Managing The Security Risks of Remote Work

Federal agencies slowly but surely have expanded their IT operations to include a wide array of cloud-based applications. These applications have increased not only the agility and scalability of their operations but also the complexity – and ***increased complexity means increased risk.*** And now, a year into remote or hybrid work, the complexity is even more pronounced.

The challenge for agency leaders and IT staff is now threefold:

→ Provide seamless secure access...

→ To an increasingly dynamic user population...

→ Scattered across a widely distributed environment.

How can you meet this challenge? This infographic shows how that can be done, from three different perspectives.

1. The End-User

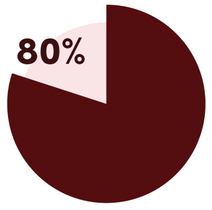
Challenge: Strengthen the Weakest Link

"The bitter truth is that legacy authentication via passwords is obsolete, and maintaining the technology in the face of ever savvier cybercriminals is a critical security threat."

- *Sean Ryan, Senior Analyst, Forrester*

For the end-user who needs to access a growing number of applications, both on premises and in the cloud, managing passwords is a nightmare. The temptation? Skip the strong passwords and keep it simple ("12345678," "abc123," "password").

For the agency, that's a security nightmare.



80% of hacking-related breaches involve compromised passwords.

Unfortunately, strong passwords (W3@kestL1nk!) are only a partial solution, because they can be cracked...or stolen.

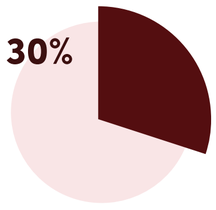
2. The Hybrid Enterprise

Challenge: Managing Complexity

"...Decision-makers recognize the need for modern cloud-based and secure tools for maintaining continuity of operations, reducing long term costs, and improving security as agencies continue to evolve and respond to COVID and beyond."

- *SAIC survey* on response to COVID-19

The pandemic proved to be a perfect use case for software-as-a-service and other cloud-based solutions, highlighting their ability to deliver IT services to remote workers quickly, efficiently and at scale. But even prior to remote work, most organizations were already expanding their use of SaaS offerings.



30% - The growth in unique number of SaaS apps per organization between 2018 and 2019.

But with workers scattered widely how can agencies manage secure access?

3. Governance

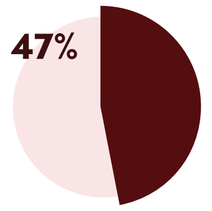
Challenge: Enterprise Visibility and Control

"Users remain largely unaware of the potential security risks of their actions or how these actions could compromise their employers' networks."

- *Identity Management Institute*

To end-users, the concept of identity governance and lifecycle control might sound abstract. But enterprise security means more than delivering secure access to individual applications. It requires managing risk across the environment.

The pandemic only heightened those risks by expanding the attack surface.



47% of individuals fall for phishing scams while working remotely.

How can agencies address these risks while providing employees with secure access to the resources they need to do their jobs?

The Solution: Multi-Factor Authentication

Agencies can strengthen that weakest link by using two or more methods to identify a user. Options for **multi-factor authentication (MFA)** include:

Hardware or software tokens

Mobile-enabled push notification

One-time passcode

Biometrics (e.g., fingerprint or face scan)

SMS text

For the hacker, MFA significantly raises the barrier to entry. ***For the agency, that's a game-changer.***

The Solution: Single Sign-On

Combining MFA with a **single sign-on (SSO)** capability in a cloud-based service reduces the complexity of the IT environment. This means:

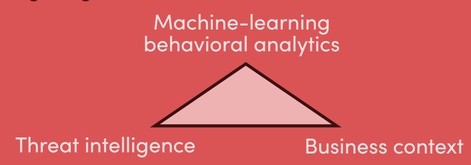
- ***Users*** can securely and seamlessly on-premises, cloud and mobile applications, while...
- ***Agencies*** can create centralized access control policies to consistently enforce different security requirements for applications based on assurance levels.

In short, it delivers both ***a better user experience and better security in one stroke.***

The Solution: Pervasive Visibility and Control

The key to managing risks in this complex environment is ***intelligent access***, based on pervasive visibility and control across the full IT environment.

- **Two concepts are foundational:**
  - **Identity assurance:** The confidence that the right people have access
  - **Access assurance:** The confidence that the access is appropriate for the user's role/job and in compliance with governing policies
- **Agencies can increase their level of assurance by gaining insights in three areas:**



- **Pervasive visibility and control will enable agencies to:**
  - **Mitigate digital identity risk**
  - **Maintain a continuous state of compliance**
  - **Enforce user access policies**

How RSA and Four Points Help

RSA SecurID Access is the world's most widely deployed intelligent multi-factor authentication solution and the identity management platform. It enables agencies to provide users (remote or on site) with access to cloud, mobile and on-premises applications securely and seamlessly.

RSA SecurID Access Federal has achieved the Federal Risk Authorization Management Program (FedRAMP) "In-Process" status, providing agencies with a secure foundation for their digital transformation efforts.

Learn more: https://www.4points.com/it-solutions-partners/securid/

RSA

FOUR POINTS TECHNOLOGY

govloop