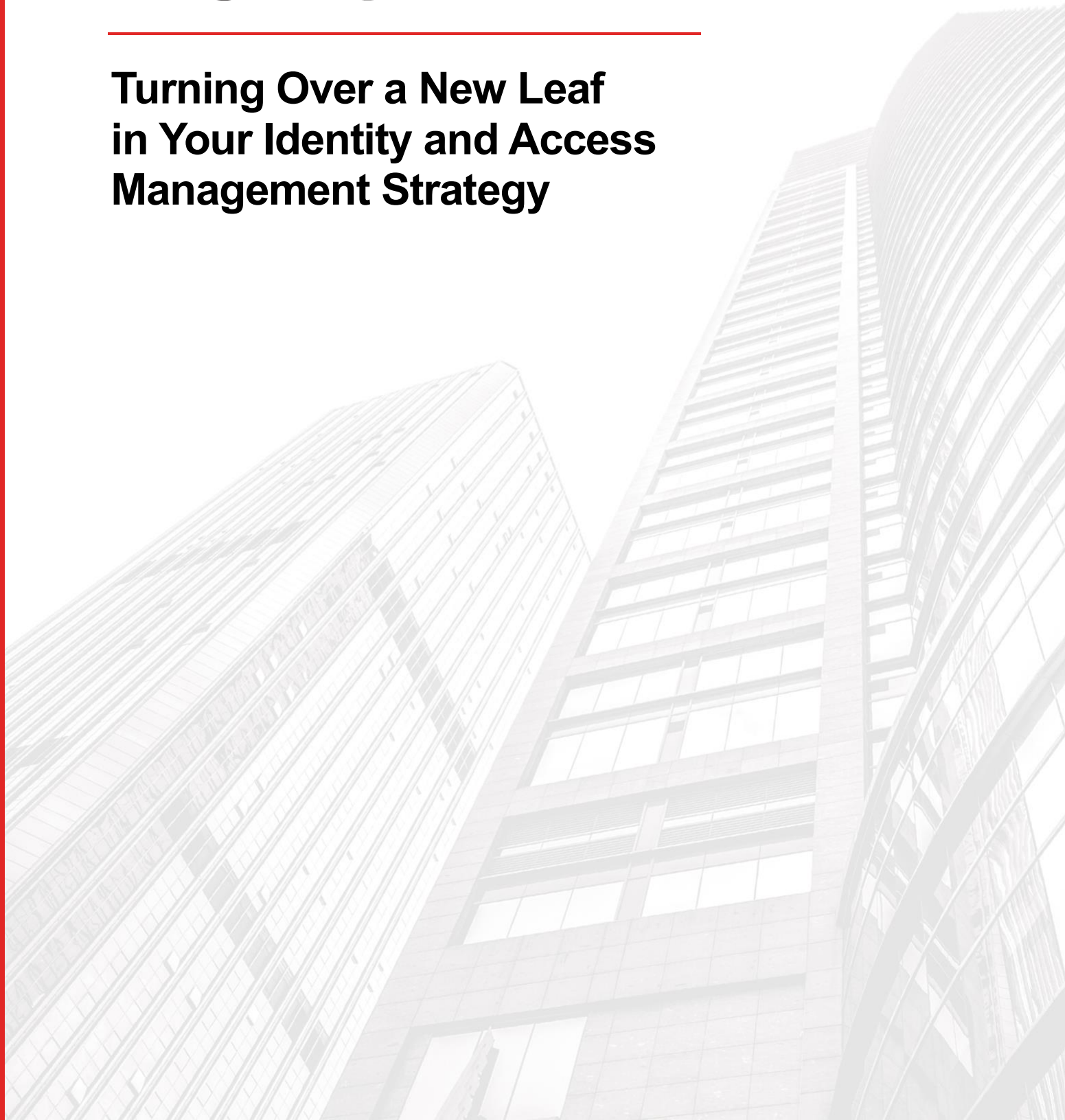
ivanti

Turning Over a New Leaf in Your Identity and Access Management Strategy



Contents

Turning Over a New Leaf in Your Identity and Access Management Strategy

A Policy-Driven Approach Will Grow Your Identity Governance and Management Effectiveness

The transition from traditional, role-centric identity and access management (IAM) to an effective, technology-enabled and policy-driven strategy can be challenging. But taking a policy-driven path that looks more holistically at identity will be much more dynamic and deliver much more power and flexibility to IT.

To understand the importance of a comprehensive identity and access management strategy, consider the mundane but crucial task of providing secure access to technology resources. Identity, and corresponding access rights, 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.

Barking up the Wrong Tree

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 brings 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 and 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.

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.

Turning of Seasons

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 worker 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 worker 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.

