YouGov

# STATE OF OFFBOARDING PROCESS AUTOMATION

oomnitza

Given increased U.S. turnover rates and its inherent data privacy, security and financial risks, automating secure offboarding processes has become a strategic business imperative for modern enterprises.

# SUMMARY

Employee turnover has been increasing over the past few years — whether due to a pandemic-ignited "Great Resignation," the lure of hybrid and remote work or due to economic uncertainty — IT organizations have to contend with the complicated process of securely offboarding departing employees and contractors. The effort associated with offboarding has been compounded due to the ever-increasing, diverse and dynamic technology footprint of each user — endpoints including laptops, smartphones and field devices, access to an increasing number of SaaS applications, and hybrid and multi-cloud infrastructure.

The offboarding process involves coordination across multiple teams and tools — IT, security, finance, legal and HR among others. Accurate and complete technology offboarding of departing employees and contractors is a multifaceted endeavor including:  deprovisioning access, reclaiming endpoints, software licenses and cloud resources, reassigning workspaces and data objects for business continuity, ensuring compliance requirements such as legal hold, and decommissioning or reallocating technology assets.

Managing this complex process manually with the sole reliance on help desk tickets to request human actions is resource intensive and often is prone to errors.  This can lead to incomplete offboarding, exposing an organization to security, compliance, audit and financial risks.

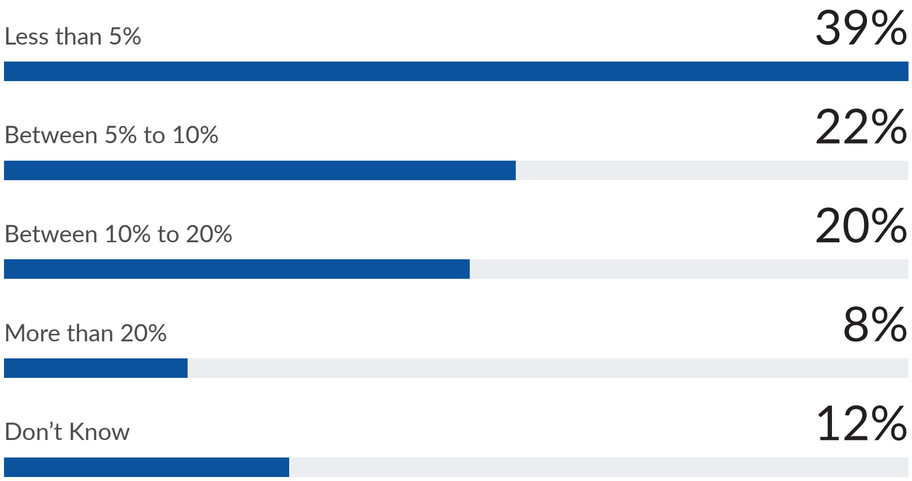
Given increased U.S. turnover rates and its inherent data privacy, security and financial risks, automating secure offboarding processes has become a strategic business imperative for modern enterprises.

2022 State of Offboarding Process Automation survey conducted by YouGov research examined how enterprises are managing the challenging process of offboarding, specifically looking at endpoint reclamation, SaaS and cloud resource deprovisioning, and how organizations are leveraging automated workflows to eliminate manual, mundane and error-prone tasks. The findings are based on a survey of 213 senior level information technology professionals in enterprises ranging from 1,000 to over 10,000 employees across multiple industries in the United States.

# ENDPOINT RECLAMATION

Reclaiming company issued endpoints and accessories is a vital step in offboarding workers due to security, audit and financial considerations. Corporate devices contain proprietary company or customer information, may be subject to legal hold and other data preservation requirements, and should be repurposed until their end of life.

To what extent has your organization experienced loss of IT assets / endpoints (e.g. laptops, computers, monitors, smartphones, storage) due to employees and contractors leaving your company with corporate-issued equipment?



