

The Memos

Auth0

To: BVP Group
From: David Cowan, Sunil Nagaraj,
and Peter Lee
Date: June 28, 2014
Re: Auth0 Seed IR



On Monday, Auth0 co-founders Jon Gelsey, Eugenio Pace, and Matias Woloski will present from Menlo Park. The Seattle-based company bills itself as the "Twilio of identity" because it enables developers to outsource their identity and access management for their web and mobile apps. With just a few lines of code, SaaS vendors and enterprise developers can use Auth0's identity-as-a-service functionality to connect their apps to a variety of identity sources making it easier for end users to sign in. The team of 12 has raised \$850K to date and is generating \$10K of MRR from 75 paying customers. Though we met the company just two weeks ago, we accelerated our diligence because this investment fits well with our developer roadmap. Auth0 appeals to developers first and foremost with superior ease of use, technical documentation, and metered pricing. We moved quickly and were able to convince the company to let us invest \$1M of additional capital in their prior \$850K seed round which is effectively a convertible note with an \$8M pre-money cap. We have also negotiated a super pro rata right to take up to 1/3 of their Series A.

Product

Auth0 allows developers and enterprises to authenticate and authorize any application or resource with any identity store with just a few lines of code. As a result, they refer to themselves as the "Twilio for identity." Whereas Twilio makes it easy for developers to enable voice and SMS, Auth0 does the same for identity and access management (IAM). They provide an IAM system that runs in the cloud or on a managed VM behind the firewall. This allows developers to offload the creation and ongoing management of their apps' login/authentication modules while retaining best-in-class functionality and security. Auth0 sits between a developer's application and the systems that know about users. These systems, often called identity providers, include any of the following:

Microsoft Active Directory domain controllers that hold all information about an organization's users, passwords, and permissions

LDAP (lightweight directory access protocol) or SAML-based identity systems (SAML = Security Assertion Markup Language, an XML standard based originally on VeriSign's X-TASS protocol)

Social networks like LinkedIn, Google, Facebook, GitHub and others that allow "Connect with Facebook" functionality

A simple username/password table for credentials unique to a particular app



There are two categories of developers who would use Auth0. First, SaaS vendors, such as Adaptive Insight, can use Auth0 to allow end users to login with their company-internal credentials, a social login, or a unique username and password. This speeds their time to market and streamlines the user experience by eliminating another username and password to remember. Furthermore, the 30+ social logins available through Auth0 provide a 1-click experience and enable a rich user profile. The other category of developers that Auth0 targets are enterprise app developers who build a company's internal apps and want to quickly enable authentication in a complex identity environment. This also means that an app can authenticate partners, vendors, consultants without having to manage their usernames and passwords. In this way, Auth0 provides automated tools for quickly setting up identity federation.

To get started, developers sign up at Auth0.com, select their programming language and identity store, and receive a few lines of code. Once they add this to their app, they get a login widget that includes whichever identity providers they have selected. The example below shows a mobile app that has selected github, Google+, Windows Live, and an app-specific login option. Auth0 serves up the entire login widget including "signup" and "forgot your password" functionality. With a few clicks, this developer could add the ability to authenticate against a company's Active Directory server as well. Despite the variety of authentication options, developers get a single, unified list of all users, regardless of how those end users chose to authenticate. Auth0 normalizes this user data so that developers can depend on standardized user fields deeper in their app.

The image shows the Auth0 dashboard interface. On the left sidebar, there are several navigation items: DASHBOARD, APPLICATIONS, APIs, CONNECTIONS, USERS (which is selected), SDK, RULES, LOGIN PAGE, and ERRORS. The main content area is titled "Users" and contains a sub-instruction: "See who is logging in and when to all your applications. Login as any user for troubleshooting." Below this is a table with columns: NAME, EMAIL, LAST LOGIN, and LOGIN COUNT. The table lists five users: Don Draper (don@company.com, Today), Joan Harris (joan@company.com, Today), Peggy Olson (peggy@company.com, Today), Roger Sterling (Roger@company.com, Today), and Pete Campbell (pete@company.com, Yesterday). At the bottom of the table, there is some sample code for integrating the Auth0 widget:

```
<script src="auth0-widget.js"></script>
<script>
  var widget = new Auth0Widget({clientID:'2M7P0Or'});
  widget.signin();
</script>
```

To the right of the dashboard, there is a graphic of a white smartphone displaying a mobile login screen. The screen features a red star logo, social media icons for Facebook, Twitter, and Google+, and fields for Email and Password. A large blue button labeled "ACCESS" is at the bottom, with "SIGN UP" and "FORGOT YOUR PASSWORD?" links below it.

