omnitza

Secure Offboarding Process Automation and Enterprise Technology Management

From Separation to Reclamation

One thing that's constant in our world is change. Increased hybrid and remote workforce, the great resignation and current economic uncertainty have created unprecedented employee turnover. Beyond the business impact, IT and security teams require a more streamlined and effective approach to remove exiting employee and contractor access to applications, cloud resources and sensitive information, as well as to warrant that respective endpoints, software and other assets are appropriately reclaimed, imaged, disposed or repurposed. Given the volume of turnover and the scope of technology, how can organizations ensure offboarding process operational and security efficacy? More so, what are the underlying challenges, considerations and best practices when it comes to secure offboarding process automation.

Trends Driving Need for Offboarding Automation

Offboarding is a crucial business process that has security implications and is often fraught with difficulties. There are several factors driving increased turnover in the near term. The increase of a hybrid workforce was massive during the pandemic — it continues and will continue. In a recent study, 64% of companies have a majority of remote workers, and 53% of organizations stated that their remote workers are deviating from set security policies.[1] As workers want to get their jobs done, sometimes they circumvent security policies. Supporting remote workers and security policies are paramount but enforcing policies can be tricky depending on the breadth of internal, industry and regulated policies that organizations must satisfy.

Beyond increased remote workers, we also have an expanding attack surface to contend with. The acceleration of multi-cloud is not slowing. An ESG survey revealed that 88% of organizations are deploying applications and workloads in the public cloud, in addition to private cloud and network infrastructure.[2] When it comes to applications, another study represented that the average enterprise uses 187 different applications.[3] Chances are, if you did an assessment of SaaS use at your organization, you would not only find known applications, but an array of unknown or unaccounted for SaaS applications.

Becoming evident during the pandemic, the great resignation trend has spurred increased turnover. In 2021, organizations experienced an average 47% turnover.[4] With current economic conditions the way they are today, we are already seeing hiring freezes and reduction in force notices. Another study indicates that 51% of employers expect job cuts and 40% of workers plan to quit their job.[5] While this is also fueling offboarding demands on IT, all the above statistics also point to the need for IT to scale. This is about efficiency and auditability in offboarding. But let's examine the situation more closely to determine how organizations can address this situation.

Offboarding Automation Factors and Challenges

In many respects, this is about the fundamentals. It gets back to the popularized quote from famous management consultant and author Peter Drucker — "you can't manage what you can't measure." Organizations need to have the visibility and details of users, assets and entitlements. This asset and operational intelligence of course has regulatory and industry compliance implications such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS). As a best practice, it is specified in numerous frameworks including NIST Cyber Security Framework (CSF) and Center for Internet Security (CIS) Critical Security Controls. These controls involve asset discovery, inventory data and operational insight, such as what users are doing, what assets have deviated from set configurations and what roles have what type of access to what applications and resources. This information is vital to manage departing employees, and it's what we are asking our IT and security staff to leverage to ensure effective offboarding.

