Ordering a chicken sandwich for lunch shouldn't come with a side of cybersecurity risk.

But that was the reality for one of Cody Brandow's education clients.

To better monitor end-user behavior at a school district he served, Cody, a Security Engineer at Heartland Business Systems (HBS), connected SaaS Alerts. Right away he saw that staff members were using their OAuth credentials to access unapproved apps.

Not good.

For example, one teacher used their staff credentials to log into, wait for it ... the Wendy's app. The teacher wasn't being devious; it was just easier for him to use the same credentials for all apps, including the one he used to order lunch.

But Cody knew that the more staff members use their official credentials to log into unapproved apps, the more potential doors they leave open for hackers.

Once Cody flagged this unapproved app usage, district leaders spoke to the teacher and nipped the problem in the bud.

Without SaaS Alerts, Cody never would have had that visibility into end-user behavior. To ensure the problem doesn't happen in the future, he also uses SaaS Alerts' automated remediation tool, Respond, to shut down accounts that try to access unapproved apps.

Whether it's an innocent lunch order or something more suspicious, SaaS Alerts provides the visibility and control MSPs need to cover their clients' SaaS. Sorry, Teach. You'll have to use your personal login for that next value meal.

SaaS Alerts
A Kaseya COMPANY

+1 (910) 887-3352
sales@saasalerts.com
www.saasalerts.com