RES Supports the Life Sciences and Pharmaceutical Industry

PROTECT YOUR IP WITH A PEOPLE-FIRST APPROACH TO SECURITY

In the life sciences and pharmaceutical industries, intellectual property is everything. From compounds under development to trade secrets and proprietary processes, IP represents years of work, millions of dollars and the very future of your business. So, imagine the damage wrought when an associate or a hacker gains access to your data and simply walks away. And your firewall does nothing to help.

The fact is, protecting IP takes a variety of approaches that many firms simply fail to consider. Firewalls, encryption, password protection — all of these are necessary. But to address the full threat spectrum today, firms need a holistic approach to security and compliance that protects IP property by securing people first. This is where RES can help.

USER-BASED THREATS — INSIDE AND OUT

RES is a leader in the area of workspace management — and whether the threat comes from behind the firewall or from outside, it's the user and their workspace that is often the weakest link in the security chain.

For insider threats — full-time employees, temporary consultants and privileged users– the goal is to control user access across all of the different devices and contexts imaginable. But this needs to be balanced against workforce productivity. Long wait times while IT grants privileges or unreasonable obstacles in the name of security will not do.

For outside threats, an important goal is to ensure that users don't make the wrong move by mistake. This is common with phishing attacks where hackers entice users to click on email attachments that open up backdoors or launch malware. Most users are savvy, but mistakes happen — and IT needs to know how to protect against them.

SECURITY AND PRODUCTIVITY FOR A WORKFORCE IN FLUX

Protecting IP in the life sciences and pharmaceutical industries is only made more difficult by a workforce that is increasingly mobile and in flux. Today, you have employees working at home and sales representatives in the field. You have physicians on location at clinical trial sites and executives touring facilities overseas. You also a wide array of contractors and consultants flowing in and out of your organization on a regular basis — from R&D, manufacturing and IT to management, clinical trials and sales and marketing roles. Across all of these scenarios, you need to manage access to data and systems in a flexible but secure way — supporting the trends toward "bring your own device" (BYOD) and cloud. Ultimately, users need to be productive quickly using the tools that make sense for them in whatever context they may find themselves.

MEETING THE CHALLENGE WITH RES

Fortunately, the holistic approach to security enabled by RES can help you rise to all of these challenges. Instead of securing the network, RES focuses on securing the user and the user's workspace with a series of technologies that help to control and automate data access while limiting the kinds of oversights that lead to data breaches. These include:

- **Dynamic privileges:** Elevate or restrict access rights to specific applications based on the user's role to protect data in the context of a dynamic and constantly evolving workforce
- **Automated provisioning (worker on/offboarding):** Maximize productivity by quickly granting or revoking policy-driven access for workers — following standardized procedures, integrated with HR, that eliminate human error and prevent non-authorized data access
- **Application whitelisting:** Define and enforce the applications and file types that users are allowed to execute and block everything else
- **Read-only blanketing:** Allow read-only privileges for designated drives and force users to save work only to preauthorized, highly secured areas
- **Device lockdown:** Shut down endpoints and prevent data access of any kind in cases of tampering, access violations, or device theft
- **Context-awareness:** Grant or deny access to data and applications based on contextual information such as location, device type, user role, time of day and much more
- **Follow-me-printing:** Ensure that sensitive information (such as trade secrets or clinical trial data) gets printed only to the printer nearest the user

With these technologies in place, RES customers have had great success defending against data breaches. And when you consider the fact that the average cost for resolving a data breach stands at $3.7 million, perhaps it's time to consider RES.

THE FREEDOM AND CONFIDENCE OF HOLISTIC SECURITY

In the end, RES makes it easier for your firm to operate securely, succeed as a business, and bring new compounds and therapies to market. With RES, you'll enjoy:

- **A more secure workplace** with better protection for valuable IP
- **Higher worker productivity** with far less risk of data breaches
- **Improved workforce flexibility** with a secure approach to mobile access
- **Faster on/offboarding** for contractors and consultants with lower risks of improper data access
- **Greater confidence** to focus on your mission and achieve your goals as a firm

LEARN MORE

To find out more about how RES can help you achieve higher levels of security, visit us online at www.res.com or call us at 1 800 893 7810.

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 01/23/17