RSA® NetWitness Platform

Version 11.6.1.0

Release Notes

Contact Information

RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

August 2021

Contents

What's New 4

GPG Key Changes 4

Upgrade Paths 4

Enhancements 4

Investigation - SIEM and Network Traffic Analysis 5

Investigation Enhancements: 5

Compact View: 5

Timeline Options 5

User Entity Behavior Analytics 6

Alert Feedback Enhancement 6

Endpoint Investigation 7

Support for OPSWAT Scans 7

Create groups with Machine OU as a filter 7

Extended Agent Support for Mac BigSur (version 11) on M1 8

Automatic download of memory DLL files 8

Added agent folder protection in the driver 9

Event Stream Analysis (ESA) 9

Optionally Persist Incident Artifacts 9

Log Collection 9

Trusted Authentication for NetWitness Export Connector 9

Support for Logstash Keystore from UI 9

Reports 10

View Creator Information 10

Fixed Issues 11

Administration Fixes 11

Investigate Fixes 11

Respond Fixes 11

Event Stream Analysis (ESA) Fixes 12

Endpoint Fixes 12

Context Hub Fixes 12

Product Documentation 13

Feedback on Product Documentation 13

Getting Help with NetWitness Platform 14

Self-Help Resources 14

Contact RSA Support 14

Build Numbers 15

Revision History 17

What's New

The RSA NetWitness Platform 11.6.1 release provides new features and enhancements for every role in the Security Operations Center.

GPG Key Changes

The GPG Signing for NetWitness has changed for releases beyond 11.6.0.0. For more information, see GPG Key Change in NetWitness Platform Beyond 11.6.0.0 GPG Key Change in NetWitness Platform Beyond 11.6.0.0.

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.6.1.0:

- RSA NetWitness Platform 11.4.1.4 to 11.6.1.0
- RSA NetWitness Platform 11.5.3.2 to 11.6.1.0
- RSA NetWitness Platform 11.6.0.0 to 11.6.1.0
- RSA NetWitness Platform 11.6.0.1 to 11.6.1.0

* If you are upgrading from 11.2.x.x, 11.3.x.x, you must upgrade to 11.4.1.4 or 11.5.3.2 before you can upgrade to 11.6.1.0

For more information on upgrading to 11.6.1.0, see Upgrade Guide for RSA NetWitness Platform 11.6.0.1

Enhancements

The following sections are a complete list and description of enhancements to specific capabilities:

- Investigation - SIEM and Network Traffic Analysis
- User Entity Behavior Analytics
- Endpoint Investigation
- Event Stream Analysis (ESA)
- Log Collection
- Reports

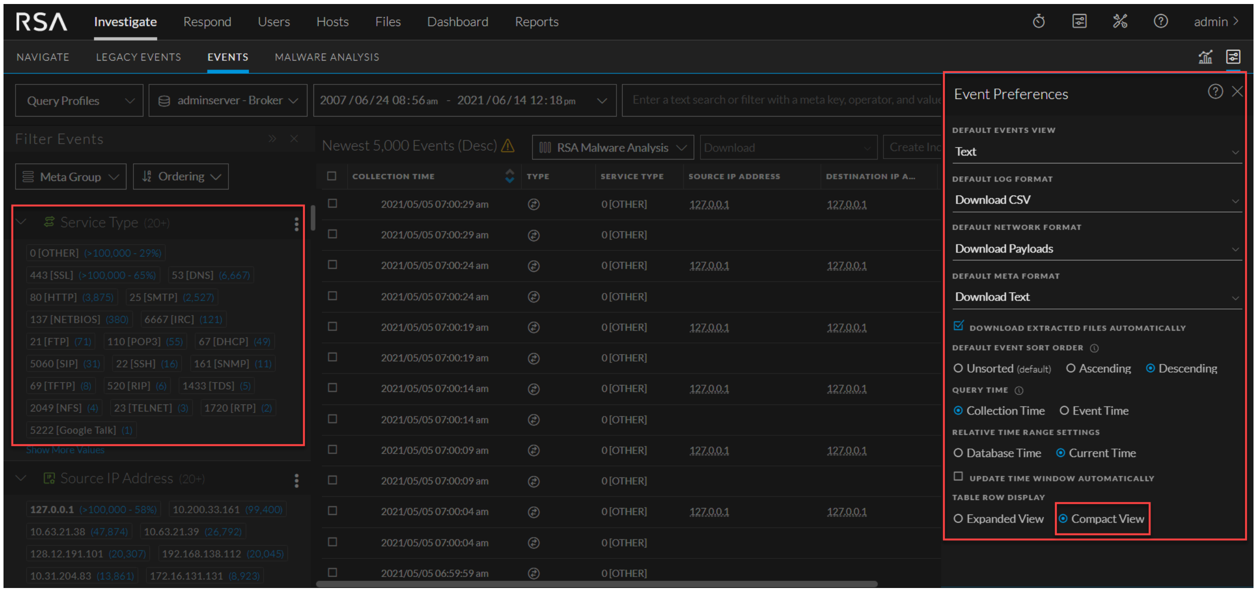
To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents. Product Documentation has links to the documentation for this release.

Investigation - SIEM and Network Traffic Analysis

Investigation Enhancements:

Compact View:

On the compact view, the Event Filter Panel and Event Meta Labels are optimized to display maximum information on a single page. With this view, analysts can easily perform the investigation. The label and icon size on the Event Filter Panel are optimized so that the meta keys and values are displayed on the same line.