Two Divergent Paths in the Woods

Imagine you have two paths before you:

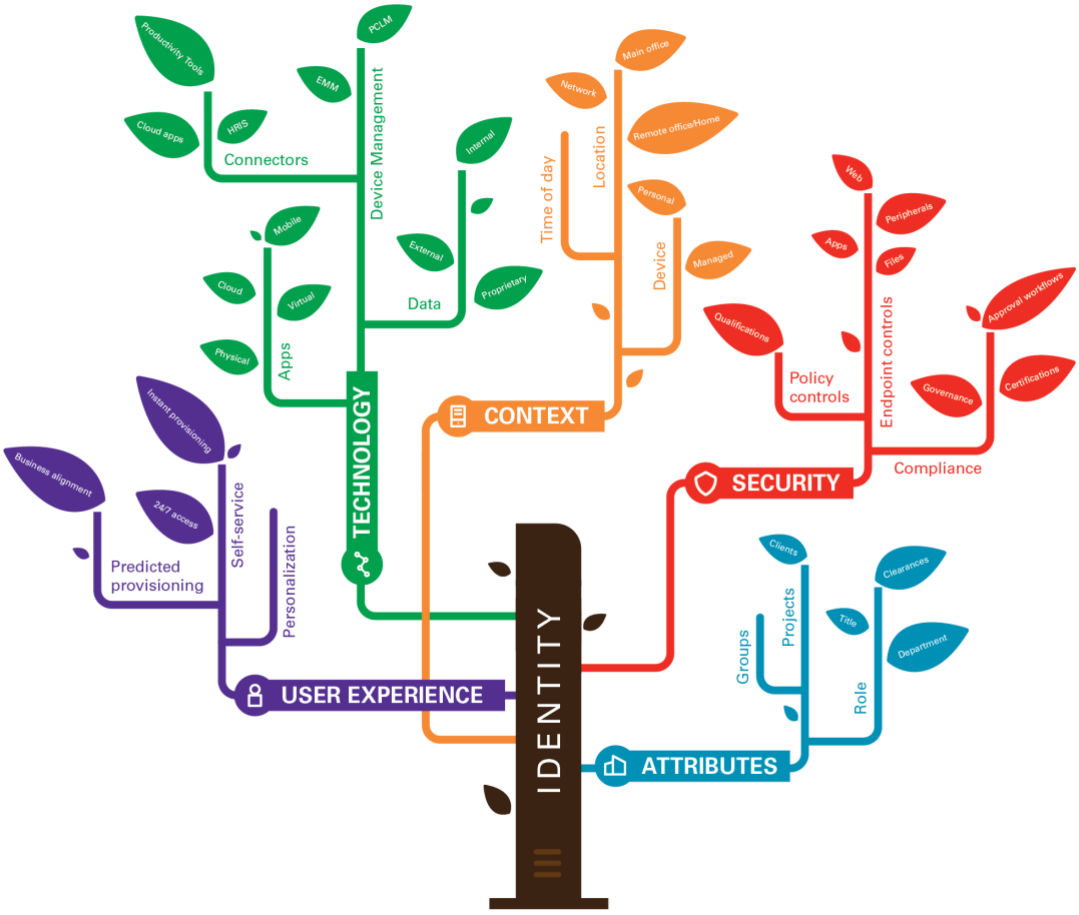
- Traditional, role-centric path
- Technology-enabled, policy-driven path

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.

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 network? 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 and technology-enabled. 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 this illustration as 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 a variety of factors. 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 their responsibilities so we can understand their apps and data needs. This is similar to the information used by role-based approaches to access management. But there's much more that we can do.
- **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 must 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 he or 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, reasonable security is in place. But when they're not, added restrictions can be put in place automatically.

Digging to the Root of the Matter

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, you could empower every worker with exactly the resources they need at exactly the right time—as well as prevent them from consuming resources unsuited to them, for reasons of cost, security, or compliance. 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 where they are 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 is 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 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 also dynamically govern the access that is granted her based on real-life context?

Growing Your View of Identity and Access Management

We're not quite finished designing our identity and access management solution. Let's proceed with a few additional 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 IAM in a static way, requiring someone in IT to directly fulfill every relevant change by performing technical tweaks in the infrastructure for each access required—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 fulfillment differently, steps can be forgotten and skipped, and incomplete information can be provided by the person requesting the action. How often have you heard of workers leaving a company, yet remaining a logical part of the IT infrastructure for days, weeks, or even 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, and quickly with low operational costs. But to properly engage automation, it must 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 IAM approach is to recognize 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 provide or revoke access rules automatically and immediately 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. How cool is that?

Seeds of Empowerment

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 fulfilled automatically? 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 shouldn't have access. There's no risk of expensive over-provisioning or of granting 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 requests 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 must handle this task themselves and can spend more time on higher-priority projects.

Turning Over a New Leaf in Your IAM Strategy with Ivanti

While many organizations have some sort of IAM activity in place, many could benefit from looking at their approach differently than they do today. By working with Ivanti, organizations can experience the following:

- Access management would be smart enough to understand both identity and context, powered by workflow-supported automation and self-service capabilities that empower your workers.
- Organizations would automate and deliver resources based on policy as opposed to roles, implementing access management that would be driven by a dynamic collaboration between IT and everyone else.

Ivanti enables organizations to make this happen in real life with a unique, people-centric approach to identity and access management that looks at identity from many dimensions and enforces policy accordingly.

Learn More


ivanti.com/contact


epg@ivanti.com