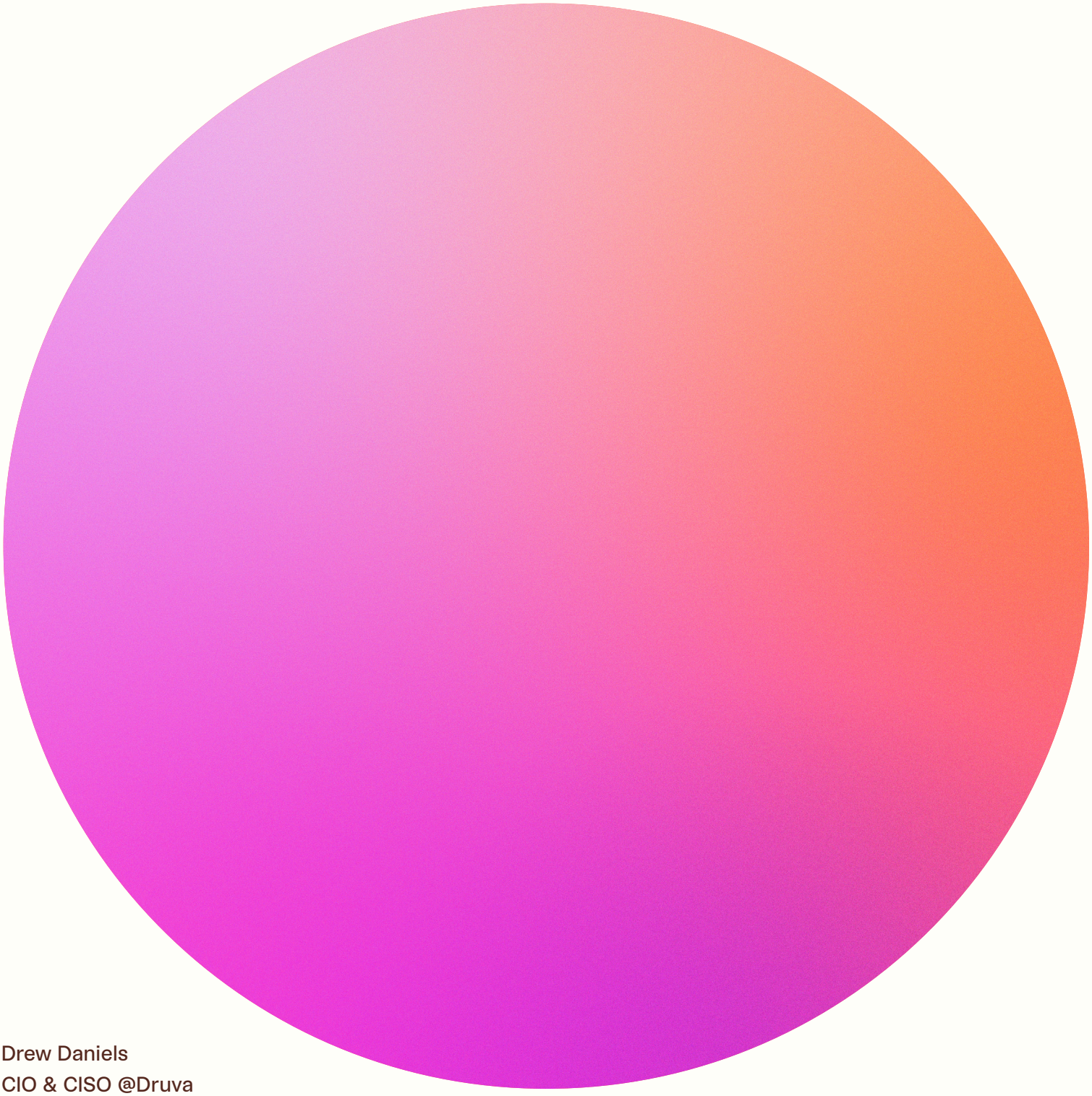
A CIO's Guide to Self-Service & RBAC

Guide
April 2022
Lumos.com

The Death of the IT Ticket

By Drew Daniels, CIO & CISO @Druva



Drew Daniels
CIO & CISO @Druva

Introduction

Companies are taking advantage of specialized SaaS apps to enable employees to better do their jobs. But that convenience comes at a price. More apps plus more employees equals more compliance concerns for CIOs and more work for IT teams. In an attempt to automate on-/offboarding, companies are implementing Role-Based-Access-Control (RBAC) to assign and unassign apps based on a person's role. However, RBAC only solves part of the problem.

