Google Cloud

Enabling a secure digital workspace at Essence with G Suite Enterprise

Colin McCarthy, VP Global IT, Essence

Essence, a global data and measurement-driven media agency, currently has over 1800 employees in 20 offices across the globe. One of the key challenges I face as a leader in our IT department is to enable each of our employees to have consistent access to the tools and resources they need to be effective at their job.

At the same time, I must ensure our company's data and intellectual property—two of our most valuable assets as a media agency—are secure and only accessed by the right people. Threading this needle has always been a challenge for us as an IT organization, but we've recently made great strides in this area thanks to our partnership with Google Cloud.

Creating a collaborative and agile work culture

The media world is very fast-paced and collaborative, and as a result, our employees require tools that enable them to easily collaborate across global teams and get work done from anywhere—at a coffee shop before a customer meeting, at the airport waiting for their flight, or catching up on email at home. Our employees also need the flexibility to work from their personal devices rather than being tethered to an IT-provided machine.

In an effort to address these needs, we started working with Google Cloud nearly a decade ago, first deploying G Suite with the goal of fostering a more collaborative workplace and encouraging stronger engagement across our teams. Shortly after this, we started to embrace mobility and adopted a bring your own device (BYOD) program, giving our employees the ability to work more freely across locations and devices. These changes improved employee productivity, collaboration, and morale, but also presented new

essence

challenges, including how to manage access to G Suite and other apps (both SaaS and on-premises) and how to ensure employee devices and accounts were as secure as possible without impacting the user experience.

Solving these challenges with Cloud Identity

Cloud Identity, included as part of our G Suite Enterprise license, helps us address these challenges in a number of ways. First, we implemented single-sign on (SSO) to give our employees easy one-click access to all of their apps, and we integrated Cloud Identity with BambooHR, our HR system of record, to automate user lifecycle management. To add an extra layer of protection to our employee accounts, we also deployed multi-factor authentication (MFA), which requires our employees to not only provide their username and password to access apps and resources, but also a second factor that helps prove they are who they say they are.

For our high-risk users, like executives, finance employees, and IT admins, we wanted to add an additional layer of protection. To do this, we recently enrolled in the Advanced Protection Program, which provides Google's strongest grade of account security and gives us peace of mind knowing that the program is continuously updated with the right security controls to keep up with the emerging threat landscape. Finally, we leveraged endpoint management to gain visibility and control over both corporate-owned and BYOD Android and iOS devices.

Moving towards BeyondCorp with context-aware access

One of the key reasons we've deepened our relationship with Google Cloud in recent years is our belief in the BeyondCorp security model, which shifts access control from the network perimeter to individual users and devices. Google began its BeyondCorp journey in 2011 as an internal initiative to enable full-time employees to work from untrusted networks without the use of a VPN, and we are eager to do the same at Essence.

Our first major step towards enabling BeyondCorp was to start using context-aware access, which provides granular access controls for G Suite apps based on a user's identity and the context of their request. There are a couple of common scenarios at Essence that we're solving for with context-aware access, including 1) allowing full-time employees to access apps from any location, on any device, so long as the device is encrypted and running a modern patched OS, and 2) blocking access to Windows 7 and outdated versions of MacOS. Prior to context-aware access, our IT department had to set numerous individual policies to provide these controls, which was resource-intensive, time-consuming, and less secure.

We're excited about the progress we've made in these areas and we're looking forward to partnering with Google Cloud to provide a secure and modern workspace for our employees for years to come.

Find out how G Suite and Cloud Identity can help your business.