RES

FIVE IMPORTANT TRUTHS ABOUT DIGITAL WORKSPACES IN A DANGEROUS WORLD

www.res.com | A RES White Paper

Work today is increasingly digital. Business performance is therefore largely contingent upon enabling the digital workforce, which, in addition to employees, may also include contractors, suppliers, and part-time or seasonal workers. Business depends on providing them with richly functional digital workspaces that they can access any time, and anywhere.

Unfortunately, organizations also face an intensifying barrage of security threats. IT challenges around security and compliance are compounded by multiple factors, including:

- The increasing number of people who are conducting work with personal devices, including personal laptops, tablet computers and smartphones
- The increased consumption of services by many multiple devices from multiple locations (such as home, remote offices, hotels, restaurants, in transit, etc.)
- The expanding threat surface that IT has to defend as IT infrastructure extends to the cloud.

Worst of all, the potential costs of a security breach — in terms of lost customer relationships, compromised brand value and regulatory consequences — continue to rise. This white paper discusses five certainties that can embraced by an organization and then be integrated into a comprehensive security strategy.

THE OBJECTIVE: MORE SECURITY, LESS FRICTION

Many organizations are investing substantial resources in maintaining high security standards and meeting compliance regulations, spending money on everything from firewalls and antispyware to biometric authentication and intrusion detection systems. Despite these investments, however, companies are experiencing more security and compliance troubles than ever.

Business leaders therefore have to ask two critical questions when considering how to secure the digital workforce:

1. What additional measures will best complement my company's existing security measures and/or build better security into our digital workspaces?
2. How can my company improve IT security without introducing excessive "friction" into our digital workspaces — which would thereby undermine productivity and business performance?

The following five truths offer answers to those critical questions.

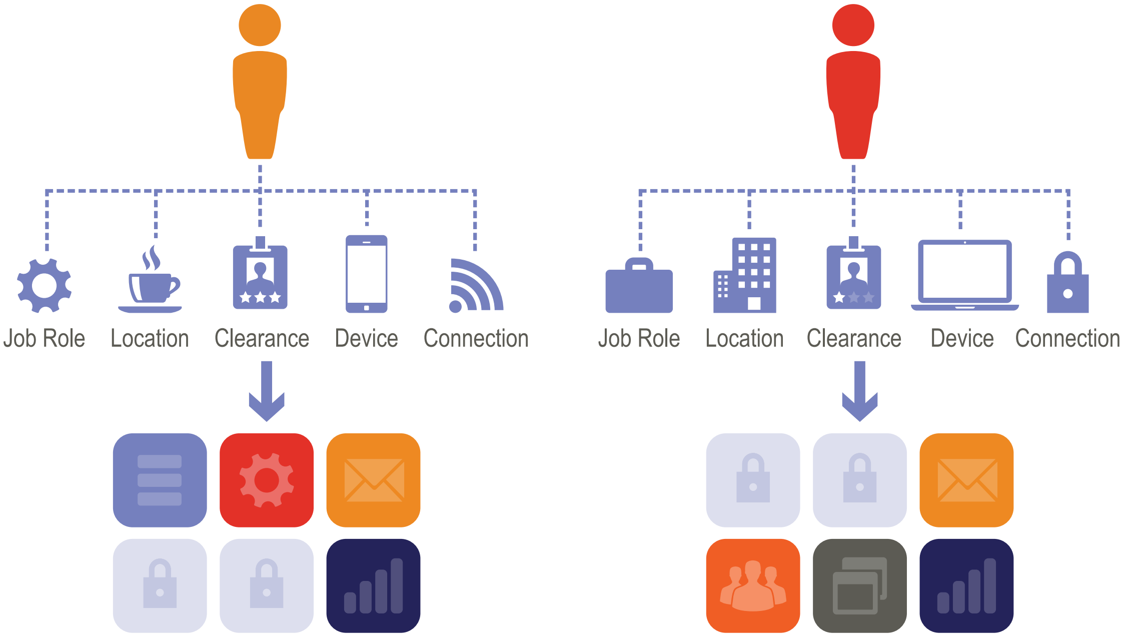
TRUTH #1:
SECURITY ISN'T JUST ABOUT THINGS. IT'S ABOUT PEOPLE.