2007 / 06 / 24 08 : 56 am - 2021 / 06 / 14 12 : 18 pm

Service Type (20+)

0 [OTHER] (>100,000 - 29%)
443 [SSL] (>100,000 - 65%) 53 [DNS] (6,667)
80 [HTTP] (3,875) 25 [SMTP] (2,527)
137 [NETBIOS] (380) 6667 [IRC] (121)
21 [FTP] (71) 110 [POP3] (55) 67 [DHCP] (49)
5060 [SIP] (31) 22 [SSH] (16) 161 [SNMP] (11)
69 [TFTP] (8) 520 [RIP] (6) 1433 [TDS] (5)
2049 [NFS] (4) 23 [TELNET] (3) 1720 [RTP] (2)
5222 [Google Talk] (1)

Source IP Address (20+)

127.0.0.1 (>100,000 - 58%) 10.200.33.161 (99,400)
10.63.21.38 (47,874) 10.63.21.39 (26,792)
128.12.191.101 (20,307) 192.168.138.112 (20,045)
10.31.204.83 (13,861) 172.16.131.131 (8,923)

Newest 5,000 Events (Desc)

□	COLLECTION TIME	TYPE	SERVICE TYPE	SOURCE IP ADDRESS	DESTINATION IP A...
□	2021/05/05 07:00:29 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:29 am		0 [OTHER]		
□	2021/05/05 07:00:24 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:24 am		0 [OTHER]		
□	2021/05/05 07:00:19 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:19 am		0 [OTHER]		
□	2021/05/05 07:00:14 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:14 am		0 [OTHER]		
□	2021/05/05 07:00:09 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:09 am		0 [OTHER]		
□	2021/05/05 07:00:04 am		0 [OTHER]	127.0.0.1	127.0.0.1
□	2021/05/05 07:00:04 am		0 [OTHER]		
□	2021/05/05 06:59:59 am		0 [OTHER]		

Event Preferences

DEFAULT EVENTS VIEW: Text

DEFAULT LOG FORMAT: Download CSV

DEFAULT NETWORK FORMAT: Download Payloads

DEFAULT META FORMAT: Download Text

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

DEFAULT EVENT SORT ORDER: ○ Unsorted (default) ○ Ascending ● Descending

QUERY TIME: ● Collection Time ○ Event Time

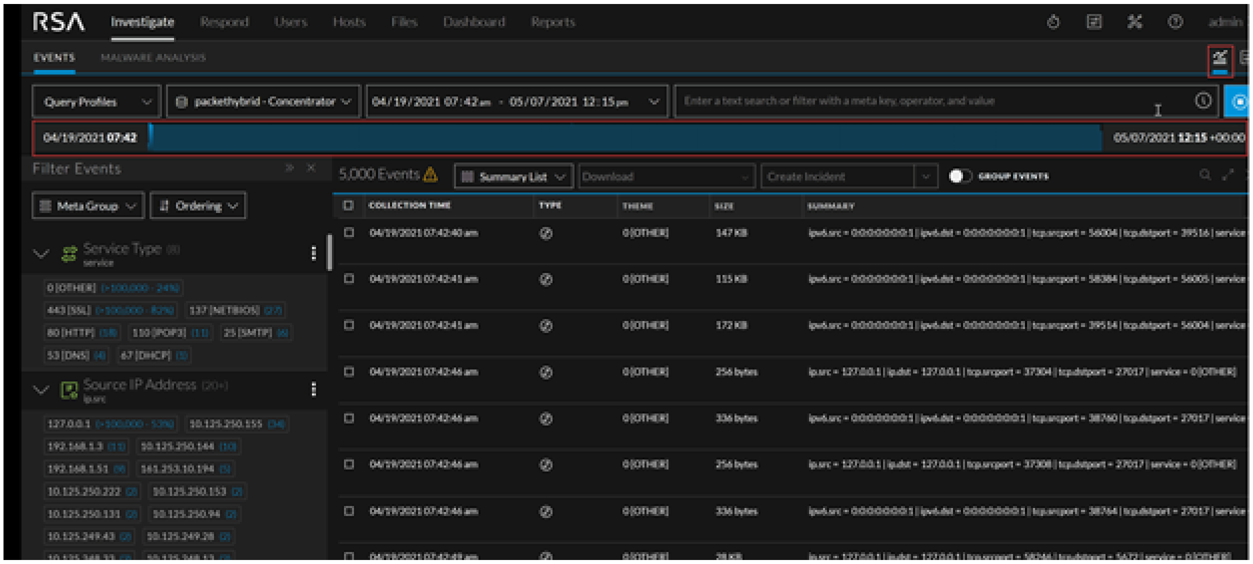
RELATIVE TIME RANGE SETTINGS: ○ Database Time ● Current Time

□ UPDATE TIME WINDOW AUTOMATICALLY

TABLE ROW DISPLAY: ○ Expanded View ● Compact View

Timeline Options

Analysts can now easily view the timeline for event by clicking on the icon. By default the timelines is enabled for all events.