Developers love this level of abstraction so they can focus on building the internals of their app. We have also heard from developers that there are a lot of obstacles and risks to building their own authentication functionality. First, it is difficult to find developers who are knowledgeable about this topic. Several developers have told us that they see authentication as absolutely critical to get right as a single mistake or vulnerability could be highly detrimental. While some have tried to build it internally, they are never sure they are doing it the right way and incorporating the latest best practices. Furthermore, the landscape of identity providers is constantly evolving, be it Facebook changing their API, Microsoft patching an Active Directory vulnerability by changing its interface, or a new enterprise identity source coming online.

We spoke with one customer (Concurix) who estimated that building a basic version of this functionality could take 2 engineers a month or two to build initially and then require an engineer plus support staff on an ongoing basis for password resets and other issues. However, this customer (a small SaaS vendor) said that if their Auth0 bill exceeds \$50K/year, they might consider doing it themselves but noted that their real concern is a mistake or vulnerability in their authentication code (such as Heartbleed). This makes the true cost of DIY authentication much higher.

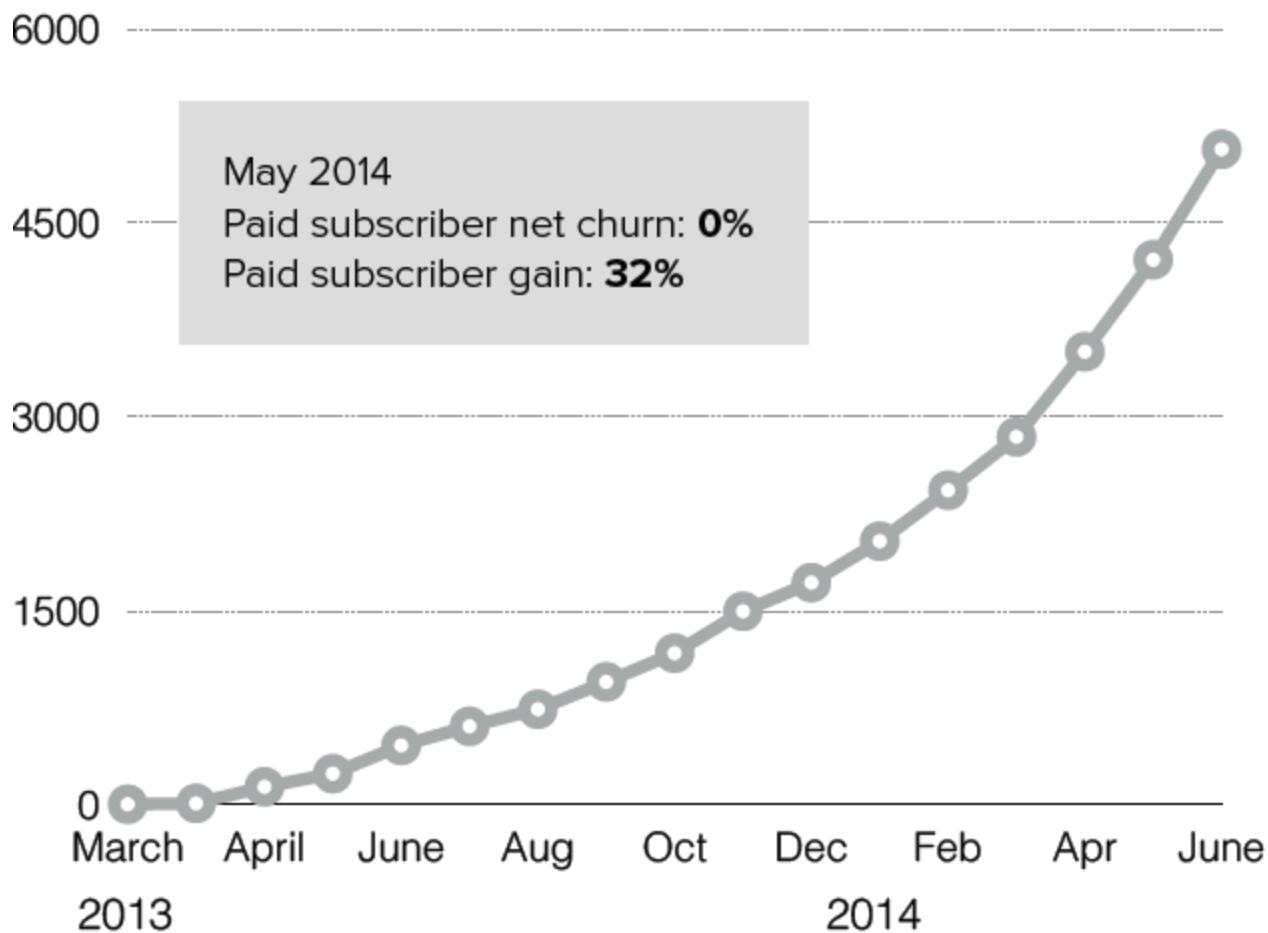
Beyond authentication, Auth0 provides several features that developers love including audit logs, analytics, outbound SSO (like Okta), and extensible rules. This last feature means that developers can use rules to extend the authentication pipeline to perform arbitrary operations: log activity to an external system; add extra validations on user access based on context such as date, time, device, network, application; etc. This gives the developer full control to execute additional authentication steps such as two-factor authentication. The Auth0 community has already created over 40 rules which are posted on their GitHub. One rule that has been popular is to create a new lead in Salesforce on first login. This rule calls Salesforce API to record the contact as a new Lead in the background when a new user signs up. Another popular rule performs "profile enrichment" by calling FullContact's API to fill in additional details on users based on their email addresses.

