HELD FOR RANSOM? LOW-PAIN/HIGH-GAIN WHITELISTING

A RES solution brief

THE WHITELISTING IMPERATIVE

One of the most serious cyber threats — ransomware — is growing with incredible speed. According to Security Magazine (November 23, 2015), McAfee Labs researchers saw fewer than 1.5 million instances of ransomware in Q3 2013. This grew to more than 4 million instances in Q2 2015. Now that hackers have solved the problem of how to monetize hacks, there's no end in sight.

But in most cases of ransomware, we've found that the hackers are exploiting vulnerabilities offered by internal employees. The hackers send phony emails – a practice known as phishing — that entice users to click on links that activate malicious code that encrypts the organization's data. All the firewalls and password protocols in the world won't protect your incredibly sensitive data from careless users.

Whitelisting is an extremely powerful weapon in the war against ransomware and other cyberattacks. It reduces risk by blocking unauthorized software, including malware, from being installed and executed. This effectively disrupts the cyber kill chain for many malware-based attacks. As technology becomes more consumerized, people are becoming more accustomed to accessing whatever apps and resources they want from the cloud. Unfortunately, this kind of indiscriminate downloading can put your organization at risk, so you need to control what people can and can't access using blacklists and/or whitelists.

Many security managers prefer whitelisting because they have concerns about the completeness of blacklists. A whitelisting approach to endpoint security can better safeguard the IT environment by enabling administrators to restrict user access to only those resources that are definitively known to be both safe and useful.

THE WHITELISTING CHALLENGE

While whitelisting is an important best practice, it can also be difficult and time-consuming to do correctly. That's because three types of change keep adding cost and complexity to whitelist administration:

1. **Changes in approved applications.** Organizations used to depend on a relatively limited number of apps that were only upgraded periodically. Today, organizations tend to rely on a growing number of applications—most of which are being updated more frequently. This larger, more dynamic application portfolio increases the administrative work required to maintain accurate and appropriate whitelists over time. It also increases the likelihood of error.
2. **Changes in people's roles and responsibilities.** Whitelists tend to be role-specific. So when someone's job changes, their whitelist has to change, too. This further adds to the cost of administration. Also, the right whitelist changes aren't made quickly enough, people may not be able to be fully productive in their new positions right away.
3. **Changes in how and where applications are used.** As users become more mobile, it has become necessary to add new types of dynamic policies to application whitelists. For example, it may be appropriate to allow certain users to access certain apps when they are onsite—but disallow access when they're not. Or an app maybe only be whitelisted for use on a secure VPN, so it gets "de-whitelisted" when the user is on public Wi-Fi. These kinds of policies create additional administrative pain even as they deliver vital security gain.

These issues and others underscore the need for a well-automated approach to whitelist administration.

THE SOLUTION: ONE-PASS, CONTEXT-AWARE WHITELISTING

RES significantly improves whitelisting in two ways:

Streamlined and automated whitelist policy administration

The RES policy engine makes it easy for IT staffs to capture whitelist baselines (including OS and application files), link people's whitelists to their roles as defined in enterprise HR systems, and define other whitelist parameters as appropriate (device, network connection, location, etc.). Where appropriate, RES also enables organizations to delegate whitelist management responsibilities to departmental managers.

