

GoodAccess VPN review:

A new twist on an old security tool designed for the smaller business

By David Strom
July 7, 2022
@dstrom
strom.com

Sponsored by GoodAccess

A [VPN](#), or virtual private network, disguises your computer and encrypts your internet activity and data by routing it through a separate server, making it harder for anyone to intercept your communications. There are lots of reasons to use a VPN, including when you are using public Wi-Fi or other untrusted networks, or to stream videos that are blocked because you are in another country. But it also can protect your internet access in a country (or a business for that matter) that censor's content ([Russian VPN subscriptions have climbed](#) since their war on Ukraine began earlier this year), improve your internet access speeds, segregate your working from home traffic from your family's (and their traffic from you too), protect your online identity, browsing history or other private data. When you run a VPN, it appears that you have been magically transported to another location, which is where the unblocking effects can happen.

There are dozens of different VPN providers available, some that are focused on consumers and others on larger businesses. The former category is usually short on features and questionable on privacy protection while the latter has tons of features and privacy but requires a lot of IT skill and/or personnel to operate effectively. This "in between" niche is the target segment that GoodAccess, based in the Czech Republic, attempts to fill. Spoiler alert: they succeed.

Despite the numerous choices, VPNs have somewhat fallen into disfavor, and that is too bad because they still have an important place in the modern security fabric. [In a survey done by Ponemon](#), only 28% of respondents say their organizations determine if remote workers are securely accessing their networks. That proves my point. As I [wrote about for CSOnline](#) earlier this year:

"Thanks to the broader interest in VPNs during the pandemic, they are getting better and deserve another look. Part of the issue with VPNs is ignoring the marketing drivel, taking a deeper dive into the technology, and finding the right place for a VPN in your [enterprise] security stack."

A great VPN should handle the tradeoffs among these three factors:

- Anonymity (moving about your online world without anyone knowing who you are),
- Privacy (keeping your data to yourself and away from others), and
- Security (prevent your devices from being compromised by a criminal or state actor).

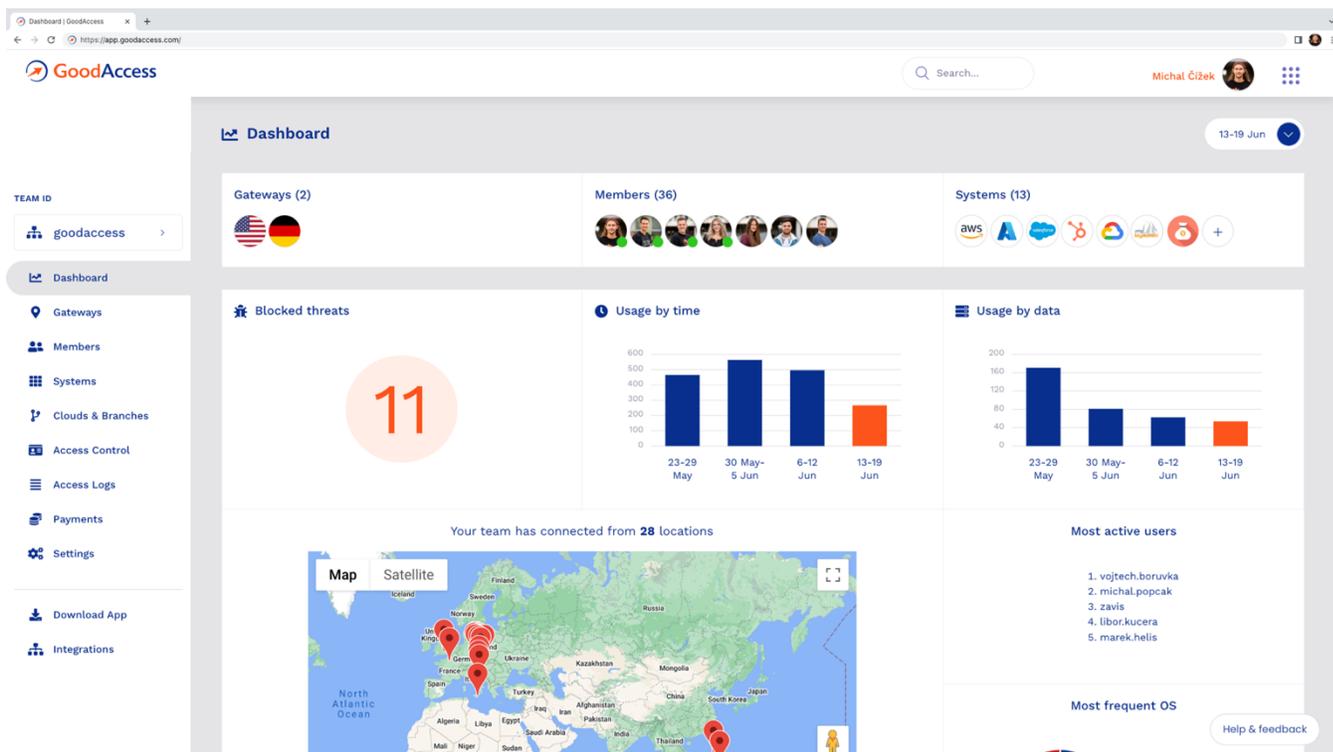
GoodAccess does a reasonable job on all three, and you'll see why as I get into the product's feature set and implementation.

