PeerSpot

Case Study

Axiad Cloud

Damon Becknel

Vice President, Chief Information Security Officer at Horizon Blue Cross Blue Shield of New Jersey

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We use it for internal employees and our contingent or contractor workforce. We extend it, additionally, to vendors who are entities that are completely offsite but not full-time contractors and who still need periodic access to the environment.

Our primary use case is for multi-factor authentication through VPN, as well as for local endpoint access and VDI. A more limited use case is for additional digital signatures or encryption, code signing and digital signatures for documents and for email, and for email encryption.

We use the solution for managing the cryptographic credentials for everyone on staff. Authentication is a process that the credentials are used for. Axiad is not controlling our authentication, they escrow and provide the certificates to support authentication.

They run the backend in a cloud. It's extended to us via a lockdown connection. They do all the administration and we're the front-end user. From a usability perspective, we load keys onto their smart cards or onto YubiKeys, which are something like a USB version of a smart card.

How has it helped my organization?

The really slick part of smart card authentication is that it's native. All too many of these modern authentication systems require additional software in your authentication environment. What attracted me to smart cards is that it's flat-out native. It just works. It's built into the operating system. You're not having to worry

about compatibility issues when Microsoft runs an update or when the vendor runs an update. It's built-in yet very easy to use.

It's also a fast solution. Everyone has been in the position where they have had to type their username and then type their password, and that password is likely rotating and rather long and cumbersome. Because of all those factors just typing in a user password might take someone 20 to 30 seconds. Whereas because of the way a smart card is built and how the credential works, we're able to simplify that to a PIN . When you insert your card and you have to type your PIN, it's a completely numeric PIN that is much easier to remember. And it doesn't rotate as often because you don't have the issue of storing a password hash or the issue of having that password hash become compromised. There is no way to get the PIN off the card. It doesn't exist there. So we don't have to rotate PINs at all. It can be a lot weaker and just be numeric. Inserting your card and typing your PIN may take 10 seconds, and five if you're fast. When we rolled this out six or six and a half years ago, it was applauded by the users because it drastically reduced authentication time.

The solution has also saved us time by having end-users troubleshoot issues through the MyCircle feature, and has definitely reduced the efforts of our administrators. It is saving us five to 10 minutes per incident.

What is most valuable?

We have some self-imposed restrictions. We want to make sure a card is being issued to the right person so they go through a lot of validation steps. We don't want something as secure as a smart card being issued in one click. But the number of steps is as minimal as it can be and as easy to use as you would hope it would be, but it's certainly more than one click. Still, it takes seconds to enroll a user. It's quite quick. You select the user and say "enroll." But then there's the other side of that, which is the user activating their credential. Generating the certificates for the user is incredibly easy, but deploying those users' certificates requires a little more involvement because you want to make sure it's the correct user pulling the credential loading it into the card. Overall, it's intuitive and simple.

What needs improvement?

It's rare for me not to have a lot to say about room for improvement in products we use, but with Axiad Cloud there isn't a lot to say. However, macOS is notoriously ever-evolving and it's difficult to keep pace with it as it pertains to certain kinds of crypto authentication. That's really not even on Axiad. That's a decision by Apple, but it makes it a moving target.

For how long have I used the solution?

I've been using Axiad Cloud for between six and six and a half years.

What do I think about the stability of the solution?

It's been flawless since we've had it.

What do I think about the scalability of the solution?

Having used it in other environments, I can tell you it scales globally and to several million. It's incredibly scalable.

We currently have between 10,000 and 12,000 users, covering every single internal employee and contractor.

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

We didn't have a full-scale previous solution. We used RSA SecurID on a limited basis. We switched because we needed multi-factor for all users, and we wanted to consolidate physical and virtual access into one token.

How was the initial setup?

The initial setup was incredibly straightforward.

We went from proof of concept to production deployment in 45 days.

Our implementation strategy was to have all local and VPN users off within six months.

For maintenance of the solution, there's the printing of the cards which is a periodic task for one person. The facilitation of the issuance and backend management, et cetera, is a part-time role. But to provide resilience, we have three or four people involved, part-time.

What about the implementation team?

We used Axiad's service and customer care for deployment. Their support for our deployment and for helping us to comply with compliance and security requirements were outstanding.

There are a lot of design parameters to consider when looking at certificates and they were very thorough in outlining the pros and cons of each design parameter. They helped us step through things and made recommendations to try to simplify it. They provided recommendations on configuration features for the endpoints themselves. It was clear they had done this numerous times before and were able to share any potential wins that we could anticipate.

Overall, it was very seamless and they were very knowledgeable in simplifying the process.

What was our ROI?

With any security technology, I don't know if there is ever a return on investment. It's more a matter of risk reduction through investment. You're not going to make any more money because you're more secure. But you're not going to lose money because you are not secure. By that calculus, we have absolutely easily recovered our investment costs based on how we've reduced our risk posture.

What's my experience with pricing, setup cost, and licensing?

This is the first multi-factor solution that we have leveraged so it hasn't saved us money, but it is incredibly low-cost for what we're getting.

It's very cheap on a per-year basis. The cards themselves last about three years and the license is on the order of double-digit dollars per user, and not hundreds of dollars per user, per year.

Which other solutions did I evaluate?

We looked at a number of options for how we could do user credentials. At the time, there was a NIST guide, 863 or 863-2, that had different levels of authentication. Username and password were level one. Username and password, plus an RSA soft or hard token that required no additional authentication were level two. At the time, smart cards and one other technology were alone at the highest level of reliance. Axiad Cloud was really standing alone as one of the most secure options for providing a credential at time of authentication.

One of the other solutions we looked at was an inferior card type. Rather than being certificate-based, it was RFID, which has no security and the software flatly did not work.

What other advice do I have?

My advice would be to read up on how public key infrastructure works and then look at extended use cases for going through that process, where you inherit digital signatures and person-to-person encryption.

The only device we have from Axiad is the card technology. The solution's life cycle is really transparent. They run impeccable security with highly restricted access and the access management from their side is incredibly tight as well, particularly based on their growth through the Department of Defense. A card stock is a card stock and its life cycle is about three or four years.

Axiad Cloud helps enable passwordless authentication for every use case, including workstation login, VPN, and cloud applications. The cloud does more than what we leverage. We use it for certificate-based authentication purposes. They do support push notification as well, we just don't leverage it. Our use cases are

local and VPN, and it's all certificate-based.

The biggest lesson I've learned from using the solution is that security doesn't have to be difficult.

It's a key part of our security posture. It's incredibly important.

Read 3 reviews of Axiad Cloud

See All Reviews