RES ONE™ SECURITY

Dynamic Security for a Productive Workforce

The business landscape has changed dramatically over the last several years with the increased volume of security threats and the large number of workers using social, mobile and cloud apps. The modern worker has more power than ever, and IT has lost the ability to fully lock down the infrastructure for maximum security — resulting in an expanded and vulnerable attack surface. Traditional software fails to adequately protect against the internal and external threats that penetrate an organization's security defenses — especially when they weren't designed with the modern and mobile workforce in mind.

While workers can be an organization's greatest asset, they are often the weakest link when it comes to security. There must be a balance between keeping the organization secure, while still providing workers the access to the apps and devices they need to do their jobs. IT is under more pressure than ever to:

- Prevent data breaches from the start by restricting the ability to open unapproved or recognized files.
- Establish single identities for workers, then adjust entitlements when an identity changes or a worker leaves.
- Manage secure access for dynamic workers across physical, virtual, mobile, social and cloud environments.
- Enforce security policies to protect workers from external threats like malware and ransomware.
- Prevent shadow IT by getting workers what they need, avoiding workarounds that expose organizations to risks.
- Balance worker security and productivity to keep digital workspaces secure while enabling workers to be productive.
- Ensure regulatory compliance by securing all endpoints from data corruption or from data loss.
- Handle more risk, with fewer resources by transitioning from a manual approach to a more proactive and repeatable one.

Business leaders and IT professionals alike are concerned because their reputations are at stake and criminals will continue to exploit vulnerabilities in increasingly new and creative ways. Organizations don't want to fail a compliance audit or be in the news tomorrow due to a security breach.

THE SOLUTION: RES ONE SECURITY FOR THE WORKFORCE, A PEOPLE-CENTRIC APPROACH TO SECURITY

With the rise in security threats, the digital workspace is more vulnerable than ever. Organizations should augment their existing security with a unique people-centric approach. With RES, comprehensive security doesn't come at the cost of worker productivity or their user experience.

RES ONE Security protects your business from external and internal threats with a new approach to managing security, identity and access management, and governance. RES secures workspaces, keeps workers productive and gives back more control to IT organizations. To help meet security goals quickly, RES can deliver quick time to value — getting RES ONE Security up and running within days, not months or years.

RES ONE Security for the Workforce

Mitigate risks & security threats
Security breaches, malware and ransomware are major concerns for IT. RES ONE Security provides app-level security, dynamic admin privileges and whitelist/blacklist capabilities to mitigate risk. Only approved apps can be executed based on various attributes, while non-approved apps are restricted or blocked.

Secure onboarding & offboarding
Workers come and go frequently, causing secure onboarding & offboarding to be a challenge for many organizations. IT typically handles provisioning and de-provisioning through a series of cumbersome manual processes. RES ONE Security automates worker lifecycle management and ensures the timely delivery and removal of access, reducing security risks.

Mobile workforce security
Establishing identity has become more complex because workers are dynamic and IT systems that rely on a static definition of identity fall short. RES ONE Security provides a single, flexible identity for each worker and allows you to align their roles and functions with qualifications as a basis for configuring access and distributing apps and services.

Simplified compliance
Establishing identity has become more The increasing number of regulations around security is causing a lot more pressure on both business and IT leaders to put compliance first. RES ONE Security can mitigate the risk of failing a compliance audit by helping secure their digital workspaces and providing insight and visibility into who has access to what.

PROTECT AGAINST EXTERNAL AND INTERNAL THREATS

Today's organizations are more vulnerable than ever. RES ONE Security combines access controls, granular file-based whitelisting/blacklisting and read-only blanketing to limit admin privileges and prevent malware from being executed. RES can secure apps, websites, data, printers and IP connections, as well as USB removable storage devices. When it comes to access, choose what workers can and cannot do on company-issued devices, then implement granular contextual conditions including person, location, device, time of day and more. Grant admin rights to install or execute specific tasks based on a list of pre-approved trusted list or identity, protecting the organization by limiting the number of workers with admin privileges. Address BYOD or other mobile concerns by applying policies to individual mobile devices and integrating with your mobility management system to extend security.

IMPROVE GOVERNANCE AND ENSURE COMPLIANCE

Regulations continue to get stricter and new regulations are being adopted on a regular basis, increasing pressure to comply with security regulations and protect critical information from attacks. RES ONE Security helps achieve compliance by tracking who has access to what data to ease the external or internal auditing process and prove that necessary controls are in place. RES allows you to open or restrict the management console for various admin roles and create on-demand configuration reports for auditors or business leadership, empowering individual application owners as needed. Report on deployed workspace details, such as changes, usage, devices, apps and configuration to evaluate future enhancements and identify potential gaps. To enforce license policies and ensure compliance with license agreements, monitor license usage throughout your organization.

MANAGE SECURITY WITH AUTOMATED IDENTITY MANAGEMENT

Managing the entire identity lifecycle is vital to ensuring that proper security controls are maintained at all times. RES ONE Security enables automated delivery of apps and services based on identity or policy, enabling secure worker onboarding and optimal provisioning for the IT organization. Because RES manages identities thorough a consolidated identity store integrated with HR, project management and other systems, access will change automatically if a worker changes roles or leaves the organization. Proper offboarding of employees, consultants or contractors ensures that all necessary IT credentials are deactivated such as privileges and access to corporate systems, apps and IT assets. Automation of manual tasks and integration of existing technologies allows IT to free up resources and take a more proactive and repeatable approach to provisioning and de-provisioning.

DRIVE WORKER PRODUCTIVITY THROUGH SECURE ACCESS

Organizations must balance keeping digital workspaces secure and enabling workers to be productive. RES ONE Security keeps the digital workspace secure, while providing web portal and mobile apps to give IT a face to the business and to automate the delivery and removal of access to apps and services based on policy and approvals. Quick delivery of access prevents workers from finding workarounds. For example, workers can securely reset and manage passwords themselves, eliminating service desk involvement and dramatically reducing costs. Also, RES allows workers to make requests on behalf of other workers, based on business policy. This allows a more flexible and comprehensive approach to request fulfillment – perfect for HR, assistants, management and the IT service desk.

Why you should secure your digital workspace with RES

RES takes a unique, people-centric approach to security that incorporates identity management, access management and governance within its security solution. This allows organizations to secure their workers' digital workspaces from external and internal threats, while their workers remain productive. Resulting benefits will include:

- ✓ Greater security without impacting worker productivity
- ✓ Superior automation to save money, time and IT resources
- ✓ Improved risk mitigation and compliant security controls
- ✓ Quick time to value, measured in days, not months or years

451 Research "RES Software gains momentum with IT Store, adds new features and capabilities."

"RES Software has been around for a long time and is well-proven." David K. Johnson, Principal Analyst, FORRESTER

BEST OF vmworld 2015 EUROPE

THE STEVIES THE AMERICAN BUSINESS AWARDS 2016

Best in Biz AWARDS 2016 international WINNER

THE GOLDEN BRIDGE AWARDS BEST WORLDWIDE

NETWORK PRODUCTS GUIDE IT World Awards 2016 BRONZE

GREAT PLACE TO WORK® Best Workplaces 2016 Nederland

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 02/19/17