ivanti

Best Practices for Secure and Efficient Onboarding and Offboarding

Contents

Introduction

Imagine hiring someone and not having a place for them to sit their first day. Or their first week. They wouldn't be very productive, nor would they be too keen on their new employer.

And yet, today's workforce depends far less on the chair or desk of a physical workspace than on the applications, content, and services that constitute the *digital* workspace.

Slow provisioning of digital workspaces isn't just a problem at onboarding time. It saps productivity and morale throughout every employee's tenure as their roles and responsibilities change—and as they experience delays in gaining access to the corresponding digital resources they require.

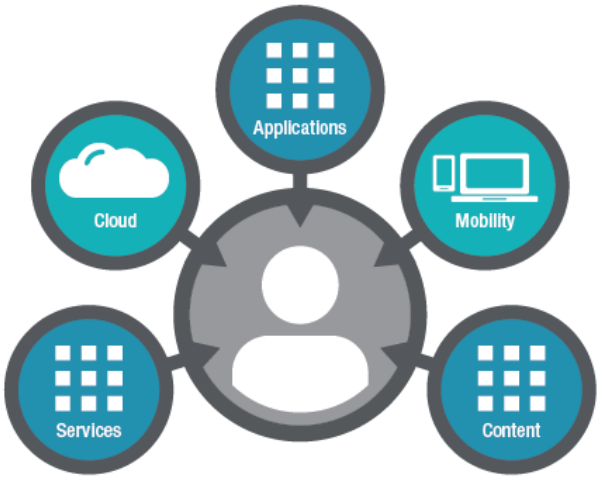

Fig. 1: The digital workspace provides workers the IT services and content needed to be productive, in harmony with increasingly mobile, multi-device workstyles.

Worse yet is what happens at the end of an employee's tenure. Few security risks are as serious as a disgruntled employee whose passwords are still active. But companies that can't de-provision their employees' digital workspaces quickly and reliably expose themselves to that risk with every termination.

Every company benefits from automating the provisioning, re-provisioning, and de- provisioning of its digital workspaces. In fact, such automation is a must-have for any company seeking to:

- Attract and retain top talent
- Motivate and equip that talent
- Optimize its organizational agility
- Mitigate digital risk
- Gain more value from IT

Employ this white paper as a guide to: 1) better understanding the most common onboarding challenges and obstacles; 2) seeking out an effective solution; and 3) realizing the business benefits when a proper solution is in place.

Understand the Challenge: Secure Workspaces for Digital Workers

What happens when the network crashes? Within seconds, cubicle aisles fill with employees wandering aimlessly and productivity halts. We all access a variety of digital resources that include:

- Applications (Word, Salesforce, SAP, etc.)
- Content such as shared documents in collaboration applications
- Services including IT help desk and corporate travel booking

Employees should be able to access the resources they need, yet it's also important for companies to not allow them to access resources inappropriately. Permissions can be restricted accordingly. The set of resources an employee (or a virtual employee, such as a temp or contractor) can access digitally is understood as that employee's "digital workspace*."

* From a technical perspective, a digital workspace differs from a "virtual desktop"—the interface an employee is given on a particular device to access certain resources in their digital workspace. However, an employee may have access to resources in their digital workspace beyond what's presented in their virtual desktop. For example, their digital workspace may include an IT help desk they can access outside their virtual desktop to obtain technical assistance even if their virtual desktop isn't functioning. Similarly, icons that remain on their virtual desktop may be functionally disabled (and thus not part of their digital workspace) if they're using a public WiFi connection.

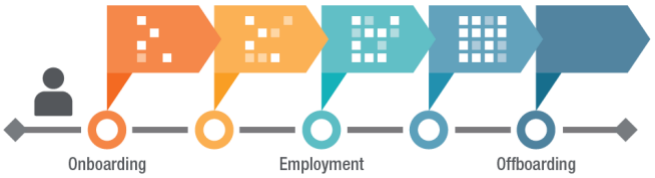

Fig. 2: Onboarding and offboarding now take place with often dizzying frequency, where workplace transitions—including changing roles in the company—pose special challenges for IT.

The lifecycle of a workspace can be divided into three phases:

- **Onboarding:** Occurs when an employee is first hired and receives their first digital workspace. It includes initial creation of the employee's identity as a consumer of digital resources.
- **Employment:** During this phase, the employee's role and responsibilities change over time, typically requiring corresponding changes in their resource requirements and authorizations.
- **Offboarding:** At this stage, all access rights should be terminated immediately. What's more, the ex-employee's identity as a potential consumer of digital resources should be disabled.

