3/2019	Bracknell, UK
RSA NetWitness Logs and Network Administration and Operations	Americas	5/15/2019	5/17/2019	Bedford, MA
RSA NetWitness Logs and Network Analysis	Americas	5/2/2019	5/3/2019	Bedford, MA
RSA NetWitness Logs and Network Analysis	Americas	6/6/2019	6/7/2019	Bedford, MA
RSA NetWitness Logs and Network Analysis	EMEA	6/25/2019	6/26/2019	TBD
RSA NetWitness Logs and Network Analysis	EMEA	6/27/2019	6/28/2019	Bracknell, UK
RSA NetWitness Logs and Network Content Creation	Americas	5/13/2019	5/14/2019	Bedford, MA
RSA NetWitness Logs and Network Content Creation	Americas	6/11/2019	6/12/2019	Bedford, MA
RSA NetWitness Logs and Network Core Administration	EMEA	4/29/2019	4/30/2019	Bracknell, UK
RSA NetWitness Logs and Network Core Administration	Americas	5/9/2019	5/10/2019	Reston, VA
RSA NetWitness Logs and Network Foundations	Americas	4/29/2019	5/1/2019	Bedford, MA
RSA NetWitness Logs and Network Foundations	Americas	5/6/2019	5/8/2019	Reston, VA
RSA NetWitness Logs and Network Foundations	Americas	6/3/2019	6/5/2019	Bedford, MA
RSA NetWitness Platform Hunting Challenge	Americas	4/9/2019	4/10/2019	Reston, VA
RSA NetWitness Platform Hunting Challenge	APJ	4/10/2019	4/11/2019	TBD
RSA NetWitness Platform Hunting Challenge	Americas	6/13/2019	6/14/2019	Bedford, MA
RSA NetWitness Platform Introduction to Hunting	APJ	4/8/2019	4/9/2019	TBD
RSA NetWitness Platform Introduction to Hunting	EMEA	6/25/2019	6/26/2019	Bracknell, UK
RSA NetWitness Platform Introduction to Hunting	EMEA	6/27/2019	6/28/2019	TBD
RSA NetWitness Platform Reporting	Americas	6/25/2019	6/26/2019	Reston, VA

## RSA NetWitness Training Updates

### Two New Hunting Courses

RSA University has expanded their curriculum to include two new Hunting courses.

1. The **RSA NetWitness Platform Introduction to Hunting** covers hunting tools as well as a recommended methodology using hands-on labs to enable you to start proactively finding suspicious behavior in your environment.
2. The **RSA NetWitness Platform Hunting Challenge** allows you to test your hunting skills in a real-world environment using a capture the flag gaming format. You will compete against other students to find real-time attacks involving multipart use cases.

### Coming Soon—RSA NetWitness v11.3 Training

The RSA NetWitness curriculum is being updated for version 11.3. This new release will include new features, updated use cases, and new courses - such as Orchestrator Incident Response and Endpoint Foundations. We will add mechanisms like role-based graphics and training bundles that will group both live and On-Demand training courses to improve your learning journey for NetWitness v11.3.

### RSA University and EC-Council Team to Address Cyber Security Skills Gap

RSA University in partnership with EC-Council now provides a portfolio of cyber security skills-based training and certification programs globally to address the cyber skills shortage which is an ongoing and growing issue.

To learn more about how RSA can provide a tailored training program which can combine RSA's NetWitness platform training and certification with EC-Council's skills-based training and certification to help you manage digital risk, visit us at RSA University (EC-Council) Partnership or contact RSA University at [RSAU@rsa.com](mailto:RSAU@rsa.com).