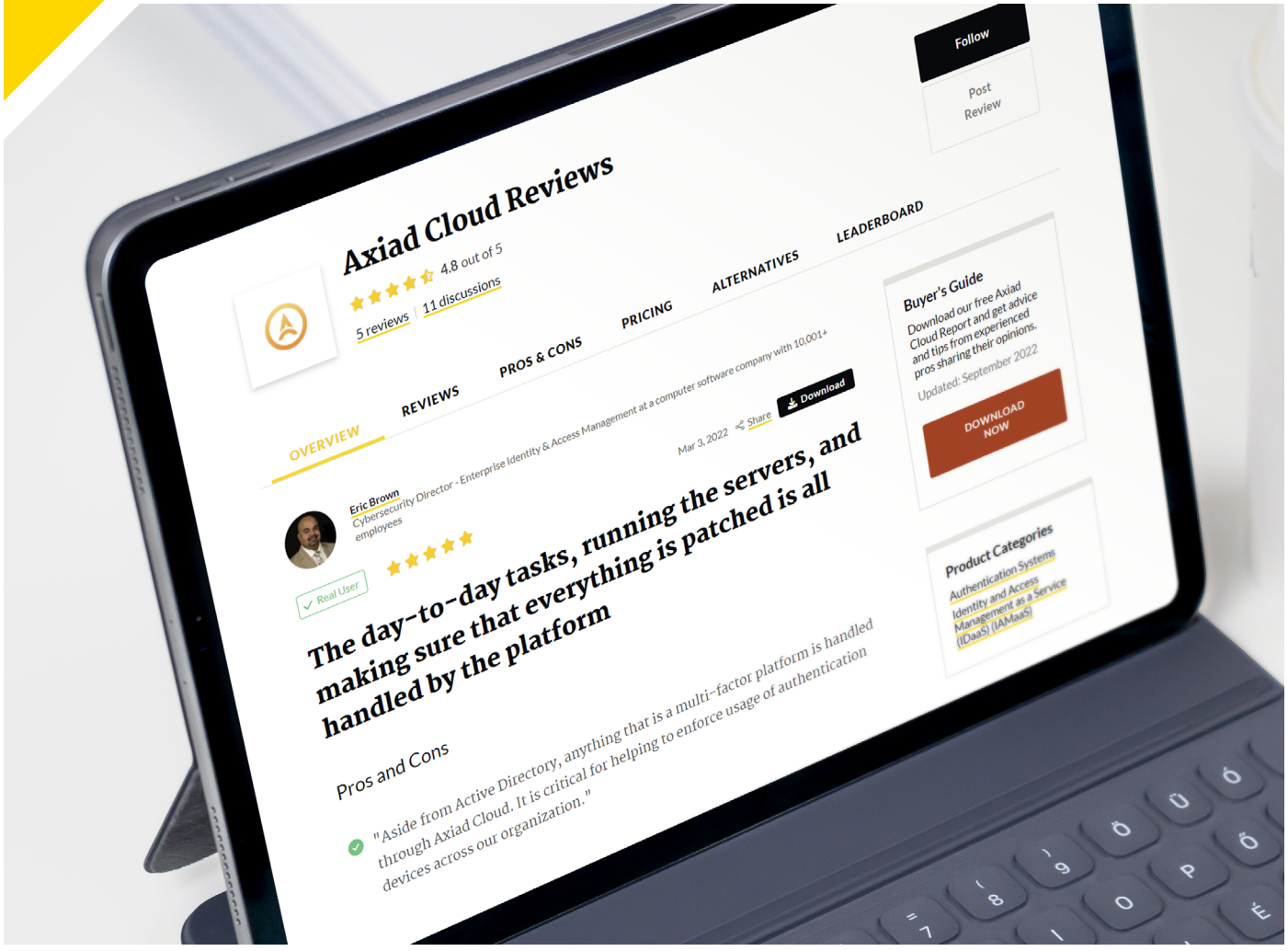
PeerPaper™ Report 2022

Based on Real User Experiences with Axiad Cloud

Rethinking Enterprise Authentication



PeerSpot

Contents

Introduction

Authentication, that foundational control upon which virtually all other cybersecurity measures rely, tends to be a complex, cumbersome workload in the enterprise. The use of multiple, seldom-connected solutions leads to risk exposure, along with inefficient administration and end user frustration. As a result, organizations are starting to rethink how they approach authentication.