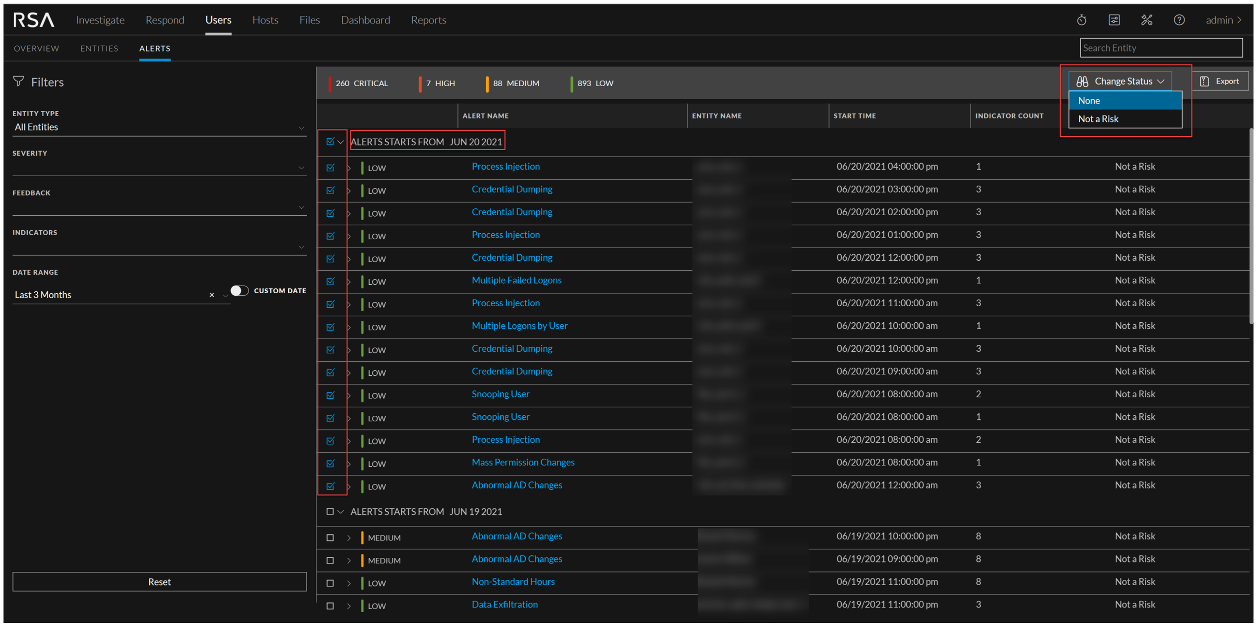
□	COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
□	04/19/2021 07:42:40 am		0 [OTHER]	147 KB	ipv6.src = 0:0:0:0:0:0:0:1 | ipv6.dst = 0:0:0:0:0:0:0:1 | tcp.srcport = 56004 | tcp.dstport = 39516 | service
□	04/19/2021 07:42:41 am		0 [OTHER]	115 KB	ipv6.src = 0:0:0:0:0:0:0:1 | ipv6.dst = 0:0:0:0:0:0:0:1 | tcp.srcport = 58384 | tcp.dstport = 56005 | service
□	04/19/2021 07:42:41 am		0 [OTHER]	172 KB	ipv6.src = 0:0:0:0:0:0:0:1 | ipv6.dst = 0:0:0:0:0:0:0:1 | tcp.srcport = 39514 | tcp.dstport = 56004 | service
□	04/19/2021 07:42:46 am		0 [OTHER]	256 bytes	ip.src = 127.0.0.1 | ip.dst = 127.0.0.1 | tcp.srcport = 37304 | tcp.dstport = 27017 | service = 0 [OTHER]
□	04/19/2021 07:42:46 am		0 [OTHER]	336 bytes	ipv6.src = 0:0:0:0:0:0:0:1 | ipv6.dst = 0:0:0:0:0:0:0:1 | tcp.srcport = 38760 | tcp.dstport = 27017 | service
□	04/19/2021 07:42:46 am		0 [OTHER]	256 bytes	ip.src = 127.0.0.1 | ip.dst = 127.0.0.1 | tcp.srcport = 37308 | tcp.dstport = 27017 | service = 0 [OTHER]
□	04/19/2021 07:42:46 am		0 [OTHER]	336 bytes	ipv6.src = 0:0:0:0:0:0:0:1 | ipv6.dst = 0:0:0:0:0:0:0:1 | tcp.srcport = 38764 | tcp.dstport = 27017 | service
□	04/19/2021 07:42:48 am		0 [OTHER]	28 KB	ip.src = 127.0.0.1 | ip.dst = 127.0.0.1 | tcp.srcport = 58246 | tcp.dstport = 5672 | service = 0 [OTHER]

For more information, see the *Investigate User Guide*.

User Entity Behavior Analytics

Alert Feedback Enhancement

Analysts have the option to mark the status of mutliple alerts as **Not a Risk** or **None**. **None** is used when the events are **Not a Risk**. Multiple alerts grouped by date can be selected to perform this action. When the status is updated, the alert contribution score will change automatically, for example, if an alert is marked as **Not a Risk**, the alert score is reduced. If the status is updated as **None**, the score increases. For more information, see the *UEBA User Guide*.