Auth0's current pricing is based on the number of applications and the number and type of users to be authenticated. The company is continuing to iterate on their pricing model.

	DEV	TEAM	PRO	MOST SELECTED
	\$ 0 per month	\$ 19 per month	\$ 99 per month	\$ 499 per month
	BASIC FEATURES	YOUR BRANDING	ENTERPRISE FEATURES	ENTERPRISE FEATURES
# of Applications / APIs ?	1	1	4	8
Active* Social Users ?	100	200	2,000	20,000
Active* Users w/ Password ?	50	100	1,000	10,000
Active* Enterprise Users ?	10	20	200	2,000

Traction/Financials

The company has generated an impressive amount of traction despite their early stage and small team. They currently have over 75 paying customers that generate \$10K of MRR at 90%+ gross margins. Though it is early, the company has had basically no churn in recent months as the v1 product has matured. Since launching, they have grown to almost 5,000 registered developers of which 350 are live and using Auth0 to authenticate users daily.



The company has not spent any money on advertising though they do regularly speak at conferences and events as thought leaders in the field. Since Jon Gelsey joined as CEO 6 months ago, we believe the company's growth has been inflecting with both self-service and enterprise customers. Currently the enterprise customers are Sancor Seguros (Argentina's largest insurance company with 4,000 users authenticating their insurance policy management and loss management apps with Auth0), FMI (a research arm of Novartis), TMZ (the media site), and The Journey (a national church). The customer pipeline is strong as well with a diverse set of large accounts in redlines right now.



Auth0 is currently doing \$5K in self-serve MRR and \$5K in enterprise/direct MRR, each growing at 15-20% a month. They currently have 71 self-serve customers and 4 enterprise customers. Based on accounts currently in the pipeline, they have visibility to a 2014 exit MRR of \$100K though we have not spent a significant amount of time vetting their pipeline. Their current plan is to exit 2015 at \$500K MRR based on 75 enterprise customers and 1,200 self-serve accounts.

We have spoken to several of their customers and they highlight a few common themes:

Auth0 has one of the sharpest teams in the identity space. Co-founders Eugenio and Matias are well known in the identity space and engender a tremendous amount of trust with their customers.

Customer support is off the charts. Every single customer (as well as many self-service customers on Twitter) rave about how fast and helpful customer support is.



@ Krzysztof Kozmic mentioned you

Krzysztof Kozmic @kkozmic 3d
I'm deeply impressed by @authzero support.

Yesterday I noticed a feature was missing. Spoke to support.

Today the feature is live.



Michele Bustamante @michele... 4d

Auth0 team is OUTSTANDING at customer support just OUTSTANDING @woloski

Their documentation is consistently cited as the best out there and a key reason developers chose to use Auth0. It is incredibly thorough and has deep code samples that automatically integrate your user keys so you can copy and paste snippets directly into your app. Their comprehensive and developer-centric documentation is a key reason that integration with Auth0 can take minutes to get up and running.

