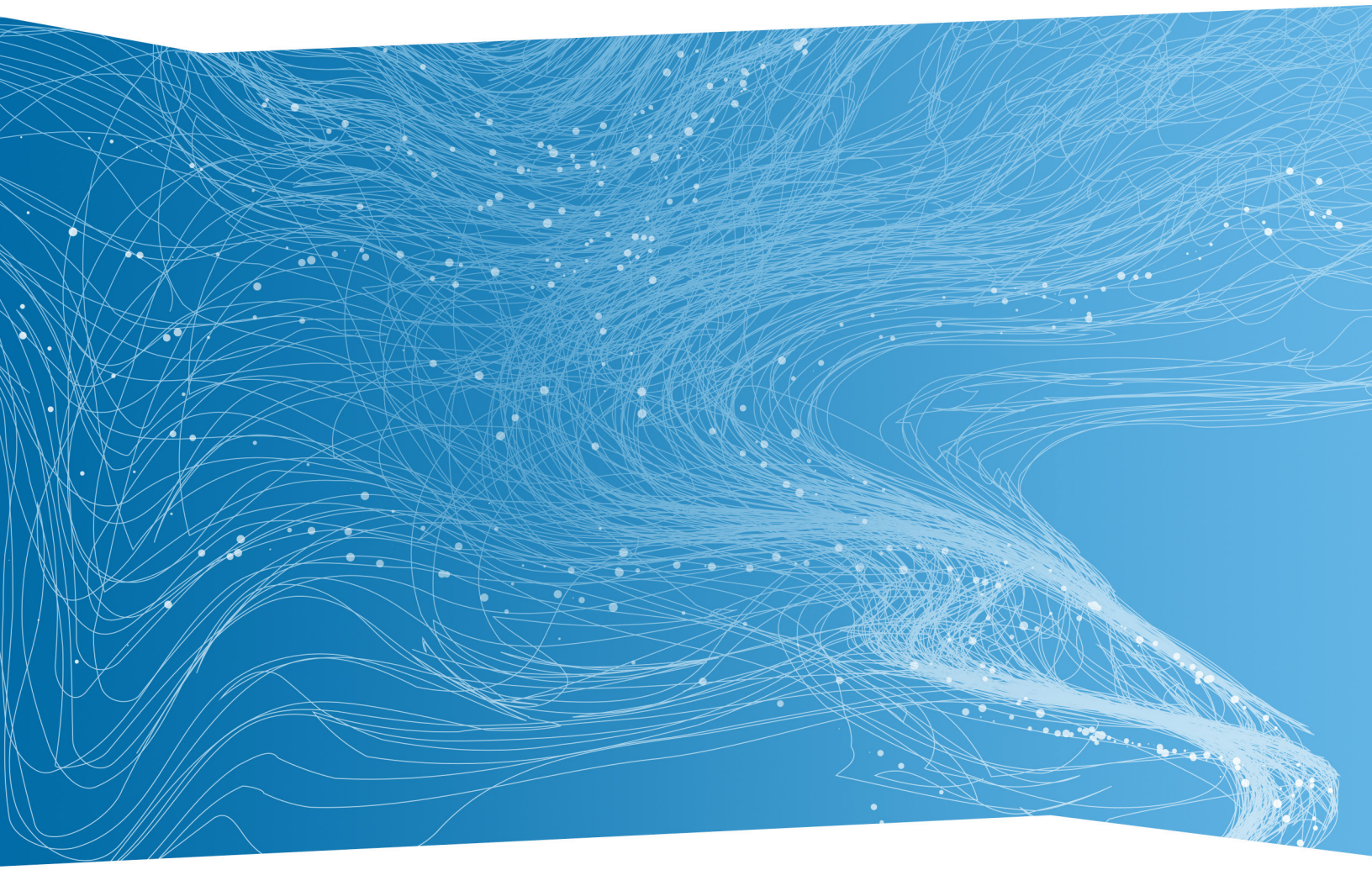
RSA



WHITE PAPER

# PROTECTING PUBLIC SECTOR IT

## MANAGING CYBER RISK WITH MISSION-DRIVEN SECURITY

RSA

A white paper for the U.S. Department of Defense; federal, state and local governments; and the intelligence community

## OVERVIEW

Public sector security teams today face a daunting task: protecting mission-critical infrastructures that have a level of complexity and interdependence never seen before.