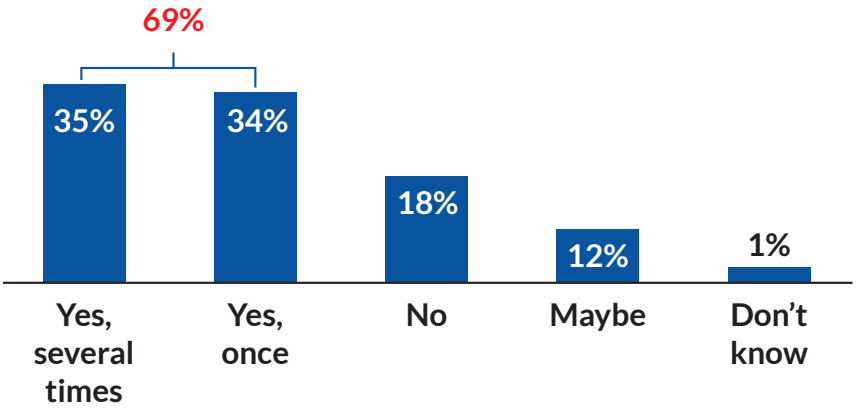

Figure 1: Lax Asset Management Risks

The research finds that offboarding, which relies on having consolidated and accurate user and asset information, isn't so easy. Incomplete offboarding, including means to securely manage assets, has serious implications. ESG research found that 69% of organizations have had an incident due to unmanaged, poorly managed, or unknown assets.[6] Threat actors are constantly scanning to exploit these types of vulnerabilities. If organizations are unaware about the assets, access or identity exposures — including those exposed due to insufficient offboarding — they become vulnerable to cyber-attacks. For example, a former employee from Block (formerly Square) downloaded customer reports containing 8.2 million names and brokerage account details, and an ex-employee of Amazon Web Services hacked into Capital One systems through a misconfigured firewall and stole personal data of 100 million people. Beyond regulatory compliance violation risks and fines, the data breaches do have significant investigation costs. Enterprises that experienced these types of attacks have been connected to offboarding deficiencies.

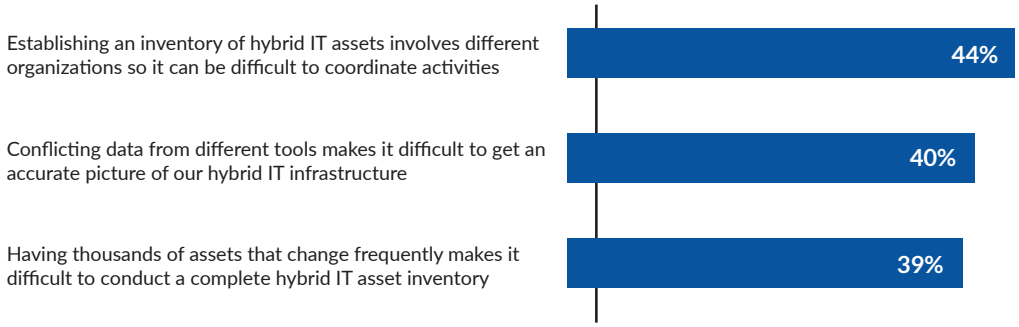

Figure 2: Top 3 Asset Inventory Challenges

The foundational element here is asset inventory and intelligence, and it remains a challenge for most enterprises. Knowing what assets exist, what the conditions of those assets, who owns them is required to start to automate business processes. ESG research explains some of the challenges. 44% of enterprises surveyed expressed difficulty in establishing hybrid IT asset inventory which involves coordinating activities across different organizations such as IT, security and business units, to attempt to get an accurate inventory. 40% expressed having conflicting data from different tools also makes it difficult to get an accurate inventory.[7] In many cases, organizations have some of the data, but do not know if it's correct. What do staff do if there are conflicts in the data — it has to be normalized. Someone must figure out what is accurate and how to structure it. This takes time and resources. In addition, 39% expressed having thousands of assets that frequently change, adding to the difficulties of completing an inventory.[8] With regards to a growing attack surface, it is not unusual for a large enterprise to have thousands of assets and some banks over a million — that are always changing due to business activities and moving employees and contractors.

Asset Intelligence and Offboarding

How are organization's keeping pace with asset inventory and user dynamics? That is a huge challenge. ESG research asked organizations how many systems are used to track IT assets. 32% expressed that they connect to at least 16 or more different databases, systems and tools.[9] This requires being granted access to these systems, obtaining the data and addressing integrity issues — just to attempt to get an accurate inventory. According to our research, the top data sources include asset management systems, endpoint management and security tools, cloud security posture management and network scanning tools. Again, this is very time and resource intensive. Some enterprises utilize multiple CMDBs and assemble various asset management tools, but there typically is no one central source. Most enterprises have several sources that might conflict with each other or may not be regularly updated.

