

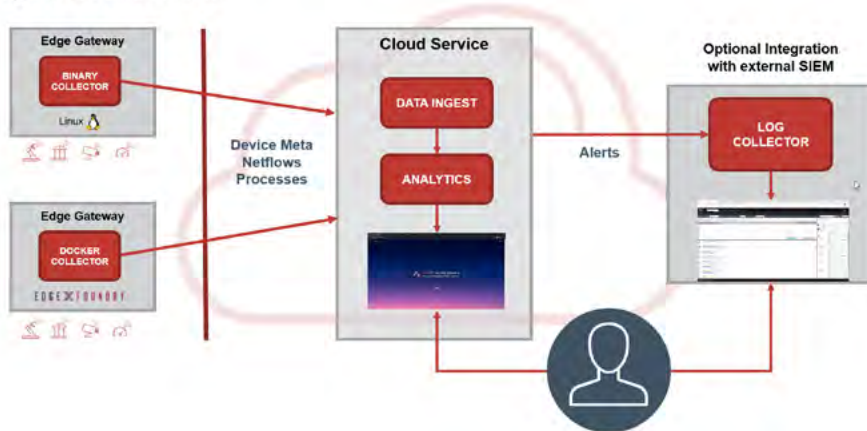
# RSA IoT Security Monitor: Edge Monitoring & Analytics for IoT

## An Innovative Approach to IoT Security

The Internet of Things (IoT) is a core element of digital transformation, along with cloud, mobile, automation and analytics. But if you work in the cybersecurity or risk areas, this proliferation of IoT endpoints creates a strain on effective operational security. The bottom line is that IoT introduces a massive volume of new, often unmonitored endpoints across your network.

RSA has developed RSA IoT Security Monitor, a solution that addresses this challenge by dramatically improving an organization’s ability to detect anomalous behavior on IoT devices. This critical capability enhances both security and risk programs. Developed by RSA Labs, RSA IoT Security Monitor features new methods and algorithms for detecting compromised devices based on anomalous behavior. The large scale of IoT deployments and the massive number of devices make this behavior-based approach both effective and efficient.

**RSA IoT Security Monitor**  
High Level Architecture



The RSA IoT Security Monitor Cloud applies threat analytics to flag known bad actions (e.g., communication with blacklisted IPs), as well as behavioral analytics to detect anomalous behavior based on the specific IoT device type and its function. Alerts are generated for analysts to view and investigate IoT incidents directly in the cloud interface.




---

Data can be sorted by gateway and device, with drilldown and pivoting functions to analyze and understand anomalous behavior including indicators of compromise. The ability to combine filters empowers analysts to pursue data in very flexible ways.

Created	Rule	Severity	Service	Message
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected
2020-06-10 10:10:10	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected

---

Alerts are assembled and displayed with the severity indicated by color. This view supplies all the major metadata and plain-language descriptions of the data that caused the alert, such as “This device connected to a destination it normally doesn’t connect to.”

Alert Name	Rule	Severity	Service	Message
Device Offline	Device Offline	Critical	IoT Gateway	Device 1234567890 disconnected

---

You can take action from the Alerts screen, either by marking “False Positive” and giving the application additional data to process about what “normal” looks like, or by viewing the metadata directly. You can mark the data as “Viewed” in either interface.

## Subscriptions

RSA IoT Security Monitor is available as a monthly SaaS subscription that includes all necessary agents for gateways and servers. The base offering includes the service and 5 GB of data storage. Additional capacity can be ordered in 10 GB increments. Customers can define a maximum storage value in either time or data size, and data will “roll out” on a first-in, first-out basis. The RSA IoT Security Monitor collector (agent) is approximately 5 MB and can be installed as a Docker container or as a Go program for Linux. For more information, contact your RSA seller or [contact us](#).

## About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. 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, visit [rsa.com](#).

