RESOLVE SYSTEMS™

Datasheet

Resolve Gateway Connector
Micro Focus ArcSight

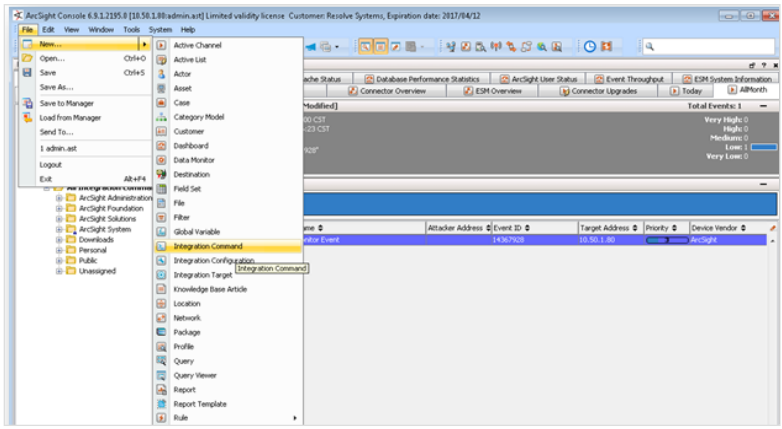
Key Benefits

- Empower security analysts with an integrated solution that extends ArcSight with powerful automation, orchestration, and accelerated response capabilities
- Fully integrated user experience & centralized incident response platform minimizes the need to access disparate systems
- Minimize investigation time by executing automations to automatically collect IOCs and key artifacts
- Large library of integrations with 3rd party security tools to automate the investigation and response of security incidents detected by ArcSight

MICRO FOCUS®

Resolve and ArcSight

Resolve Systems and ArcSight offer a fully integrated solution to validate, investigate, and remediate Security Incidents. Resolve, the market leading enterprise-wide security incident response platform, integrates ArcSight SIEM capabilities with Resolve's powerful automation, process guidance, and human-guided automation capabilities enabling customers to quickly investigate, contain, and remediate incidents.

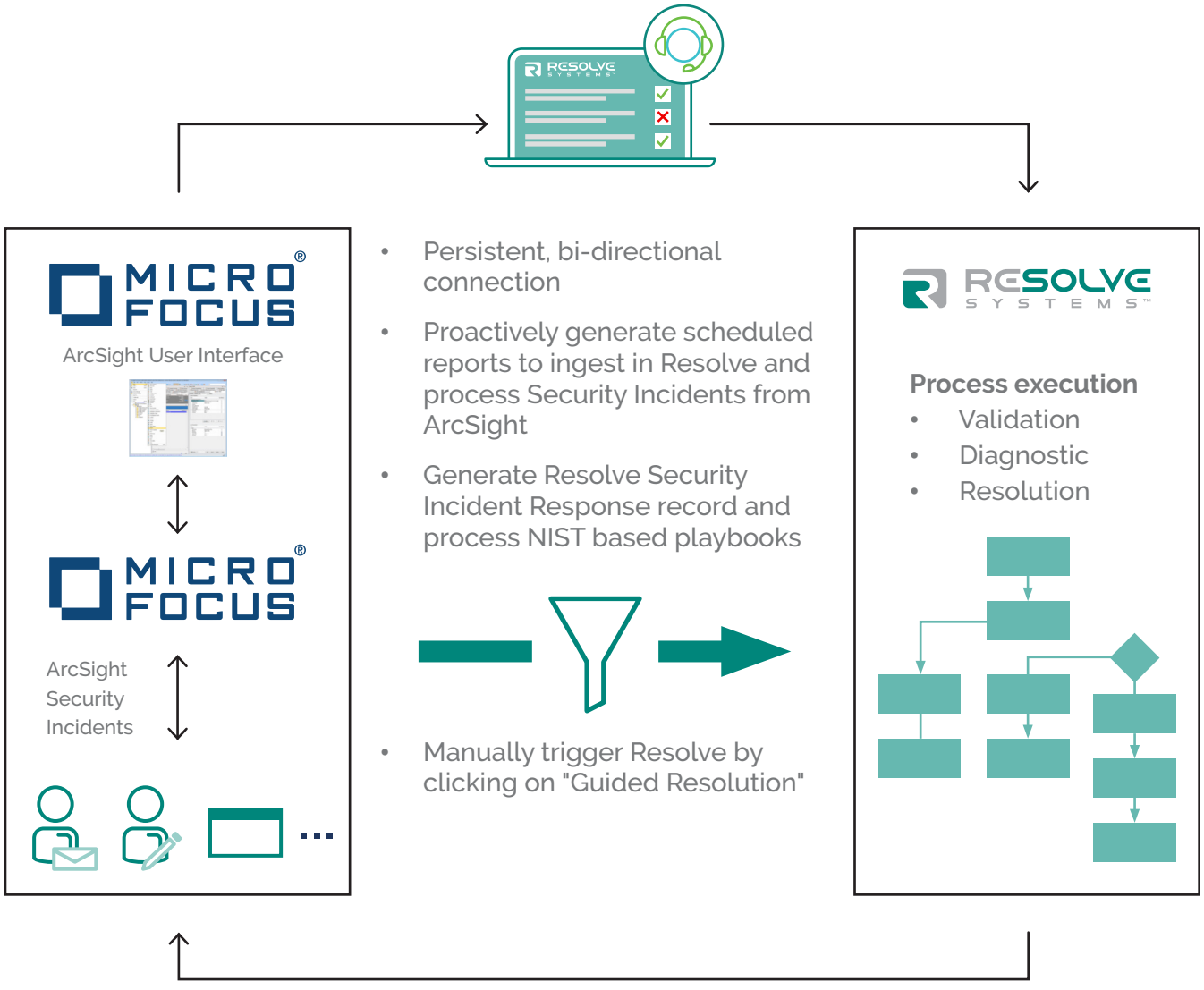


Key Capabilities

- Manually click on incident in ArcSight incident console to execute Resolve automations and process guidance.
- Periodically poll ArcSight for new incidents and trigger new automations and process guidance based off predefined conditions.
- Prepopulate Resolve with critical and relevant ArcSight event details such as event ID, priority, source/target IPs, target ports, etc.
- Create a Resolve security case following NIST 800-61 rev2 based playbooks and procedures enabling additional investigation, artifact collection, containment, and remediation.
- Enable automations and actions to be executed against 3rd party infrastructure systems and devices as a part of the investigation and remediation process.
- Update ArcSight events with status and comments after the Resolve automation and process is completed.

How It Works

The Resolve Gateway Connector for ArcSight leverages ArcSight's generally available API calls. For the ArcSight console integration, the Gateway Connector is configured to execute an ArcSight integration command to send URL and event attributes to Resolve for further processing and execution of automations and process guidance. For the automated polling of events from ArcSight, the Resolve Gateway Connector leverages the ArcSight getReportID call to extract a list of events to trigger the execution of automations and process guidance against the events. Additionally, status updates are executed though the ArcSight update CaseStageID and updateEventStage calls.



About Micro Focus ArcSight

ArcSight Investigate is a next generation hunt and investigation solution built on a new advanced analytics platform to serve the evolving needs of security teams. It helps hunt and defeat unknown threats by processing large volumes of data almost instantly.