Many government agencies and departments are finding that embracing new technologies is critical to remaining efficient; these technologies also underpin many key administrative and operational innovations. The number of devices, identities and systems that interact with any given agency, whether from inside or 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.

This explosion in the number of devices, identities and systems isn't just transforming government; it's also transforming cybersecurity, through challenges related to scale and complexity. Government organizations have a huge and still-growing attack surface—and with it an expanding assortment of weak points an attacker can exploit to enter an environment. Compounding the issue is the need for government architectures and highly sensitive data to be accessible and open to constituents and the general public.

Yesterday's security tools are not effective at keeping today's organizations safe, and neither is yesterday's security strategy. With a legacy view that no data loss is acceptable and all data should be equally protected, some government agencies are suffering from security fatigue; in spite of intense, prolonged effort, they struggle to effectively manage risk and protect their most important data.

Forward-thinking public sector organizations, in contrast, are beginning to realize that all data is not created equal. They are prioritizing and dedicating a higher level of protection to sensitive information about mission-critical infrastructures (such as transportation and power grids) and personal data. They're working with operational leaders to identify where sensitive data lives in the infrastructure. And they're focused on protecting what matters most as part of a comprehensive operational and enterprise risk management strategy.

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.

RSA

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.

Mission-driven security is the concept of creating explicit linkage between what security technology is telling you and what that information means in terms of mission and operational risk. This approach mandates a new way of thinking about how to protect what matters most to an organization. Many security strategies have grown by reacting to a new threat or security incident. But zero-day and ransomware attacks happen every day—and no one really knows what type of threat will come next. What we do know is which systems, processes and data are most important to our organization's mission. And we absolutely can proactively align security strategy to protect those critical areas.

## IT FOR MODERN GOVERNMENTAL AGENCIES

Modern governmental agencies are deriving efficiency and agility from four key IT trends:

- Cloud
- Mobility
- The Internet of Things (IoT)/cyber-physical convergence
- Third-party access

### CLOUD CONVENIENCE INTRODUCES SECURITY COMPLEXITY

Cloud technologies provide agencies—and the general public they serve—with anytime/anywhere access to key applications, data, services and platforms. Government-approved cloud systems (e.g., FedRAMP and DoD's Cloud Security Guidelines) are typically housed in mature data centers with excellent uptime. And cloud vendors often assume the burden of user support, relieving weary help desks. Many cloud vendors serving the public sector use monthly subscription payment models to absorb some or all of their implementation costs, minimizing initial financial barriers.

But all of this convenience is at the heart of a growing security problem, one that has created blind spots. Cloud vendor selection decisions tend to be departmental or decentralized. Even government-approved cloud systems can often be purchased and implemented while bypassing formal approval channels, and without the knowledge of IT—a practice referred to as shadow IT. Operational processes such as formal sourcing processes, budgeting and implementation support would normally pull IT and security teams into a tool-selection conversation or alert IT to a tool's existence, but with cloud technology that's often not the case. Typically accessed through the user's browser, cloud systems may not even require a user to install software.

RSA

Meanwhile, malicious insiders and other attackers increasingly target the dark corners of IT. Cloud systems often interact with other administrative and operations systems or are used to store valuable data, such as information about mission-critical infrastructure or constituents' personal data. Attackers can attempt to compromise cloud systems in order to steal critical or confidential information without triggering attention from network-monitoring technology. Furthermore, data can be orphaned in the cloud when a user's relationship with a provider has ended; without knowing the cloud is being used, IT can't properly decommission this data or the underlying cloud system.

In short, to maintain security, a modern agency must gain visibility into the cloud infrastructure and services—being used throughout its organization and supported by multiple vendors—then prioritize and employ appropriate controls.

