WHITE PAPER

RSA IoT SECURITY MONITOR: EDGE MONITORING & ANALYTICS FOR IoT

IoT GROWTH CREATES NEW SECURITY AND RISK REQUIREMENTS

The Internet of Things (IoT) is a core element of digital transformation, along with cloud, mobile, automation and analytics. Strong business benefits are driving adoption. "Gartner forecasts that 14.2 billion connected things will be in use in 2019, and that the total will reach 25 billion by 2021, producing immense volume of data."[1] Sensors, cameras, meters, thermostats and other networked controls deliver game-changing capabilities to organizations of all types and sizes. Industrial control systems (ICS) deliver power, water and transportation services as well as manufacturing processes like robotics. Large-scale government projects like smart cities initiatives break new ground in delivering services and improving quality of life for residents.

> **"Gartner forecasts that 14.2 billion connected things will be in use in 2019, and that the total will reach 25 billion by 2021, producing immense volume of data."[1]**

But if you work in the cybersecurity or risk areas, this proliferation of IoT endpoints creates strain on effective operational security. As with other types of digital transformation, IoT creates digital risk. The bottom line is that IoT introduces a massive volume of new, often unmonitored endpoints across your network; from the same Gartner release: "CIOs should ensure they have the necessary skills and partners to support key emerging IoT trends and technologies, as, by 2023, the average CIO will be responsible for more than three times as many endpoints as this year." And they are all targets for attack.

This paper describes an approach 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. RSA IoT Security Monitor delivers this solution by monitoring the edge and leveraging targeted analytics for IoT deployments.

IoT SECURITY IS NOT JUST ONE THING

Based on research and discussions with customers and analysts, RSA has identified six areas that are critical for IoT end-to-end security (Figure 1).

These six areas are:

- **Discovery, Identification & Classification**—The discovery process detects the existence of an endpoint at a certain IP address. The identification process then takes this to the next level by detecting the specific information about the device; for example, detecting that a device is a motor from a certain manufacturer. Additional information such as model number, serial number and firmware version number may also be captured. This metadata is correlated with additional information such as known vulnerabilities, operational strengths and weaknesses, and common misuse and misconfiguration scenarios about the device. This deep classification creates additional granularity in tracking and reporting.
- **Risk Management**—Once IoT devices are identified, they must be assessed continuously for associated risk. The risk profile of an IoT deployment changes over time, affected by activities such as adding and removing devices to/from the network, changes to access policies, discovery of new vulnerabilities and the firmware/software updates applied to devices. Third-party risk arises, associated with the exchange of IoT data between the enterprise and external service providers. And as digital transformation continues and IoT technology matures, there will be an increasing number of regulations and guidelines for enterprises to track and comply with, such as FDA guidelines for cybersecurity of connected medical devices.

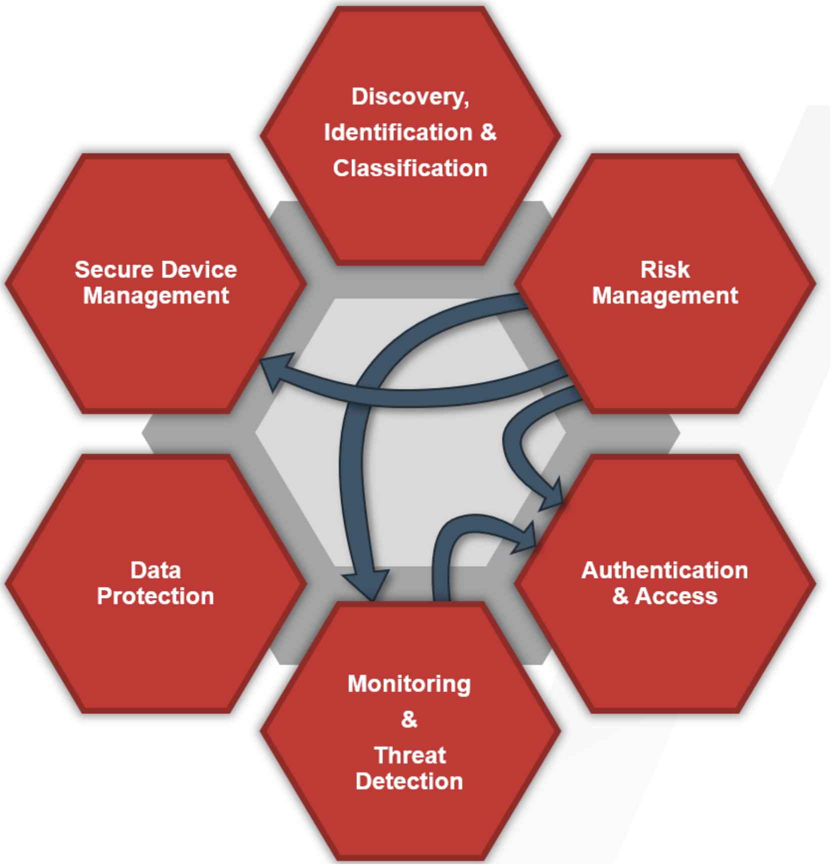


Figure 1. Six areas critical for IoT end-to-end security.