As the Snowden affair so dramatically demonstrated, even the most sophisticated IT security won't keep you safe if you ignore the human part of the equation. Data and applications are accessed and shared by people — so it's essential to effectively govern the access to IT resources you give people with appropriate business rules and policies.

This requires more than just technologies such as identity and access management (IAM) and mobile device management (MDM). These technologies are important as infrastructure-level gatekeepers that securely authenticate a given user or device. But they do not provide a means of managing the rules and policies that govern access by those users and devices in real-time.

In other words, your company doesn't just need technical mechanisms that prevent users from accessing resources inappropriately. You also need a unified layer of management logic that can tell your IAM, MDM and other security mechanisms what is policy-appropriate access for a given person's digital workspace at a given time and place — and what isn't.

Access to business and IT services should be people-centric. It should be dynamic and personalized, depending on each person's individual context.



TRUTH #2:
SECURITY CAN'T COME AT THE COST OF USER ENABLEMENT.

Some companies try to optimize security by "erring on the side of safety" — taking an approach that excessively limits users' access to IT resources. This is an unsafe approach for several reasons:

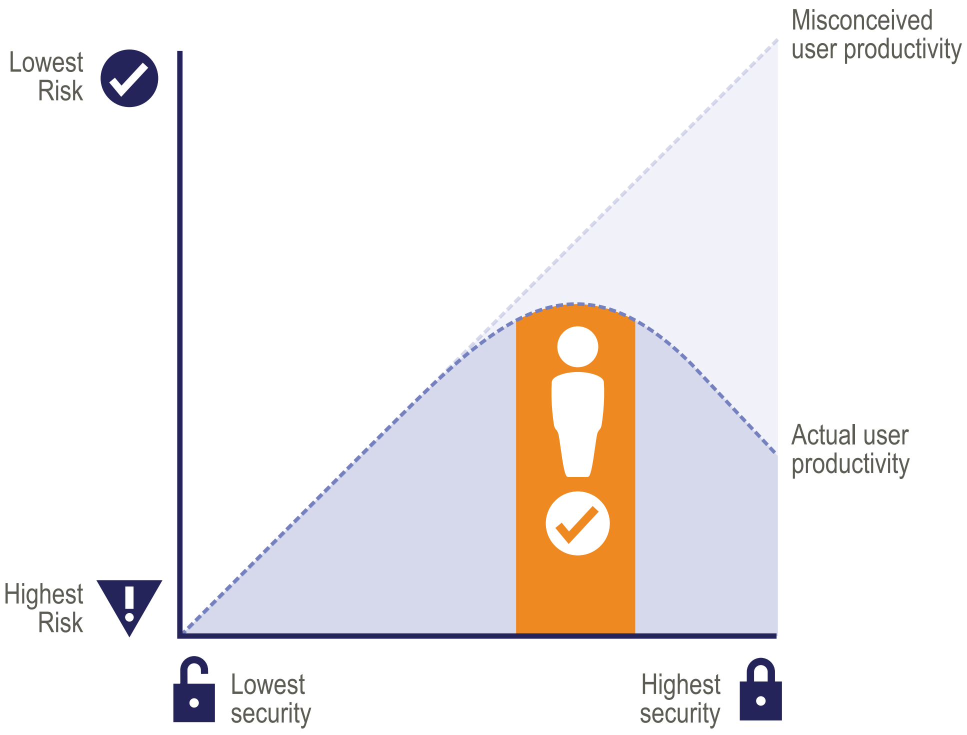
- **Under-enablement has its own bottom-line consequences.** When users don't have access to the resources they need to be productive, business performance suffers. So there's actually nothing "safe" about blocking users from resources they can and should be using.

- **Frustrated users will find workarounds.** If you don't give today's tech-savvy employees users a legitimate and governable means of getting what they need, they will find alternatives (such as Dropbox) that are illegitimate and ungovernable. The result will be "shadow IT" that creates a whole new set of security and compliance risks.

- **It's no way to attract and retain millennial talent.** For your nextgeneration workforce, technology is like oxygen. If they find their workspace suffocating, they will take their skills and connections elsewhere.