The implications for both security posture risks and offboarding risks are numerous. Which endpoints have vulnerabilities, inactive defenses, or have defenses that have not been maintained. What portfolio of applications are installed or being accessed in the cloud. With the pervasive use of cloud computing, when and where are new instances of cloud workloads being spun up. Who owns them? What changes were made — are they correctly configured or vulnerable to being scanned. The same is true for private cloud and network resources. Despite the scope of inventory sources and variety of data points, most organizations still rely on more manual processes to aggregate and manage this information — research indicated that 73% are still relying on spreadsheets for analysis. The majority of survey respondents indicated that it takes more than 80 person hours just to gather and analyze the data. This asset inventory process remains an inefficient, point-in-time data collection and analysis problem.

The issue still reflects the Peter Drucker quote of "you can't manage what you can't measure." Applied to offboarding processes, it is challenging to offboard users effectively if an organization does not know a person's role, department and location, what systems and application they have access to, and what devices are in possession, as well as an understanding of their work behavior and if there are deviations from normal activity. For effective offboarding, these are the basic questions that the organization must know. For example, does the organization have an accurate inventory of all users and contractors who are access systems, applications and cloud resources and related entitlements. It is this matrix of data that organizations use to apply a policy (guidelines to be met) that drive the processes (actions to be taken) and procedures (detailed steps that comprise the action) — these three elements serve as the basis for automation.

Offboarding Considerations and Enterprise Technology Management

Key Secure Automated Offboarding Process Considerations

1. Does the organization have an accurate inventory of all users (including contractors), assets and entitlements?
2. Does the organization have a full understanding of ALL processes and procedures used for various offboarding scenarios?
3. Can the organization automate offboarding processes across all separation conditions, roles, technologies and data – and can successfully completed tasks be validated for audit purposes?
4. Can offboarding status be communicated to HR, IT, finance, procurement, facilities, etc. and how are these systems coordinated to ensure complete and effective offboarding?
5. Can the business quantify the cost-benefit (saved time, recouped licenses, reallocated devices)?

Does the organization have a full understanding of the processes and procedures used for various offboarding scenarios, including someone quitting or getting fired, or possibly laying off a group of employees or terminating contractors. Secure offboarding process automation needs to encompass all the conditions, roles, technologies and data to ensure successful completion. This would include having validation data for audit purposes to support IT, HR and financial purposes as well as to satisfy regulatory compliance concerns. Beyond communication by email or via ticketing system to various staff members and departments, can the organization ensure that the applications, used by different departments to manage different systems, be connected in a way to ensure offboarding completion — crucial to enable offboarding efficiency and scale. Lastly, can the business quantify the cost benefit and risk mitigation benefits of secure automated offboarding, especially given the data on increased hybrid workforce and expected turnover. Answers to these questions are important for IT and security leads to address to enable secure automated offboarding.

Once these questions are addressed, IT and security professionals can further apply best practices for offboarding process automation. Organizations should examine how to better orchestrate the use of data and actions that can be taken through their IT management tools including endpoint management, H.R. management, endpoint management, identity management and network infrastructure and cloud management systems. Organizations can also consider interfacing with their financial management systems, procurement systems and even third-party systems that comprise their supply chain. These disparate systems, where an enterprises most current user, asset and operational state data exists, is the foundation for an Enterprise Technology Management framework, where the data can be systematically aggregated and correlated — resulting in the context needed to monitor and manage technology, as well as build workflows that effectuate secure automated offboarding. ETM offers a system of record for enterprise technology management and action.