- **Authentication & Access**—Enforcing authentication and access policies ensures operational integrity of the connected environment. This includes protecting access to and from the device. The strengths and weaknesses of access policies should be dynamically reflected in the continuous risk assessment of the overall environment.
- **Monitoring & Threat Detection**—The massive scale of IoT deployments and prevalence of low-power devices creates security and risk challenges but offers one advantage: an abundance of IoT operational data and use data. Analytics can profile devices, baseline the normal behavior, and detect and alert on anomalous activities and compromised devices. Leveraging machine learning and with no requirement to changing IoT devices, these techniques can secure large deployments of sensors and actuators.
- **Data Protection**—The data collected from connected devices is critical to the success of any IoT project. The integrity of IoT data is fundamental to arriving at the desired business insight, reliable operational decisions or sound security analysis. The protection of the data at rest, in transit or in process is critically important in today's privacy-focused landscape.
- **Secure Device Management**—It is essential to have a secure solution for device management in an IoT deployment. As a minimum, this includes secure remote maintenance and over-the-air or over-the-net updates for the software and firmware on the device. Similar to modern IT operations, these features provide better agility for the security staff to deal with vulnerabilities and security incidents, especially given the scale of IoT.

As with other types of digital transformation, IoT creates digital risk. The bottom line is that IoT introduces a massive volume of new, often unmonitored endpoints across your network.

Additionally, as depicted in the diagram, there are interdependencies among these areas. Examples of interdependencies:

- Through the process of risk assessment, sensitive assets may be given higher priority for protection through identity and access management (IAM) or monitoring services.
- When a monitoring tool alerts on a potential threat, IAM services may automatically be invoked to control access to affected assets, control connectivity to outside networks, etc.
- Sensitive or high-risk assets may require tighter maintenance inspection and update policies.

IoT SECURITY PRESENTS SPECIFIC CHALLENGES

To be sure, the IoT device industry is gaining security capabilities quickly, mainly as a result of threats presented by attackers around the world, from hacktivists to cybercriminals to nation-states. The 2016 Mirai botnet attack on Dyn, a major DNS service, took down major platforms across Europe and North America. Previously, botnets had been primarily an issue with unpatched computers, but Mirai hijacked IoT devices by the millions—among them a huge number of security cameras and DVRs. Even with relatively low computing power in IoT devices, the sheer number of hijacked devices, each originating from unique IP addresses, created catastrophic failure for hours.

To be sure, the IoT device industry is gaining security capabilities quickly, mainly as a result of threats presented by attackers around the world, from hacktivists to cybercriminals to nation-states.

Certainly Mirai raised awareness of IoT as an attack vector, driving changes in the way devices are secured and updated going forward. However, the large population of brownfield (existing) IoT devices, especially in operational technology (OT) use cases, will continue to make it difficult to implement comprehensive IoT security patterns. Many brownfield devices and protocols weren't designed for open networking, lack compute and power required for performing security functions, are difficult or impossible to update or patch, and have limited replacement options. They are designed to be deployed for decades, far beyond the typical IT refresh cycle.

There are other important challenges to securing IoT, including historic patterns. Traditionally, security and identity systems have operated separately from IoT systems. Cybersecurity teams secure and monitor IT systems; IoT systems are often managed by business operations with separate engineering teams. Additionally, IoT devices may be deployed in the field and in potentially hostile locations with no physical security guarantees (e.g., an unmanned wind turbine or traffic sensors in a smart city use case). In such scenarios, the IoT devices require additional protection measures against physical attacks such as manipulating or replacing devices.

AN INNOVATIVE APPROACH TO IoT SECURITY

RSA is a technology and market leader in many of the areas necessary for securing IoT environments, including risk-based authentication, user and entity behavior analytics (UEBA), and fraud detection at scale for IT. With RSA IoT Security Monitor, RSA delivers new methods and algorithms for monitoring and detecting compromised devices based on anomalous behavior. The large scale of IoT deployments and the massive number of devices provide a rich medium for this type of solution.

RSA IoT Security Monitor leverages an important development in IoT evolution: open solutions for IoT edge management. IoT edge gateways and servers consolidate and integrate IoT devices, in an “edge to core to cloud” continuum, taking control of any IoT deployment, no matter how diverse. This foundational IoT technology, along with compatible solutions extending the platform, addresses the critical IoT risk areas of Identification, Data Protection and Device Management.