For these reasons and others, your governance of user access to IT resources has to be as focused on enablement of what is appropriate as it is on preventing what isn't.

Security must meet usability. Although higher security may result in lower risk for organizations, too much security creates lost productivity from employees and the proliferation of "Shadow IT."



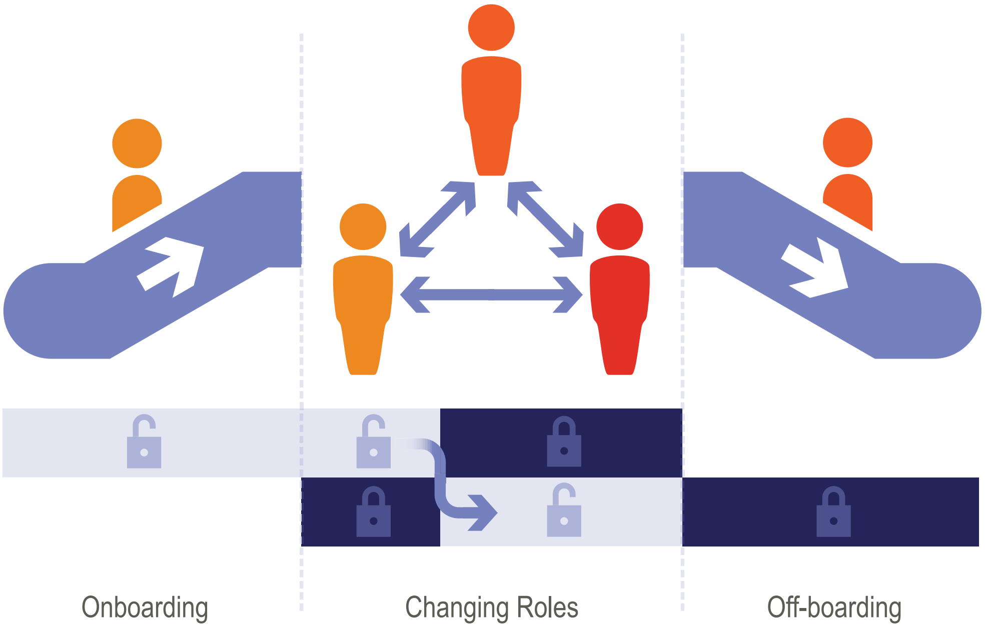
TRUTH #3:
IN AN INCREASINGLY DYNAMIC BUSINESS ENVIRONMENT, YOU HAVE TO BE PREDICTIVE — NOT REACTIVE.

Stable lifetime employment is a thing of the past. Today's highly agile companies are constantly onboarding and offboarding people. They also move people up and around the enterprise as they seek to optimally align the evolving talents of their employees with the changing demands of a volatile and competitive marketplace.

Given this dynamic business environment, no company can afford to be slow or imprecise in providing its people with the access to the right IT services — and only the right IT services. This is because delays in providing the right digital workspace have an adverse impact at every stage of the employee lifecycle:

- **Slow onboarding** prevents new hires and contractors from getting up to speed on Day One. This results in days or weeks of lost productivity, missed business opportunities, poor integration with the rest of the team and lower morale. It also promotes a "workaround" mentality from the get-go.
- **Slow response to promotions, transfers and other changes in employee roles and responsibilities** has all of the same consequences. In addition, it can result in security and compliance problems — since a change in role can make it no longer appropriate for an employee to access applications or data associated with their previous position.
- **Slow offboarding** is worst of all. It can be especially dangerous when employees are disgruntled. In fact, any failure to de-provision users upon termination represents both a security risk and a compliance failure.

It is important to accelerate time to productivity throughout the employee's lifecycle with the organization.

