

Selecting Software as a Service with Security in Mind

By Kai Dailey
Program Manager and GRC Analyst

Why Baseline Online Security Shouldn't Be a Luxury for Nonprofits

When you look for a cloud tool to support your team—whether it's Google Workspace, HubSpot, Little Green Light, or any of the hundreds of platforms built for remote work and productivity—you usually arrive with a specific wish list. You want smooth collaboration, intuitive dashboards, fair pricing, and clear answers during vendor demos about how painful data migration will be.

Security rarely tops that list.

It makes sense why. If you lead a nonprofit, like most leaders, you focus on serving your communities first, which means when it comes to purchasing cloud services, you are evaluating tools from a perspective of utility and affordability. But if your team handles donor records, employee data, or sensitive client files in the cloud, you face the exact same threats large enterprises face. Security features must be factored into the software budget. Yet for small nonprofits foundational safeguards are routinely locked behind unaffordable paywalls or omitted entirely from entry-level license tiers.

The reason for this, in part, is that the software industry has benefitted from consumers who have not historically known what security features to ask for. For decades, software vendors have treated essential security controls as premium add-ons, tucking them away inside expensive enterprise licensing tiers. They reserve these protections for large teams and big corporations because it is big enterprise technology and legal teams that have the leverage to demand them.

When small organizations seek security advice, experts often respond with a laundry list of expensive software subscriptions and specialized hardware. And if an organization has an unlimited budget, that approach might work. Most nonprofits do not. Every dollar and team member hour must deliver real value toward an organization's purpose.

A more realistic security approach requires a sensible balance among three components:

1. Getting as many baseline online security protections from the online services you purchase as you can afford, particularly in the form of built-in features.
2. Practical rules defining how work gets done, who has access to what, and how policies are actually enforced to create clear operational governance that encompasses cybersecurity.
3. Compensating actions, low-tech or no-cost habits, like strict employee separation processes and structured data handling, that reduce risk without requiring expensive new software.

Asking Better Questions Before You Buy

To level the playing field, we built a shareable [Essential SaaS Security Features Checklist](#). It outlines a list of basic security features that should be bundled as standard with any online software service. We know this isn't the case. As a results, every small organization needs to determine which security features they can safely operate in the cloud without and then verify what features are present before buying licenses, signing a contract, or migrating workflows to a new platform.

To demonstrate how everyday tools stack up against these criteria, we also put together:

- A breakdown of Google Workspace security features across license tiers, highlighting where key protections drop off.
- A direct side-by-side comparison of two widely used nonprofit SaaS platforms, Give Butter and Little Green Light, to show how standard donor databases measure up against our baseline checklist.

Except for advanced enterprise logging and monitoring integrations (SIEM and CASB on our list), nothing on this checklist is optional in today's internet environment.

The next time you evaluate software or sit down with a sales representative, take this checklist with you. Ask them plainly which of these protections exists right out of the box on their standard plans. Ask them to explain why any missing piece belongs behind a paywall.

It is long past time that we demand a baseline of standard security features from software vendors.

If you have questions about reviewing your current tools or building practical safeguards for your team, send us an email. We are here to help.

Further Questions to Consider

What cloud software services do we use?

What data and accounts do we need to protect?

How do the security features of our current software services measure up?

Is it worth it to pay more per license for better security features?

Do we have the time to implement, monitor, and manage more robust (and complex) security features?

Are data and file storage structured so that we can easily limit access by role and keep data restricted to only those who need it?

Are our daily processes compatible with using single sign-on, role-based permissions, and minimum necessary access without breaking everyday workflows?