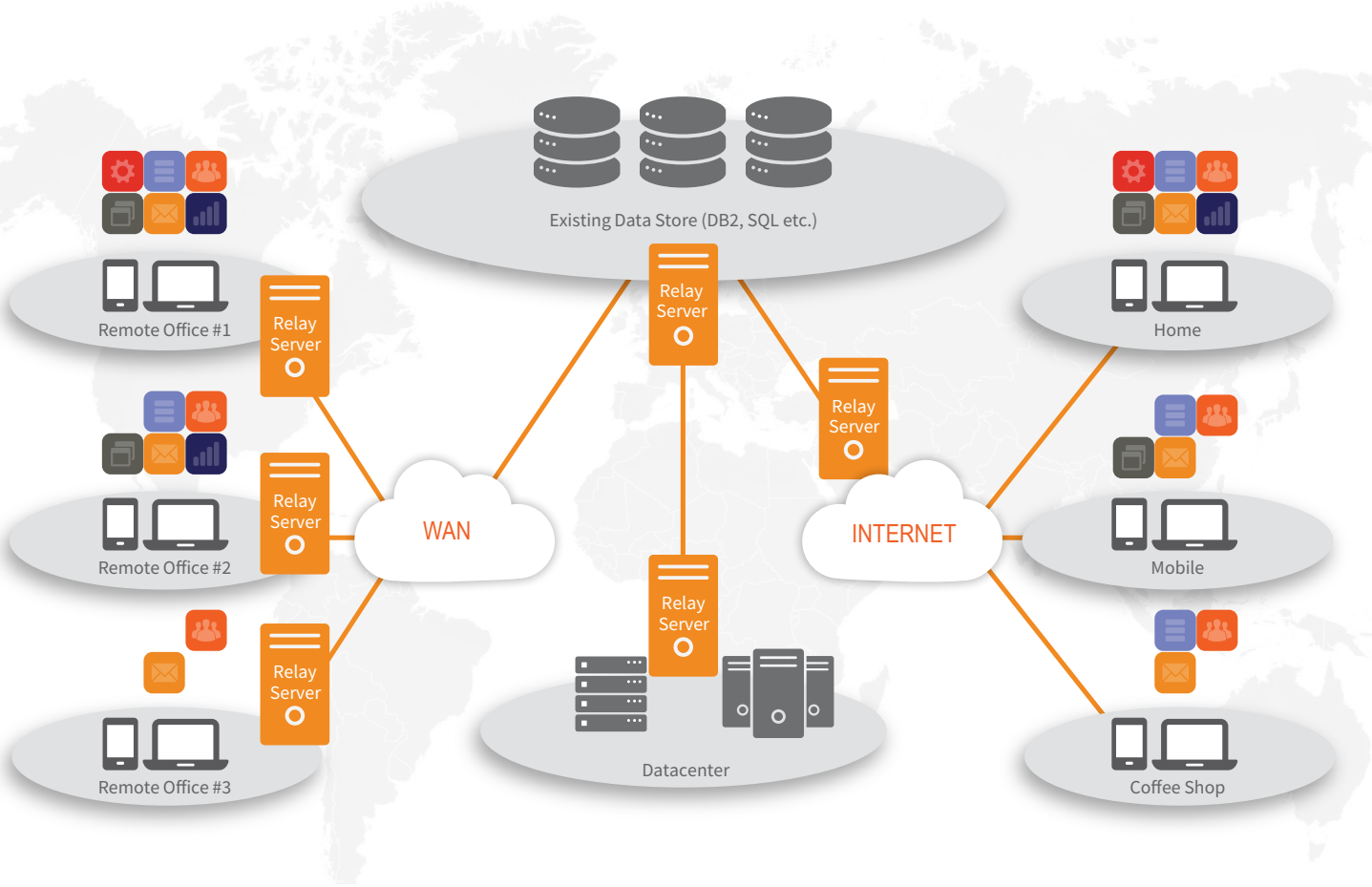
Integration with security administration tools

This integration allows organizations to distribute and enforce the whitelists they create and update using the RES policy engine across their environment via their existing infrastructure (i.e. Microsoft SCCM, IBM BigFix). It also allows the RES policy engine to automatically update whitelists to include any applications, upgrades, patches, etc. This combination of an intelligent whitelist policy engine and security administration integration delivers several valuable benefits, including:

This combination of an intelligent whitelist policy engine and integration with IBM BigFix delivers several valuable benefits, including:

- **Better security.** Accurate, up-to-date whitelists protect organizations from malware, data loss, non-compliance and other threats posed by unauthorized use of application and cloud services that have not been appropriately reviewed and approved for safety, legitimacy, etc.
- **Minimized labor costs.** The automation provided by RES dramatically reduces the manual work required to maintain whitelist accuracy over time. This generates cost savings and free IT staff to work on other high-value projects.
- **Reduced technology costs.** By leveraging existing investments in security management, RES enables IT to avoid redundant software license and maintenance expenses
- **Increased end-user productivity.** RES ensures that user whitelists are quickly updated so they have access to all the resources they need to get their jobs done—and they don't have to waste time making help desk calls just to get access to the legitimate resources they need.
- **Enhanced compliance.** Automated, policy-based control of app access helps fulfill regulatory mandates regarding best-efforts/best-practices for IT safety.
- **Greater organizational agility.** Organizations that can keep their whitelists current even as they add resources, shift employees, merge with other organizations, etc. can be much more responsive to changing conditions than those that continue to depend on slow, manual access management processes.
- **IT modernization.** A well-automated whitelist management process can help facilitate many of the other technology initiatives that organizations undertake—including those related to mobility, desktop virtualization and cloud.

For these reasons and others, organizations currently using security management frameworks should strongly consider adopting RES ONE™ Workspace for whitelist policy administration.



By leveraging the RES automated policy engine, organizations can keep their app whitelists accurate and up-to-date with less cost and effort.

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 3.0 01/09/17