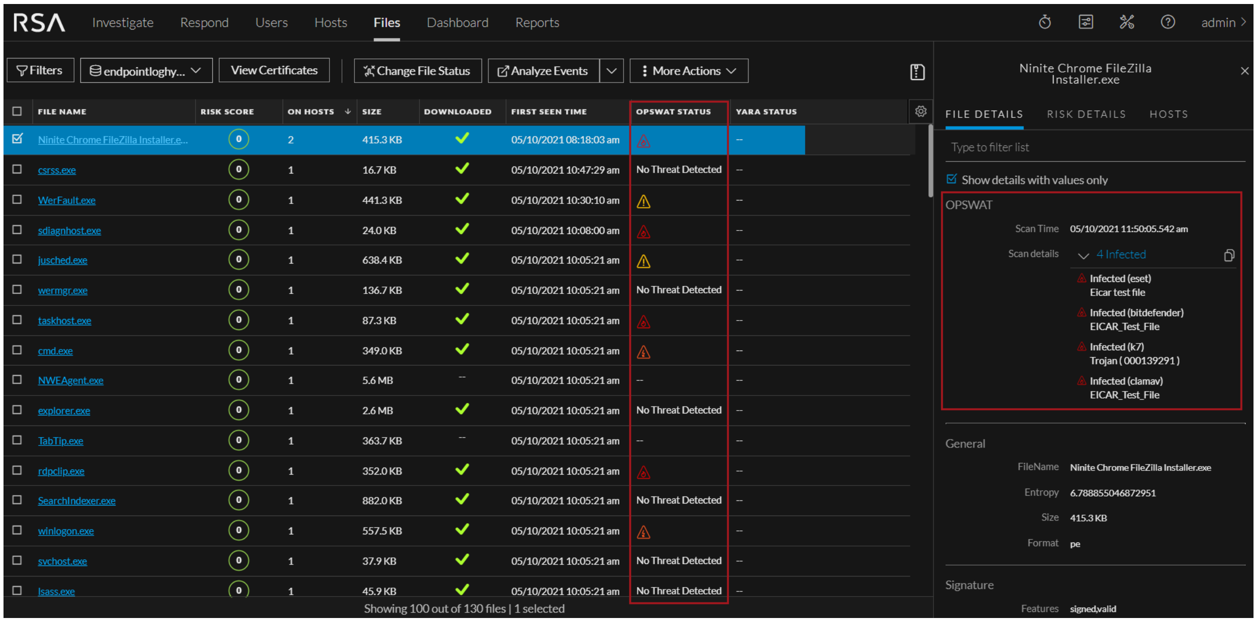


		ALERT NAME	ENTITY NAME	START TIME	INDICATOR COUNT	
☑	ALERTS STARTS FROM JUN 20 2021					
☑	LOW	Process Injection	[redacted]	06/20/2021 04:00:00 pm	1	Not a Risk
☑	LOW	Credential Dumping	[redacted]	06/20/2021 03:00:00 pm	3	Not a Risk
☑	LOW	Credential Dumping	[redacted]	06/20/2021 02:00:00 pm	3	Not a Risk
☑	LOW	Process Injection	[redacted]	06/20/2021 01:00:00 pm	3	Not a Risk
☑	LOW	Credential Dumping	[redacted]	06/20/2021 12:00:00 pm	3	Not a Risk
☑	LOW	Multiple Failed Logons	[redacted]	06/20/2021 12:00:00 pm	1	Not a Risk
☑	LOW	Process Injection	[redacted]	06/20/2021 11:00:00 am	3	Not a Risk
☑	LOW	Multiple Logons by User	[redacted]	06/20/2021 10:00:00 am	1	Not a Risk
☑	LOW	Credential Dumping	[redacted]	06/20/2021 10:00:00 am	3	Not a Risk
☑	LOW	Credential Dumping	[redacted]	06/20/2021 09:00:00 am	3	Not a Risk
☑	LOW	Snooping User	[redacted]	06/20/2021 08:00:00 am	2	Not a Risk
☑	LOW	Snooping User	[redacted]	06/20/2021 08:00:00 am	1	Not a Risk
☑	LOW	Process Injection	[redacted]	06/20/2021 08:00:00 am	2	Not a Risk
☑	LOW	Mass Permission Changes	[redacted]	06/20/2021 08:00:00 am	1	Not a Risk
☑	LOW	Abnormal AD Changes	[redacted]	06/20/2021 12:00:00 am	3	Not a Risk
□	ALERTS STARTS FROM JUN 19 2021					
□	MEDIUM	Abnormal AD Changes	[redacted]	06/19/2021 10:00:00 pm	8	Not a Risk
□	MEDIUM	Abnormal AD Changes	[redacted]	06/19/2021 09:00:00 pm	8	Not a Risk
□	LOW	Non-Standard Hours	[redacted]	06/19/2021 11:00:00 pm	8	Not a Risk
□	LOW	Data Exfiltration	[redacted]	06/19/2021 11:00:00 pm	3	Not a Risk

Endpoint Investigation

Support for OPSWAT Scans

Analysts can simultaneously perform threat detection with multiple anti-malware engines with OPSWAT (MetaDefender Core). Executable files(PE, Macro, Script, ELF) will automatically be sent to the OPSWAT server for scanning. Analysts will get alerts if a file is found Infected or Suspicious (critical for Infected and High severity for Suspicious files). The risk score will also increase for the file and the corresponding host, thus helping to respond to threats quickly. For more information on how to use OPSWAT within the NetWitness Platform, see the *NetWitness Endpoint User Guide*. And, for more information on how to configure OPSWAT on endpoint servers, see *NetWitness Endpoint Configuration Guide*.