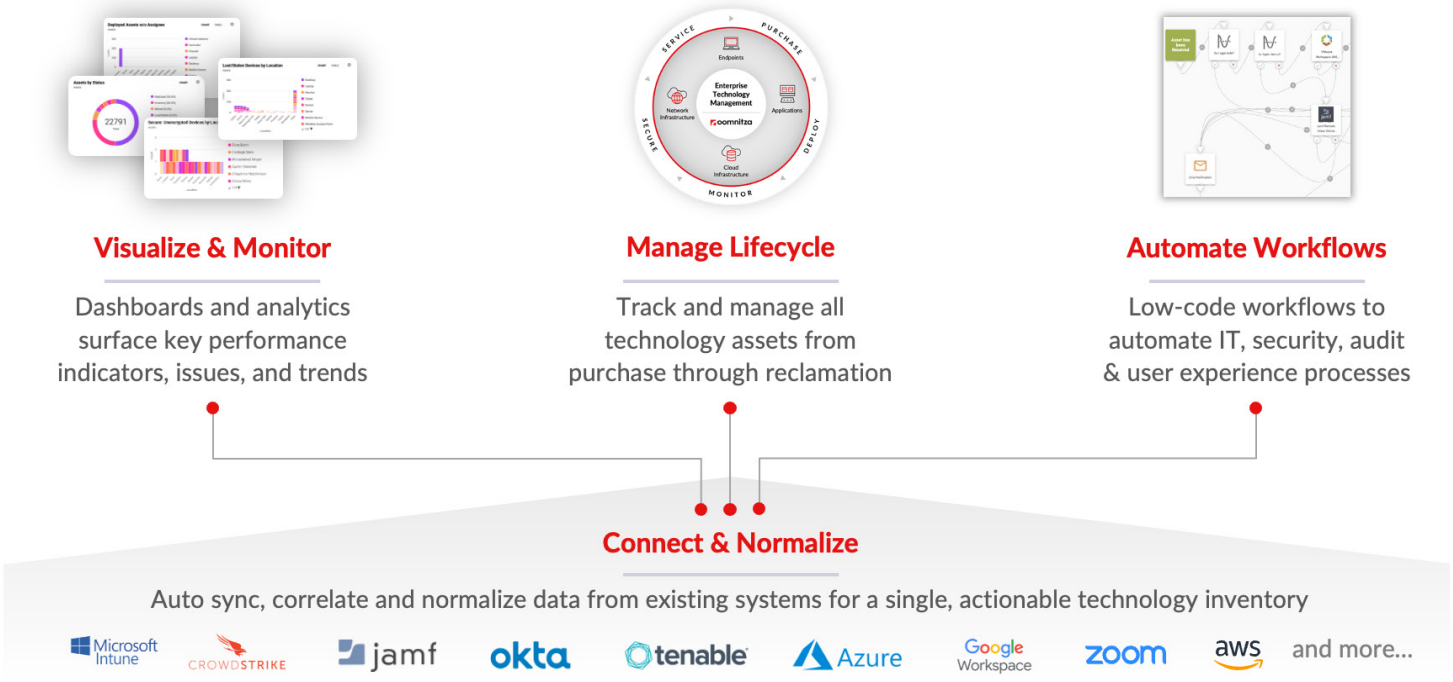

Figure 3: Enterprise Technology Management Framework

End to End Offboarding Process Automation

The objectives for an automated secure offboarding are to continuously improve process efficiency and to eliminate the blind spots that introduce operational and security risks. This would cover steps to aggregate, cross-correlate, report and monitor inventory, create workflows that connect related systems and inform inter-departmental staff, disable access to systems and resources, reclaim devices, work product and licenses and enable process tracking and verification for auditing purposes. As depicted below, the offboarding process, from Separation to Recovery, is comprised of four parts: separation, deprovisioning, reassigning and recovery.

Figure 4: Security Offboarding Process: From Separation to Recovery

Separate. As we are referring to managing the departure of employees and contractors, an ETM platform would integrate user information from Identity Access Management (IAM) systems by obtaining and consolidating user, role and entitlement data among existing directory services, identity platforms, single sign-on (SSO) and other tools managing access to applications and resources. In addition, the ETM platform would integrate with IT tools at the API-level across the enterprise, from endpoints and applications to network and cloud infrastructure. The Separation process may start with an employee/contractor status being changed from active to pending termination with a term date for example in a Human Resources Management System (HRMS). As discovered by an ETM platform, the status change would initiate a set of internal workstreams. This would include the people elements of creating a manifest for endpoints and accessories to be returned with ETM notification to the manager, the employee/contractor and IT. The ETM platform could also send notifications to HR, finance and other stakeholders, while logging verifications and even sending a process ticket update to the service desk.