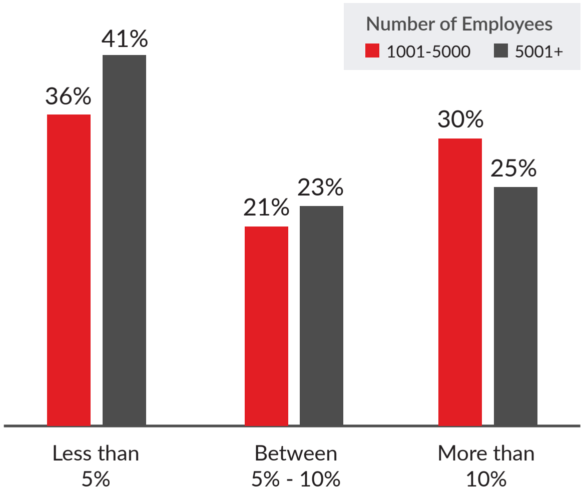
**49%**

of companies lost at least 5% of corporate-issued assets during employee offboarding

## Key Findings

- 49% of all respondents lost at least 5% of IT assets/ technology during offboarding which can be a substantial number of endpoints for large organizations.
- 27% of organizations lost at least 10% of assets which can have significant security and financial implications.
- Small and medium enterprises (under 5,000 employees) were 36% more likely to lose a significant number of assets (10% or higher) than large enterprises.
- Technology, healthcare and manufacturing organizations have poorer asset reclamation (> 36% report more than 10% loss) compared to other industries.

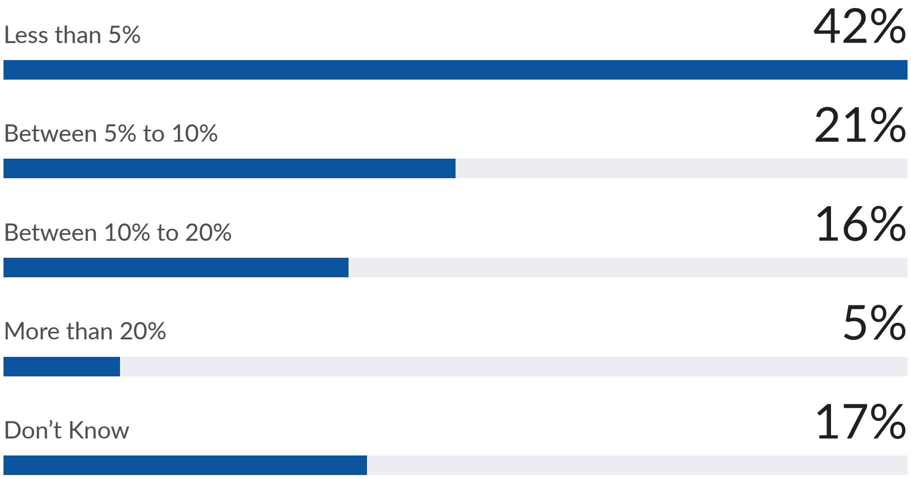
**IT Asset/Technology Loss**



# DEPROVISIONING ACCESS

With increasing SaaS and cloud adoption, revoking access to applications, network and cloud infrastructure, typically by modifying user status within identity access management (IAM) tools, within single sign-on (SSO) tools, or directly within the application or resource, is essential to prevent unauthorized access, data loss and security exposures.

To what extent has your organization experienced unauthorized access to SaaS applications and cloud infrastructure due to incomplete deprovisioning of employees and contractors that are no longer with your company?



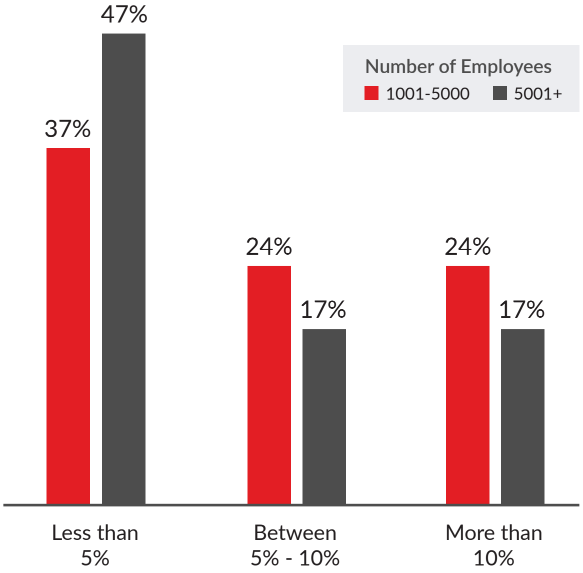
35%

of medium and large enterprises reported more than 5% instances of unauthorized access to SaaS and cloud resources after employees or contractors are no longer with the company

## Key Findings

- 21% of respondents experienced pronounced instances of unauthorized access (between 5%-10%) to applications and cloud resources after employees or contractors left the company.
- 21% of organizations reported significant instances of unauthorized access (above 10%) from departing workers.
- Small enterprises (1000-5000 employees) have 37% higher reported instances of unauthorized access to SaaS applications and cloud infrastructure (> 5% unauthorized access) compared to medium and large enterprises.
- Technology, healthcare and services have higher instances (roughly 50%) of unauthorized access post employee departure compared to others — suggesting either lower maturity of deprovisioning processes or higher awareness of access exposures.
- Results indicate that organizations have a lot more work to do in accurately and completely deprovisioning departing employees. Former workers that have access to a single system can lead to operational, data privacy, and security issues.