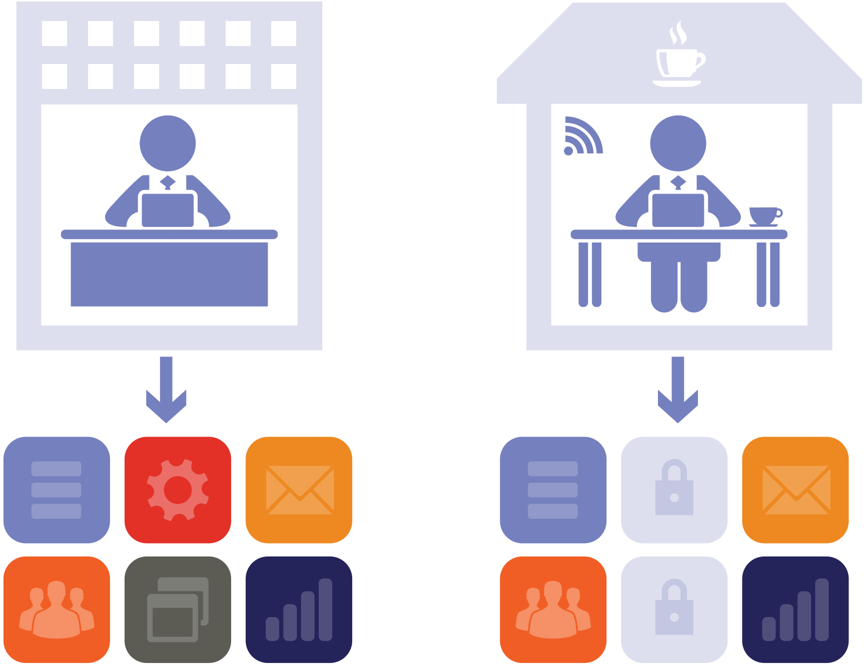


To ensure timely, precise provisioning and de-provisioning of IT services over time, you have to do more than just make your manual processes a little faster. You have to manage your employees' digital workspaces predictively. This predictive digital workspace requires a combination of well-automated provisioning/de-provisioning.

TRUTH #4:
A MOBILE/CONSUMERIZED WORLD REQUIRES REAL-TIME CONTEXT AWARENESS.

When employees accessed IT services exclusively from fixed desktops, security only required keeping them from accessing the wrong resources. But with the advent of mobility and consumerization, security also requires keeping people from accessing resources under the wrong conditions. Those conditions can include being outside an authorized location, using an insufficiently secure wireless network or being on a "rooted" device. So, while it's important to empower employees with the best, most personalized digital workspace wherever they happen to be at any given moment, it's also necessary to adapt that workspace to the employees' current context in real time.

Context-aware digital workspace delivery prevents people from accessing resources under the wrong conditions that may cause security breaches and compliance issues.

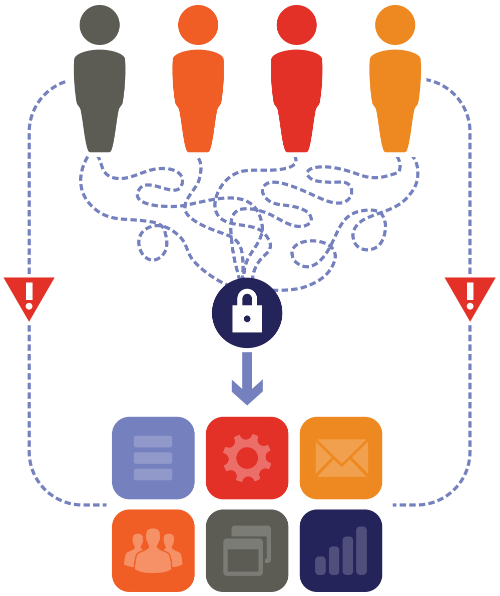


As with on-boarding and offboarding, context-aware access control requires well-automated processes and well-managed policies. To securely enable a digital workforce, however, those policies must also address any relevant real-time context concerns such as network security and location. This means that your policy engine must be able to leverage security mechanisms such as geo-fencing. To further safeguard corporate data, you also need to be able to define and enforce policies regarding removable media such as USB devices — so users are either denied access, given read-only access or granted full access depending on context attributes (such as whether the USB device's serial number is on an approved whitelist).