Employee responsibilities can change quickly, and duties don't always align with predefined RBAC roles. Even when RBAC is used with workflow automation tools, such as BetterCloud or Okta, under or overprovisioning happens. The result? Employees submit IT tickets to request app access. And IT teams are wasting cycles on tasks that can be automated, and handled much more quickly. Leading to better customer service outcomes and even better employee satisfaction (both with employees and the internal IT staff).

Eliminating IT tickets is possible, and it crucially involves structured self-service. By enhancing RBAC with a self-service portal (with roles, rules and workflow), IT and IAM teams can automate the on and offboarding process, ensure security and compliance, and kill the IT ticket.

Welcome to the APPocalypse

As a CIO, I know firsthand about the kind of pressure we're under. Employees want access to the tools they need asap. However, our IT team needs to maintain compliance at the same time. With employees located around the globe, cybersecurity and compliance are critical to ensure data is protected and audit practices are in place. At the same time, the pandemic made hybrid or remote work standard, which propelled remote enablement to the top of the priority list. IT must keep companies compliant and secure while setting employees up for success, regardless of location.

To give employees the tools they need, companies are adopting SaaS apps at a breakneck speed. Lumos research shows that companies with > 500 employees use anywhere from 600 to 1,000 SaaS apps. And that number continues to grow. On average, Okta customers have deployed 22% [1] more apps over the past four years. From Dropbox to Zoom, users can easily sign up for apps for free or with the swipe of a credit card. It has created an APPocalypse

67%

The number of developer companies offering a free plan or trial–making apps more accessible than ever [2]

While this plethora of apps enable employees to be better and faster, IT is stuck managing this complex SaaS-based web. From onboarding to offboarding, every new app request, multi-factor authentication reset, and access recertification fires off a new IT ticket. And every task needs documentation to ensure compliance. The larger a company grows, the harder managing tickets becomes. While IT works, employees wait.

[1] https://www.okta.com/businesses-at-work/2021/

[2] https://openviewpartners.com/2021-product-benchmarks/#.YhQylBNufdo

Is RBAC the Answer? Not Quite.

Decreasing IT tickets hinges on auto-assigning apps for employees that join, change teams, or leave the company. And automation starts with role-based access control (RBAC). For example, a new sales rep will be assigned a "sales" role when hired. That sales role enables access to tools, such as Salesforce. Or, a marketer moves from product marketing to demand generation, and the new role automatically grants access to Marketo. RBAC simplifies onboarding, offboarding, and everything in between.

Sadly, RBAC alone won't mitigate IT ticket volume. Even with workflow automation and provisioning tools like Okta or BetterCloud, Lumos research shows that 25% of all IT tickets are requests for access. In cross-functional teams, employees quickly outgrow the standardized roles defined by RBAC. So they submit IT tickets.

However, RBAC also results in overprovisioning. Employees keep access to tools or permissions long after they stop using the app, creating security issues. Segment's security team compared their employees' access to usage over a 30-day period and found that a whopping 60% [3] of access wasn't being used. Why? Because they don't have the bandwidth to weed through permissions.

The bottom line? RBAC is hard. Just ask any IT leader: "Have you ever had success in eliminating access request tickets or over provisioning with RBAC?" Building groups in an SSO provider takes time, but maintaining those groups is even more of a pain. Today's permissions are outdated tomorrow, and making IT maintain roles for 200 (or more!) apps in today's APPocalypse simply doesn't scale.

[3] https://www.okta.com/businesses-at-work/2021/

Behold: Self-Service

Decreasing – and ultimately eliminating – IT tickets requires the holy grail of efficiency: self-service access requests. Think about your iPhone. Your phone comes with a number of pre-installed apps based on your country, which is the consumer version of RBAC. However, you usually go straight to the AppStore to download more apps yourself. No Apple support ticket required.

