RES

The Policy-driven Approach that Transforms Access Management

ROLES & RABBIT HOLES

TRANSFORMING ACCESS MANAGEMENT THROUGH A POLICY-DRIVEN STRATEGY

Perhaps you remember the story of Alice's Adventures in Wonderland, where a child goes on an underground adventure, following a white rabbit wearing a waistcoat and pocket watch down a rabbit hole. The journey down the rabbit hole was just the beginning for Alice and she had no idea that it would lead to a mad, illogical world for which she was ill prepared.

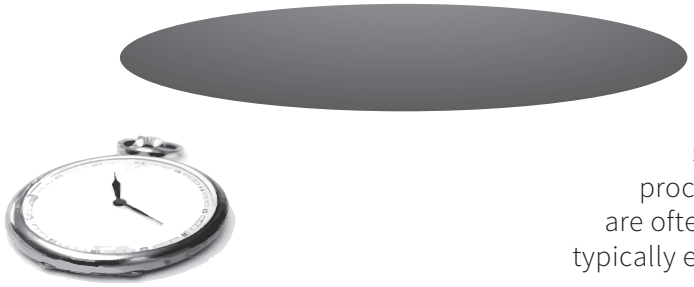
> *"… suddenly a White Rabbit with pink eyes ran close by her…. when the Rabbit actually took a watch out of its waistcoat-pocket, and looked at it, and then hurried on, Alice started to her feet, for it flashed across her mind that she had never before seen a rabbit with either a waistcoat-pocket, or a watch to take out of it, and burning with curiosity, she ran across the field after it, and fortunately was just in time to see it pop down a large rabbit-hole under the hedge. In another moment down went Alice after it, never once considering how in the world she was to get out again."*
>
> *— Alice's Adventures in Wonderland by Lewis Carroll*

Sometimes the simplest-seeming actions become wildly complex, and widely-accepted approaches can lead to unpredictable outcomes. But what does this have to do with access management? Going down a rabbit hole with our access management strategy doesn't mean that we will find ourselves at a tea party with the Mad Hatter, but we may find ourselves in a spot we weren't fully prepared for – and without a proper strategy for getting back.

Read this whitepaper to learn how to make the transition from traditional role-centric access management to an effective technology-enabled and policy-driven strategy. Understand how taking a policy-driven path will be much more dynamic and deliver much more power and flexibility to IT. Continue reading to get prepared for your next adventure.

A JOURNEY DOWN THE RABBIT HOLE

To understand the importance of a comprehensive access management strategy, consider, for example, the mundane but crucial task of providing secure access to technology resources. Access is often approached on the basis of roles: each worker's role equals a set of assumed resources; then systems and processes are established to grant the inevitable exceptions. Once an individual worker has been suitably identified, access is then delivered — often through either a complex and cumbersome identity and access management solution, or through a home-grown host of scripts and a patchwork of manual and automated processes. And then there are exceptions requests. These are often handled via service desk ticketing systems, which typically entail significant costs per ticket to the organization.



THERE ARE SOME CHALLENGES WITH THIS

First, traditional identity and access management solutions are complex systems that require extensive integration and maintenance in their own right. They're expensive to acquire and maintain and, while they may get the job done, each new system drags along its own maintenance headaches for IT.

Second, the "let's just script it" approach has serious drawbacks of its own. These solutions can be precarious and costly. If an individual process glitches or a technology change is introduced, scripts and workarounds can quickly prove unwieldy — meaning there's a good chance you'll have a "failure to access" on your hands and unhappy, unproductive workers at your shoulder.

Identity and access solutions regardless of type are mission critical. Without them you can wind up with sensitive information in the wrong hands, serious compliance issues that can cost your organization its reputation, money or more — not to mention it can mean a real speed bump for your career.

DREAMING OF WONDERLAND

What if today's cobbled-together solutions to identity and access management could be replaced with a powerful, easy-to-manage and automated solution that is easily implemented and operated across the most fragmented of hybrid infrastructures?