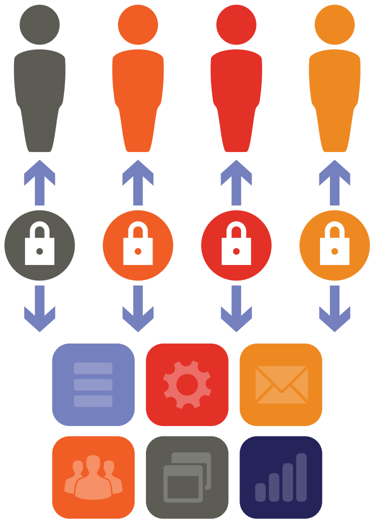
Again, companies have to be careful not to take an overly conservative approach to mobile workspace policies. The high-performance people who make companies successful do a lot of work outside the office and outside of regular business hours. So any unnecessary constraints on their capacity to work when and where they desire will have an adverse impact on the business. It is therefore important to continually fine-tune access policies so they mitigate risk to match the tolerances of the business — while keeping the fires of after-hours, out-of-office productivity fully stoked.

TRUTH #5:
EMBRACE EMPLOYEE AND BUSINESS UNIT EMPOWERMENT.

As technology becomes increasingly central to work, employee self-service and business unit delegation are becoming musts.



1. Employees lose valubale time waiting for IT services they need due to manual processes and overworked IT teams.



2. Reduce the complexity. Provide employees a personalized digital workspace with self-service and automation to increase productivity, lower costs with reduce risk.

Employees can't wait around for someone else to provide them with the tools they need. And business unit managers rightfully want to make their own decisions about how they are going to technology-enable their teams. Information security professionals have historically had mixed feelings about this kind of empowerment, because ceding control to "lay people" seemed fraught with risk. But in today's consumerized, technology-intensive business environment, these empowerments can work for — rather than against — your company's security interests. Here's why:

- **Employee self-service dis-incentivizes "shadow IT."** When users can quickly get what they want from an approved whitelist of IT resources, they are that much less likely to try getting what they want from an unauthorized one. The result is better content governance and a lower likelihood of creating highvulnerability "blind spots."

- **Business unit delegation frees up IT resources for proactive security.** IT budgets are not growing at the same rate as IT threats. Given this reality, IT security can be enhanced by re-allocating resources from routine administrative tasks to more proactive defense of the IT environment.

- **Rules-based automation is more reliable than manual processes.** To ensure that business users operate within safe parameters, IT has to codify and automate authorization and provisioning policies. This codification forces IT to systematize its approach to digital workspace management — making it more trustworthy and consistent than it is when IT relies excessively on ad hoc actions of individual human technicians.

Business leaders concerned with security and compliance should therefore complement good governance with user and business unit empowerment in order to achieve optimum outcomes for both productivity and risk mitigation.

MEET DIGITAL WORKSPACE SECURITY OBJECTIVES

Companies must protect themselves from the growing information security threats that can compromise their finances, their intellectual property and their customer relationships. At the same time, they cannot allow security measures to create the kind of excessive operational friction that can threaten business performance.

In fact, the real goal of today's tech-centric companies is to simultaneously improve both security and organizational agility.

These twin goals can be accomplished by securing the digital workforce — with predictive, context-aware policy logic that drives IT service delivery and governs user self-service. Traditional security technologies will, of course, continue to play an important role in protecting the enterprise. But for IT services that have a human end-point, effective policy-based management of the digital workspace is essential. And, implemented correctly, that management can be a powerful enabler of competitive business advantage.

TAKE A PEOPLE-CENTRIC APPROACH TO SECURITY WITH RES

The digital workspace is more vulnerable than ever, so organizations should augment their traditional security approaches with a more people-centric approach to security. Taking this approach means that your comprehensive security plan doesn't come at the cost of worker productivity or experience.

RES ONE Security ensures your business is protected from threats with a unique people-centric approach to managing security, identity and access management and governance.

- Protect against external and insider threats
- Reduce risk and ensure compliance through insight and visibility
- Manage worker security through automation and a single identity
- Drive worker productivity with secure access and automated service delivery

RES secures workspaces, keeps workers productive and gives back more control to IT organizations. To help meet security goals quickly, RES ONE Security can be up and running within days, not months or years. To learn more or speak with a RES support agent, visit www.RES.com/Security.

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.