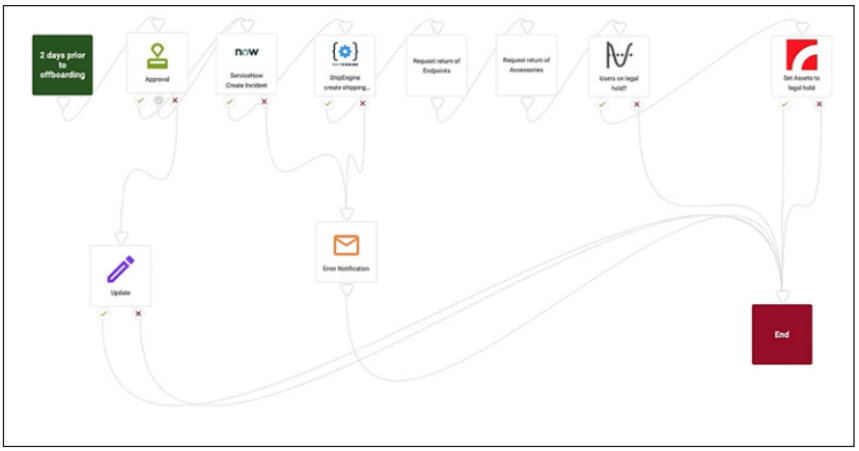

Figure 5: Security Offboarding Process: Separate

Deprovision. The next step in the offboarding process is to revoke access to systems, applications and resources across on-premises, SaaS and multi-cloud — very often initiated on the day of termination. This may include the ETM platform invoking system, endpoint and security management tools to activate endpoint agents to terminate browser sessions and even lock up the endpoint from access. ETM would connect to IAM and SSO systems to deactivate the user from access to SaaS-based applications. This would also include invoking revoking user access rights to management applications and cloud resources that may be outside the purview of SSO.

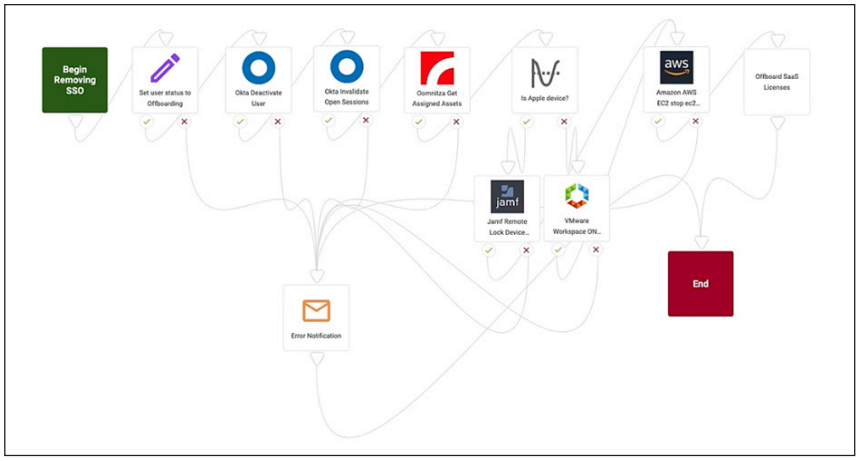

Figure 6: Security Offboarding Process: Deprovision

Reassignment. This important next step following deprovisioning focuses on continuity. The ETM platform can be integrated with a variety of SaaS applications and cloud management systems to reassign ownership of documents, data and access from the terminated user to other pre-designated users such as their manager. For example, the ETM system can leverage API calls to the respective application to transfer Google workspace or Asana ownership, change cloud resource owner association, set up mail forwarding and auto replies, delete recurring calendar invitations and more. As illustrated below, this key step ensures that the data and business conducted across the multitude of SaaS applications and resources that a user has access to is preserved and appropriately reassigned.