The following digital-workspace provisioning objectives are generally similar across this entire lifecycle:

- **Speed:** Employees become productive sooner, not later
- **Accuracy:** Security concerns dictate that employees only be given access to appropriate resources
- **Efficiency:** Because operational budgets and staff are limited
- **Agility:** Because business needs and digital resources are in constant flux
- **Scalability:** To accommodate future growth in employee count and digital resources
- **Accountability:** Because compliance requires auditability of who could access what at any given time
- **Self-service:** To empower employees and meet their workplace expectations

The question now is, how well can organizations meet these goals today—and how might they go about meeting them in a faster, easier, and lower-cost way?

Identify the Obstacle: Inadequate Process Automation

If employee workspace provisioning were automated sufficiently, someone somewhere could click the right button and ding! – a new employee would have the digital workspace they needed immediately. Or by the same token, a terminated employee's digital access rights would be removed.

Given that so many other business processes have been automated effectively, why haven't companies applied the same principles to digital onboarding, lifecycle re-provisioning, and offboarding?

Fig. 3: Multiple stakeholders make automating workspace provisioning a special challenge for IT.

These factors have typically delayed the effective automation of workspace provisioning at most organizations:

Factor 1: Multiple stakeholders

The automation "low-hanging fruit" at most companies has been business processes that center in a single department, such as sales, marketing, or finance. Employee workspaces present a somewhat more complex challenge because there are four sets of stakeholders involved.

All these stakeholders have an interest in the automation of workspace provisioning, but the differences in these

interests must be resolved and orchestrated properly so that automated workspace provisioning becomes a reality.

Human Resources owns the employee lifecycle from start to finish. It's responsible for overall workplace quality and compliance issues, of which digital workspace is a piece. Improved workspace provisioning will help HR fulfill its talent-retention goals—but, given its limited resources—HR can't afford to get involved in the day-to-day technical issues associated with authorizing employee access to a company's various applications, content, and services.

Line-of-Business managers supervise employees' work and are responsible for assigning roles and responsibilities. Improved workspace provisioning will help LOB managers fulfill their productivity objectives, but that provisioning must be flexible enough to meet their constantly changing needs—rather than having it impose counter-productive restrictions on their ability to give their people the needed resources.

Employees experience frustration when they can't access digital resources quickly. Improved workspace provisioning can eliminate this frustration and empower them to achieve, but it must provide a reasonably "consumer-like" self-service experience or they'll simply work around it, which can lead to compliance and security issues.

IT owns and operates the digital environment, which includes: 1) the digital resources themselves (or, in the case of cloud, the relationships with resource providers); 2) the network that connects employees to those resources; and 3) the access-control mechanisms that secure those resources. Improved workspace provisioning frees IT from many small but time-consuming tasks, while also helping it shed its "bad guy" image as the cause of aggravating delays. Yet it must retain appropriate control over allocation of the digital resources in order to maintain security and protect service levels.

Factor 2: Lack of a champion

Because workspace provisioning involves multiple stakeholders, it hasn't always been clear who should lead automation efforts. Obviously, IT and HR have an important role to play, but neither is typically able to fund a workspace initiative on its own. Individual LOB leaders may also view workspace provisioning as an enterprise-level issue to be driven from the C-suite, rather than their individual business units.

Workspace automation may also have failed to attract necessary champions/sponsors in the past because it was not viewed as a sufficiently strategic issue.

Alas, workspace automation initiatives can languish despite their tremendous potential for business value.

Factor 3: Inadequate technology

Even if stakeholders could agree on the appropriate champion, workspace automation may have been difficult to achieve in the past due to a lack of available technology solutions.

Virtual desktops provide a mechanism to deliver access to digital resources dynamically, but they lack business-driven policy controls. Identity management tools provide policy-based access controls, but don't balance their ability to deny unauthorized access with a corresponding ability to let employees know proactively about available services that they can access. Nor do identity management tools selectively deny access based on awareness of the employee's or contractor's current context—such as being outside a geo-fenced area or using an unsecure public WiFi connection.

Fortunately, companies' need to improve how they deliver digital resources to their employees—a need now perceived by IT, LOB managers, HR, and employees alike—has resulted in an emerging class of solutions designed specifically to meet this need.

Recognize the Solution: Policy-driven Digital Workspace Automation

Companies can automate the provisioning, re-provisioning, and de-provisioning of employees' digital workspaces in a variety of ways using a variety of technologies. But, at its core, any effective workspace automation solution must provide several core capabilities:

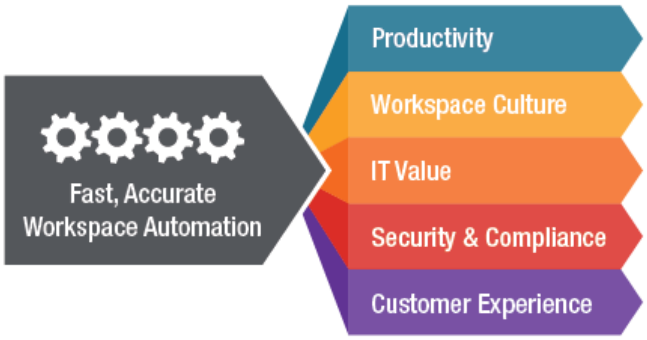

Fig. 4: Agile, digital workspace automation helps IT empower its workforce with speed and ease of use—while retaining the security and compliance critical to the organization.