☐	FILE NAME	RISK SCORE	ON HOSTS	SIZE	DOWNLOADED	FIRST SEEN TIME	OPSWAT STATUS	YARA STATUS
☑	Ninite Chrome FileZilla Installer.e...	0	2	415.3 KB	✓	05/10/2021 08:18:03 am	⚠	--
☐	csrss.exe	0	1	16.7 KB	✓	05/10/2021 10:47:29 am	No Threat Detected	--
☐	WerFault.exe	0	1	441.3 KB	✓	05/10/2021 10:30:10 am	⚠	--
☐	sdiagnhost.exe	0	1	24.0 KB	✓	05/10/2021 10:08:00 am	⚠	--
☐	jusched.exe	0	1	638.4 KB	✓	05/10/2021 10:05:21 am	⚠	--
☐	wermgr.exe	0	1	136.7 KB	✓	05/10/2021 10:05:21 am	No Threat Detected	--
☐	taskhost.exe	0	1	87.3 KB	✓	05/10/2021 10:05:21 am	⚠	--
☐	cmd.exe	0	1	349.0 KB	✓	05/10/2021 10:05:21 am	⚠	--
☐	NWEAgent.exe	0	1	5.6 MB	--	05/10/2021 10:05:21 am	--	--
☐	explorer.exe	0	1	2.6 MB	✓	05/10/2021 10:05:21 am	No Threat Detected	--
☐	TabTip.exe	0	1	363.7 KB	--	05/10/2021 10:05:21 am	--	--
☐	rdpclip.exe	0	1	352.0 KB	✓	05/10/2021 10:05:21 am	⚠	--
☐	SearchIndexer.exe	0	1	882.0 KB	✓	05/10/2021 10:05:21 am	No Threat Detected	--
☐	winlogon.exe	0	1	557.5 KB	✓	05/10/2021 10:05:21 am	⚠	--
☐	svchost.exe	0	1	37.9 KB	✓	05/10/2021 10:05:21 am	No Threat Detected	--
☐	lsass.exe	0	1	45.9 KB	✓	05/10/2021 10:05:21 am	No Threat Detected	--

Showing 100 out of 130 files | 1 selected

Ninite Chrome FileZilla Installer.exe

FILE DETAILS | RISK DETAILS | HOSTS

Type to filter list

☑ Show details with values only

OPSWAT

Scan Time	05/10/2021 11:50:05.542 am
Scan details	4 Infected
	⚠ Infected (eset) Eicar test file
	⚠ Infected (bitdefender) EICAR_Test_File
	⚠ Infected (k7) Trojan (000139291)
	⚠ Infected (clamav) EICAR_Test_File

General

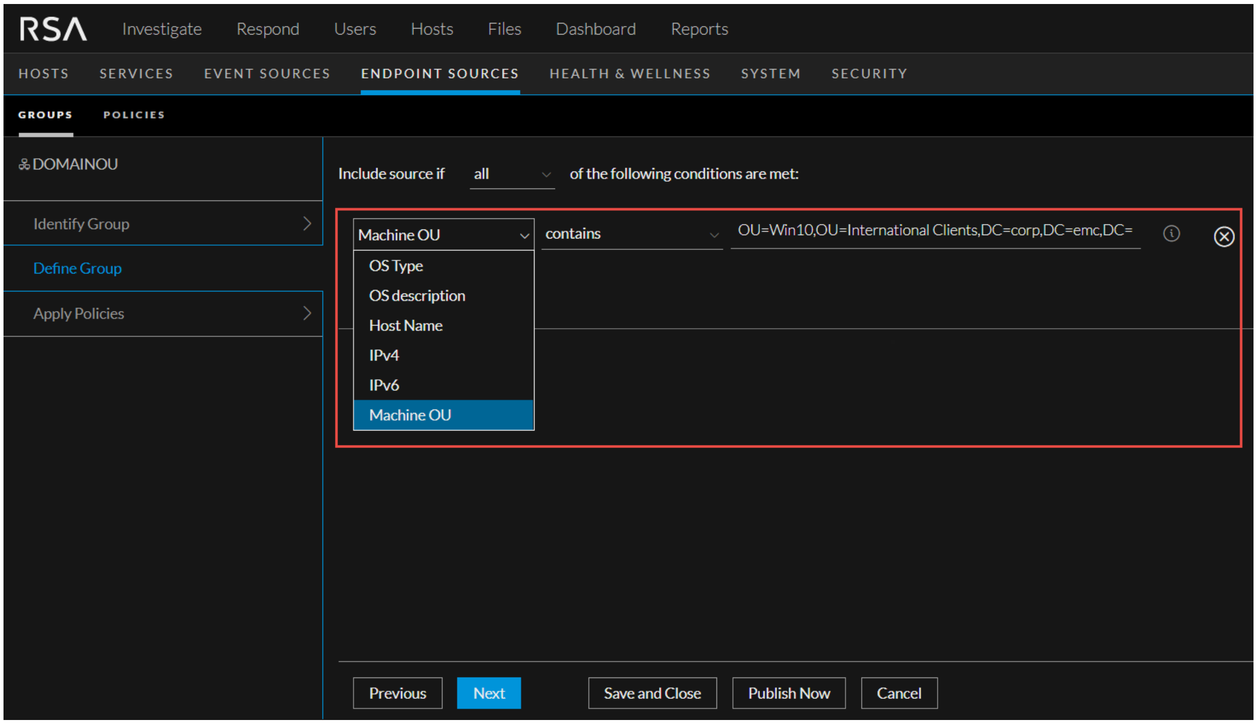
FileName	Ninite Chrome FileZilla Installer.exe
Entropy	6.788855046872951
Size	415.3 KB
Format	pe

Signature

Features	signed,valid

Create groups with Machine OU as a filter

Analysts can use Machine Organizational Unit (Machine OU) as a filter while creating groups on the **Admin** > **Endpoint Sources** > **Groups** view. Using Machine OU to filter hosts can save much time and effort as it is more effective than using IPV4 or domain names in an environment with thousands of agents.



