RSA

SOLUTION BRIEF

RSA MISSION-DRIVEN SECURITY FOR THE PUBLIC SECTOR

MANAGING THE NEXUS OF RISK & SECURITY

RSA

A CHANGING LANDSCAPE—AND A NEW APPROACH

Public-sector technology continues to become increasingly complex. Many government agencies and departments are finding that they must embrace new technologies just to maintain efficiency. These technologies also underpin many key administrative and operational innovations. The number of devices, identities and systems that interact with any given agency, from both inside and outside the organization's firewall, is growing rapidly. This situation is driven by factors including increased collaboration in the cloud, the mobility of operations and service delivery teams, an expanding number of internet-capable devices and sensors, and an increase in privileged external users.

Together, these factors pose a serious challenge for risk, security and fraud teams needing to protect critical infrastructures, customers and data. And as problems multiply, so do security offerings. Public-sector IT professionals must weigh literally hundreds of options, seeking the best solution—or combination of solutions—that can achieve their goals and evolve with their mission.

At RSA, we embrace the concept of business-driven security—an approach that operates at the nexus of business and security. This additional layer of intelligence across your risk management and security programs prioritizes security efforts by aligning risk with business goals, and uses tools to manage IT risk as a core business process.

While not ruled by the same for-profit incentives as private industry, government and public-sector organizations share many of the same strategic security and risk imperatives. Both need to support the organizational mission. In the public sector, business-driven security becomes mission-driven security. Our offerings for the public sector are designed to work on your IT architecture, with your IT product ecosystem and in support of your goals.

SECURITY THAT UNDERSTANDS YOUR MISSION AND GOALS

RSA software and security services have helped organizations stay secure for more than 35 years. Today we offer a range of security and risk management products and services for security-aware organizations like yours. Our leadership across several major security segments has given us unique insight into public-sector risk and security domains.

RSA public-sector customers are some of the world's most security-conscious organizations, and they trust us to protect them from threats and risks. Our solutions are built to simplify and automate that messy area at the intersection of mission and security. We make it happen by translating the language of mission risk into the details of cybersecurity.

At RSA, we see mission and security strategy interweave in three essential areas:

- **Inclusion** means using identity and access management to make sure the right people have access to the right information, in a way that isn't disruptive to users. As trends, industry standards and government regulations evolve, inclusion has become a key component of public-sector mission and security strategy.
- **Exclusion** means keeping bad things out of your network. Here, public-sector organizations use traditional tools such as AV, firewalls and IDS systems operating at the IT perimeter—but more and more, these are bolstered by detection and response activities designed to catch attacks that perimeter controls can't block.
- **Contextual intelligence** informs both of the above functions, incorporating mission factors to more effectively address risks, threats and fraud. Identify what's most critical to the organization, and you make those controls far more effective.

This concept becomes very important in specific use cases. For instance, many public-sector organizations have increased their use of external partners, vendors and consultants. Third parties may be called upon to provide support in a disaster response, offer expertise during deployment of an enterprise tool or manage a privatized operation directed by in-agency teams. This practice can allow government organizations to better focus on core activities, provide access to expertise lacking internally or reduce costs associated with creating full-time roles for part-time needs.

The problem is that such third-party access can be used as a conduit into an organization's infrastructure—one often exploited by attackers. It becomes difficult to determine whether a third party is protecting data from unauthorized access, use and disclosure. On the other hand, agencies may have access to a third party's systems—access that an attacker could use as a conduit back into the third party's network. The security of each organization is vitally linked to that of the other.

A TARGETED SECURITY PORTFOLIO FOR THE PUBLIC SECTOR

The RSA portfolio of products and services is uniquely capable of supporting the most demanding use cases in the public sector.

The **RSA Archer® Suite** is a Gartner Magic Quadrant GRC platform that empowers organizations to take command of business and cyber risks. It ensures that organizations can control risk, including emerging sources of cyber risk. With RSA Archer, public-sector organizations can establish and manage enterprise and operational risk across all organizational units as well as third-party suppliers.

The **RSA NetWitness® Suite** is an evolved SIEM platform that provides the essential visibility to detect and respond to advanced threats wherever they reside, across physical, virtual and cloud infrastructure. It supports the principles of Business-Driven Security through broad and deep integration with business context, multiple types of security controls and governance platforms such as the RSA Archer Suite.