It isn't the most anonymous VPN – that goes to consumer-grade providers that have taken pains to even avoid having customers provide their email accounts. But they have been diligent otherwise: "We don't need to make unrealistic promises such as to claims about 'military-grade encryption,' or other terms that the consumer VPN providers use

loosely,” said Artur Kane, their CMO. “We publicly share information about third parties operating our infrastructure, and our admin panel doesn't contain any sort of tracking code that would allow us to gather profitable data.” As the company [states in its privacy policies](#), “we put a significant amount of effort into protecting our gateways.” I would tend to agree.

Several consumer-grade VPNs tout their “anti-tracking” features, but these seem more marketing hype, taking built-in features already found in the more modern web browsers that can detect and block third-party script communications. “We believe that if a gateway operator can secure their infrastructure better, they should do it without trying to monetize only those who are willing to pay extra. And certainly, a provider shouldn't market it as rocket science and create unrealistic expectations,” says Kane.

Most of its power lies in its web-based administrative interface, with the main dashboard shown below. You can see the various configuration options down the left-hand menu, a summary of usage statistics, and a map geo-locating your end users' location.



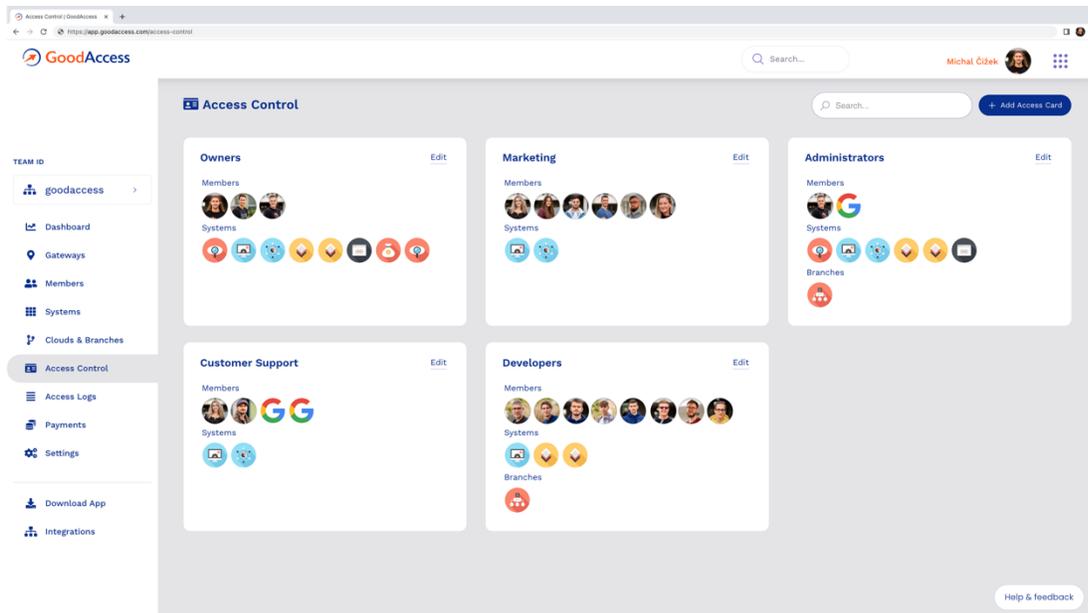
One of the items on the dashboard is the number of threats blocked by the software. This is a nice feature of GoodAccess: they make use of threat feeds to automatically isolate known malware. While this won't catch everything, it shows that the company is trying to stem this tide.

