RES

RES ONE™ SECURITY FOR THE WORKFORCE MATRIX OF KEY CAPABILITIES

CAPABILITY	SECURITY	GOVERNANCE	IDENTITY	ACCESS
Context awareness — control access rules based on granular context (e.g., person, location, device, time of day, etc.), securing apps, websites, data, removable storage, printers and IP connections.	✓			
Whitelisting and blacklisting — implement granular whitelisting and blacklisting for defense against ransomware and control over apps and files that can be executed.	✓			
Dynamic privileges — control which workers can execute specific tasks within an app based on their identity and without granting full admin rights.	✓			
User-installed apps — grant workers admin rights to install specific software based on a list of pre-approved, trusted apps — protecting the business by limiting the number of workers with admin privileges.	✓			
Device lock down — control what workers can and cannot do on a particular device based on context. In one click, implement read-only blanketing to make all local hard drives read-only or integrate with your mobility management system to extend security.	✓			
Environment snapshot — get a cloud-based, real-time snapshot of app usage, device usage and environmental topology with RES Viewpoint — to better plan for future projects and make IT aware of any unknown changes.	✓	✓		
Workspace analysis — give administrators visibility into a user's workspace environment and specific configuration settings. This not only gives IT more insight from the perspective of the users, but allows IT to see if and when errors occur.	✓	✓		
Audit tracking — leverage log reports for auditors to prove access and policy controls are in place and to determine where data is or is not accessed.		✓		
Delegation of control — open or restrict the management console for different administrative roles and create real-time configuration reports to empower individual application owners.		✓		
On-demand reporting — improve infrastructure management with the ability to report on changes to the workspace, current status and license usage data for all workers. Monitor the actual use of app per worker, per app or per server		✓		
License compliance — track license usage and enforce license policies by controlling all apps from the single workspace management layer.		✓		

CAPABILITY	SECURITY	GOVERNANCE	IDENTITY	ACCESS
Web-based management console — use a central portal to build and manage workflows, maintain audit trails and track permissions, providing IT with the visibility and the ability to align with the business.			✓	✓
Consolidated identity store — unite data from multiple back-end systems to create a single, customized identity for each worker, ensuring that workers and the business remain secure.			✓	✓
Third-party connectors — integrate with a broad set of third party systems for maximum value (HRIS, SaaS, EMM, Active Directory, IaaS, etc.)			✓	✓
Dynamic workflow engine — use an automated workflow engine with mobile approval capabilities and fully documented audit trail to ensure workers remain secure and policies are enforced.			✓	✓
Identity lifecycle management — automate delivery and removal of apps and services based on identity or policy, enabling optimal provisioning and ensuring secure offboarding where all necessary worker credentials are deactivated.			✓	
Secure self service — use a web and mobile app to give IT a face to the business, so users can review the apps, devices and services that they are qualified for and make requests in a secure and compliant way.				✓
Password management — enable workers to securely reset and manage passwords themselves with challenge questions, PIN codes or alternate email addresses, eliminating service desk involvement and dramatically reducing costs.				✓
User-initiated workflows — automate the delivery and removal of access to apps and services based on policy and approvals, enabling quick delivery of access to workers and ensuring security is maintained.				✓
Delegated access — enable workers to make requests on behalf of other workers, based on policy. Our service panels allow for a more flexible and comprehensive approach to request fulfillment – perfect for HR, management and the IT service desk.				✓
Service versioning — track changes made to a service, including the workflow for streamlined management of processes and the added visibility into what changes have been made and who has made the changes. Also, helps to simplify and align DTAP processes.			✓	✓
Data Masking — conceal sensitive or personal data so that only those with proper qualifications or reason can view the personal data (for example, answers to password reset questions, salary information and social security numbers). This ensures that privacy is preserved, security controls are enforced and compliance with data protection regulations is maintained.			✓	✓
Workspace management — implement basic digital endpoint management with RES ONE Workspace Core, including global context awareness controls, session-based folder synchronization and native integrations.	✓	✓	✓	✓

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.

RES®

v 1.0 06/08/17