Microsoft Azure Active Directory Premium

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Microsoft Azure Active Directory Premium

Read 11 reviews of Microsoft Azure Active Directory Premium

Review by a Real User

Verified by IT Central Station

Consultant with 10,001+ employees

it_user623721

WHAT IS OUR PRIMARY USE CASE?

The primary use case is collaboration. So it's all about federation of identity and permissions. Identity is one of those things that you need to be separate from your actual tenant. There's a benefit for it being separated from your actual tenant for reasons of security and containerization. It's very easy to run and it's part of their ecosystem and I don't think it's going anywhere anytime soon.

HOW HAS IT HELPED MY ORGANIZATION?

Back in '96, '97, '98, nobody was doing intake. So that was a new thing that came in 2000. And it created the container based inherited permissions, which was new for that stage. Before that it was very static, there wasn't inheritance, there wasn't assertions. Then they introduced that and they've slowly built it, and then it just got too big and old, and really the database that MT's on is just vulnerable to all these attacks. And that's primarily why they want people to get off it. There's about four or five open attacks that make it very easy to both intercept the credential requests, and also attack the database itself.The ability to speed up delivery is a nice benefit, because rather than having external dependencies there's a certain guarantee that if you use anything within that technology platform. Whether it's full of applications, or various other things, there havee already been regression tests by the vendor. And you don't see the same defects that you get when you have integrated systems.

WHAT IS MOST VALUABLE?

The fact that it's an ecosystem in itself is probably the best one. It fits into the whole Microsoft stack. Everything this year is all about stacks, and I tend to agree. The inter-operability and complexity of things these days is just too big. These things change too much. So you don't really want to be stuck between three technology stacks that are changing. If there's a defect, you won't know which one it's in. Trying to hold the service provider to account is quite hard. I'd probably say, yeah, stay with the stack if you can.

Microsoft Azure Active Directory Premium

Read 11 reviews of Microsoft Azure Active Directory Premium

WHAT NEEDS IMPROVEMENT?

I guess price would be the thing, and some of the proprietary lock-in. But, I guess documentation and support would be good. The features are fine. I wouldn't suggest any features because you can keep adding to it. But, its simplicity is that it works under its own ecosystem. It's nice and reliable. If you start adding all these extra things to it, it'll probably cause complications with some of the legacy things that are still slowly just hanging onto them. But, to look at more documentation, engineering, or an open standard would be nice.

FOR HOW LONG HAVE I USED THE SOLUTION?

One to three years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's like any technology. It appears that if it did have stability problems they don't really exist anymore in the same way. It's like any introductory development technology. Because its identity, it has to be perfect. It is either secure, or it's not, and unfortunately there's a million ways for things to go wrong and there's only one way for things to go right when there's no give. You do see a lot of issues with it at the beginning. It is mathematical. So, it's like most things. Took a while to get the XAML certificates and all that sort of stuff working. But,now it's a very common thing. You get a session certificate on your phone when you're doing things. When you join a session on your browser on your mobile phone. It's just very common things now.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

I'd say there's about 5,600 users of this solution in our organization. There are set rules. But, it's a security mechanism. If you try and get your swipe card pass for your office, and then you try and integrate it with one across the road, they're literally being designed not to integrate with each other by design. This is because if you want it secure, you don't want to have it integrate. The same thing works with changing the posture of something after you've initiated it. Expect this sort of behavior.

HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?

The tech support is OK. I'm talking more about the engineering structure of it. As I said, you can understand why security things have a tendency to not document it, because it's one of those things. Do you want more people to review it and make it harder, or do you want to covet it and reduce the exposure of it? It's catch 22. You're damned if you do, damned if you don't. Doesn't matter which way you go.

WHICH SOLUTIONS DID WE USE PREVIOUSLY?

We have prior experiene with Novell.

HOW WAS THE INITIAL SETUP?

It's easy in its essence, but part of the ease is like anything that seems easy is generally complex when you try and fix it because you've skipped over so many configurations. It's like a wizard that you go, "Yep, it's done." And then it breaks, and you say to yourself, "Oh, hang on, I clicked one button. How could I have done that differently?" It's a lot more stable than it used to be. They've got into a maturity plateau where they're not developing it anymore within for reasons of functionality and the product doesn't really break much.

Microsoft Azure Active Directory Premium

Read 11 reviews of Microsoft Azure Active Directory Premium

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

There's no such thing as a "free lunch." If you'd save money here, it costs money there. If you pay more upfront, you pay less when you get off. The market equals itself out, like a free market. So, it generally does. It's more about convenience at the end of the day. As a user, I'm not an owner of the tech, so as a consumer, even if I am a specialist, I still don't own the technology. I just want to lease it, subscribe it and make sure that the owners of it are able to meet the facilities of it in its life-cycle.

WHICH OTHER SOLUTIONS DID I EVALUATE?

There's a couple of other options on the market like Okta, and a few things like that. They're quite simple, and because they're separate from the whole Microsoft ecosystem, they do have some benefits in that they're completely focused on only that product and only that requirement. With Microsoft, they're like an octopus. They have so many different requirements and priorities that sometimes they don't invest all their energy into the products that you have expectations to investigate.

WHAT OTHER ADVICE DO I HAVE?

Last year Microsoft had said that the onsite Active Directory ,as we know it, is going to be deprecated. So that means group policy, that means security groups, the NTLM and all that we've relied on for so long is going to come to an end with this modern management philosophy. That's why I did those group policy changes. From group policy, which is essentially the ability to control the operating environments of managed devices, rather than that, Microsoft wants only a mobile device management policy. So it's pretty much a HTTPS or SSL assertion to manage devices off the domain, and they will all come from Intune. So, they're not going to be managed by a set of static policies. They're going to be set by a whole heap of compliances. Does that make more sense? It's not conforming. It's when you assert yourself, and us for a particular requirement from the domain. They check your requirements per request, which takes the load off the environment quite a bit. So they only validate you when you ask. It's a lot easier to get an engineer to understand the Microsoft stack then some esoteric random "Joe." There's just are not enough people in the field. You're better off creating a pilot tenant on your own. You can set up one that's free using one of their 30 day trials, and while you're doing that try and make it as realistic as you can to the environment you're coming from. Make sure that it is true in terms of network, commissuib and integration. If you're going to use a MDN for mobile device management, or you're going to use applications for the federated sign-ons. Try and get as much as you can in it. You've got 30 days and they're quite liberal with allowing you to trial it. Most of the capabilities are there internally. You can't expose external DNS names or anything and use it as an external platform, but internally you can. So spin up a VM or something internally and do the same things you would. I'd dare say: test it and prove it. You've got to prove it to yourself before anybody. I wouldn't trust anything from a brochure or anything else. Your reputation's on the line. You're doing something important for someone else and you've got to verify it yourself and put it through the paces. Spend enough time doing proof of concepts and pilots.

Read 11 reviews of Microsoft Azure Active Directory Premium