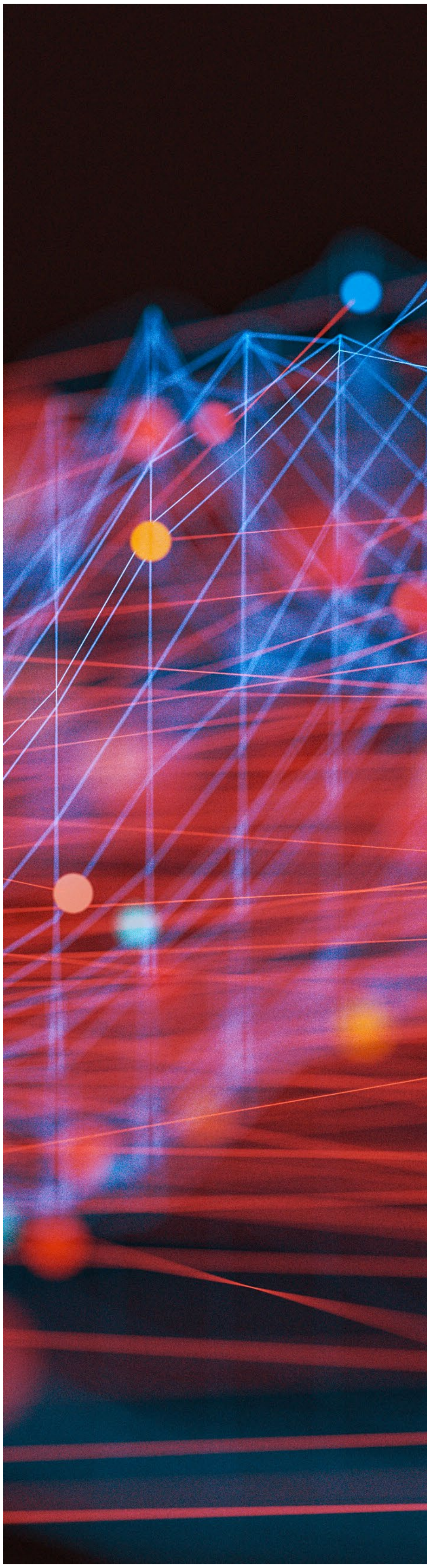
NETWITNESS

DATA SHEET

NetWitness® Orchestrator



The structure of how cybersecurity performs is broken.

There are system-wide issues that prevent enterprise security operations from being both efficient and effective. Security stakeholders are challenged by increasing cyberattack sophistication, a shortage of skilled cybersecurity professionals, and a lack of threat intelligence that causes dangerous delays.

How can you get your security operations to where they must be?

For the security of your organization and your customers, the focus must be on:

1. **Collaboration and automation.** Keep pace with ever-increasing volumes of aggressive threats by streamlining the process of incident detecting to resolution.
2. **Threat intelligence everywhere.** Relevant and timely threat intelligence relieves security analysts of the burdens of mundane and repeatable tasks, to address what matters most: stopping cybercriminals from causing damage.
3. **Deploying proven, efficient automation.** Organizations cannot sacrifice valuable personnel to constantly manage, test, and update automated actions.

The integration of security orchestration, automation, and threat intelligence

NetWitness Orchestrator streamlines your security operation's response actions by leveraging the first and only technology that weaves threat intelligence with every step of workflow automation and cross-team orchestration.

The result? Incident resolution accelerated.

NetWitness Orchestrator is built on the first and only technology to tightly weave threat intelligence with security orchestration and automation. Think of it as a fully-integrated and more intelligent security orchestration, automation, and response (SOAR) solution—the engine behind more efficient security operations.