Include source if all of the following conditions are met:

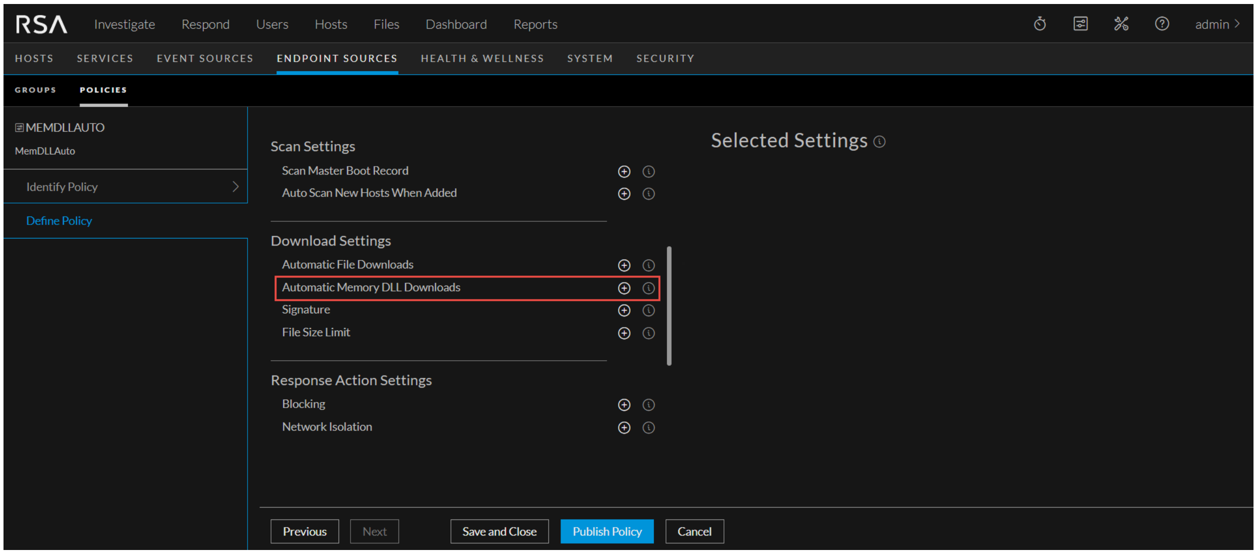
Machine OU contains OU=Win10,OU=International Clients,DC=corp,DC=emc,DC=

Extended Agent Support for Mac BigSur (version 11) on M1

NetWitness Endpoint agents now support Mac BigSur on both M1 and Intel. For more information, see *NetWitness Endpoint Agent Installation Guide*.

Automatic download of memory DLL files

Analysts can now investigate the memory DLL files in detail. All memory DLL files that are detected during a scan, are automatically downloaded to the server irrespective of the file size.



Added agent folder protection in the driver

Netwitness platform version 11.6.1 and higher, the files inside the agent folder are protected from delete, rename, or modification operations. This protection will prevent malware from locking files inside the agent folder to block sending the tracking data.

Event Stream Analysis (ESA)

Optionally Persist Incident Artifacts

You can persist events that are associated with particular incidents, thereby enabling you to view the incident in the future, regardless of its age. You can also add a new journal entry in the **JOURNAL** tab for the persisted events for future reference. The event data will always be available for viewing and reconstruction as long as the event is persisted, enabling you to easily refer back to details, even if the original event has rolled over from the NetWitness database.

Once you persist an event, the data is copied from the NetWitness database into a long term storage cache within the data source. The persisted events are saved in the directory `/var/netwitness/pin-<servicetype>`, by default. You can manually change the event storage location from the default directory to any other directory, as per the requirement. For more information, see the *Respond User Guide*.

Log Collection

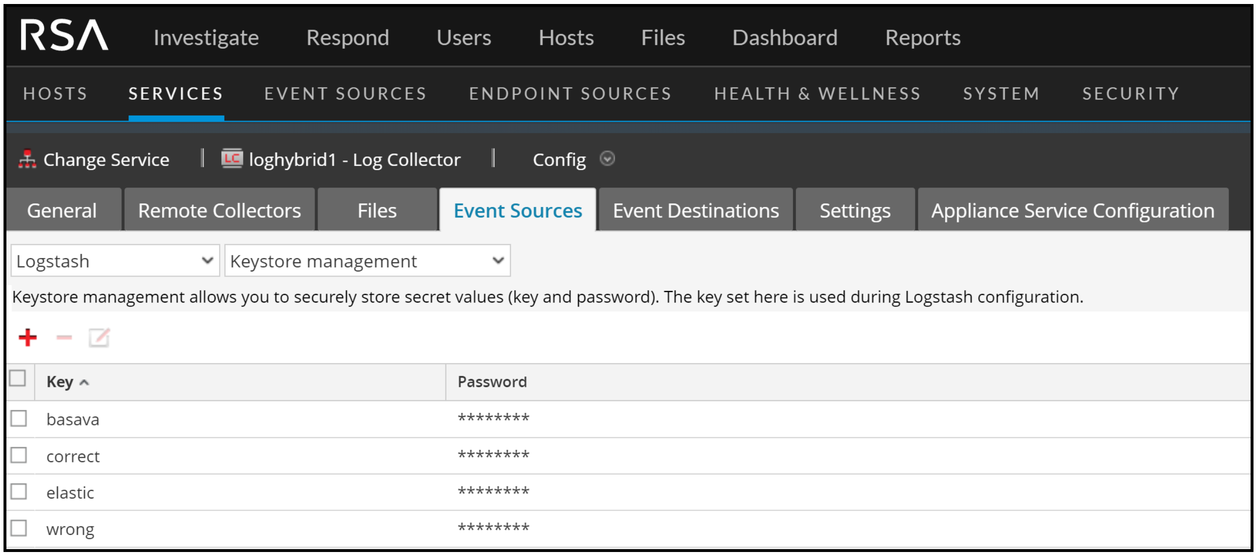
Trusted Authentication for NetWitness Export Connector