Sound like a pipe dream? Maybe not. Let's see what it would take to build a secure access solution that stands up to the toughest challenges IT is ever likely to face, makes workers more productive than ever before, and is a breeze for IT to deploy and manage.

GETTING STARTED

Here's a question: how many job roles exist in the average enterprise today compared to 100 years ago? Well, finding stats on that can prove more difficult than you might think. But can we accept that the diversity of work roles is increasing? And it isn't just roles, it's apps, IT services and the mix of office-based vs. mobile workers, to name just a few of the growing pressure points on IT.

With work roles diversifying, access needs are growing more complex as well. Mapping the service needs and entitlements for every individual worker requires defining both:

- Policies that govern who should get access to what and when
- Information, at just the right time, that is needed to deliver access in accordance with policy

But wait! There's more. The breakneck pace of business change means that workers' access requirements are dynamic, due to frequent changes in role and work environment. Add some common business scenarios — mergers, acquisitions and transitional workforces — and…. Well, let's agree that managing access may sound simple, but it's a seriously tough problem for IT to solve. Fortunately, it can be cracked. So let's start looking at solutions.

CHOOSING THE RIGHT TUNNEL

On your journey to access wonderland, let's imagine that you have two paths before you once you've entered the tunnel:

- Traditional **role-centric** path
- Technology-enabled **policy-driven** path

Let's start with the traditional, **role-centric** path. This means that a worker's role is used to define his or her basic access needs, and major changes to that role trigger further changes to access. When workers are hired, they are granted access to the resources that are considered necessary for people in that role. Sales people get CRM licenses, for example, and managers are granted HRIS access privileges so they can see information for their direct reports. Over time, as workers change jobs, their new roles may require them to have different access as a result. And when their role is terminated altogether — that is, when they leave the company — they lose all access.

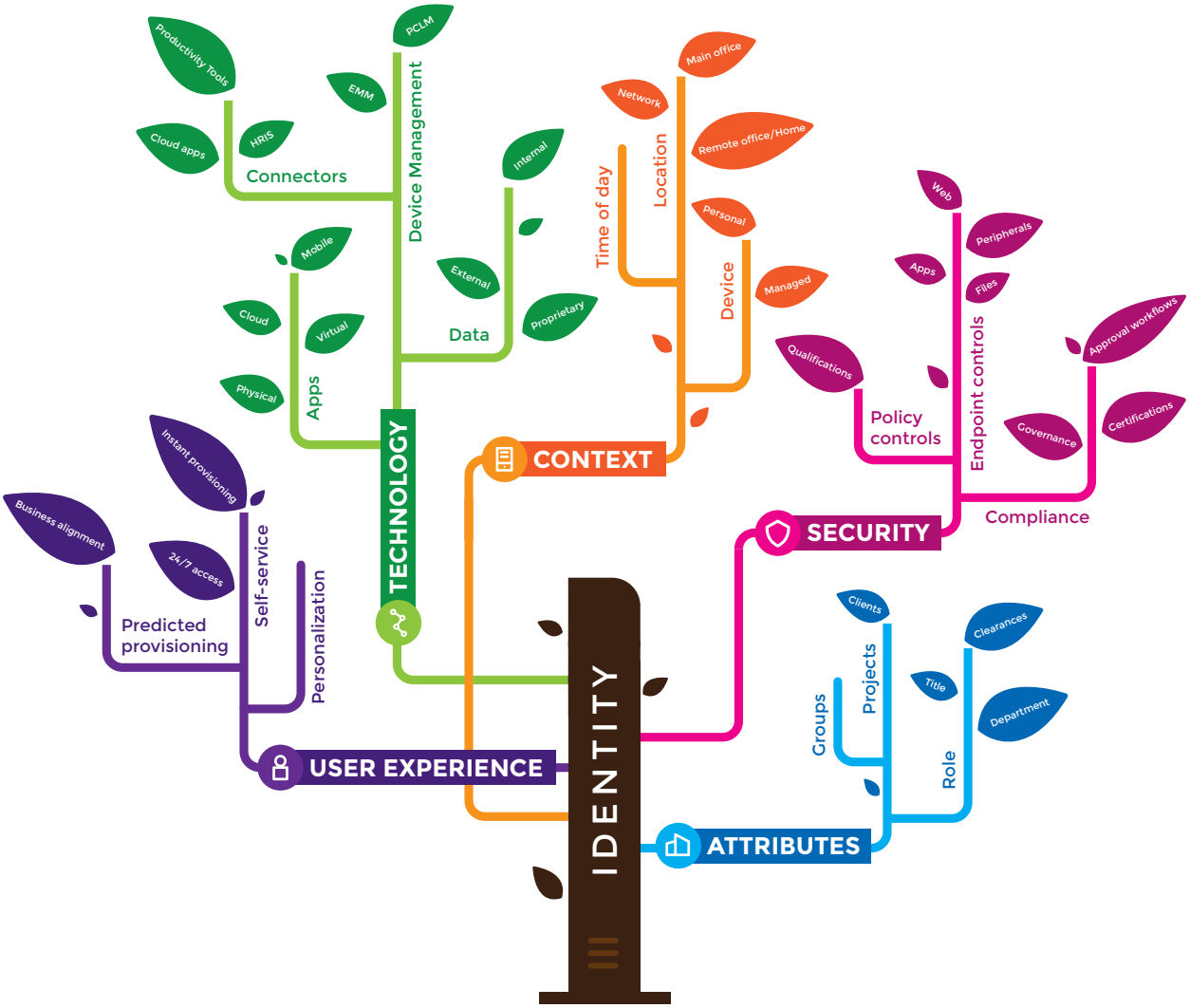
Policy-driven access management focuses on understanding the access that each individual worker needs based on his or her context.

