PeerSpot

Case Study

Axiad Cloud

reviewer1925592

Sr. Manager, Training Services at a transportation company with 10,001+ employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

The main use case is to register and manage smart cards for all of our users. We have investigated using Axiad for other forms of multi-factor, but haven't had the time to implement those projects yet.

How has it helped my organization?

A great example of how it has helped our organization is as a result of our partnership with them and implementing multi-factor authentication for all of our users. Eight months after implementation, we started to see a decline in help desk calls for security issues, to the point that the number of calls about our multi-factor solution is less than our historical number of password-related calls.

We've enabled all of our users, except for our administrative users, to enroll through self-service tools, all the way up to our executives. We felt so comfortable with the solution that they're enrolling themselves and re-enrolling their tokens when they expire.

Another benefit is that it has definitely saved us a lot of time. The money savings come into play through the reduction of risk and having a simpler method for our users to authenticate. There is no more changing of passwords, there are no more expiring passwords, and we no longer have to rely on users for the security of our authentication tokens by forcing them to choose appropriate passwords.

What is most valuable?

What I have found most valuable is the overall

way Axiad listened to our problems and helped us solve them. They provided guidance and expertise, with their experience, that enabled us to be successful in a very challenging space.

Also, our users required almost zero training once they were in the Axiad portal.

We are using Axiad for workstation, cloud, as well as our web single sign-on and our VPN access. They've covered everything.

What needs improvement?

We've sat down with them multiple times to discuss things they could do better, and they've done them. I'm looking forward to seeing how they move to FIDO U2F as their primary authentication method across all of their solutions.

For how long have I used the solution?

We have been using Axiad Cloud for just over four years.

What do I think about the stability of the solution?

The stability is excellent; no issues.

What do I think about the scalability of the solution?

The scalability is also excellent.

We have in the neighborhood of 20,000 users, from clerks through to our CEO. It's used by the entire organization. The only increase in use will be through growth.

How are customer service and support?

The technical support is very good. We haven't had a lot of problems, but when we have had something, we have gotten engagement from them.

If it's a large problem, we typically see a very short turnaround. If it's a problem that is more of an inconvenience or we're looking for a report, we usually see that taken care of in the normal lifecycle of the product, in the next upgrade or a future version.

How would you rate customer service and support?

Positive

Which solution did I use previously and why did I switch?

We had a number of different point solutions for multi-factor, and we've now consolidated on

Axiad's solution.

We are an older organization and we had always relied on usernames and passwords. The move to MFA not only required changes to technology, but the solution had to be robust enough to remove friction that might be caused by requiring our users to change behavior.

How was the initial setup?

Since we're on-premises, the setup was really complex. We had to build infrastructure underneath. The Axiad part of the solution was implementing the credential management, and that was relatively straightforward, but the overall integration was complex. Having their expertise engaged was really how we got through it.

We have a specific flow, a manual process, when it comes to authentication, following the NIST standard for identifying our users. We force them to show government credentials to identify themselves before we'll issue credentials. My team takes care of that for our users.

But I've walked through the deployment of Axiad Cloud, and it's a very different experience. That infrastructure isn't required, the certificate authority and the hardware HSMs aren't necessary. It takes a lot of the complexity out of the equation when you just use their native cloud offering.

The deployment of the technology for us, being on-premises, took about four months. We took a risk-based approach. We started with the users with the most access and ended up rolling out to the entire organization over about a two-year period.

The deployment was done by a team of four within our organization and maintenance is about half of one FTE.

What about the implementation team?

Any multi-factor implementation involves a complex set of technologies. The Axiad solution made it easier, but it really was due to their help in implementing it that we were able to solve a lot of difficult problems. Without them, our project timeline would have been much longer.

Their professional services had a guide and we worked with them to follow that, implementing things based on available standards. When we were done with the implementation, a second representative from Axiad came in and audited the work of his peer from Axiad, along with our team's work, to ensure that we met the requirements that we documented before the start of the project and that we followed best practices and written standards.

What was our ROI?

ROI in the security space is always a challenge. I would liken security programs to insurance policies, so a set ROI is probably not achievable. It would not fully recognize the value of reducing

risk in the org. We could quantify how many fewer tickets and how much less help desk time we're using, but that would ignore that reduction in risk.

The overall risk reduction and ease-of-use have been our two, longer-term returns on our investment.

Which other solutions did I evaluate?

We have a rigorous supplier process that we have to follow, and we put out a request for proposal. Axiad won that and we then went through the implementation with them.

Axiad's price was very competitive and the solution they proposed was based directly on our requirements and customized to our needs. The other vendors were all selling something of a turnkey, "Here's what you get and make it work" type of solution. Axiad was the opposite: "We're going to make it work for you," which was awesome.The only con is that they are a small, but growing, organization. For a large enterprise, sometimes the viability of an organization is a concern. But it was about five years ago that we started talking with them, and four years ago when we started implementing. They've shown that they have some staying power.

What other advice do I have?

It's really about ease of use and focusing on your users. Security is always paramount, but if you give people something that is secure yet hard to use, they're going to find ways around it. With the solution we have been able to give our users, I see a lot of happy users, and our adoption is such that I don't see users trying to circumvent our processes.

If someone were to tell me they've deployed multi-factor authentication for most of their use cases but not all of them, I would say that multi-factor is the best control to stop initial access in the attacker lifecycle. If done correctly, the long-term impact to users becomes a positive. If people are hesitating based on the concern that users won't like it or it's hard to use or implement, what we have found is that as long as you have support from management, you can get it done and you can prove to users that you can do it in a way that it's useful to them.

The Axiad Cloud Airlock feature wasn't available when we first implemented the solution, but we're investigating its use. Our main use case for it would be to do some additional programming on our security tokens when the users first register them.

The solution is a critical security control for our organization. It has visibility at the board level and is visible to every one of our users, yet it is very unusual for me to hear a negative about the Axiad solution that we've implemented.

I work with very few vendors that I don't have some kind of suggestion for on how they could improve, but Axiad is one that just provides a great solution. And they continue to grow that

solution to do more, but they covered all of our use cases.

Using Axiad, I have learned that there are organizations out there that are engaged in helping their customers be successful on this journey. The proposal they gave us was really built around our requirements and not just, "Here's a solution." That was key to our being successful: understanding our business, understanding our use cases, and catering to those aspects. I have really seen success in this space, one that some of my peers have found it very difficult to be successful in.