In this paper, users of Axiad Cloud share how they have successfully balanced protecting the organization and reducing friction by switching to a new generation of integrated, holistic solutions for authentication. The switch drives improvements in security and operations, as well as reductions in support costs. These users also share the qualities that make for an effective authentication solution, which include automation, visibility, breadth of functionality, and integration with other security tools.

Except where noted, the companies referenced in this paper have over 10,000 employees.

A Brief Overview of Authentication and its Role in Cybersecurity

Authentication is the process of establishing that a person or device requesting access to a system is who they say they are. The process historically involved the user sharing a password or some other unique identifier.

Authentication is the backbone of numerous business-critical cybersecurity operations, including helping organizations become more phishing resistant and prevent ransomware attacks and account takeovers. It is also a core element of a Zero Trust strategy, as continuously authenticating every user, machine, and digital interaction helps security professionals validate everything before granting access to an enterprise's most valuable assets.

Without authentication, it is impossible for almost any other cybersecurity strategy to work as intended. If admins cannot be sure of who is who, then security for data, applications, operating systems and more will be deficient.

PeerSpot members' use of Axiad Cloud demonstrates the centrality and importance of authentication in cybersecurity. For example, an Enterprise Security Architect at a retailer uses Axiad to back a multifactor authentication project. He said, "Axiad Cloud will make us more compliant and secure. We need to use it to comply with certain regulations."

Horizon Blue Cross Blue Shield, an insurance company with more than 5,000 employees, uses Axiad to authenticate employees as well as the their contingent (contractor) workforce, according to their Chief Information Security Officer (CISO).

Holistic Platform for Authentication

Drivers of Change in Authentication Solutions and Processes

Change is afoot in authentication. IT departments and security teams are looking for ways to become more efficient and secure while improving and simplifying the user experience. The use of point solutions (or siloed approaches to authentication), for example, is falling out of favor, as a Senior Manager of Training Services at a transportation company explained. He said, "We had a number of different point solutions for multi-factor, and we've now consolidated on Axiad's solution." He also shared that they wanted a solution that was robust enough to remove friction caused by requiring users to change behavior.

"Our old solution was cumbersome and inflexible," said a Director of Information Technology Services at a legal firm with over 1,000 employees. "There were a lot of problems that we just had to live with because there was no way to address them." Referring to the previous solution as "a necessary evil," he described how he sought a new solution because, as he put it, "These days, anyone who is not using multifactor authentication likely cannot demonstrate due diligence or due care in their cyber program. Everyone needs to be doing multifactor."

A desire for resiliency and efficiency drove change in authentication technology at a software company. According to their Cybersecurity Director, "Before Axiad Cloud, it used to take 10 or 15 minutes to enroll a user. That solution was all on-prem. We wanted something cloud-based that had higher resiliency and less administrative overhead. That is where we made the switch to Axiad Cloud."

For Horizon Blue Cross Blue Shield's CISO, change came because they lacked a full-scale solution. He said, "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."

> **"Before Axiad Cloud, it used to take 10 or 15 minutes to enroll a user."**
>
> Read review »

Benefits of Adopting an Integrated, Holistic Authentication Solution

PeerSpot members who shifted from a siloed to an integrated, holistic authentication framework shared the benefits they experienced from the move. For one thing, the enhanced approach led to important overall improvements in how they protected the organization. The evolution also delivered improvements in operations, savings in IT support, and welcome reductions in complexity.