This role-centric path is intuitive and simple, and seems pretty solid. But does it reflect the true range of possibilities that take place in the real world? What happens when a worker wants to access a sensitive database while working remotely — say, in a hotel lobby on a public Wi-Fi? Or, what if a worker — dissatisfied with the user friendliness of the organization's file-sharing technology — logs on to his or her personal file-sharing cloud solution and uploads proprietary company information? Should this action be granted or denied? In both of these examples, different access rights are called for; but in neither case was the worker's role affected. Therefore, a role-based access solution would not have triggered a change to his or her access rights, even though doing so may be required under company security policies.

The alternative path is **policy driven**. Instead of focusing on roles, policy-driven access management focuses on understanding the access that each individual worker needs based on his or her context. This is done by defining policies that are used to govern access dynamically. For example, policies can be defined by security requirements: don't grant anyone access to our sensitive customer database that's chock full of credit card and other personal data if they're attached to a public Wi-Fi network. Instead, give them a security alert upon each access attempt that advises them to move to a secure network.

This is a vastly more dynamic approach that delivers much more power and flexibility to IT professionals. But it also demands a vast amount of information that must be consumed by the system that is managing this access.

To understand how this works let's use the "identity tree" model. Consider the illustration on the next page for our IT example.



Our identity tree describes the information needed to understand how to use pre-defined policies to determine what access should be granted for every individual based on their actual context and how. And you can see from the get-go that this is a far more comprehensive approach than role-based access alone. So let's take a closer look. The tree breaks access information down into five basic categories:

- **Attributes** define who the worker is and tell us enough about what she's responsible for to allow us to understand her needs for apps and data. This is similar to the information used by role-based approaches to access management. But there's much more that we can do.
- **Technology** tells us what technologies a worker will be accessing and how they are delivered by IT. This is especially important if, for example, you allow the use of personal devices for use with company systems and data.

