SECURE ONBOARDING & OFFBOARDING FOR EMPLOYEES & CONTRACTORS IN THE CLOUD

One of the most fundamental challenges of securing the identity-defined perimeter is the ability to easily manage and secure the cloud identity lifecycle. This priority comes into sharpest focus with offboarding users, or more accurately, the failure of so many organizations to revoke standing access privileges to DevOps environments and other sensitive IT resources.

Companies today use hundreds or thousands of cloud services, and a typical DevSecOps operation can easily generate thousands of data access events every day. The result is that each human and machine user ends up having multiple identities and standing privilege sets sitting vulnerable to exploitation. If those privileges are not revoked or expired when an employee or contractor leaves the organization, that massive threat surface remains in place indefinitely.

The most effective way to manage the identity lifecycle is through the maintenance of least privilege access (LPA) and zero-standing privileges (ZSP) for those users while they are working in the cloud. Likewise, with the complete removal of accounts and access when terminated employees and contractors leave the organization. These offboarding steps are especially critical in today's dynamic work environment, with employees and contractors frequently joining and leaving your organization.

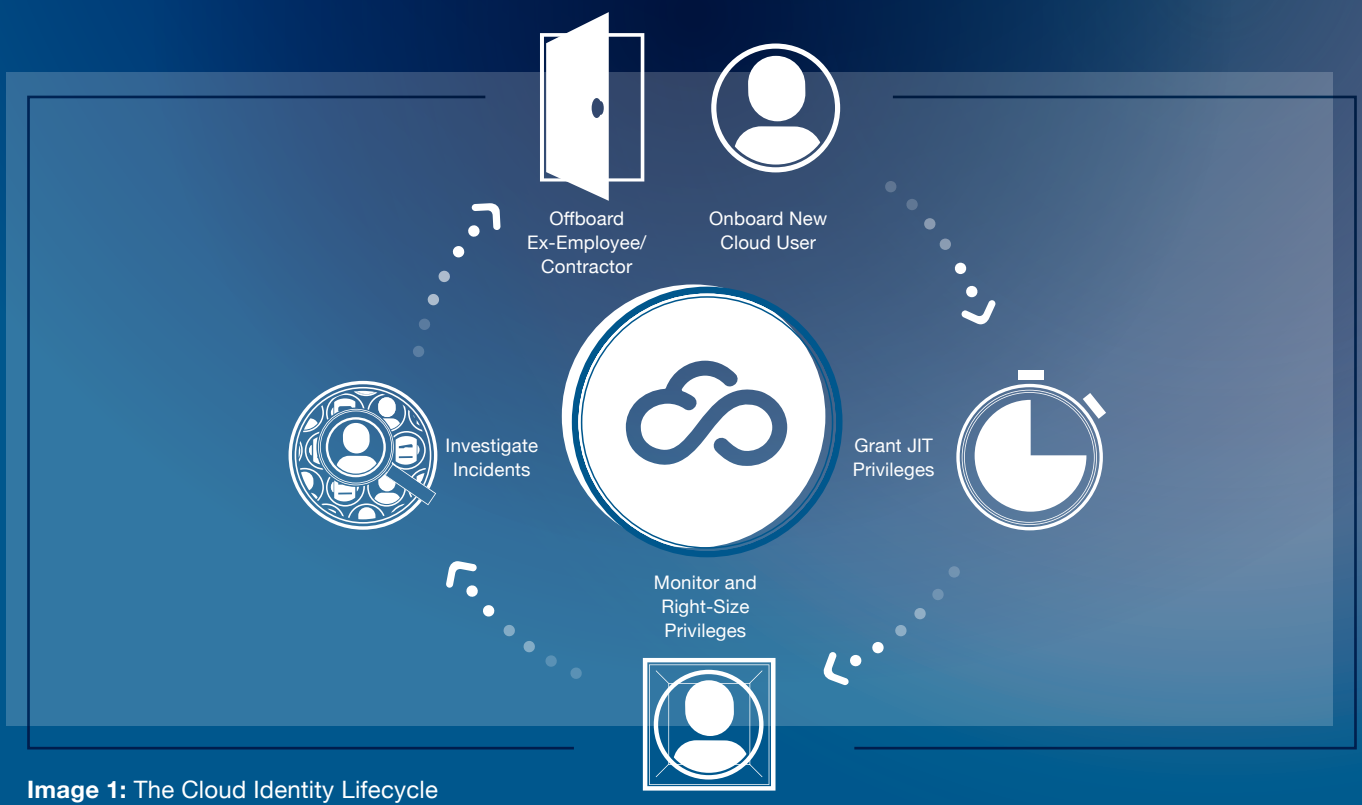

Image 1: The Cloud Identity Lifecycle

AUTOMATED ONBOARDING WITH BRITIVE

With the Britive Dynamic Permissioning Platform, you can quickly and easily grant role based-dynamic access control (RBAC) to new users, manage their permissions while they are working for your organization, and quickly and completely offboard them when they leave. You can use the Britive Platform on a standalone basis, or integrate it via API with your organization's existing identity governance and administration (IGA) systems (e.g., Sailpoint), identity directory (e.g., Azure AD, Okta), or human resources management system (e.g., Workday) that houses employee identities.