Programmable automation fabric. Workspace automation requires an underlying operational capability to perform the necessary technical actions to activate or de-activate access to the applications, content, or services appropriate for any particular employee repeatedly, without requiring error-prone manual intervention. These actions can include account creation, password set and reset, creation of an appropriate virtual desktop on a VDI server, and/or creation of a VPN session. Ideally, a solution should also enable IT staff to define these provisioning-related actions for each resource.

Adaptive rules/policy engine. In addition to being able to activate or deactivate resource access, an effective workspace automation solution must be capable of performing those actions when, and only when, certain criteria are met. In some cases, those criteria will be defined by business rules—such as an employee getting promoted or a department contracting with an approved Software-as-a-Service (SaaS) provider. In other cases, those criteria will be defined by security and compliance policies—restrictions on remote access or recent excessive/anomalous utilization, for example.

Stakeholder-appropriate interfaces. Because there are multiple stakeholders in the digital workspace, an effective automation solution must provide them with functional interfaces appropriate to their needs. An authorized LOB manager desiring that team members use a particular application, for example, should be able to activate that resource for that team. Individual employees should likewise be able to self-serve from a menu of available resources.

Open integration. A workspace automation solution must integrate tightly with many other systems in the enterprise environment. These include:

- Hardware and software infrastructure management controls such as PC lifecycle management, mobile device management, etc.
- Identity and access management systems
- Virtual desktop infrastructure (VDI)
- HR systems
- Third-party cloud resources (SaaS, PaaS, IaaS, etc.)
- Security, mobility, and other management/monitoring systems

Every organization's IT and HR environments are different—and the enterprise technology landscape is in a constant state of flux. Therefore, the integration capabilities of a workspace automation solution should be sufficiently open and extensible to accommodate any third-party system that can help facilitate the delivery of the right digital workspace to the right employee at the right time.

Auditability and reporting. Compliance, security, and good governance require that both employee access and the actions of those managing employee access be fully auditable. In fact, an inherent advantage of unified, automated provisioning processes over disparate manual ones is this auditability. A truly enterprise-class workspace automation solution should provide full after-the-fact auditability, in addition to current-state reporting.

Workspace automation solutions can be differentiated in many ways—including ease of implementation, policy-control granularity, predictive vs. purely reactive provisioning, etc. But these five core attributes discussed above are essential for companies seeking to respond to the increased importance of digitally enabling their workers.

Realize the Benefits: Better People Doing Better Work with Security in Place

When employees are provisioned with the digital resources they need, when they need them—and with far less work from IT—lots of good things happen. These include:

Improved security and enhanced compliance. Automated workspace provisioning enables the revoking of digital privileges immediately upon termination. And making it easier for employees to access needed tools means they're less likely to resort to potentially non-secure workarounds.

And when it comes to enhanced compliance, such provisioning brings a new level of auditability to both employee-access histories and the past actions of those with employee-access management privileges. It also concretely demonstrates best-practices due diligence to regulators.

A more productive, engaged workplace culture. Every business leader knows that culture trumps strategy. A highly productive and engaged workforce therefore has strategic value when it comes to recruiting, retaining, and motivating talent.

Better allocation of IT staff time. IT spends a lot of time activating and de-activating resource access for employees with constantly changing needs. Much time is also spent on password resets and other services that could be handled via automated self-service. Re-allocating this time benefits companies looking to achieve more strategic technology objectives.

Greater business value from IT investments. Companies gain more value from their IT investments when those investments are deployed to more employees sooner. Also, most IT organizations currently spend a lot of time activating and de-activating resource access, resetting passwords, and other services that could be handled via automated self-service, freeing staff to accomplish more strategic technology objectives.

More effective leveraging of the non-employee workforce. Certain industries are marked by massive-scale seasonal transitions and many companies are making more use of contractors, freelancers, and other non-employee talent. However, leveraging digital resources to include these non-employees with employees in virtual teams is often difficult. Automated workspace provisioning empowers LOB managers to give non-employees access to team resources while ensuring that proper IT security safeguards are in place.

Superior customer experience. Every company must deliver superior customer experiences—or risk losing customers to competitors. Automated workspace management impacts customer experience by better equipping employees to respond to customers' needs in real time at any touchpoint.

The simple reality is that the digital nature of work, the need to optimize the engagement of Millennials, and the need to free IT from routine operational tasks make the automation of employees' digital workspaces essential. Ivanti's identity and access management solutions can help you secure workspaces, keep workers productive, and return more control to IT departments. With a quick time to value, you get up and running in days, not months or years.

Learn More

ivanti.com/contact

epg@ivanti.com