- **User Experience** decides how the worker can be equipped with the right services at the right times. Workers are more productive when their technology is readily and easily accessible and personalized.
- **Security** looks at what policies and controls need to be in place to protect the worker (or to protect the organization from a worker's careless or malicious actions), as well as capturing the information needed for compliance-related audit trails.
- **Context** tells us when our worker is in a suitably secure and appropriate environment, or whether she needs additional protection to keep data secure. We're confident that when a worker is attached to the company network at a known location and using a company-issued device, that reasonable security is in place. But when they're not, restrictions can be automatically put in place.

DIGGING TO THE ROOT

If you had a rich set of information, such as that in our identity tree, readily available to you as a means of governing access, it would allow you to empower every worker with exactly the resources they need at exactly the right time — as well as prevent them from consuming resources that are unsuited to them, either for reasons of cost or security. But how practical is it to harness this information?

A lot of identity information such as name, level and job role can be readily extracted from HRIS. But there's more. Where are they at the moment of any given connection? Working at the office on a secure connection? Working from home, a hotel lobby or a local coffee shop? You can't follow them around, but your network knows via IP detection. Likewise, what device are they using for that access: company issued or personal? You may want to assign careful controls to actions that can be performed when a non-company-issued USB device, for example, is inserted into the port of a company machine.

All of this data and more are readily available through the systems you have in place today within your infrastructure. They can be used to determine an individual's access requirements — not just based on a static list of apps, data and services, but on their movements and working contexts throughout the day and night.

Imagine the Solution in Real Life.

Imagine a worker accessing an app that houses sensitive data. She's toiling away in her company office, tucked safely behind the firewall. Now imagine it's lunchtime and she begins accessing that same app with a personal smart phone in a public coffee shop over an unsecure WLAN. Yes, she's still the same person — at least, most identity solutions would think so. But her working context is now dramatically different; and that difference should be enough to demand a change in access permissions to apps and data while sipping her venti pomegranate machiatto on an untrusted network, in the interest of keeping the company's data secure. Shouldn't any identity system be smart enough to figure that out and respond accordingly? And then dynamically govern the access that is granted to her based on her real-life context?

ADDING THE MAGIC

No, we're not finished designing our identity & access management solution. Let's proceed with a few basic questions:

- How much manual labor does your current access management approach require?
- How quickly can you adapt to changes in worker roles or context?
- Who's initiating worker provisioning, de-provisioning and access management requests?
- What sources of truth are you using today to define worker identities, and are they allowing for accurate access management?
- Are those solutions easy to work with or do they require constant tinkering?

Traditional identity and access management solutions are notoriously cumbersome. As a result, many companies pursue access management in a static way, requiring someone in IT to directly fulfill every relevant change by performing technical changes in the infrastructure for each access requires — either by hand or by executing scripts that only work at particular points in the overall process.

The result is an error-prone, time-consuming process that can expose your company to serious risk. And since each IT admin may execute fulfilment differently, steps can be forgotten and skipped, and incomplete information can be provided by the person requesting the action. How often have you heard, for example, of workers leaving a company, yet remaining a logical part of the IT infrastructure for days, weeks or months? Maybe it's even happened to you. But it's a security nightmare, to say the least.

These challenges can be readily dealt with by taking manual labor and piecemeal solutions out of the picture and harnessing the consistent and predictable power of automation. Automation can implement access changes accurately, consistently, quickly with low operational costs. But to properly engage automation, it needs to be accompanied by a workflow solution. Define the workflow processes and approvals needed for each given task — for ordering a new device or adding access to a new database — then automate those workflows in a way that can be adjusted easily and quickly as business needs change.

The goal of a **policy-based access management system** is to recognize that each worker's context changes dynamically, and those changes should be taken into account and adapted to when governing access. This means your infrastructure can automatically and immediately provide or revoke access rules based on perceived security risks, as determined by the IP address, device type, time of day and more at the very moment that access is requested. And that is definitely cool.

AND STILL MORE MAGIC

Who initiates service requests for access to new apps, data and services? Most often, the workers themselves trigger the process by submitting a request (typically to a service desk). But what if their service request could be requested via a self-service portal, and then automatically fulfilled? Workers, after all, are most aware of their own needs; by empowering them to request changes in provisioning or new IT services, the organization will typically get the fastest possible response to the business need — much faster than if the request must originate inside IT.