## MOBILE ACCESS INCREASES PRODUCTIVITY AND RISK

Many government and public sector organizations rely heavily on mobile technologies, allowing employees and other users to work remotely, from devices that may or may not have been issued by the organization. Two primary variables create mobile security risks here: devices and connections. It's common to see access from devices and/or connections that are not owned, managed or controlled by the organization.

While many government organizations, particularly federal and the Department of Defense, are continuing to manage and monitor their own devices, other agencies mirror the private sector's embrace of personal devices. This means that, to remain secure, they must begin monitoring activity for all devices from which organizational data is accessed. In part, agencies are working to identify the personal and operational data that is accessed by and saved to mobile devices. In the event of a user's departure or a security incident involving a mobile device, the resulting administrative and operational risks from the compromise of related data can then be understood. A security team can use knowledge of data and access history to help reconstruct a security incident, while an organization's administrator can use remote-wipe technology to instantly delete organizational data stored on a device as needed (for instance, when an employee leaves the organization).

## INTERNET OF THINGS: THE NEXT INDUSTRIAL REVOLUTION?

It seems that everything sold today that could potentially have an internet connection does, from baby monitors to medical devices and refrigerators to vehicles. The impact is no less striking in government settings, where printers, environmental controls, equipment and even weapons systems are internet-enabled. Many of these devices send an ongoing stream of operational activities data across the internet to vendor databases, where it is harvested for insights. Some are calling the Internet of Things (IoT) the "next industrial revolution" because access to detailed performance data promises

RSA

to dramatically increase production and efficiency of physical systems, such as transportation and power generation.

With so many devices now capable of connecting to the internet, organizations must put in place a much broader security strategy, one that takes into consideration both the diversity of devices, platforms and operating systems and the massive quantity and new types of data generated by IoT devices. This strategy must also consider the pervasive connectivity of these devices; the ability to maintain a constant connection to the outside world means 24x7 penetration of the perimeter.

Today, while continuing to defend traditional devices and software, including phone systems, laptops and applications, agencies must also prevent potential attacks on smart electrical systems; connected heating, cooling and video surveillance systems; connected industrial equipment; and handheld devices. Because many IoT technologies interact with physical environments, it's easier than ever for an attacker to create a real or spoofed emergency. For instance, an attacker could interrupt operations with a false alert on an environmental system, or increase the real-world temperature in industrial freezers. Attackers could force the evacuation of a building, or use IoT access to shut down critical public services.

Agencies understand that IoT cyber attacks can have physical impacts—and they're considering how to manage the security of these devices at scale.

### THIRD-PARTY ACCESS CREATES SECURITY PIVOT POINTS

Over the last decade, many public sector organizations have increased their use of external partners, vendors and consultants. For instance, third parties may be called upon to provide support during 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 in-agency or reduce costs associated with creating full-time roles for part-time needs.

The problem is that government organizations provide third parties with access that attackers can potentially use as a conduit into an organization's infrastructure. 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.

Governmental organizations are considering how to defend against attackers that use third-party access to compromise the organization, or that use an organization's access to third-party systems to compromise the third party.

RSA

## RESULT: MASSIVE EXPANSION OF ATTACK SURFACE

All four of these technology trends are expanding the attack surface of the modern public agency, and each introduces a level of complexity that at first might not be obvious.

Traditional security strategies, which rely on creating a perfect perimeter to prevent attacks rather than managing attacks based on mission and operational risk, prove ineffective here. Another fault line: Traditional security protects all assets equally, which isn't feasible when the number of assets to be protected is increasing so rapidly. In addition, some core systems once exempt from security testing or patching need to be scrutinized.

Many security teams are asking their operational leaders new questions: Which information or systems are the most sensitive or most important to protect? What is the potential impact if attackers obtain that data or can manipulate those systems (e.g., an inability to meet service obligations, notification to regulators or interruption to normal operation)? The true impact of these modern security challenges may be realized only in the event of a security incident, when an organization is unable to readily answer the most important question: How bad is it?