Figure 7: Security Offboarding Process: Reassignment

Recover. This is the last step in the automated offboarding process whereby endpoints, software licenses and cloud resource and infrastructure licenses are recovered, repurposed or end of life. The ETM platform can connect to service depots and shipping services, such as FedEx web services ShipAPI, to facility delivery of boxes with return labels to the departing user, as well as to enable the corporate IT service stockroom team to track those return packages of endpoints and accessories in transit and received. Advanced requirements for those systems that need to be on legal hold or have their data archived can also be tracked by the ETM platform and verified by IT staff or interfacing with respective archive systems. Desktop application seats, SaaS software and cloud resource licenses can also be recovered and reassigned back into their respective licensing pool.

Figure 8: Secure Offboarding Process Automation: Recover

Decommission. An ETM platform streamlines asset lifecycle management and reduces waste or redundant expenditures by repurposing of devices and licenses for greater financial efficiency. Prior to or as endpoints and accessories are returned, the ETM can invoke data wiping through the system management tool for those endpoints that are not on legal hold. The ETM system can receive confirmation of sanitization and then can facilitate endpoint reallocation and decommission decisions by assessing their remaining warranty or assigned useful life. A workflow block rule can determine if that endpoint should be redeployed (added to the inventory pool), recycled, or destroyed. Depending on the extent of process requisites, the ETM platform can even track assignment to destruction or recycling services, certificates of destruction, and updating of Fixed Asset Management (FAM) to adjust the residual value of assets at their end-of-life (EOL).

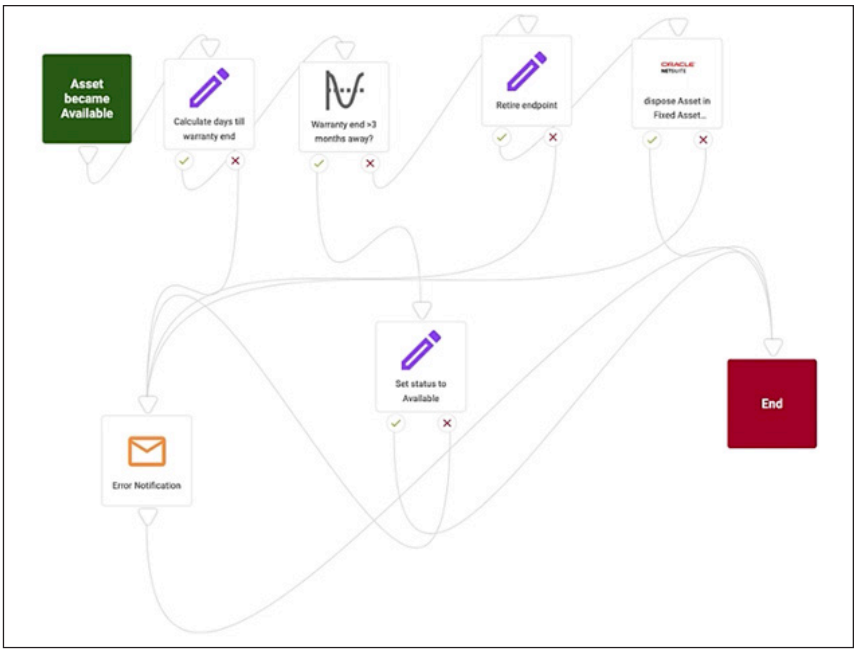

Figure 9: Secure Offboarding Process Automation: Decommission

Enterprise Technology Management solutions provide the system of record and action for unified asset/technology intelligence, lifecycle management and process automation across an organization's IT estate that enables IT, HR and security teams to achieve offboarding efficacy with greater operational and cost efficiency, policy compliance and risk mitigation.

1 Cybersecurity Insiders, 2022 Attack Surface Management report
2 ESG, Cloud Native Applications report, May 2022
3 Okta, Businesses at Work 2022 Report
4 PwC Pulse Survey: Managing Business Risks, Aug 2022
5 2022 McKinsey Great Attrition Report
6-9 ESG, Security Hygiene and Posture Management N=398

About Oomnitza

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.

oomnitza

Schedule a solution demo to see what powerful Enterprise Technology Management can do for you.
oomnitza.com /request-a-demo