

Customer Profile

Size: Fortune 1,000 Companies

Industries: Finance, Oil & Gas, Energy, Telco, Healthcare, Government, Retail, Pharma/Biotech, SLED & Manufacturing

Personas: CISO, CIO, Director of Security, SOC Manager, Security Analyst, Threat Specialist

Threat Detection Topics

- Cyber Incident Management & Security Operations
- Endpoint Detection and Response
- Network Monitoring and Forensics
- Orchestration and Automation
- Incident Response
- Security Information and Event Management (SIEM)
- User Entity and Behavior Analytics

Things to Listen For

- Advanced Persistent Threat (APT)
- Endpoint Forensics
- Incident Management
- Insider Threat
- Malware
- Network Forensics/Visibility
- SIEM
- Security Operation Center (SOC)
- Security Orchestration, Automation & Response

RSA

NetWitness Platform

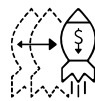
Customer Problem

Staff Shortages: Security teams struggle with a lack of resources, skills, and budgets.

Alert Overload: Need for effective threat detection and prioritization.

Visibility: Need to see everything that is happening in the environment

Disconnected Silos: Unable to correlate and analyze data across security tools



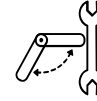
Speed of Value



Complete Response



Prebuilt Integrations



Flexible Deployment

RSA Solution

RSA NetWitness Platform provides **essential visibility** and actionable insight to **detect and respond to threats faster**. The platform offers **flexibility and ease of deployment** to monitor all modern infrastructures. It is a force multiplier helping organizations to **close the security skills gaps**. Customers can **rapidly link security incidents with business context** to respond effectively and **protect what matters most**.

RSA Differentiators

Speed of Detection & Response:

Correlation across security tools, automated playbooks, UEBA and real-time enrichment leading to reduced dwell time

Completeness of Detection & Response:

Unmatched visibility.. Connects silos and create automated response playbooks.

Integration with Security Programs:

Full platform of solutions that can integrate into existing security stacks. Better ROI on all security tools.

Track Record: Globally Recognized Industry & Product Market Leader

DOD Certified as well for the **Common Core**

Questions to Ask

- How quickly are your security analysts able to identify, investigate, and act on security events?
- How do you integrate IT and operational teams into your incident response during a critical event?
- Which forensic tasks does your team run? Can they get the IOC and system data and evidence they need easily and quickly from a central location?
- Do you feel like there are any gaps in visibility across the enterprise?