> **IoT edge gateways and servers consolidate and integrate IoT devices, in an “edge to core to cloud” continuum, taking control of any IoT deployment, no matter how diverse.**

RSA IoT Security Monitor focuses specifically on the Risk Management and Monitoring & Threat Detection challenges. It gives organizations a tool to view and analyze the consolidated data set of their entire IoT deployment (Figure 2). The data and corresponding alerts can be seen using a web interface or ingested into popular security tools including existing security information and event management (SIEM) threat detection platforms for visibility alongside other IT assets.

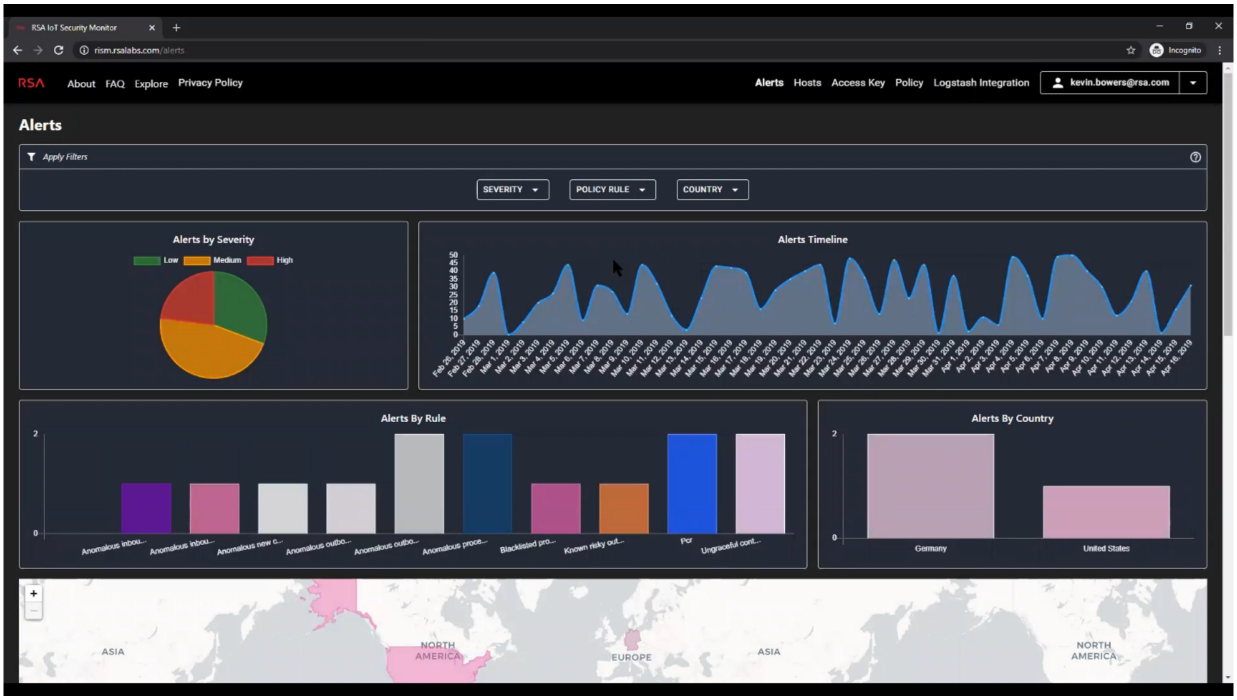
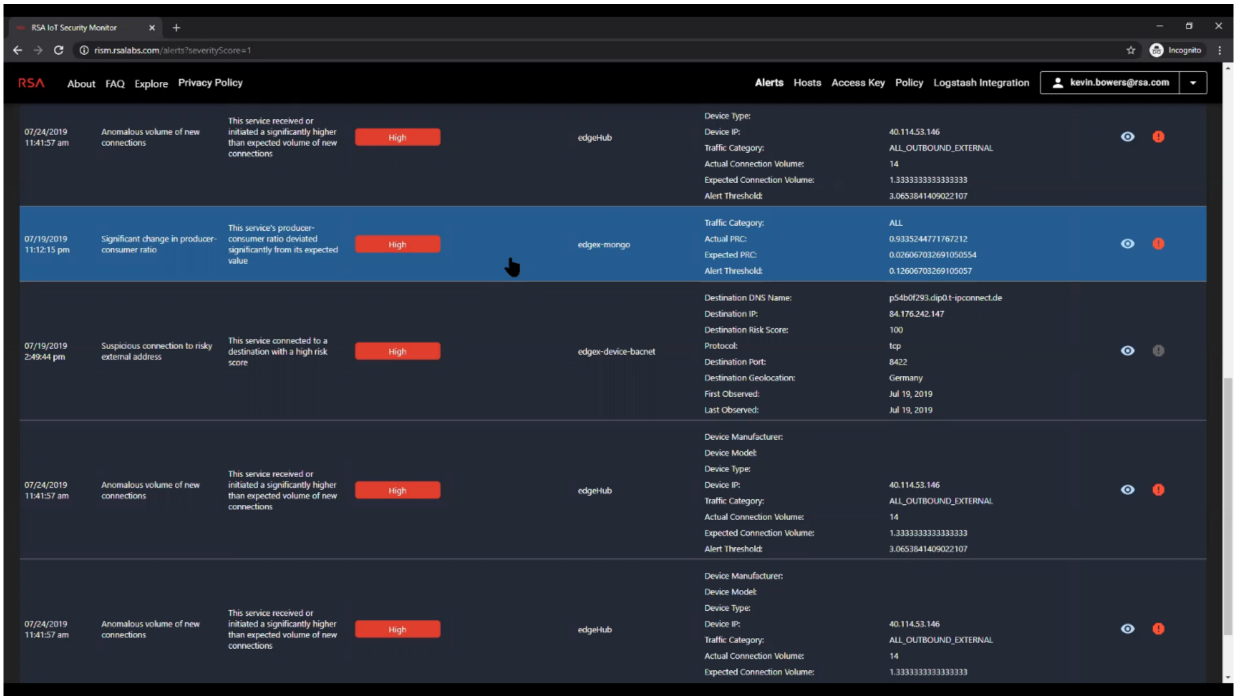