**Unauthorized Access Instances**



# PROCESS AUTOMATION MATURITY

Given increased workforce turnover rates, IT and HR teams must progress their current onboarding and offboarding process automation capabilities, from separation to recovery, to ensure user experience that scales while reducing financial and security exposures.

## How confident do you feel that your organization implemented process automation workflow system(s) coordinated between departments (such as HR, IT, security and procurement) and across IT management tools to streamline onboarding and secure offboarding of employees and contractors?

**Very confident.** We have well-coordinated processes and tools. Deprovisioning and reclamation actions are fully tracked, audited, and improved. 47%

**Somewhat confident.** The majority of defined processes and tool integration work well. There is room for improvement as deprovisioning and reclamation issues are experienced periodically. 44%

Not very confident. We have ad hoc coordination between departments and only some processes are automated. The organization experiences equipment loss and unauthorized access issues. 3%

**Not confident at all.** We have little to no coordination between departments. Most processes are manual and nominally tracked. The organization frequently experiences equipment loss and unauthorized access issues. 1%

Don't Know 5%

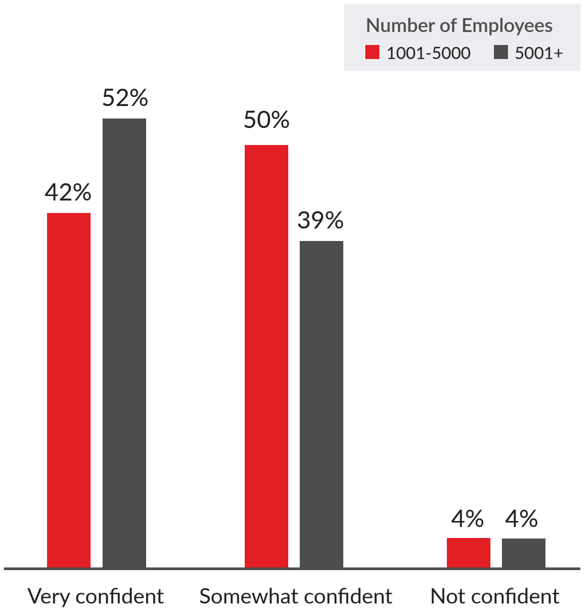
48%

of respondents expressed doubt about the process automation workflows implemented within their organization to streamline onboarding and secure offboarding

## Key Findings

- 48% of respondents were somewhat to not confident (expressed doubt) about the process automation workflows implemented within their organization to streamline onboarding and secure offboarding — indicating issues, deficiencies and room for improvement.
- 47% of respondents expressed high confidence in their organization's use of automated workflows, across departments and IT tools, to streamline onboarding and offboarding processes. This is somewhat at odds with lower efficacy of endpoint reclamation and access deprovisioning reported in the survey — indicating either over-confidence and/or the need to further optimize process automation capabilities.
- The largest organizations (more than 5,000 employees) seem more confident in their companies' use of automated workflows, irrespective of whether they are continuously optimized and updated.
- Retail and technology expressed lower overall confidence (> 60%) towards their onboarding and offboarding automation capabilities.

**Onboarding and Offboarding Automation Confidence**



# Research Methodology

The survey was conducted online and data compiled in September 2022 by YouGov plc, an international research data and analytics group. The independent research surveyed 213 senior level information technology professionals from companies of more than 1,000 employees across a diverse set of industries within the United States.

YouGov is an international online research data and analytics technology group with a mission is to offer unparalleled insight into what the world thinks. As the pioneer of online market research, we have a strong record for data accuracy, a wide range of quantitative and qualitative research, and innovation. With a proprietary panel of over 22 million registered members globally, YouGov has one of the world's largest research networks.

Oomnitza offers the industry's most versatile Enterprise Technology Management platform that delivers key business process automation for IT.

Our SaaS solution, featuring agentless integrations, best practices and low-code workflows, enables enterprises to quickly achieve operational, security and financial efficiency leveraging their existing endpoint, application, network infrastructure and cloud infrastructure systems.

We help some of the most well-known and innovative companies to optimize resources, mitigate cyber risk, expedite audits and fortify digital experience. Learn more at Oomnitza.com.