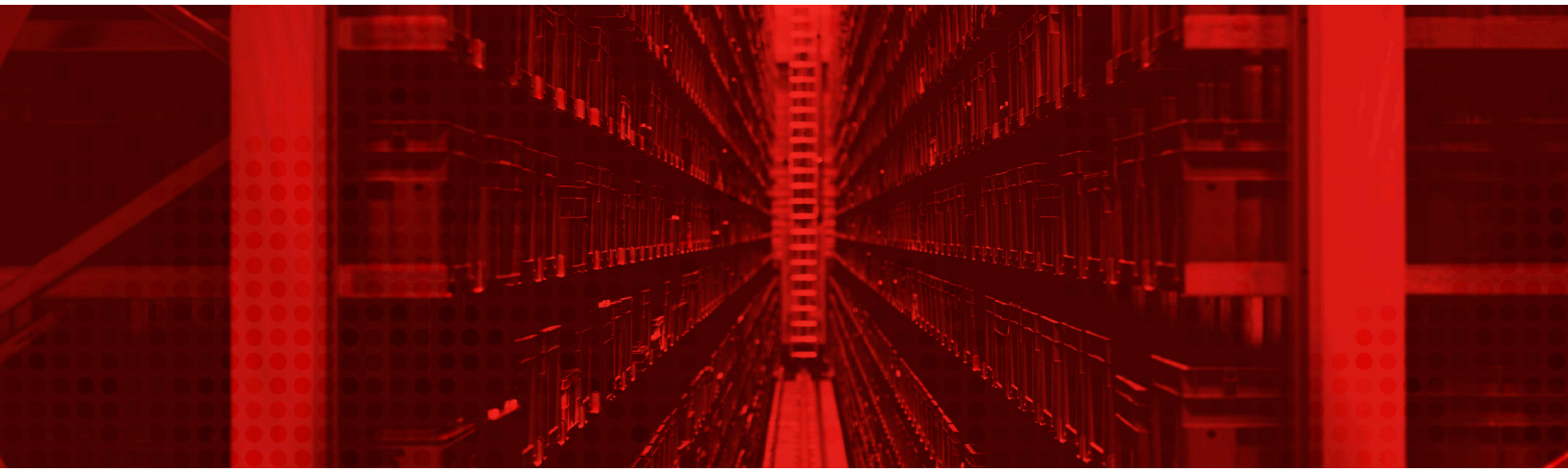
RSA

SOLUTION BRIEF

THREAT DETECTION & RESPONSE FOR IT AND OT SYSTEMS

DEFENDING CRITICAL INFRASTRUCTURE WITH RSA NETWITNESS® SUITE



IT AND OT CONVERGE—AND THREATS DO TOO

Before the Information Technology (IT) Revolution, the world experienced an Operational Technology (OT) Revolution—all the water, power, manufacturing and distribution systems that lifted humanity into the modern age. OT systems typically are deployed in the form of an industrial control system (ICS), with management performed using a supervisory control and data acquisition (SCADA) system.

Traditionally, OT has been managed and monitored separately from IT. OT systems were commonly "air-gapped" from IT infrastructures and treated as a separate environment, managed by different analysts and with different primary goals. For OT, it's all about uptime and availability, and thus SCADA tools traditionally focused on monitoring for misconfiguration and malfunctions—which are genuine problems, but not malicious in nature.

That's what's changed. OT systems today take full advantage of the power of software and networks, which lower costs and increase sophistication and performance. Air gaps have given way to connected solutions, with one-third of industrial sites connected to the internet.[1] As OT has become increasingly accessible and exposed to attackers, the need for operational threat detection and response is rising quickly.

In practice, the process of OT cyber defense is very similar to its IT counterpart. IT security has dealt with threat actors for decades, which has led to the development of practices and solutions optimized to detect and neutralize the most advanced threats. In practice, the threats you see in IT share many of the same characteristics of the attacks that are now targeting OT, including the same tactics, techniques and procedures (TTPs). This drives both the opportunity and the need for solutions that work across both of these critical infrastructures.

