RSA

SOLUTION BRIEF

MANAGE DYNAMIC WORKFORCE RISK

STRENGTHEN THE WEAKEST LINK IN YOUR SECURITY CHAIN

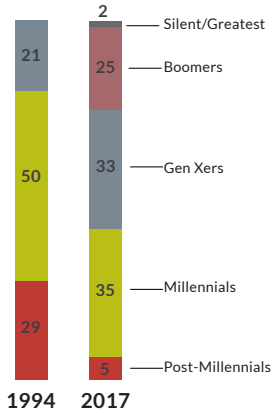
The face of today's workforce is undergoing profound changes sparked by globalization, shifting demographics, digital transformation, and the immutable truth that the ways we connect to information and to each other will continually evolve.

SHIFTING WORKFORCE DEMOGRAPHICS

Your workforce probably includes a mix of Baby Boomers, Gen Xers and millennials working in full-time, part-time, temporary and contract positions. Each of these groups has different attitudes toward employment and preferences about how and where they do their work. For example, millennials now make up the largest share of the U.S. labor force, yet they typically spend less than eighteen months with any one employer and they currently account for nearly half of freelance workers who are not always vetted with the same rigor as full-time employees. Because millennials comprise such a large portion of the labor force and because their job-hopping accelerates the revolving door of "joiners-movers-and-leavers" inside organizations, they represent a large part of what makes the workforce dynamic.

Figure 1: Millennials in the U.S. Workforce

% of the U.S. labor force



Note: Labor force includes those ages 16 and older who are working or looking for work. Annual averages shown. Analysis of monthly 1994 and 2017 current population survey (IPUMS).

Source: Pew Research Center

BUSINESSES GOING GLOBAL

The workforce isn't just shaped by shifting demographics: Globalization continues to have a far-reaching impact, too. As just one example, consider the many organizations using offshore development and customer support centers to complement "onshore" staff. These may be "captive centers," meaning they're owned and operated by the company that set them up, or they may be run by a third party. Regardless of who owns these centers, the people working in them make up your extended enterprise, and they need access to your organization's systems.

Globalization also means that companies operating in different locations need to address regional variations in workers' attitudes toward data privacy and how data should be handled with consistent policies and procedures. For instance, the 2019 RSA Data Privacy & Security Survey found that Germans are far more concerned with data privacy than Americans and even the French. In addition, globalization also brings technology and regulatory complexity. The more regions in which a company operates, the more technologies it needs to assimilate into its IT infrastructure and the more privacy and security regulations it likely needs to harmonize.

The bottom line: More people working in more places creates a more dynamic workforce, which in turn brings a new set of risks.

DIGITAL TRANSFORMATION

Regardless of where you live or which generation you belong to, there's no denying the fact that the way in which we all work and interact has become more automated, more digital and more mobile, and digital transformation is only hastening this trend. Gone are the days of one-size-fits-all workspaces. Many workers around the world seek collaborative environments, the freedom to work from anywhere, and the ability to choose the applications and devices they need to do their jobs. In this application economy, mobility and the consumerization of IT are driving personalized and frictionless user experiences across a variety of device platforms. This is leading to a growing number of on-premises, cloud and mobile applications, and an exponentially larger number of personally owned mobile and IoT devices. All of these different platforms and devices generate new risks and conflicting requirements for security, support and the user experience.

GETTING YOUR ARMS AROUND DYNAMIC WORKFORCE RISK

The dynamic workforce has become an increasingly complex challenge for cybersecurity and risk management practitioners to address. Growing and diverse populations of users, applications, devices and data all over the world give attackers more vulnerabilities to exploit, while organizations have more security and privacy regulations to navigate. All of this adds up to increased risk: The more people you have accessing your systems and data from different places, the more identities you need to manage, the harder it is to know when access is legitimate, and the greater the odds that one (or more) of these identities will be abused or fall into the wrong hands, potentially leading to a cyber attack or data breach. What's more, with global security and privacy laws shining a spotlight on identity and access management, if you don't manage identities and access properly, you expose your organization to potentially time-consuming and costly litigation, not to mention hefty fines and compliance violations.

CUSTOMER SUCCESS STORY

Infosys

It giant infosys deploys RSA® solutions to protect and manage extensive global infrastructure.

ISSUES

- Needs to secure access for 200,000 employees.
- Uses nearly 100 types of logs for different purposes.
- Faces complex, multinational compliance requirements.

SOLUTIONS

- RSA SecurID® Access
- RSA® Identity Governance & Lifecycle
- RSA Netwitness® Platform
- RSA Archer® Suite

OUTCOME

- Improved the effectiveness of its security and compliance operations.

"We have such a large environment and are growing so quickly that it was imperative that any security measures we put in place didn't compromise our users' ability to continue working efficiently."

K Lakshmi Narayanan
AVP and Head of
Cyber Security
Tech and Ops
Infosys

To manage dynamic workforce risks effectively, organizations must be able to answer these fundamental identity and access related questions (see Figure 2):

Figure 2: Can You Answer These Questions Definitively?

Source: RSA

These questions may not be new, but the effects of globalization, demographics and digital transformation have made them much more difficult for most organizations to answer.

IDENTITY ASSURANCE – KNOW WHO USERS ARE

Managing dynamic workforce risk starts with having a high level of confidence that the users and entities accessing your critical systems are who they claim to be. User verification (authentication) solutions can be a boon here, provided they offer users a consistent experience across applications and devices that doesn't slow them down. Authentication solutions should also match the level of access security to the potential risk the access creates. RSA SecurID® Access for managing dynamic workforce risk:

- Empowers traditional employees, independent contractors and temporary workers to work anywhere without compromising security.
- Eliminates friction and frustration for your workers (and your help desk) with transparent authentication that only asks for additional authentication when machine learning algorithms identify it's necessary.
- Supports the broadest range of use case scenarios including those where smartphone-based authenticators are not an option.
- Accommodates the work styles and technology preferences of different demographic groups.
- Preserves the simple user experiences that cloud and mobile technologies provide.

