

NetWitness and ThreatConnect

Integrated Products:

- ThreatConnect
- NetWitness Platform

ThreatConnect® and RSA® have partnered to enable users to detect and act on ThreatConnect intelligence in the NetWitness Platform. With this integration, users can aggregate their internal logs and combine them with validated threat intelligence, so they can easily spot trends or patterns that are out of the ordinary and act on them efficiently as well as providing a workbench for comprehensive case management.

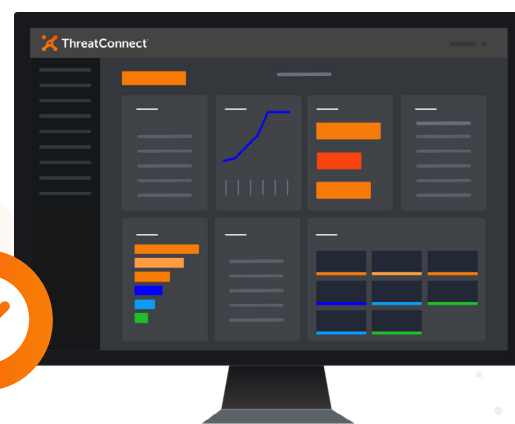


Integration Overview

The NetWitness Platform is a modular threat detection and response solution that is the centerpiece of an evolved security operations team. It enriches data at capture time, creating metadata to dramatically accelerate alerting and analysis and quickly understand the full scope of an attack. Core NetWitness Platform capabilities include its common data model, radical scalability and flexible deployment options, as well as its sophisticated analyst toolset, forensic capabilities and reporting engine.

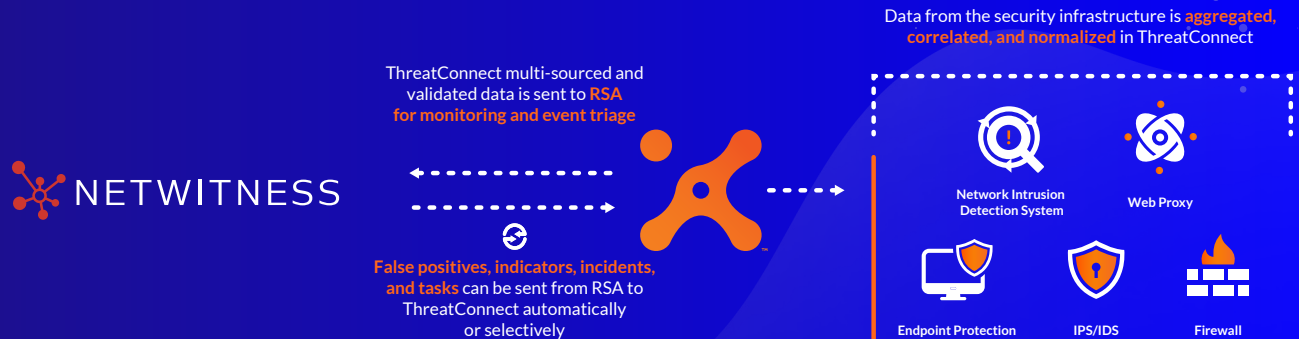
The ThreatConnect Platform delivers orchestration and automation capabilities that reduce job complexity for every stakeholder – from security executives, to risk teams, to threat intelligence experts, to security operations personnel and incident responders.

Together, ThreatConnect and The NetWitness Platform helps users to drive investigations and remediations by using highly correlated and validated Threat Intelligence. This integration consists of multiple apps that work across multiple NetWitness Platform products and the ThreatConnect Platform. These apps can be used together or separately to enable numerous use cases that help security teams protect themselves against sophisticated attacks.



Indicator Matching

As part of a security process, you can send high fidelity threat data from ThreatConnect into the NetWitness Platform for validated alerting and provide the necessary context to be able to take action on malicious indicators.



Alert Triage and Incident Investigation

As part of an investigation, you can now ingest Incidents and Alerts from NetWitness Platform as Cases in ThreatConnect. From there ThreatConnect Workflow can orchestrate a predefined Alert triage process and guide you through a combination of automated and manual tasks to resolve the Incident. Additionally, the original Incident in NetWitness Platform can automatically be updated with a Journal entry containing the results of the investigation, and the status can be marked as closed or as a false positive.

Comprehensive Case Management

Using ThreatConnect Workflow, you can drive comprehensive investigations across Network, Log, and Endpoint data in the NetWitness Platform. Information such as host details, files, logs, network traffic and more can be used to enrich and guide an investigation. This information can be added to the Case as artifacts that are automatically enriched further by the intelligence in ThreatConnect and ThreatConnect CAL.

Retroactive Hunting

As part of an investigation, you may want to search NetWitness Platform events for matching ThreatConnect indicators. Automate this process to introduce efficiency and consistency without introducing tedious tasks to your analyst team.

Track False Positives from SIEM

As part of a reporting process, ThreatConnect can track the number of False Positives and Observations found by NetWitness Platform. Create Dashboards to report important ROI metrics that can then be shared with other relevant team members and business leaders.



Features and Benefits



Send all available threat data from ThreatConnect into the NetWitness Platform for alerting and automated detection of advanced threats



Ensure that validated threat Intelligence is being sent to the NetWitness Platform and providing the necessary context to be able to take action on the indicators



Enable more efficient investigation and remediation with real-time threat analysis and indicator correlation



Clearly communicate important metrics using Dashboards to track performance on items such as false positives being reported

How to Get Started

If you are already a ThreatConnect customer, these Apps can be downloaded and installed from the ThreatConnect App Catalogue or by contacting your Customer Success Representative. If you are not a current ThreatConnect customer or user and would like to know more about this, or any of our other third-party apps or integrations, please email sales@threatconnect.com.


RSA


NetWitness® Platform enables organizations to quickly detect threats and determine which pose the greatest risk, and mount a coordinated response. The platform is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.




Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

 3865 Wilson Blvd., Suite 550
Arlington, VA 22203

 sales@threatconnect.com

 1.800.965.2708