IT analyst firm Gartner predicts the convergence of IT and OT solutions: "It is Gartner's opinion there will be less distinction between different market sectors for digital security after 2020 due to phases of technology integration, resulting in products that can function for specific security needs across all markets."[2] As systems and processes converge, so too will OT and IT security teams. A common language and methodology will need to evolve as well. The RSA NetWitness® Suite provides a single platform that can deliver visibility to threats across both IT and OT operations so that organizations can start this journey of convergence and start to tackle the evolving threat landscape across OT operations with a proven security platform.

THREAT-BASED VISIBILITY

RSA NetWitness Suite is designed to find cyber threats wherever they are—on IT systems or OT systems, across servers and desktops, whether deployed on-premises or in the cloud. The key is visibility across data types and sources, and the ability to process the massive amounts of data that result. Threat intelligence and machine learning are applied to spot anomalous behavior—the footprints left by threat actors—and reveal the full scope of an attack, so it can be appropriately remediated.

As IT and OT continue to converge, the ability to monitor across both domains becomes more important. Connected systems introduce complexity and broaden the attack surface. OT managers, traditionally measured by uptime and availability, now must secure their systems against skilled and determined attackers.

RSA NetWitness Suite monitors and identifies anomalies—leveraging network data inspection for proprietary protocols—and correlates them across IT and OT systems. The flexibility to ingest and normalize data from myriad systems, via logs, packets or endpoint, leaves attackers with little room to hide.

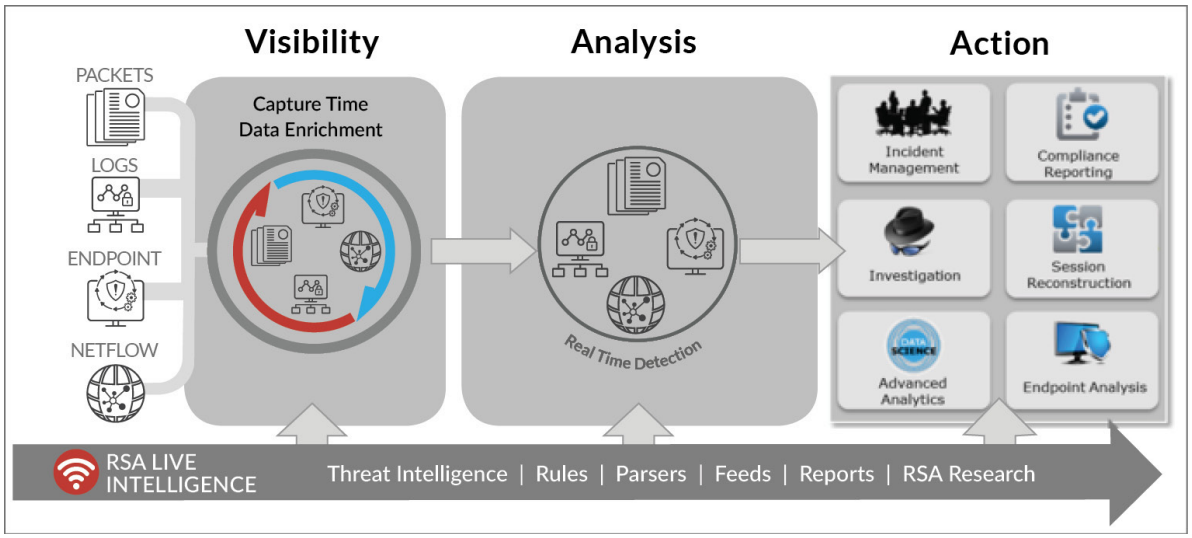


Figure 1: Data and Content Types

COMPREHENSIVE DETECTION AND RESPONSE

As with their IT counterparts, OT systems are creating ever-increasing amounts of data to analyze. System interconnections and components such as wireless sensors are being integrated into the management of industrial environments. It's important to note that many OT systems were not originally designed for remote accessibility, so concepts like regular updates and patches have not been as widely adopted as in IT security.

RSA NetWitness Suite is designed to optimize the productivity of security personnel of all skill levels, from new security and network analysts to the most experienced threat hunters and incident responders. Its modular architecture handles massive amounts of raw data, enriching it with security context at time of capture, and applying machine learning, behavior analytics and threat intelligence. This process correlates disparate events and alerts into discrete incidents, automatically and accurately scoring each according to risk.