GoodAccess doesn't have the wide collection of gateways that is found with some of the consumer VPN providers – at the latest count there are just three dozen – but it [does list them here](#). Most are in the northern hemisphere, mainly Europe and the US. Its

[pricing page](#) is also very transparent, offering both forever free and various paid plans, with 14-day free trials. The paid plans range from \$5-\$12/mo/user, with annual discounts of up to 20% if paid in advance. The forever free plan handles up to 100 users and is missing numerous features available on the paid plans, such as no MFA, no static IP, no chat and email support and no custom domain blocking, just to name a few of the missing elements. (My recommendation is to choose the free trial of the premium plan if you want to investigate all these features.)

GoodAccess offers several [different endpoint clients](#): MacOS, Windows, ChromeOS, Android and iOS. Missing are any browser extensions and a Linux app. Speaking of gateways, a potential customer should pay attention to the composition of its work teams in deciding how to match up the best location with each team member. GoodAccess prices by the gateway, so if you need multiple ones to support distributed team members, you will pay additional monthly fees.

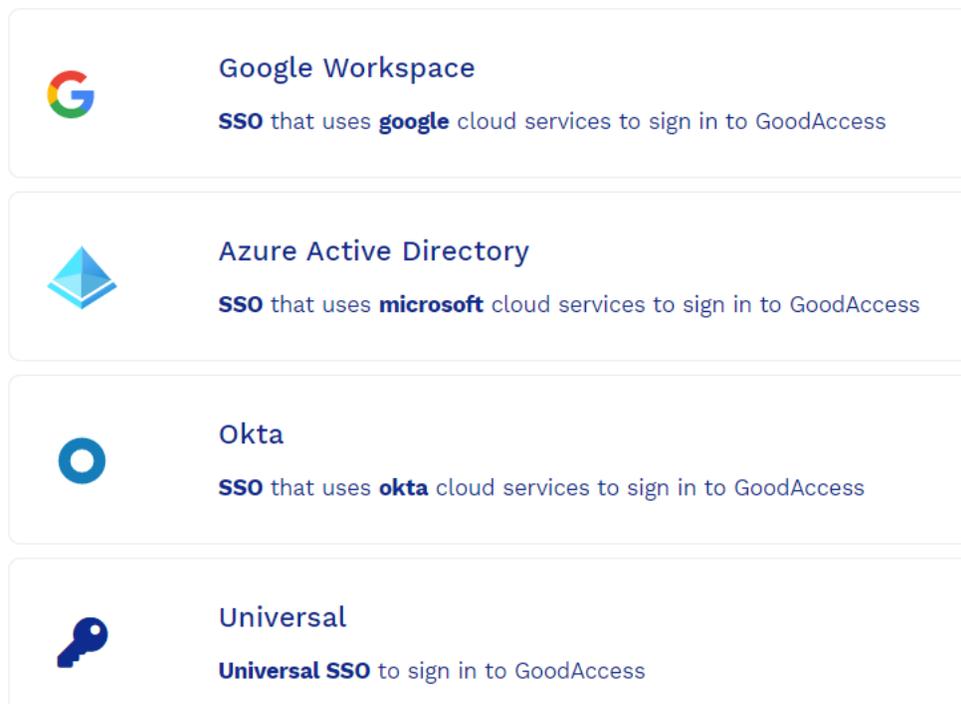
GoodAccess also supports a few open-sourced routers, such as the [Linksys WRT](#) and [Asus OpenVPN](#) models and supports both IKEv2 and OpenVPN protocols across all of its gateways. Support for both protocols is significant and illustrates how the VPN market has matured. More than a decade ago, there were just two: IPsec and SSL. But IKEv2 improves upon IPsec tunneling with quicker reconnections and is built into most current endpoint operating systems. IKEv2 is also supported by many enterprise VPNs, such as Cisco's SSL AnyConnect and Juniper's VPN products. [OpenVPN](#) has several projects using the name—the protocol, the VPN server code, and various clients. Its protocol has improved upon SSL and has become widely adopted by the consumer VPN vendors. Both IKEv2 and OpenVPN protocols can employ AES with 256-bit encryption keys, the contemporary standard. Setting up protection and access rights for various services shown on the screen below.