Overall Improved Cybersecurity Posture

Axiad users felt they were able to better protect the organization with an end-to-end solution. For the CISO of Horizon Blue Cross Blue Shield, the investment in Axiad has helped make the organization more secure. "We've reduced our risk posture," he said, before adding, "Axiad Cloud was really standing alone as one of the most secure options for providing a credential at time of authentication. It's a key part of our security posture. It's incredibly important."

"The solution is a critical security control for our organization," explained the transportation company's Senior Manager of Training Services. "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 [comment] about the Axiad solution that we've implemented." He characterized the overall risk reduction and ease-of-use as "our two, longer-term returns on our investment."

The software company's Cybersecurity Director said, "The added security has helped us mitigate quite a few breach attempts since the system was implemented."

> **"Axiad Cloud was really standing alone as one of the most secure options for providing a credential at time of authentication. It's a key part of our security posture."**
>
> Read review »

Operational Efficiencies for the Security Team

Important as it is for security, authentication is also an operational workload. If a solution can improve the efficiency of that workload, it will deliver profound benefits. As the legal firm's Director of Information Technology Services remarked, "It [Axiad Cloud] was very impressive in terms of its utility right from the get-go, and has shown its ongoing utility when we have reached these catch points, issues it has been able to resolve."

This user then elaborated, saying that Axiad's One-Click Issuance made it "super easy" to enroll a user—"far easier than the solution we replaced," he said. It takes less than a minute with Axiad, whereas before it was taking three to five minutes. He then said, "In addition, it's super simple for deploying and managing authentication devices. Our IT department is rather small, so all the incremental wins that we can get are hugely important to us."

Axiad Makes the Complex Simple

Horizon Blue Cross Blue Shield is finding efficiencies in saving its security team time. According to their CISO, "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."

Reductions in Complexity

Cybersecurity tends to be a complex undertaking. Solutions that can reduce that complexity are always favorably regarded. To that point, Horizon Blue Cross Blue Shield's CISO revealed, "The biggest lesson I've learned from using the solution is that security doesn't have to be difficult."

For the legal firm's Director of Information Technology Services, the return on investment in Axiad came from reduction in staff time and complexity. He commented, "The biggest lesson I've learned using Axiad Cloud is that it has really helped to highlight some of the mistakes we made in the past. In particular, we made the mistake of deciding to do PKI [Public Key Infrastructure] ourselves, rather than outsourcing it and doing it this way via a managed service."

> **"The added security has helped us mitigate quite a few breach attempts since the system was implemented."**
>
> **Read review »**

Helpdesk and Support Savings

Difficulties with authentication frequently translate into calls to the helpdesk. Users who cannot access apps and data because of authentication issues need support, which translates to real and opportunity cost. New, holistic, and integrated authentication solutions can address this problem and generate savings in support.

The transportation company's Senior Manager of Training Services put it this way: "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." Figure 1 depicts this process.