Figure 2. RSA IoT Security Monitor analyzes the consolidated data set of their entire IoT deployment.

The code is delivered as a containerized agent application or Go program that plugs directly into your edge infrastructure. The agent is deployed on all edge gateways and edge servers, and passively collects data about the edge device itself and the devices managed by it, capturing logs, network data, and even process and resource consumption information. The RSA IoT Security Monitor Cloud applies threat intelligence 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 (figure 3). 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.

The RSA IoT Security Monitor Cloud applies threat intelligence to flag known bad actions as well as behavioral analytics to detect anomalous behavior based on the specific IoT device type and its function.

Alerts are assembled and displayed with the severity indicated by color (Figure 3). 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.”



07/24/2019 11:41:57 am	Anomalous volume of new connections	This service received or initiated a significantly higher than expected volume of new connections	High	edgeHub	Device Type: Device IP: Traffic Category: Actual Connection Volume: Expected Connection Volume: Alert Threshold:	 40.114.53.146 ALL_OUTBOUND_EXTERNAL 14 1.3333333333333333 3.0653841409022107
07/19/2019 11:12:15 pm	Significant change in producer-consumer ratio	This service's producer-consumer ratio deviated significantly from its expected value	High	edgex-mongo	Traffic Category: Actual PRC: Expected PRC: Alert Threshold:	ALL 0.9335244771767212 0.026067032691050554 0.126067032691050 57
07/19/2019 2:49:44 pm	Suspicious connection to risky external address	This service connected to a destination with a high risk score	High	edgex-device-bacnet	Destination DNS Name: Destination IP: Destination Risk Score: Protocol: Destination Port: Destination Geolocation: First Observed: Last Observed:	p54b0f293.dip0.t-ipconnect.de 84.176.242.147 100 tcp 8422 Germany Jul 19, 2019 Jul 19, 2019
07/24/2019 11:41:57 am	Anomalous volume of new connections	This service received or initiated a significantly higher than expected volume of new connections	High	edgeHub	Device Manufacturer: Device Model: Device Type: Device IP: Traffic Category: Actual Connection Volume: Expected Connection Volume: Alert Threshold:	 40.114.53.146 ALL_OUTBOUND_EXTERNAL 14 1.3333333333333333 3.0653841409022107
07/24/2019 11:41:57 am	Anomalous volume of new connections	This service received or initiated a significantly higher than expected volume of new connections	High	edgeHub	Device Manufacturer: Device Model: Device Type: Device IP: Traffic Category: Actual Connection Volume: Expected Connection Volume:	 40.114.53.146 ALL_OUTBOUND_EXTERNAL 14 1.3333333333333333

Figure 3. Alerts are assembled and displayed with the severity indicated by color.

CONCLUSION

RSA IoT Security Monitor is a new service offering that vastly improves organizations’ ability to secure the huge and varied universe of IoT. For operations or security managers who need a consolidated view of digital risk for devices of every type, RSA IoT Security Monitor delivers leading-edge security in a simple, machine learning-based solution.

For more information and to request a consultation, please visit rism.rsalabs.com.

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.

[1] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

©2020 Dell Inc. or its subsidiaries. All rights reserved. RSA and the RSA logo, are registered trademarks or trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 4/20 White Paper, H18296 W362932.