## MODERN SECURITY STRATEGY

### SECURITY PILLARS: VISIBILITY, RISK, INSIGHT, CONTEXT AND RESPONSE

As the security environment shifts, agencies must move from creating an impenetrable perimeter to managing a dynamic, distributed infrastructure. Four pillars of modern security come into play:

- **Full visibility.** The security team must be able to see what's happening in the agency at all times—across processes, networks, devices, people and transactions. Only with this 360-degree ability can the team identify security risks across the whole environment.
- **Risk awareness.** Organizational leaders and operational personnel should establish a foundation of infrastructure and data risk that they apply across the enterprise, assuring proper focus on high-risk assets.
- **Rapid insight.** Faster "time to insight," through better analytics and detection capabilities, is paramount in today's environment of external partners, cloud computing, personal devices and the like. Time to insight for security teams is collapsing to zero; the more time you need to interpret an event, the greater your risk.
- **Operational context.** The security team can't rely only on seeing what is happening on its network and among its system users; team members must also be able to interpret those events quickly, while understanding the criticality of affected systems and processes. Such contextual intelligence facilitates faster and better decisions. Understanding operational context (such as the criticality of an asset) can also help analysts determine how urgently to escalate incidents.

RSA

- **Efficient, comprehensive response.** Today, many security teams take the findings from their security tools and remediate in a highly manual way that doesn't scale. The most effective way to turn insights into action is to orchestrate and automate response. Spot a user acting suspiciously, and the control plane of identity goes into action, stepping up authentication to ensure that this user is legitimate.

## CAPABILITIES NEEDED FOR A PUBLIC SECTOR DEFENSE

Public sector organizations are increasing operational efficiency and bolstering cybersecurity by adding capabilities that defend against cloud, mobile and IoT risks, as well as risks caused by third-party users. In some high-security organizations, the challenge is exacerbated by the "need-to-know" policies that limit data access, even to security teams. Mature tools and processes help overcome these challenges.

| | | |
|---|---|---|
| Cloud | **Make identity management consistent across cloud, mobile and on-premises systems.**<br><br>Most agencies are already working to retire monolithic, application-specific, on-premises identity management tools. Such systems create islands of identity, or identity silos—whose lack of visibility in turn increases risk. Many agencies are also considering how to get a unified view (for instance, through identity-as-a-service) of anomalous activity on on-premises systems, cloud infrastructure and cloud services.<br><br>Large agencies increase efficiency by centrally managing user privileges, along with an authentication method that allows each user to seamlessly log into multiple applications with single sign-on. Provisioning and deprovisioning users centrally eliminates the risk that a user's access to an application might be accidentally preserved when other access is removed. | **Gain visibility into shadow IT and the use of cloud systems.**<br><br>Agencies need to assess the degree to which shadow IT is an issue, answering key questions such as these:<br>• What critical information is accessed or housed by the system?<br>• Who can access it, including external users?<br>• What security measures does the cloud application or service vendor use? Are the connections trusted?<br>• Does the vendor have all the necessary certifications, such as CDM?<br><br>Security tools that offer network monitoring can be very helpful in identifying shadow IT. |

RSA

| | | |
|---|---|---|
| Mobile | **Monitor all mobile endpoints including BYOD.**<br><br>Modern agencies are beginning to monitor activity for all mobile devices from which organizational data is accessed, regardless of who owns each device. To better understand operational risk, organizations are also identifying data accessed by and saved to such devices.<br><br>In addition, many agencies are implementing remote wipe, allowing administrators to immediately eliminate mobile access to organizational data if and when needed. | **Leverage mobile capabilities to improve and expand authentication.**<br><br>Agencies should consider the benefits of modern, next-generation authentication.<br><br>Agencies that have large numbers of users working off site should consider taking advantage of mobile as a second authentication factor. With added mobile authentication, a successful attacker could linger in a system or network for only one session, until the user logs out; the attacker wouldn't be able to continue the attack on next login, even if the user's password is compromised.<br><br>Mobile devices also offer inherent biometric and haptic capabilities that can become part of the authentication process—allowing all mobile device users to operate more securely, without significant additional effort. |