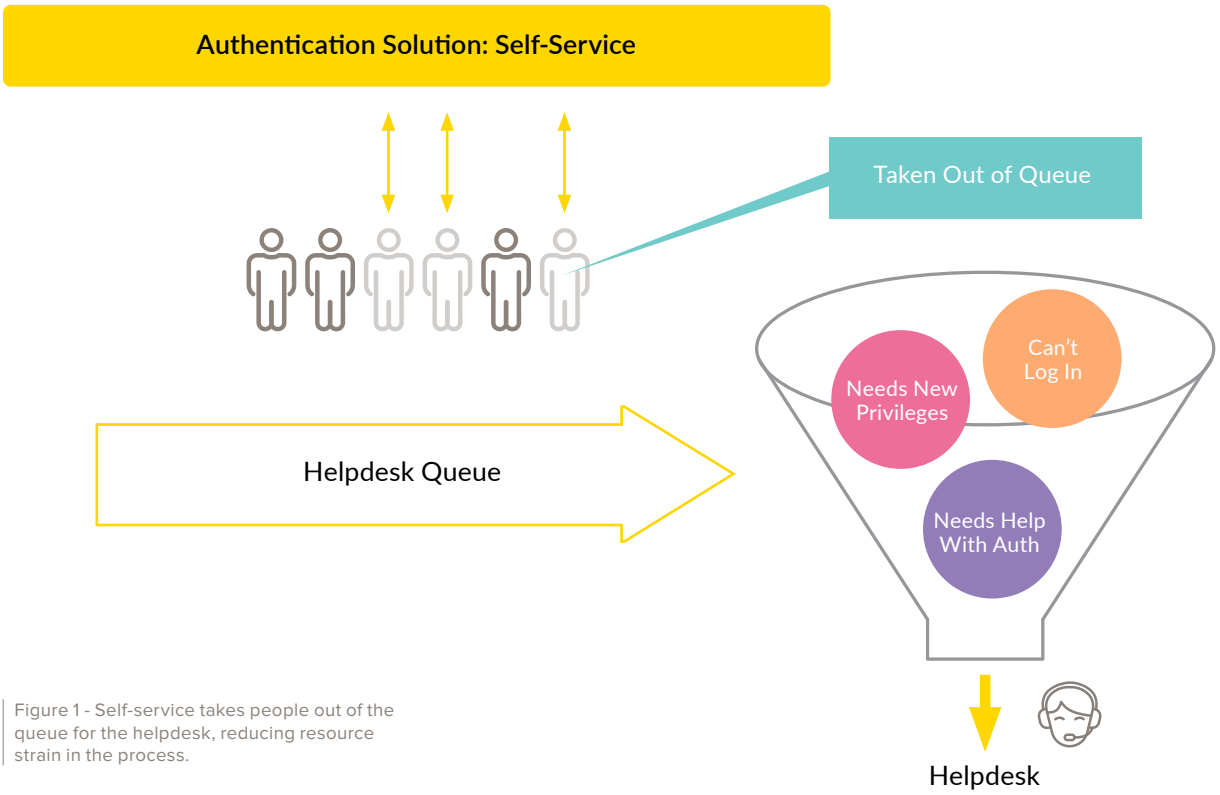


Figure 1 - Self-service takes people out of the queue for the helpdesk, reducing resource strain in the process.

This user elaborated further, noting that they have all of their users, except for administrative users, enroll through self-service tools. This includes executives. He added, "We felt so comfortable with the solution that they're enrolling themselves and re-enrolling their tokens when they expire. Also, our users required almost zero training once they were in the Axiad portal."

Other notable comments about savings in administration and support include:

- "It also empowers users to self-issue their authenticators and manage them over time and that's important to our organization. We don't want a help desk ticket every time somebody needs to issue a new authenticator or change one. The more that the users can do themselves, the better." - Enterprise Security Architect at a retailer

- "It has driven down the number of our calls. This, in turn, saves labor hours on both our service desk and on the users. At this point, our calls to the service desk for multi-factor have dropped by about 35%." - Cybersecurity Director - Enterprise Identity & Access Management at a software company

"It has driven down the number of our calls. This, in turn, saves labor hours on both our service desk and on the users."

Read review »

Qualities of an Effective Solution

What makes for an effective integrated authentication solution? PeerSpot members cite breadth of functionality, meaning that a solution can work with multiple authentication methods, as well as integration with multiple tools. Automation is important, as are usability and visibility. Users want control over credentials.

Breadth

A good authentication solution will work with more than one authentication method. The software company's Cybersecurity Director spoke to this need when he said, "Deploying and managing authenticators is very easy, either done by a mobile application or enrollment of an OTP token."

"Axiad overwhelmingly helps enable passwordless authentication for workstation log on, VPN, and cloud applications," said the legal firm's Director of Information Technology Services. For context, he pointed out that his company has about 3,200 smart cards in the form of E-tokens, which have a PKI certificate on them. They had been managing them through their own PKI but they are now moving that to Axiad. He added, "We have another 4,500 machine certificates for desktops, laptops, and servers, that we are also moving to Axiad."