Apple's self-service model is now everywhere. Supermarkets have self-checkout and AirBnB eliminated the need for travel agencies with a simple website that allows you to book your own place to stay.

Let's adapt this model for employees. When employees can solve IT-related problems on their own, IT tickets dwindle. With self service, your IT team can make employees more productive and companies more compliant at the same time.

Companies need both RBAC and self-service to manage the APPocalypse. But which comes first to make employees more successful? You can't just rely on your iPhone's default apps to get what you need, so RBAC first isn't the answer. However, you can turn a blank iPhone into a custom solution with a self-service AppStore. Modern IT teams start with self-service first, learn which apps are most requested, and then add RBAC for the most common apps.

The Self-Service Startup Guide

Automating provisioning through IT self-service is possible. Self-service and role-based access control (RBAC) will not only kill the access request ticket, it will increase both security and compliance. Here's how to get started.

01. Find the Apps

Self-service starts with app awareness. Employees often use non-approved apps, and it's up to IT to find them. From Dropbox to Notion, Clockwise to Postman, IT teams must gather a list of apps – sanctioned or not. Tools like Google OAuth [4] and Lumos can audit app usage and uncover which apps are hiding in the background.

02. Centralize Requests

A company AppStore is a centralized channel that allows employees to request apps, permissions, internal tools, or even developer resources without IT help. But first, IT teams must pick which apps are on the AppStore. Once defined, the AppStore becomes a one-stop-shop for all approved apps. You can start defining your AppStore within a Confluence page or Lumos.

03. Create Approval Workflows

Once the AppStore is in place, IT teams must decide who can approve requests for apps. This creates clarity whether to notify a manager or app admin for an access request. You can either define approvers on a central Confluence page and, then, let employees request apps through your ITSM. Or, you can use Lumos to make approvers accept or reject requests through Slack, auto-create the requested access and log everything for compliance purposes. No IT ticket needed.

04. Define Visibility

In an advanced self-service tool like Lumos, IT can set which roles should see which apps. For example, only sales needs to be able to request a sales tool like Outreach. Role-based visibility removes the clutter – and ticket requests.

[4] https://support.google.com/a/answer/6124308?hl=en

05. Pick Direct App Assignment or Group-Based Assignment

With most SSO providers [5], you can assign the user directly to the app or assign them to a group that adds them to the right app. For example, you can either assign the salesperson to Salesforce or assign them to the group "Salesforce_Admin" within your SSO provider, which then assigns the person to the right group within Salesforce. Make it clear for which apps IT should assign users to apps directly or via groups.

06. Focus on Compliance

IT must define the audit process for access requests in the event of an auditor request. You can use an ITSM for this. Or, a self-service app like Lumos that creates an audit log plus – if wanted – opens and closes an IT ticket within your ITSM for the access request.

07. Educate the User

A central onboarding hub, or knowledge base, can arm employees and approvers with the tools they need to use the AppStore. Lumos, for example, has a Slack-native app that makes it easy for employees to request apps where they spend most of their time.

[5] https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-migrate-users#an-example

About The Author

Drew Daniels is an experienced information technology & security executive and current Chief Information Officer & Chief Information Security Officer at Druva. Drew has led Information Technology, System/Network Operations, Engineering, Business Intelligence, and Security and continues to be closely aligned and current in those areas.

Drew believes that decisions should be factual and data-driven where possible. Drew has led hundreds of projects and programs over the years including cloud migrations, complex IT Operations revamp and refresh programs, multiple ISO certifications, SOC 2, Sarbanes Oxley, Payment Card Industry (PCI), HIPAA and many more to meet ongoing customer and business needs.

Follow Drew on LinkedIn for more insights into IT technology and operations.

About Lumos

Employees shouldn't be admins for hundreds of web apps with excessive permissions. But then again, nobody wants to be stuck in IT ticket queues for days to get the right access.

With Lumos, you make your company more productive and compliant with self-service app requests, access reviews, and license removals. Learn more at Lumos.com.

A CIO's Guide to Self-Service & RBAC

The Death of the IT Ticket

By Drew Daniels, CIO & CISO @Druva

Drew Daniels
CIO & CISO @Druva

Guide
April 2022
Lumos.com