

# RSA NETWITNESS® PLATFORM PROFESSIONAL SERVICES

## ACCELERATING TIME-TO-VALUE

### EXECUTIVE SUMMARY

#### TECHNOLOGY EXPERTISE

RSA NetWitness® Platform Professional Services are for organizations that want to maximize their return on investment from RSA NetWitness Platform. Customer requirements and expectations are best met when product deployments are adequately planned, implemented and maintained with regular upgrades and tuning.

RSA NetWitness Platform Professional Services are also suited to organizations seeking to complement their in-house resources with RSA subject matter experts.

### PERSONNEL RESOURCING TRENDS

#### A SHORTAGE OF CYBERSECURITY SKILLS

Organizations continue to face a shortage of IT talent, with cybersecurity skills topping the list. This trend is expected to continue for the foreseeable future, particularly when it comes to specific needs, such as advanced threat detection and proactive hunting for signs of attack before harm is done to the organization.

With the demand for trained and experienced cybersecurity professionals exceeding supply, organizations have struggled to develop the measures required to counteract more sophisticated adversaries. Professional Services from RSA and partners provide a viable solution to address the problem:

- Globally distributed team of practitioners
- Trained and accredited security professionals
- Experience gained from thousands of engagements across a range of industries in the commercial and government sectors
- Enterprise-level solution fulfillment addressing complex solution deployment requirements
- Project management services to drive successful outcomes, remediate engagement risks and streamline communications

RSA NetWitness Platform Professional Services are part of the RSA Services organization, which provides a variety of complementary services including consulting services from the RSA Incident Response and Advanced Cyber Defense Practice, training and education services from RSA University and 24x7x365 product maintenance services from RSA Support.



*RSA Solution Fulfillment Framework*  
Our services portfolio ranges from requirements analysis and solution design to deployment and ongoing solution management.

## **RSA NETWITNESS PLATFORM**

### **RESPOND IN MINUTES, NOT MONTHS**

RSA NetWitness Platform Professional Services address requirements to deploy a holistic solution across each of the following component products:

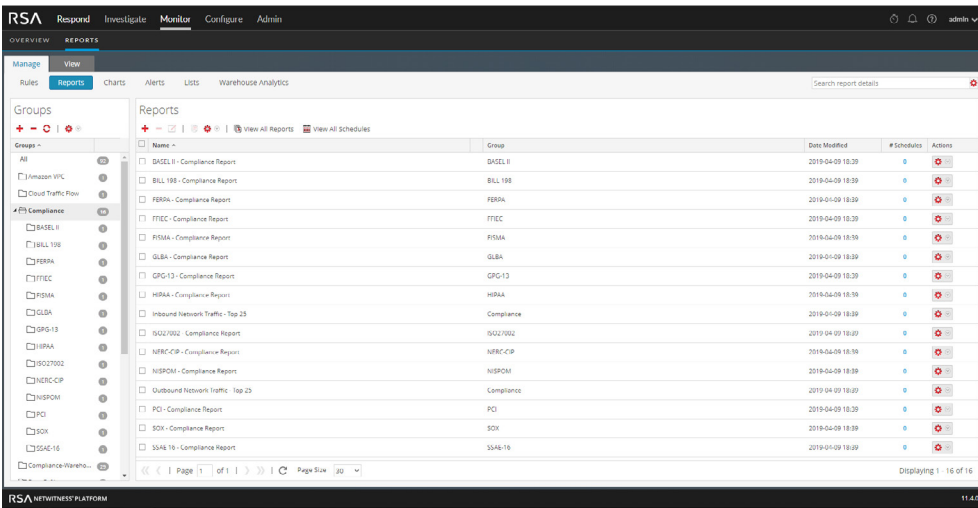
- RSA NetWitness Network—deployed to gain better network visibility and detect advanced threats and anomalies that bypass traditional security controls.
- RSA NetWitness Logs—optimized to aggregate and correlate log data from traditional security alerting tools and mechanisms.
- RSA NetWitness Endpoint—configured to highlight anomalies and conduct analysis on host systems.
- RSA NetWitness Orchestrator—tailored to the organizational structure for automated workflows, improving the efficiency and effectiveness of incident response.
- RSA NetWitness UEBA—integrated with logs, packets and endpoints to correlate across data types and apply threat intelligence and user behavior to detect, prioritize, investigate and automate the response to threats.