Trusted authentication allows you to authenticate using the existing certificates for aggregation while configuring NetWitness Export Connector. This eliminates the need to manually enter the credentials (username and password) and avoid storing passwords locally.

Support for Logstash Keystore from UI

Logstash keystore management allows you to securely store and maintain (add, edit, or delete) secret values key and password through NetWitness Platform UI. The key set is used during the Logstash pipeline configuration.

This eliminates the need to manually create or update credentials on the Log Decoder or Virtual Log Collector using Logstash Keystore CLI commands. For more information, see the *Log Collection Guide*.



Keystore management allows you to securely store secret values (key and password). The key set here is used during Logstash configuration.

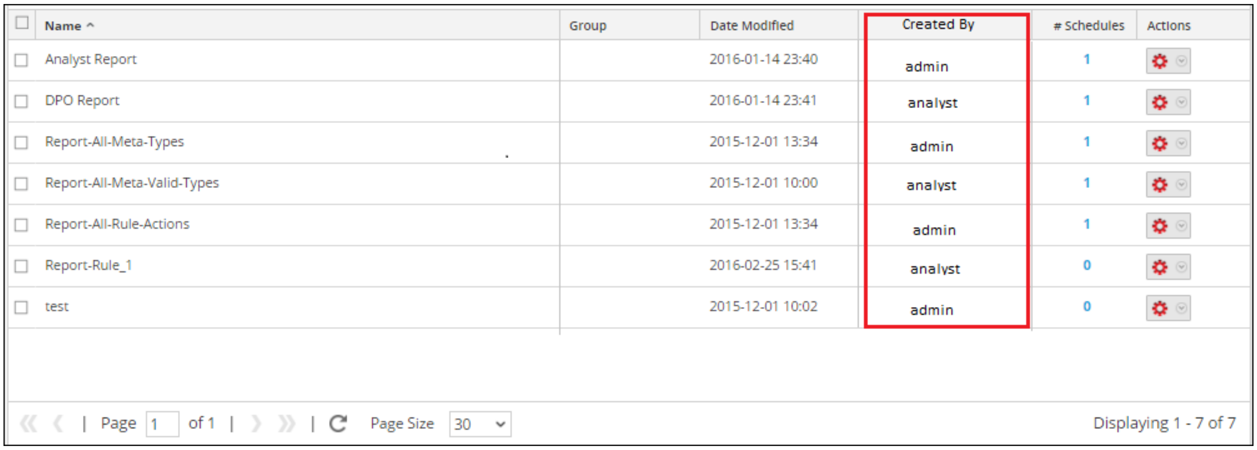
□	Key ^	Password
□	basava	********
□	correct	********
□	elastic	********
□	wrong	********

Reports

View Creator Information

The Created By column has been added to the Reports List page. This column enables you to view and analyze the ownership information of all the reports that exist in the system, which includes new, copied, and imported reports. When a report is exported, the owner details are retained. However, when a report is copied, the owner of the report changes to the user who created the copy. For more information, see the *Reporting User Guide*.

Note: When you upgrade from a previous version to NetWitness Platform Release 11.6.1, the Created By column does not display the ownership information for the reports that exist prior to the upgrade.



□	Name ^	Group	Date Modified	Created By	# Schedules	Actions
□	Analyst Report		2016-01-14 23:40	admin	1	
□	DPO Report		2016-01-14 23:41	analyst	1	
□	Report-All-Meta-Types		2015-12-01 13:34	admin	1	
□	Report-All-Meta-Valid-Types		2015-12-01 10:00	analyst	1	
□	Report-All-Rule-Actions		2015-12-01 13:34	admin	1	
□	Report-Rule_1		2016-02-25 15:41	analyst	0	
□	test		2015-12-01 10:02	admin	0	

Fixed Issues

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the RSA NetWitness Platform Known Issues list on RSA Link.

Administration Fixes

Tracking Number	Description
SACE-16066	Data access privileges does not match with that of the privileges that are configured for specific user roles. Accessibility to information is not in concurrence with the user role privileges.
ASOC-110359	The meta keys in the custom context feed wizard does not display information accurately. Parameters such as netname, ip.org are not displayed. When you deploy the feed, the context hub conversion fails.
ASOC-109855	The configuration and administration icons, and the user name in the top navigation bar does not display accurately for non-Admin users.

Investigate Fixes

Tracking Number	Description
ASOC-110979	The filter provided in the **Events** page displays the top 20 results for each RSA provided meta group.
ASOC-110864	In the **Filter Events** page, meta key values are displayed even when the **Default Action** parameter is set to **closed** in the Index file.

Respond Fixes

Tracking Number	Description
ASOC-110028	Owing to the missing files that are used to calculate the score for alerts, the Respond Server generates error logs constantly.