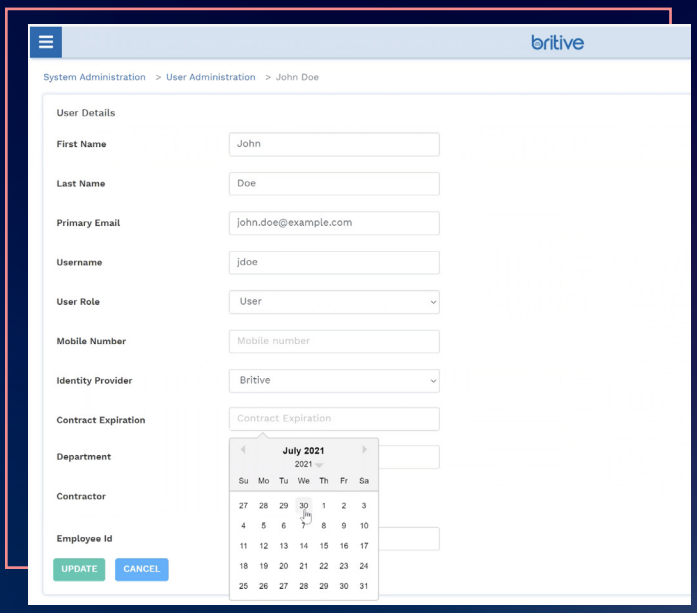

Image 2: Britive provides complete control over privileges tied to identities.

In essence, Britive becomes your integrated directory for managing employee access privileges. You can define attributes by job role—for instance, full-time employee, contractor, senior executive—that will define exactly what kind of access privileges are granted, how long those privileges will last, and most importantly: exactly when authorizations will expire.

FOR CONTRACT EMPLOYEES OR FOR INTERNAL EMPLOYEES ASSIGNED TO A GIVEN PROJECT, ACCESS RIGHTS CAN BE TIED TO THE LENGTH OF THE CONTRACT OR PROJECT

OFFBOARDING USERS UPON TERMINATION

When an employee or contractor leaves your organization, Britive ensures that all access to operation-critical cloud services such as AWS gets terminated. This includes expiring API keys, tokens, and secrets that are stored in frequented cloud repositories, i.e., command line credential files stored locally on desktops. For instance, you can manually remove a user from their RBAC group to automatically terminate their access to their Britive access profiles, effectively revoking their access to the associated cloud services. Additionally, for contract employees or for internal employees assigned to a given project, access rights can be tied to the length of the contract or project.

In the example right, the expiration of a contractor's privileges is set to coincide with the end of the contract.

Enforcing least privilege access through automated privileged revocation is the most effective way to secure and govern the cloud identity lifecycle. Britive makes it easy for you to right-size privileges, eliminate over-privileged accounts, and minimize your attack surface.

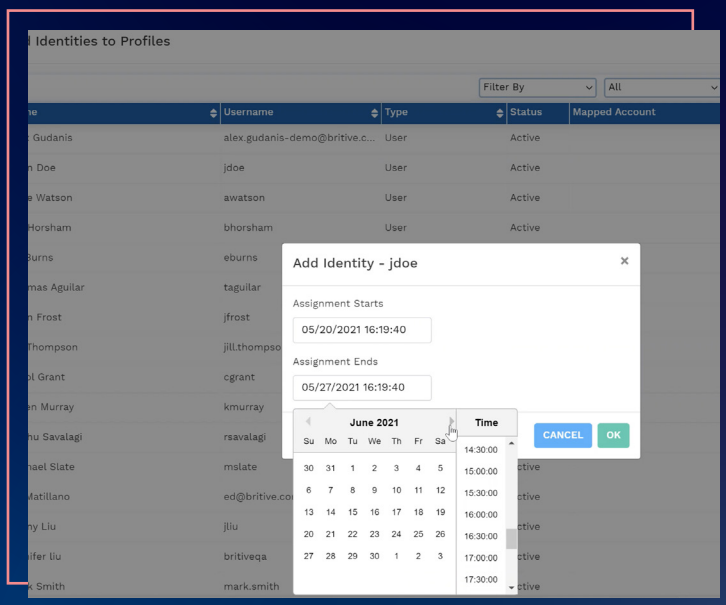

Image 3: Tying privileges to the scheduled term of a contractor's project means administrators no longer need to manually audit and rescind access rights—it happens automatically. This saves valuable time and eliminates the risk of manual errors.

britive

ABOUT BRITIVE

Britive (www.britive.com) is a cloud-native security solution built for the most demanding cloud-forward enterprises. The Britive platform empowers teams across cloud infrastructure, DevOps, and security functions with dynamic and intelligent privileged access administration solutions for multi-cloud environments.

The Britive platform helps organizations implement cloud security best practices like just-in-time (JIT) access and zero standing privileges (ZSP) to prevent security breaches and operational disruptions, while increasing efficiency and user productivity.