There are also 16 different application integrations, and this is a real strength of the product, especially for smaller businesses that use a variety of SaaS apps such as WordPress, Google Cloud, Magento and others. These integrations setup a secure private and encrypted tunnel from your app to your endpoint, to prevent man-in-the-middle attacks and to help improve your login posture with these apps. There is also copious documentation on how to implement each one. I used the WordPress plug-in to protect my blogging server, and it worked as promised. There are a series of steps that have to be followed precisely which is to be expected, but the directions and workflow sequence are both clear.

And you can also setup a single-sign-on provider, such as Okta, Google or Azure, as seen in this setup screen below. The process of creating a SAML link will take some effort, and obviously this isn't for every small business network. But it is nice that GoodAccess has taken the time to handle this situation, because there are some customers who will want this extra protection, or who have made the decision to use SSO as their main authentication method.

Log in through an identity provider



	Google Workspace SSO that uses google cloud services to sign in to GoodAccess
	Azure Active Directory SSO that uses microsoft cloud services to sign in to GoodAccess
	Okta SSO that uses okta cloud services to sign in to GoodAccess
	Universal Universal SSO to sign in to GoodAccess

There are a few points that need further work by the company and are mostly smaller matters. First is a need for greater transparency, such as what has been done by numerous consumer VPN providers. GoodAccess has no public audit or independent evaluation posted on their website, and they should move towards doing this as soon as possible to enhance their credibility. (They have done private assessments however.)

Second is that some of the configurations need better context: for example, as shown below, there are two places you can use to set up MFA to protect your logins: one is for your entire team, the other is for your individual account. I was initially confused between the two, but it makes sense to have them both, just that they need better explanation.

Two Factor Authentication:

With 2FA enabled, you will be asked to enter your 2FA code each you login to your GoodAccess account.

Enable 2FA for account login:

Admins & Roles **Login** Security Shield DNS Management Subscription

Standard login **Active**

Login with an identity provider

With a more secure Two-Factor Authentication enabled, your team members will be prompted to enter a six digit security code from a special mobile authentication app every time they login into **GoodAccess mobile and desktop client applications**. To learn how to set up SSO in GoodAccess, visit our [support site](#)

Enable Two-Factor Authentication

Next is the matter of log retention. GoodAccess does retain connection logs (with origin IP addresses and time stamps that are retained for up to three months) and publicly claim to do so, which is a feature that can help business owners audit their VPN usage or notify a business of potential fraudulent usage. They claim they don't share these logs with anyone other than the customer. They explain their situation and their decision in various places on their website, but it bears repeating.

Finally, while it is great that the software can quickly be used to protect very complex network infrastructures, this flexibility has one downside: scalability. To set things up to support a complex network means you must manually assign access rights and systems permissions across all your end users, which could be tedious for larger installations. One of their largest installations is a company that supports six thousand end users, and the company took the better part of a week to deploy their GoodAccess VPN. For these larger deployments, some kind of automation solution should be on their radar. On the positive side, there are [screencast videos that show you how to set the various parameters](#).

My bottom line: GoodAccess has taken the best bits from the consumer-grade VPNs and created a very robust business-class tool that can be used by smaller enterprises to protect their remote users. It is a VPN provider that you can quickly start using and grow

into more sophisticated protection and doesn't require a lot of IT resources to deploy and maintain.

About GoodAccess

This review was sponsored by GoodAccess but contains independent editorial content. GoodAccess is the global company dedicated to simplifying “anytime, anywhere” secure connectivity and access for small and medium businesses around the world, beginning with its free GoodAccess Starter product for unlimited usage for up to 100 employees. For companies with more than 100 employees and with the need for static IP addresses, Zero Trust access and other requirements, GoodAccess provides a competitively priced platform that maintains simplicity and ease of use. GoodAccess products are designed for set-up within 10 minutes and the flexibility to meet varying conditions. www.goodaccess.com

About the author

David Strom has been writing about business IT topics for more than 30 years and was the founding editor of Network Computing magazine and ran editorial operations for Tom's Hardware and ReadWrite.com. He has written two computer networking books and thousands of shorter articles and blog posts for dozens of publications, using his vast experience testing hundreds of business security and productivity products. He can be reached on Twitter @dstrom or his blog at strominator.com.