Event Stream Analysis (ESA) Fixes

Tracking Number	Description
ASOC-108914	Error Notification on Admin Server while processing ESA Correlation rules. NetWitness displays the RSAContext annotation error **onError = STOP_ALL_RULE_ PROCESSING_ AND_WAIT** when `reclaim_group_ aged` annotation is used in the ESA rule.

Endpoint Fixes

Tracking Number	Description
ASOC-109505	Security log-in events from systems installed with non-english Windows operating systems are not collected by the endpoint agent.

Context Hub Fixes

Tracking Number	Description
ASOC-109826	You can configure data source in the Context Hub server, by importing CSV files. However, when you edit the CSV file, the first row is deleted.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.x Master Table of Contents	https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentation
RSA NetWitness Platform 11.6 Product Documentation	https://community.rsa.com/
RSA NetWitness Platform 11.6 Upgrade Guide	https://community.rsa.com/t5/rsa-netwitness-platform-online/upgrade-instructions-for-rsa-netwitness-platform-11-x-to-11-6/ta-p/606727

Feedback on Product Documentation

You can send an email to nwdocsfeedback@rsa.com to provide feedback on RSA NetWitness Platform documentation.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness Platform:

- See the documentation for all aspects of NetWitness Platform here: https://community.rsa.com/community/products/netwitness/documentation
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here: https://community.rsa.com/welcome
- See the RSA NetWitness Platform Knowledge Base: https://community.rsa.com/community/products/netwitness/knowledge-base
- See Troubleshooting the RSA NetWitness Platform: https://community.rsa.com/community/products/netwitness/documentation/troubleshooting
- See also RSA NetWitness® Platform Blog Posts.
- If you need further assistance, contact RSA Support.

Contact RSA Support

If you contact RSA Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the RSA NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com In the main menu, click **My Cases**.
International Contacts (How to Contact RSA Support)	https://community.rsa.com/docs/DOC-1294
Community	https://community.rsa.com/community/support

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.6.1.0.

Component	Version Number
NetWitness Platform Audit Plugins	rsa-audit-plugins-11.6.1.0-4675.5.125cbe904.el7.noarch.rpm
NetWitness Platform Appliance	rsa-nw-appliance-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Archiver	rsa-nw-archiver-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Broker	rsa-nw-broker-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Concentrator	rsa-nw-concentrator-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Config Management	rsa-nw-config-management-11.6.1.0-2106011535.5.226be97.el7.noarch.rpm
NetWitness Platform Config Server	rsa-nw-config-server-11.6.0.0-210331045328.5.6fe2c5e.el7.centos.noarch.rpm
NetWitness Platform Console	rsa-nw-console-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Content Server	rsa-nw-content-server-11.6.1.0-210610030158.5.260bb95.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	rsa-nw-contexthub-server-11.6.1.0-210527073405.5.776a0e0.el7.centos.noarch.rpm
NetWitness Platform Correlation Server (ESA)	rsa-nw-correlation-server-11.6.1.0-210623130413.5.801d125.el7.centos.noarch.rpm
NetWitness Platform Decoder	rsa-nw-decoder-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	rsa-nw-deployment-upgrade-11.6.1.0-2105141642.5.020fcff.el7.noarch.rpm
NetWitness Platform Endpoint Agents	rsa-nw-endpoint-agents-11.6.1.0-2106281731.5.6419012.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.6.1.0-210623060837.5.c42b8ae.el7.centos.noarch.rpm
NetWitness Platform Endpoint Server	rsa-nw-endpoint-server-11.6.1.0-210623044726.5.cc6f46e.el7.centos.noarch.rpm

NetWitness Platform Integration Server	rsa-nw-integration-server-11.6.1.0-210623130114.5.e583a97.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	rsa-nw-investigate-server-11.6.1.0-210625040931.5.5a9444e.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	rsa-nw-legacy-web-server-11.6.1.0-210623175328.5.c439d52.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	rsa-nw-logdecoder-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Log Player	rsa-nw-logplayer-11.6.1.0-12016.5.5ce591371.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	rsa-nw-malware-analytics-server-11.6.1.0-210610053500.5.486a578.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	rsa-nw-metrics-server-11.6.1.0-210622025741.5.0e81e5a.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	rsa-nw-orchestration-server-11.6.1.0-210608142450.5.5284c88.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	rsa-nw-re-server-11.6.1.0-5904.5.a3b77d346.el7.x86_64.rpm
NetWitness Platform Respond Server	rsa-nw-respond-server-11.6.1.0-210623130310.5.0899ac3.el7.centos.noarch.rpm
NetWitness Platform Security Server	rsa-nw-security-server-11.6.1.0-210610025428.5.d1f841d.el7.centos.noarch.rpm
NetWitness Platform Source Server	rsa-nw-source-server-11.6.1.0-210608040726.5.d739c95.el7.centos.noarch.rpm
NetWitness Platform User Interface	rsa-nw-ui-11.6.1.0-210624040340.5.4c0db5909d.el7.centos.noarch.rpm
NetWitness Platform Workbench	rsa-nw-workbench-11.6.1.0-12014.5.20bbb64cf.el7.x86_64.rpm
NetWitness Platform SMS Runtime	rsa-sms-runtime-rt-11.6.1.0-4675.5.125cbe904.el7.x86_64.rpm
NetWitness Platform SMS Server	rsa-sms-server-11.6.1.0-4675.5.125cbe904.el7.x86_64.rpm

Revision History

Date	Description
August 2021	Release to Operations