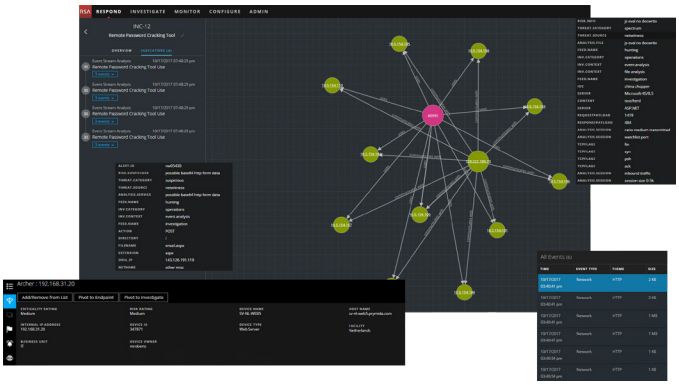


Figure 2: RSA NetWitness Suite "Respond" Visualization Screen

THREAT ANATOMY

Advanced threat actors have various motivations (e.g., competitive, philosophical, financial) and goals (e.g., espionage, IP theft, customer data exfiltration). But their TTPs—their modus operandi, if you will—are limited to a small set of general actions:

- An exploit is designed to land on the target's infrastructure while evading detection.
- Communication with a command and control (C2) system is established.
- The exploit analyzes the infrastructure for purposes of exploitation, i.e., data exfiltration or credential harvesting.
- The exploit performs its intended action.

There are variations at each step. For example, the method of exploit injection could range from a phishing email (common for IT systems) to a USB drive introduced via social engineering (for an air-gapped OT system). And the C2 and analysis steps might be limited on a commercial ICS system with a low range of variability. But the general model is quite similar.

For the good guys battling these threats, both prevention and detection are core activities.

Prevention is provided by traditional solutions such as virus detection and IPSs, and activities such as patch management. Detection presumes that some threats will still get through, as threat actors increasingly leverage strategies like polymorphic code. These stealthy exploits can land undetected on an IT or OT infrastructure, but eventually they'll have to do something, and it's these activities which can be detected with the right tools and skills.

SUPPORT FOR OT SYSTEMS

RSA industry partnerships extend to the OT industry. The RSA Ready program highlights interoperability with hundreds of vendor solutions. In the OT industry, RSA has partnered with leading vendors in OT system management and security. For a complete, current list, please visit rsa.com/rsaready.

PRIORITIZING OT ALERTS

One challenge with OT systems is that the majority are designed with proprietary protocols. RSA NetWitness Suite addresses this gap with its "parse everything" capability and support for custom parsers, part of a real-time rules engine that facilitates incorporating OT alerts into the primary threat detection and response solution. Professional services, including partners with OT expertise, provide a "decoder ring" to interpret messages and logs from various OT systems, while correlating with activity from other IT and OT platforms. When augmented with machine learning and threat intelligence, the resulting rich metadata helps deliver meaningful alerts.

RSA SERVICES AND SUPPORT

The RSA NetWitness Suite is backed by RSA world-class professional services and support.

The RSA Global Services team is comprised of over 650 cybersecurity experts delivering services in over 100 countries. RSA Professional Services provides implementation, tuning and training services to deliver business value fast.

Within the RSA Risk and Cybersecurity Practice, two groups provide critical security capabilities:

- The RSA Advanced Cyber Defense (ACD) Practice delivers services to assess breach readiness, Security Operations Center (SOC) or (CIRC/CIRT) assessment and design, incident response planning and testing, and "Expert on Demand" services.
- The RSA Incident Response (IR) Practice helps customers design, manage and perform the Incident Response function, with both proactive and reactive services. Available on both retainer and ad hoc bases, the RSA IR Practice extends your organization's security skills to deal with security incidents of all types and severities.

For more information about RSA NetWitness Suite, visit rsa.com/DoMore.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit **rsa.com**.

1. Global ICS IIoT Risk Report. CyberX
2. Gartner—Market Guide for Operational Technology Security, August 2017; Earl Perkins, Ruggero Contu, Saniye Burcu Alaybeyi