The portfolio includes services that accommodate different customer requirements and maturity levels:

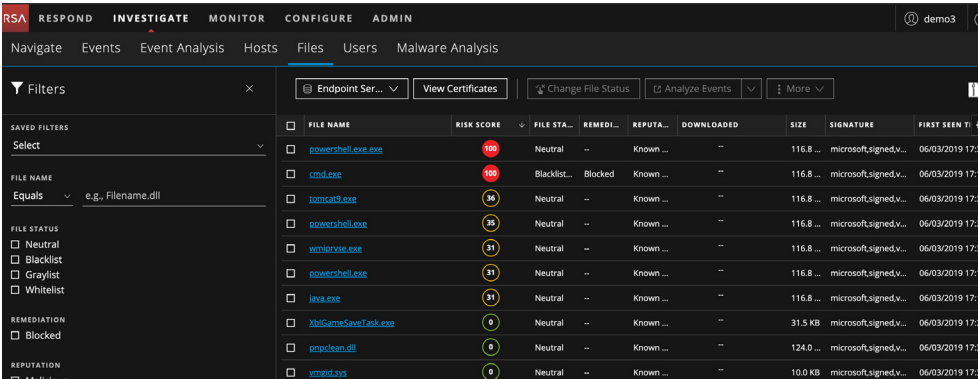
- Design and implementation services—to get the solution up and running, achieve early wins and accelerate time-to-value.
- Subscription services—to provide flexible, ongoing access to RSA experts when you need them.
- Performance services—tuning and optimization to ensure customers get the most from their product investment; planning for upgrades and migrations; and periodic performance assessments to ensure the deployment aligns with evolving business requirements.
- Event source integration services—to accommodate the integration of log event sources, which are not otherwise supported “out of the box.”
- Custom services—tailored consulting for platform migrations, technology integration, high availability configurations, residencies and “expert-on-demand” staff augmentation.
- Offshore services—lower cost solution fulfillment by RSA’s Virtual Services Delivery (VSD) team.
- Analytic intelligence services—to share techniques that facilitate advanced threat detection. These are complementary services, such as the RSA Jumpstart for Analytic Intelligence, which is delivered by the RSA Incident Response and Cyber Defense team.
- SOC services—to support the integration of RSA NetWitness Platform with organizational incident response and breach management requirements. These are complementary services, such as the Strategy and Roadmap for Security Operations, which is delivered by the RSA Incident Response and Cyber Defense team.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
01/14/2020 11:50:57	LOW	0	INC-44	File Upload from Critical Systems to Dynamic DNS	Assigned	Sam Polanco	1
01/14/2020 11:50:55	HIGH	70	INC-43	Phishing - Obfuscated Link	Assigned	Sam Polanco	1
11/13/2019 10:28:49	LOW	30	INC-42	Failed Login Activity for Failed Logins Outside Business Hou...	Assigned	Alex Lane	4
11/13/2019 10:28:49	MEDIUM	50	INC-41	Failed Login Activity for Multiple Failed Logins Followed By ...	Assigned	Alex Lane	4
11/13/2019 10:28:49	LOW	30	INC-40	Failed Login Activity for Multiple Failed Logins from Same S...	Assigned	Alex Lane	2
11/13/2019 10:28:49	MEDIUM	50	INC-39	Suspicious Configuration Activity for Detects Router Config...	Assigned	Sam Polanco	23
10/28/2019 10:58:10	CRITICAL	50	INC-38	Phishing attempt from 41.140.181.156	Assigned	demo9	1
10/21/2019 03:36:15	CRITICAL	50	INC-37	New Phishing alert	New		1
10/17/2019 16:56:12	HIGH	50	INC-36	大量印刷 - プリンタ送信	Assigned	demo9	1
08/15/2019 21:25:07	CRITICAL	70	INC-31	大量ファイルの圧縮化	New		1
07/31/2019 19:01:30	CRITICAL	50	INC-30	外部記憶媒体への大量ファイルコピー	Assigned	demo10	1
07/17/2019 05:14:13	CRITICAL	50	INC-29	特定サイトへのアクセス	Assigned	demo3	1
06/03/2019 18:35:16	LOW	0	INC-28	特定ファイルサービスへの大量アクセス	Assigned	Sam Polanco	1
06/03/2019 18:28:12	MEDIUM	50	INC-27	Failed Login Activity for Multiple Failed Logins Followed By ...	Assigned	Alex Lane	2
06/03/2019 18:25:13	LOW	30	INC-26	Failed Login Activity for Failed Logins Outside Business Hou...	Assigned	Alex Lane	2