It's also safe to do so when a self-service portal is working in partnership with your policy-based access solution. Policy would determine what services each worker should be eligible for automatically. The person logging in will then see those services only — not services to which he or she should not have access. There's no risk of expensive over provisioning, or of getting access to systems and data that need to be closely protected.

Approvals for selected services can be implemented once a request is made. This happens automatically through notifications sent to designated approvers. Common requests can be given automatic approval, which provides both tracking and instant access, while other request can run through approvals as defined by the business.

Beyond faster response time, the company benefits from higher productivity — both from the worker, and from the managers or IT employees who no longer have to handle this task themselves and can spend more time on higher-priority projects.

THE CIRCLE OF ACCESS

Don't think of identity and access management in terms of provisioning only. Instead think of a closed loop — a cradle-to-grave lifecycle of access management for each person receiving services from the organization. A new worker's onboarding is equivalent to his or her birth (as far as the organization is concerned), and "life" ends with termination — the last phase of the loop. Under this lifecycle approach, each organization should be able to:

- Identify the needs of each new worker and provision them (automatically) even before the worker has even reported to work.
- Enable automated self service for new resource requests that occur at any point throughout the worker's lifecycle.
- Immediately and automatically revoke services and access the moment a worker's termination is recorded. No more email, no more licenses, no more access to systems sensitive or otherwise.

Through policy-driven automation, removing worker access is much faster; and the window of opportunity in which access privileges might be abused by the ex-worker, or for that matter a rogue hacker, a criminal organization, or anyone else, also shrinks. The benefits — lower business risk and costs — are pretty compelling.

HOW GREAT WOULD WONDERLAND BE WITH RES? THIS GREAT:

- Access management would be smart enough to understand both identity and context, it would be powered by work-flow supported automation, and it would include self-service capability that empowers your workers.
- Organizations would automate and deliver resources based on policy as opposed to roles, implementing access management that would be driven by dynamic collaboration between IT and everyone else.
- Organizations would take into account the full context in which access rights are requested, as well as empower users to initiate requests themselves via self-service mechanisms.

This isn't just Wonderland. RES ONE Security enables organizations to make this happen in real life with a unique people-centric approach to identity and access management:

- Drive worker productivity through secure access – keep the digital workspace secure, while providing web portal and mobile app to give IT a face to the business and 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. 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 policy. This allows for a more flexible and comprehensive approach to request fulfillment, which is perfect for HR, assistants, management and the IT service desk.
- Manage security with automated identity management – automate the 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 connected to 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, 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 deprovisioning.

We offer a flexible, context-sensitive solution that provisions and manages incredible digital workspaces for everyone, throughout the complete employment lifecycle of each worker. Workers get faster, more complete access to the resources they need without unwanted security shortfalls or compliance headaches. RES ONE Security can get you out of that rabbit hole in days, not months or years. To learn more or speak with a RES support agent, visit www.RES.com/Security.

PARTING SHOTS: 3 ACCESS SCENARIOS GUARANTEED TO KEEP YOU UP AT NIGHT

1: MERGERS & ACQUISITIONS

What happens when you need to onboard hundreds or thousands of people at once? That's the case in a merger or acquisition, which — for better or worse — is a common occurrence. As two companies become one, IT has a host of thorny problems to solve, and secure access is high on the list.

2: WORKERS IN TRANSITION

What happens when you have large pools of rotating, seasonal or high turnover workers? Clinical care organizations, tax professionals, delivery companies, call centers that churn people at dizzying rates — all have especially tough access (and security) challenges.

3: AUDIT COMPLIANCE

Who has access, when did they get it and what person approved it? Repeat when access is revoked. Add cloud apps and mobility to the picture. With mobile and cloud apps a finger poke away, who's keeping track of those audit trails now?