> **"Axiad overwhelmingly helps enable passwordless authentication for workstation log on, VPN, and cloud applications."**
>
> Read review »

Multi-factor authentication through VPN, local endpoint access and Virtual Desktop Infrastructure (VDI) are the use cases that require multiple authentication methods for Horizon Blue Cross Blue Shield's CISO. He requires authentication, signing, and encryption. Figure 2 depicts this kind of breadth, with use cases like VDI and passwordless authentication being supported by authentication methods ranging from Fast IDentity Online (FIDO) keys to Trusted Platform Modules (TPMs).

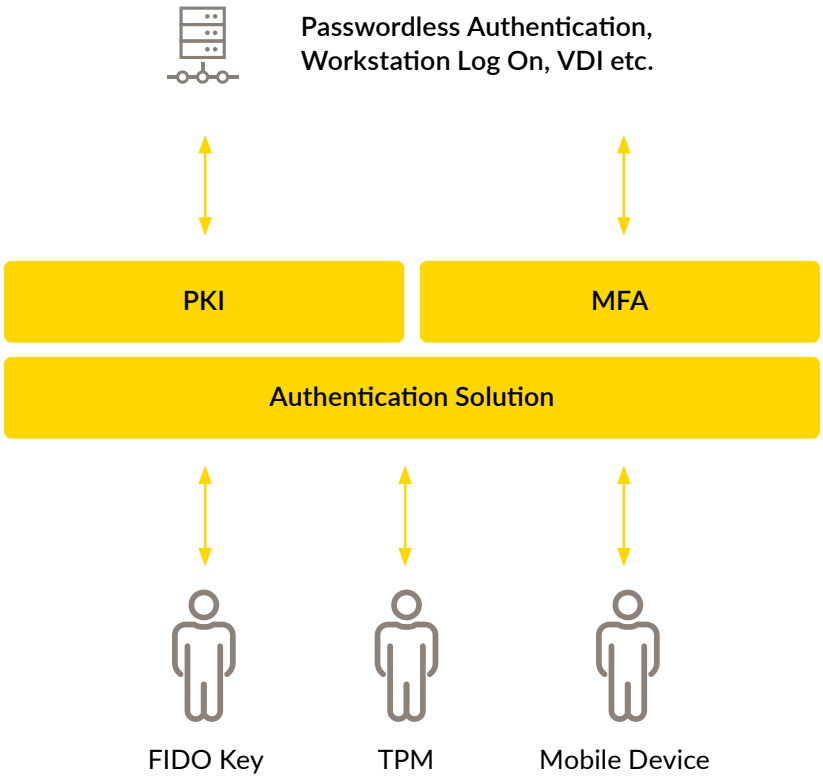


Figure 2 – An integrated, holistic authentication solution can handle multiple methods of authentication.

Integration with Multiple Tools

Authentication solutions are naturally part of a bigger ecosystem of security products. In most cases, organizations will have a variety of IAM tools in place that are delivering value. Security professionals do not want to rip and replace them. These might include access management, identity governance and administration, and privileged access management solutions – a web of tools often called the identity fabric of an organization.

Integration with multiple tools is therefore a "must have" characteristic for an authentication solution, as interoperability allows IT managers to fortify existing investments and supplement native tools instead starting over from scratch at every intersection point. The retailer's Enterprise Security Architect commented on this need, saying, "It is also the single platform to manage all the authentication requirements for our staff…and we're also going to extend it over the next couple of months..."

The software company's Cybersecurity Director similarly noted that Axiad Cloud provides passwordless authentication for everyone and every use case, including workstation log ons, VPN and cloud applications.