Team

Auth0 was co-founded by Eugenio Pace and Matias Woloski in February 2013. In January 2014, Jon Gelsey joined as CEO. The team is now up to 12, with Jon and Eugenio in Seattle and the rest of the team in Buenos Aires, Argentina. All but 3 are engineers.



Jon Gelsey, CEO – We have been impressed with Jon and the impact he has made in 6 months since he joined the team. He brings a diverse business background including 7 years at Microsoft in corporate development and 6 years at Intel Capital. We have found him to be very thorough and detail-oriented. Eugenio and Matias brought in Jon to serve as CEO and we believe he is the right fit at this stage.



Eugenio Pace, VP of Customer Success and Co-Founder – Eugenio may be the most impressive of the group as he is adept at the business and technology sides of Auth0. He can seamlessly transition from deep technical architecture to high-level business strategy. He brings 13 years of product experience at Microsoft, mostly leading the patterns and practices group of Microsoft which creates technical guidance for all Microsoft developers. Along with Matias, he wrote Microsoft's book on identity and federation and it is from this work that he came up with the idea for Auth0.



Matias Woloski, CTO and Co-Founder – We have spent the least amount of time with Matias but from what we know, he is the technical expert behind Auth0 and leader of the engineering team in Buenos Aires. He worked with Matias on his identity work as a Microsoft contractor. Prior to Auth0, he spent 8 years at a technology consulting company that created developer evangelism materials. It is here that he honed his technical skills and this is reflected in Auth0's ease of use and phenomenal technical documentation.

Competition

The core issue that Auth0 addresses is the tension between a heterogeneous IT landscape of legacy behind-the-firewall Identity and Access Management (IAM) systems (Active Directory, LDAP, etc. from vendors like Microsoft, CA, IBM, Oracle, NetIQ and others) and the rapid adoption of best-of-breed SaaS applications (Salesforce, Box, etc.) each with their own username and password schemes.

The rapid move to SaaS creates tension for both IT and SaaS vendors. IT struggles to maintain a consistent IAM policy across legacy and new applications (Which users have access to which applications, how do we enforce the right level of access, how do we retract access when an employee is terminated, etc.). Vendors struggle to support all the various flavors of enterprise IAM that IT needs, particularly when IAM is not a core competency, as described in the Product section.

The first wave of startups attacking this problem addressed IT needs first with a single sign-on (SSO) solution. Essentially an abstraction layer across SaaS applications, these companies raced to build app catalogs or portals, to allow IT to maintain a single set of credentials, and then federate those to as many SaaS applications as IT wished to support. On the vendor side, they urged the adoption of the authentication standard SAML, as a way of leveling out the field. In practice, SAML is implemented by only a fraction of SaaS vendors, and so Cloud SSO vendors often bundle sizable professional services contracts to build custom connectors for the long tail of apps.

Of this set, Okta is the largest, and primarily targets the enterprise segment. They just raised a \$75M Series E, with an estimated \$30M ARR at the end of 2013. (BVP uses Okta as our own internal SSO solution.) OneLogin is also doing quite well, aiming more at the mid-market, with an estimated \$10M ARR at the end of 2013. While there are several businesses rapidly gaining traction with this model, we've stayed away from making an investment here, as our ultimate view is that SSO will commoditize, and all vendors will ultimately support the full catalog of apps. (In our interviews with customers, while they confirmed the strong need for an SSO solution, they are already beginning to view SSO as a commodity, and expect to evaluate their next contracts primarily on price.)

On the SaaS developer side, while the more nascent space, there are several emerging players:

ForgeRock is one of the best-funded, having just raised a \$30M Series C. Led by former Sun employees, ForgeRock is focused on supporting the Sun Identity Stack, now open source, with a variety of services and training to help support the ecosystem. While a powerful IAM solution, the model is very different from Auth0, and less accessible to developers looking for a Twilio-like service to get them up and running quickly.

Stormpath is the closest in terms of model, with a similar developer-centric approach. However, after 18 months in market, they seem primarily web-focused at the time (Facebook, Google+, etc.) with limited traction of ~100 developers. They have just begun to add support for enterprise identity providers, so this is a competitor we continue to watch closely.

Gigya is an Israeli company that also delivers an IAM solution focused on social login; however, their target customer is the Chief Marketing Officer, with login support primarily used as a way to gather marketing and targeting data. This application is best suited for large consumer sites, with customers like ABC, CBS, CNN, etc.