RSA

| | | |
|---|---|---|
| IoT | **Discover and monitor IoT devices on the network.**<br><br>Agencies need to discover and monitor the connected and smart devices on their networks. They must also understand the extent of IoT activity involved in connecting to systems and recording and storing mission-critical information. | **Control access to configure and manage IoT devices.**<br><br>IoT devices should be considered as identities on the network, since they are granted access to network resources. Agencies should ask questions similar to those for other user types. For instance, do these devices need to be deprovisioned at times, and what is the process for doing so? What level of authorization do they need, and to which systems? |
| Third Parties | **Manage the identity of third-party users throughout the identity lifecycle.**<br><br>As with employees, third parties' roles and responsibilities in an agency change over time. All identities including those for third parties should be actively managed and periodically reviewed throughout the identity lifecycle.<br><br>Agencies should also require the same security rigor for external users who access sensitive systems and data as for public employees.<br><br>When selecting identity tools, agencies need to consider the volume of third-party provisioning, management and deprovisioning; not all are built for scale. | **Perform regularly scheduled security/risk assessments of third parties.**<br><br>When connecting to a third party's systems or allowing a third party to access its systems, an agency should investigate the security and risk posture of that party. To understand whether its risk level is an appropriate match for the organization's risk appetite, the agency must conduct security evaluations and audits, checking whether real-life practices follow established policies and procedures.<br><br>Because the environments of both parties are organic and the relationship between parties dynamic, risk is ever changing. Evaluation of third parties should not be a once-and-done activity; security evaluations and audits must be conducted on a regular basis. |

RSA

## CONCLUSION

The goal of a government or public sector organization's security strategy is to create harmony between the security strategy, IT environment, and administrative and operational priorities. This is difficult because IT environments, like organizations themselves, are constantly in the process of transformation—making each agency's risk and security posture equally dynamic.

An agency can take proactive steps to operate more securely—for instance, taking measures to inventory cloud applications in use, understanding how mobile devices (both agency-owned and personal) are used for professional interaction, assessing the security of devices that transmit information over the internet, and better managing the lifecycle of identities, including those of third parties and IoT devices.

A rapidly expanding and increasingly complex IT infrastructure cannot be secured purely through more technology. Governmental agencies must drive success by including people and processes in their security strategies. In part, security teams should collaborate with operational leaders, cloud providers and technology partners to identify the level of security each information assets requires, and to integrate security into every phase of an organization's initiatives.

In summary, modern government agencies must understand security risk in the context of impact to mission-critical operations and public service. With a mission-driven security strategy, agencies can connect security risk to operational risk that is contextual and specific to the organization's mission, and achieve consistently high levels of organizational efficiency and security—even as their attack surfaces continue to expand with every added device, identity and system.

## MISSION-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA delivers products and services that empower an agency to adopt a mission-driven security approach—optimizing both risk and IT security. Our capabilities work on your IT architecture and within your IT product ecosystem.

All RSA products are designed to support the Continuous Diagnostics and Mitigation (CDM) program managed by the U.S. General Services Administration (GSA) and the U.S. Department of Homeland Security (DHS). Individual certifications are also in place for specific products; for example, RSA NetWitness® Suite has been included on the U.S. Department of Defense Information Agency (DISA) Approved Products List (APL) and RSA Archer® carries common criteria and FIPS 140-2 certifications.

The **RSA Archer Suite** ensures that organizations can take command of risk, including emerging sources of cyber risk. With RSA Archer, government organizations can establish and manage enterprise and operational risk across

all organizational business units as well as third-party suppliers. RSA Archer is the approved dashboard and platform for the CDM initiative.

The **RSA NetWitness Suite** is an advanced security information and event management (SIEM) and threat detection and response platform that provides the visibility essential to detecting advanced threats and delivering the right response, in minutes not months.

**RSA SecurID® Access** provides world-leading authentication and access assurance solutions, protecting 25,000 organizations and 55 million users. With RSA SecurID Access, organizations can have secure access to cloud and mobile applications without creating roadblocks for users.

**RSA Adaptive Authentication** is a comprehensive authentication and fraud detection platform designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators.

## ABOUT RSA

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