ACCESS ASSURANCE – KNOW WHO HAS ACCESS TO WHAT

The rapid expansion of SaaS applications, cloud infrastructure, IoT devices and third-party relationships has made it difficult for many identity managers to get a complete picture of the resources each user has access to. This kind of business and technical complexity has also made it harder for them to pinpoint and prioritize identity risks as they arise, not to mention ensure compliance with a variety

of internal and external security and privacy requirements. RSA® Identity Governance and Lifecycle for managing dynamic workforce risk offers the following capabilities to help identity managers accomplish those critical objectives:

- Provides deep, granular visibility into every user, application and entitlement so identity managers can be sure users have appropriate access.
- Manages the massive amount of entitlement data that independent contractors and temporary workers generate as they continuously move in, around and out of organizations.
- Makes it easy to quickly onboard new users with simplified processes for access requests and reviews.
- Reduces complexity for identity teams with plug and-play connections and configuration-based policies and workflows that eliminate a need for custom coding and ongoing maintenance.
- Minimizes the risks associated with temporary workers and non-traditional employees having inappropriate access by prioritizing requests for access based on risk metrics (e.g., segregation of duties violations, excess privileges and more).

ACTIVITY ASSURANCE – KNOW WHAT USERS ARE DOING

Protecting and managing access to critical resources is mandatory for neutralizing dynamic workforce risk. However, once a user is logged in, traditional identity and access management (IAM) tools lose visibility into and control over what activities users or entities engage in. In order to determine whether user activity is appropriate and spot abnormal behavior or incidents that could signal an attack in progress, you need continuous visibility and insight into what your workforce is doing across your extended IT environment.

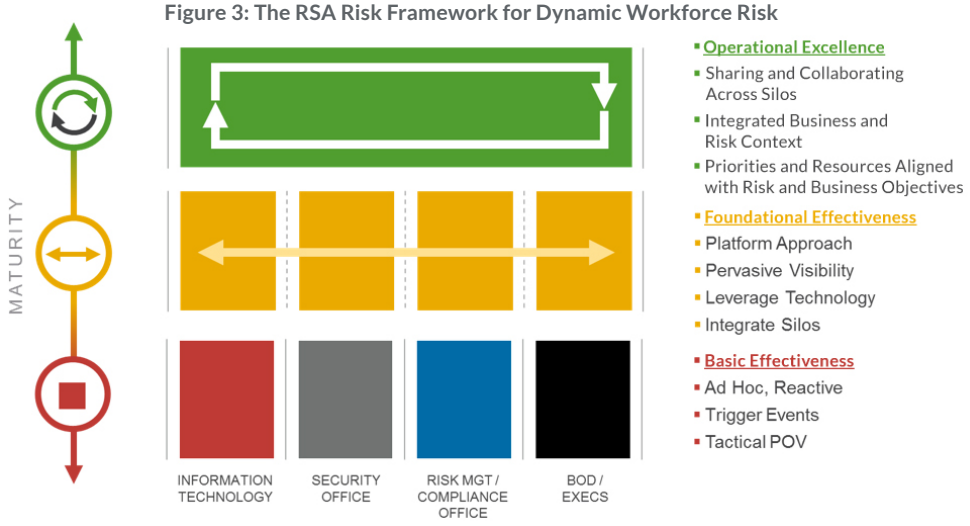
RSA NetWitness® Platform helps organizations protect themselves from a variety of dynamic workforce risks, including exploitation of compromised credentials and insider threats, by doing the following:

- Continuously monitoring traditional employees' and temporary workers' behavior to facilitate early detection and investigation of identity-based threats and anomalies.
- Uncovering hidden workforce risks associated with vulnerable devices and software "brought in" by traditional employees and temporary workers; taking quick action to limit identity and access exposures.
- Speeding response to workforce-related threats by correlating user access and authentication logs with captured network, log, packet and endpoint data.

HOW WELL CAN YOU MANAGE WORKFORCE RISK?

The RSA approach to managing dynamic workforce risk starts with a comprehensive assessment that gauges your organization's ability to identify, protect, detect and respond to workforce-related risks. The assessment is grounded in our own proprietary risk framework, the RSA Risk Framework for Dynamic Workforce Risk, which leverages more than 30 years of RSA security and risk expertise. The RSA Risk Framework for Dynamic Workforce Risk is based on industry standard guidelines (including the NIST Cyber Security Framework and ISO standards for cybersecurity and risk management) and uses a maturity model that reflects the perspectives of IT and security leaders, the C-suite and board of directors. Based on the assessment results, we provide your organization with strategies for improving its capabilities and minimizing this critical and growing risk.

Figure 3: The RSA Risk Framework for Dynamic Workforce Risk



Source: RSA

EMPOWER YOUR WORKFORCE

The dynamic workforce has become an increasingly complex challenge for cybersecurity and risk management practitioners. Workforce globalization, changing demographics and rapid technology development have dramatically increased the risk associated with a progressively diverse and decentralized workforce. To effectively manage this risk, organizations must know who their users are, what they have access to, and what they are doing with that access. Only RSA has the people, the technology, the experience, the partnerships and the vision to help organizations effectively manage dynamic workforce risk and enable individuals to do more by giving them the freedom to work wherever, whenever and however they choose.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.