NetWitness® Platform XDR

Version 12.0

NetWitness Endpoint Quick Start Guide

Contact Information

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

Trademarks

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 NetWitness Community. 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.

July, 2022

What is NetWitness Endpoint?

NetWitness Endpoint is an endpoint detection and response tool that continuously monitors the behavior of all endpoints in the network to provide deep visibility and analysis of executables and processes. It helps to detect new, unknown, and targeted attacks, highlights suspicious activity for investigation, exposes anomalous behaviors, and determines the scope of compromise to help analysts respond to advanced threats faster.

About this Guide

This guide provides end-to-end instructions to configure NetWitness Endpoint and to use Endpoint features.

NetWitness Platform Documentation in NetWitness Community Portal

NetWitness Platform product documentation is organized along functional lines. If you are looking for a specific guide or version, go to the a.

Use these links to view the NetWitness Platform documentation. Both links provide the same documentation, in these two formats:

- HTML Guides include the latest information for currently supported versions: NetWitness Platform Documentation.
- PDF Guides provide the information for a specific version: NetWitness Platform PDFs

Use these links to access documentation that is not related to a particular version of the software:

- Hardware setup guides: https://community.netwitness.com/t5/netwitness-platform-hardware/tkb-p/netwitness-hardware-documentation
- Documentation for Content such as feeds, parsers, application rules, and reports: https://community.netwitness.com/t5/netwitness-platform-threat/tkb-p/netwitness-threat-intelligence.

Getting Started

The following tasks can be performed in any sequence.

Description	References
Incident Responder (T1 Analyst) Threat Hunter (T2/T3 Analyst) System Administrator	

Description	References
View information about product updates, improvements, and known issues.	*Release Notes*
Understand NetWitness Endpoint.	"Getting Started with NetWitness Platform" and "Investigate" in the *NetWitness Platform Getting Started Guide*

Setup and Installation

Fresh Installation

The following tasks must be performed in the sequence listed.

Description	References
System Administrator	
Obtain a license for Endpoint Log Hybrid.	Licensing Management Guide
Review the supported hardware.	"Supported Hardware" in the *Physical Host Installation Guide*
Review the Endpoint architecture; plan your deployment based on the number of endpoints, distribution, and location of these endpoints; and choose one of the following deployments: • Single Endpoint server • Multiple Endpoint server	"NetWitness Endpoint Architecture" in the *Deployment Guide*
Configure the ports on your firewall.	"Network Architecture and Ports" in the *Deployment Guide*
Install NetWitness Server and other components. For a single Endpoint server deployment, you need to install - NetWitness Server, Endpoint Log Hybrid, and ESA. For a multiple Endpoint server, in addition to the above components, you need to install - Additional Endpoint Log Hybrid, NetWitness Broker along with Endpoint Broker installed on it.	- *Physical Host Installation Guide* for instructions on how to set up physical hosts - *Virtual Host Installation Guide* for instructions on how to set up virtual hosts

Description	References
Install Endpoint Log Hybrid.	"NetWitness Endpoint" in the *Physical Host Installation Guide*
Review the services installed.	*Hosts and Services Getting Started Guide*
Note: Review the default policies and modify them accordingly. Install Endpoint agent on hosts.	"Endpoint Sources" topic in the *Endpoint Configuration Guide* *NetWitness Endpoint Agent Installation Guide*

Upgrade

The following tasks must be performed in the sequence listed.

Description	References
System Administrator	
Install the 11.5 Relay Server	"Install the 11.5 Relay Server" in the Upgrade Guide
Upgrade Endpoint Agents	"Upgrade Agents" in the *Endpoint Agent Installation Guide*

Configuration

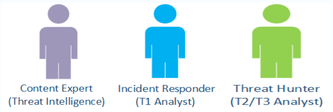
The following tasks can be performed in any sequence.

Description	References
System Administrator	
Understand NetWitness Endpoint and high-level tasks required for configuration.	"NetWitness Endpoint Overview and Endpoint Server Configuration" in the *Endpoint Configuration Guide*
Review Groups and Policies for agents.	"Endpoint Sources" topic in the *Endpoint Configuration Guide*

Description	References
Set up the RSA Live account and verify if the ESA content and Application Rules for Endpoint are available. **Note:** The file reputation service is automatically enabled on RSA Live.	*Live Services Management Guide*
Create role-based access control (RBAC).	"Role Permissions" in the System Security and User Management Guide
Configure data retention policy.	"Configure Data Retention" in the *Endpoint Configuration Guide*
Manage inactive agents.	"Manage Inactive Agents" in the *Endpoint Configuration Guide*
Configure Memory Dumps and MFT retention policy.	"Configure Retention Policy for Memory Dumps and MFT" in the *Endpoint Configuration Guide*

Investigation

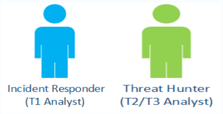
The following tasks can be performed in any sequence.

Description	References
 Content Expert (Threat Intelligence) Incident Responder (T1 Analyst) Threat Hunter (T2/T3 Analyst)	
Understand how investigation works.	"How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*
Configure investigate views.	"Configuring NetWitness Investigate Views and Preferences" in the *NetWitness Investigate User Guide*
Begin an investigation in different Investigate views.	"Beginning an Investigation" in the *NetWitness Investigate User Guide*
Review best practices for files and hosts and set up your Investigate view for investigation.	"Best Practices" under Investigating Files and Investigating Hosts in the*NetWitness Endpoint User Guide*
Investigate files.	"Investigating Files" in the *NetWitness Endpoint User Guide*
Investigate hosts.	"Investigating Hosts" in the *NetWitness Endpoint User Guide*

Description	References
Investigate process.	"Investigating Hosts" in the *NetWitness Endpoint User Guide*
Analyze downloaded files.	"Analyzing Downloaded Files" in the *NetWitness Endpoint User Guide*
Change file status and remediate.	"Changing File Status or Remediate" in the *NetWitness Endpoint User Guide*
Analyze events.	"Analyzing Events" in the *NetWitness Endpoint User Guide* "Analyzing Raw Data and Metadata in the Events View", "Investigating Metadata in the Navigate View", and "Examining Raw Events in the Events View" in the *NetWitness Investigate User Guide*
Perform host forensics.	"Performing Host Forensics" in the *NetWitness Endpoint User Guide*
Isolate hosts from network.	"Isolating Hosts from Network" in the *NetWitness Endpoint User Guide*
Investigate using REST APIs	*API User Guide*

Respond and Reporting

The following tasks can be performed in any sequence.

Description	References
 Incident Responder (T1 Analyst) Threat Hunter (T2/T3 Analyst)	
Respond to Endpoint incidents.	*NetWitness Respond User Guide*
View reports related to Endpoint data.	*Reporting User Guide*

Maintenance

The following tasks can be performed in any sequence.

Description	References
System Administrator	
Monitor health and wellness.	*System Maintenance Guide*

Integration (for Legacy NetWitness Endpoint)

The following tasks can be performed in any sequence.

Description	References
System Administrator	
Configure NetWitness Endpoint 4.4.x metadata with NetWitness.	"Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Platform" topic in the *Endpoint Configuration Guide*
Configure integrated operation of NetWitness Endpoint 4.4.x with NetWitness.	NetWitness Endpoint Integration Guide