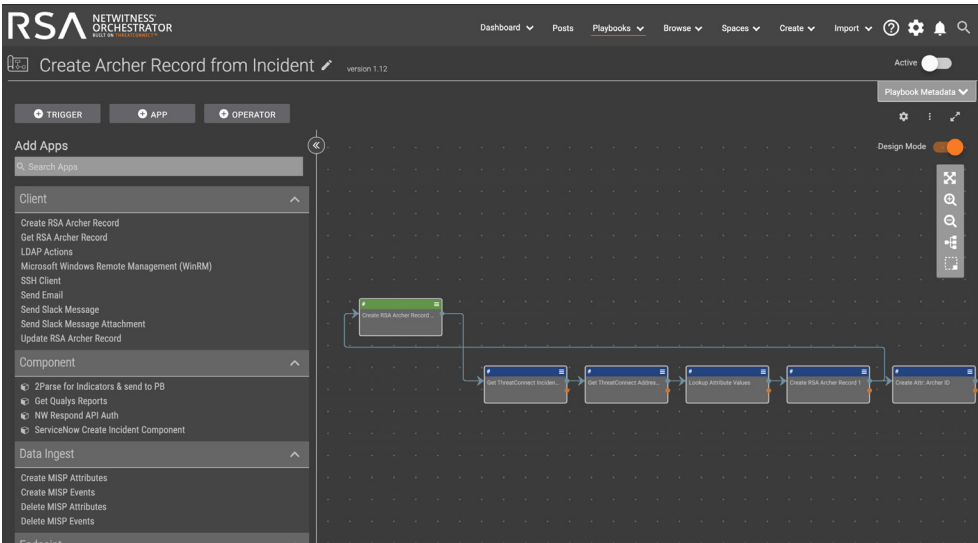
RSA NetWitness Platform Incidents dashboard used to correlate alert data, assign priority and track the remediation status of the incident response team.



RSA NetWitness Logs  
Reports dashboard used to manage compliance and the potential impact of threats and incidents.



RSA NetWitness Endpoint  
Endpoint dashboard using a numerical scoring system to depict the risk level of host systems, while highlighting those with files which may be a threat to the organization for prioritized attention.



RSA NetWitness Orchestrator  
Automated playbooks with step-by-step instructions used to accelerate response time and enhance overall SOC efficiency and effectiveness.

## PUTTING IT ALL TOGETHER

### RSA TARGETED ATTACK DETECTION

Protecting an organization's critical assets requires the right combination of technology and expertise. Attackers leave clues at both the network and the host levels, where valuable indicators of activity can be gathered for analysis. Security teams need to look for subtle indicators of compromise and risky behavior rather than expect that preventive control mechanisms will succeed in blocking sophisticated adversaries.

RSA NetWitness Platform comprises a set of comprehensive and key technologies that provide organizations with the opportunity to gather early signs of compromise. When combined with the skills and knowledge transfer capabilities of RSA NetWitness Platform Professional Services and the RSA Incident Response & Cyber Defense team, organizations can begin to retake the high ground and protect the organization's most critical assets.

### ABOUT RSA

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](https://rsa.com).