> "Axiad has saved us time...Just in the provisioning process it has saved us at least 200 hour."
>
> Read review »

Automation

Automation helps reduce the administrative burden of authentication, which can strain IT resources. According to the legal firm's Director of Information Technology Services, "Typically, our biggest service desk volume, about one-third of our calls, was related to authentication-specific issues with expired certificates or not being able to provide a challenge-response, or forgetting passwords. A lot of that stuff is now automated and democratized in the product so that users can do those things themselves. Axiad has saved us time, for sure. Just in the provisioning process it has saved us at least 200 hours, and that's a conservative estimate for one person and one part of the life cycle."

What mattered to the software company's Cybersecurity Director was that the solution could scale seamlessly through an automated process. He said, "In the mornings, when we have our highest user load, the system scales by itself in the back-end to handle the increased user load. Then, during the day, it scales back down to save resources." For context, his organization has 40,000 users. He added, "The solution is used and heavily integrated with all our multi-factor authentication entryways. We have plans to expand it to other devices and other platforms as well."

Visibility

Security managers and IT admins want to know what's going on at all times. They need transparency, and authentication is no exception. Solutions that offer visibility across the whole of the organization—across use cases, identity types, and operating systems—are particularly valuable because they help ensure that authentication is being done in a systematic fashion. To this point, the software company's Cybersecurity Director shared, "It enables users to self-issue their authenticators and manage them over time in a single pane of glass in a simplified platform."

> **"It enables users to self-issue their authenticators and manage them over time in a single pane of glass in a simplified platform."**
>
> Read review »

Usability

End user experiences count when it comes to authentication. Indeed, authentication is a process that users go through many times each day. If it is a hassle, or takes too long, users will attempt to circumvent it. The right authentication solution will help avoid user friction. The transportation company's Senior Manager of Training Services explained, "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."

Requiring almost zero training stood out as the solution's best quality to the transportation company's Senior Manager of Training Services. For the retailer's Enterprise Security Architect the most valuable aspect of the solution was that it was "very user-friendly."

Enterprise-Wide Passwordless Authentication

Control Over Credentials

Admins who are responsible for authentication do not want their credentials comingled with those from other organizations when they choose a cloud-based solution. Without airtight segmentation of credentials in a hosted solution, bad actors can gain access to an organization's keys simply by breaching another organization in the same system. In other words, one's credentials are only as protected as one's most-vulnerable neighbor.

The Axiad virtual private cloud ensures that an organization's credentials are segmented and under its control. This capability emerged as a valuable feature in the eyes of the legal firm's Director of Information Technology Services, who praised Axiad for having a private instance in a public cloud. Horizon Blue Cross Blue Shield's CISO concurred, noting the importance of Axiad running the backend in a cloud that is extended to his team via a lock-down connection.

Conclusion

Authentication is undergoing a profound change. Disconnected point solutions, or siloed approaches, are on the way out. Organizations are rethinking authentication, looking to a new generation of integrated, holistic solutions that make them more secure and operationally sound. As PeerSpot members who use Axiad Cloud have found, the solution drives improvements in security and end user experience. IT and security operations become more efficient. To get to these outcomes, an authentication solution must offer automation, work with a breadth of authentication methods, integrate with other tools and provide visibility into authentication workflows. As these factors come together, authentication becomes easier to manage and a more reliable factor in ensuring a strong overall security posture.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Axiad

Axiad delivers enterprise-wide passwordless orchestration to connect users and machines to data and applications from anywhere with a simple and secure integrated authentication platform. Unlike many approaches that are done in silos across multiple authentication methods, identity types, use cases, and existing IAM systems, Axiad allows customers to move to a passwordless future without the friction and risk of fragmented solutions.

By delivering a complete and holistic solution, Axiad helps organizations systematically authenticate across all people, devices, and operating systems, regardless of underlying IT complexity. This integrated approach helps organizations become more phishing resistant, prevent ransomware attacks/account takeovers, and take a critical step forward to implementing a Zero Trust. It also provides a balance between protection and usability – empowering end users to easily access what they need/when they need it, without compromising security.