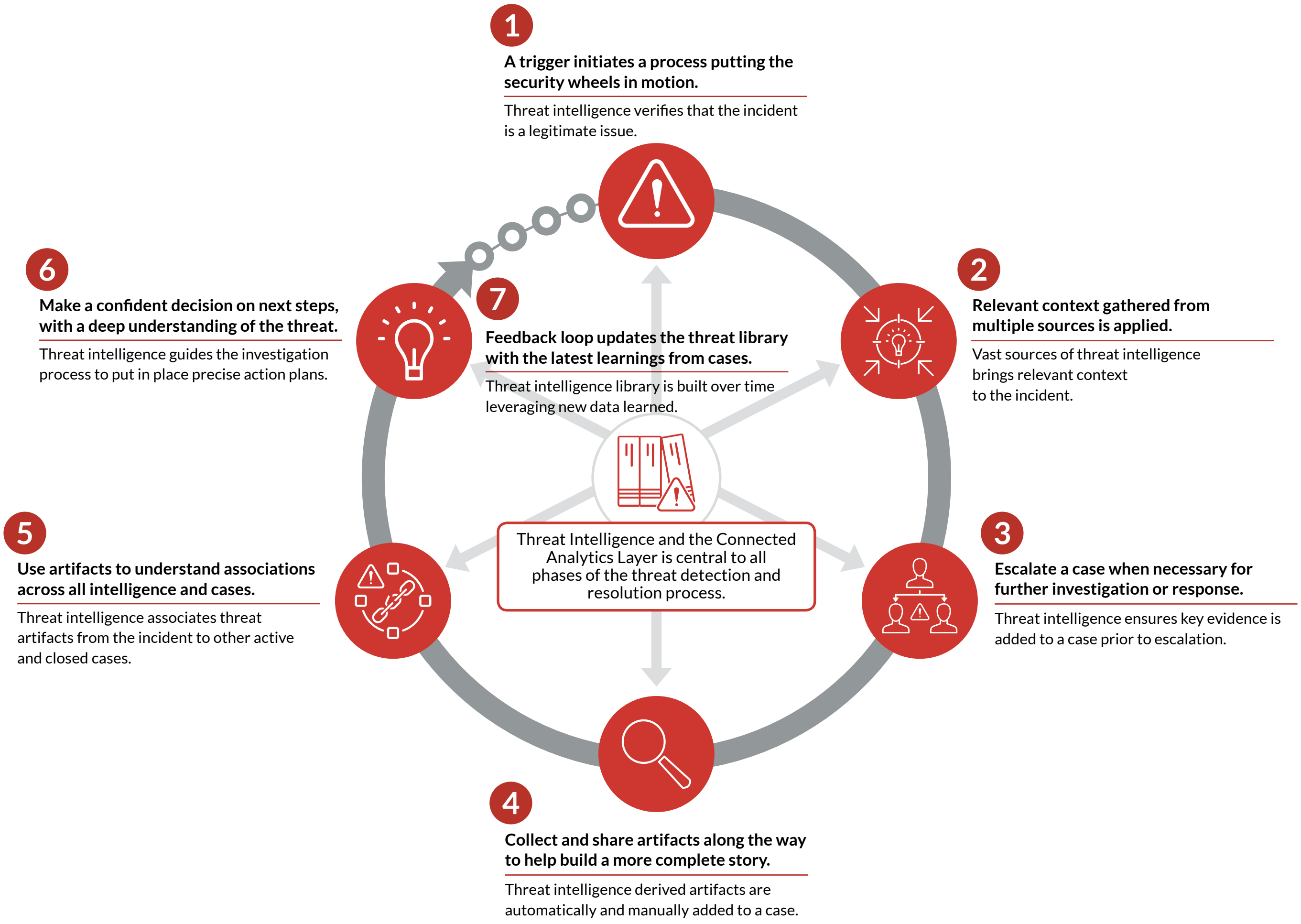
What does NetWitness Orchestrator deliver?

1. Streamlined collaboration that accelerates incident remediation.

- **Collaborative case management.** Enables the entire security team to work from the same game plan with logical and efficient workflows to effectively reduce the time it takes to resolve incidents. Centralize incident information collected and actions performed to understand what has been accomplished and the next logical step in to resolve issues.
- **Automate activities.** Pre-configured or customized playbooks eradicate known or low-risk threats for more precise incident response, while freeing analysts to focus on higher-risk issues.
- **Integrate with your entire security arsenal.** Take advantage of over 500 apps and integrations or APIs to power playbooks. Increases visibility and speed actions. Enables organizations to coordinate intel-driven automation through an ever-growing library of apps and integrations.

2. Leveraged threat intelligence every step of the way.

- **Detect threats with confidence.** Score each potential incident of compromise by comparing it against validated external, internal and crowd sourced threat intelligence to reduce false positives and better understanding impact.
- **Get ahead of common threats through automation.** Launch machine-based automated actions against low-risk threats faster and frees analysts to focus on higher-impact activities to accomplish more with fewer resources.
- **Automatically collect and memorialize key evidence during investigations.** Build stronger case profiles with threat intelligence that automatically identifies evidence and artifacts and add those learned tactics and activities to the centralized threat library.



1 **A trigger initiates a process putting the security wheels in motion.**
Threat intelligence verifies that the incident is a legitimate issue.

2 **Relevant context gathered from multiple sources is applied.**
Vast sources of threat intelligence brings relevant context to the incident.

3 **Escalate a case when necessary for further investigation or response.**
Threat intelligence ensures key evidence is added to a case prior to escalation.

4 **Collect and share artifacts along the way to help build a more complete story.**
Threat intelligence derived artifacts are automatically and manually added to a case.

5 **Use artifacts to understand associations across all intelligence and cases.**
Threat intelligence associates threat artifacts from the incident to other active and closed cases.

6 **Make a confident decision on next steps, with a deep understanding of the threat.**
Threat intelligence guides the investigation process to put in place precise action plans.

7 **Feedback loop updates the threat library with the latest learnings from cases.**
Threat intelligence library is built over time leveraging new data learned.

Threat Intelligence and the Connected Analytics Layer is central to all phases of the threat detection and resolution process.

3. Playbook creation: simplified, verified, and automated.

- **Easy-to-use playbook building and management.** Playbooks bring data from multiple tools together to speed playbook creation, allowing more analysts to create playbooks when/where needed.
- **Build and test along the way.** Deploy playbooks with confidence by testing during development. Understand how playbooks will operate before deployment, saving users time and frustration.
- **Proactive playbook failure notification.** Receive notification of playbook failure without status checks and be assured that playbooks are running when and where they are needed.

4. Flexible and agile deployment.

- **Multi-environment orchestration.** Orchestrate across cloud, multi-cloud, hybrid, or on-premises environments and avoid architectural limitations.
- **Scale to meet new demand.** Easily add resources and automated actions to meet new requirements without re-architecting the solution.
- **Prioritize/dedicate playbooks to different groups.** To remediate an issue faster, align playbooks and processing power to organizations so high-priority actions run without conflicts.

Want to learn more about NetWitness Orchestrator?

Visit the **NetWitness Orchestrator** page for more information.

NETWITNESS
An RSA Business