RSA SecurID® Access provides world-leading authentication and access assurance solutions, protecting 25,000 organizations and 55 million users—and providing organizations with secure access to cloud and mobile applications without creating user roadblocks.

The **RSA Fraud and Risk Intelligence Suite** helps organizations align modern, effective fraud prevention efforts with risk tolerance and business priorities across all digital channels. It offers financial institutions an unprecedented ability to reduce fraud while maintaining—and often growing—transactions from legitimate consumers.

MISSION-DRIVEN SECURITY IN REAL LIFE

To help customers in the public sector get the benefits of Mission-Driven Security, each of these offerings addresses core security requirements, while operating at the nexus of mission and security. At RSA we call this bridging the gap of grief—aligning goals and vocabulary across the organization, while making security a core mission dimension.

Here are some real-life examples of how RSA solutions help bridge that gap:

- **Asset criticality.** As the volume of data explodes, so does the need to prioritize data assets that present the most risk to an organization. In practical terms, the CIO's personal laptop inherently exposes more risk than the web server hosting the cafeteria menu. Make such vital context a foundation of the security analytics process, and you make threat detection and response much more effective.

  To identify critical assets, the RSA NetWitness Platform is designed to incorporate data from a vast variety of sources, including GRC solutions such as the RSA Archer Suite. And asset criticality is just one data point that can be integrated. Any relevant data can be fed into the RSA NetWitness Platform analytics engine, including information from services such as those that enable open-government initiatives. This adds a layer of intelligence and helps protect organizations from the threats that matter most.

- **Security integration.** To function at a high level, a security system must integrate with enterprise authentication systems such as the RSA SecurID Suite. Put another way, it must connect the "include" and "exclude" functions at the foundation of cybersecurity, to benefit the mission as a whole. Traditional systems tend to favor one goal at the expense of the other, but that's no longer sufficient.

RSA

An example: Suppose a user account fails repeated attempts to log in. Traditionally, this would cause a threat detection and response solution to trigger an alarm. The user might be taken off the network until she is proven not to be a malicious actor abusing a hijacked account. But every time a legitimate user is prevented from working while you investigate, that creates an operational issue. In contrast, with the RSA NetWitness Platform, such an alert triggers step-up authentication for that user—multi-factor authentication or some other challenge that a real user could be expected to pass. Legitimate attacks could still be thwarted, with little disruption to the user or the mission.

THE DESIGN, OPERATION AND INCIDENT RESPONSE EXPERTS

Mission-Driven Security practices are employed across RSA, including by the RSA Global Services team of 650 cybersecurity experts in more than 100 countries. RSA Global Services has helped secure many public-sector organizations, often designing and implementing comprehensive risk and security management programs.

RSA Global Services combines deep security skills and broad public-sector knowledge to help bridge your organization's gap of grief:

- RSA Professional Services provides implementation, tuning and training services to deliver value fast.
- Within the RSA Risk and Cybersecurity Practice, two groups provide critical security capabilities:
  - RSA Advanced Cyber Defense (ACD) delivers services to assess breach readiness, security operations center (SOC) or cyber incident response team (CIRT) assessment and design, incident response planning and testing, and "Expert on Demand" services.
  - RSA Incident Response (IR) helps customers design, manage and perform incident response functions via both proactive and reactive services. Available on a retainer or ad hoc basis, RSA IR extends your organization's security skills to deal with security incidents of all types and severities.

MISSION-DRIVEN SECURITY IN THE PUBLIC SECTOR

Public-sector security programs continue to be affected by changes both inside and outside the industry. Mission considerations continue to drive rapid and accelerating changes in computing models. The cloud, virtualization and the mobile revolution have obliterated the IT perimeter—and IT security can no longer be isolated from other systems and processes. In this new world, the RSA Mission-Driven Security approach makes your security teams and cyber risk management more effective.

RSA

As you review security and GRC solutions, evaluate each option based on how well it protects your strategic assets and supports your strategic goals.

For more information, or to get started with RSA solutions and services, visit rsa.com or the RSA Link Community.

ABOUT RSA

RSA helps leading organizations around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to rsa.com.

04/18, Solution Brief, H17089.