For the SaaS developer market, we actually believe DIY will be the strongest competition. Particularly with no marginal COGS (unlike Twilio which bundles communications services) at some price point a SaaS vendor might be tempted to roll their own solution. Moreover, if only a few, high-value customers have a single identity system to implement, perhaps a DIY solution is not too difficult, or at least worth the cost savings. In the case where an enterprise has multiple identity stores however, the problem becomes much more difficult. The Auth0 team contends this latter scenario is much more common. Moreover, they contend that while the adoption of SSO solutions like Okta and OneLogin will help rationalize some of this heterogeneity, like many "standards" not all SAML implementations are the same, leaving developers to implement multiple versions anyway. Given our customer conversations to date, we're inclined to agree, but plan to confirm further with diligence.

Lastly, it is possible that as SaaS vendors mature in their needs, they ultimately "graduate" to an enterprise solution like ForgeRock, or need to extend the feature set beyond what Auth0 offers, but this has not yet happened. As detailed in the Product section, customers we've spoken to are quite happy with the solution, even in its V1 state, and the early cohorts are promising. We believe that Auth0 will grow with these smaller customers and continue to add functionality rapidly so these customers never consider more cumbersome enterprise solutions.

Risks

Competition – the IAM space is a crowded one with several legacy competitors going after lucrative enterprise contracts. We believe Auth0's focus on developers and rich documentation make it stand out among the audience of developers. This combined with the fact that our developer roadmap hinges on the increasing ability of developers to select critical technology components for an organization means that Auth0 should win in this space.

Market size – The company has enjoyed strong early traction with 75 paying customers, but we may find that the product only resonates with early adopters. The majority of customers may want a heavier weight solution and Auth0's message may get lost in the noise for them.

Technology – Is the current product, which has found traction with so many developers, complex enough to justify its existence? Will developers prefer to build authentication themselves? We have had this question with several of our developer roadmap companies, and the answer is almost always that developers want to focus on their core problem and outsource/abstract away everything else.

Deal

We have verbally agreed to invest \$1M in Auth0's prior seed round, along with a super pro rata right for 33% of the Series A. We are aiming to close by this Thursday 7/3. Last quarter, the team closed an \$855K seed round as a SAFE with an \$8M pre-money valuation cap. A SAFE, or "Simple Agreement for Future Equity", is a YCombinator-devised financial instrument that behaves much like a convertible note but the investment earns no interest and has no maturity date. This \$1M of capital, combined with the \$780K currently on the balance sheet, should take the company through the end of 2015 on a conservative plan. However, if the company achieves its top-line growth goals, we can expect the company to spend more aggressively and raise a Series A in early- to mid-2015. Just for historical context, Twilio raised its Series A with only about \$20K of MRR, though I believe that Sendgrid's MRR was much higher at the time of its Series A (it was already \$800k when we led the Series B).

Scenario Analysis

Outcome	Exit Value	Exit Date	Prob.	Seed		
				Gross Proceeds	Mult.	IRR %
Wipeout. Auth0 has team issues and falls apart.	\$0	Jun-15	30%	\$0.0	0.00x	-100.0%
Team sale. Auth0 is not able to attract more customers but the team's strong reputation drives a fairly attractive team sale to competitor	\$10	Jun-15	30%	\$1.0	1.00x	0.0%
Slow Growth. Auth0 grows from \$10K to \$150K of MRR (75 to 1,000 customers) but slower than planned. 25% add'l dilution from Series A.	\$30	Jun-16	20%	\$2.3	2.28x	52.2%
Strong Growth. The company becomes a leader in identity-as-a-service with 150 enterprise customers and 2,000 self-serve customers. 35% add'l dilution.	\$150	Jul-17	19%	\$9.9	9.90x	112.1%
Home Run. Auth0 powers identity for most SaaS vendors and enterprise app developers. Goes public at 8x 2019 revenues of \$125M (1,000 enterprise and 5,000 self serve customers). 50% add'l dilution.	\$1,000	Jul-19	1%	\$50.8	50.76x	117.0%
Weighted Average (to BVP)					3.15x	51.2%

Summary

Auth0 sits at the intersection of our cyber security and developer API roadmaps: with its strong vision, compelling team, and promising early traction, Auth0 could be the Twilio of identity. Our diligence has made us more confident that Auth0 is the ideal identity-as-a-service provider for a growing number of developers. We believe this \$1M seed investment represents an attractive opportunity to get in early and maintain ball control for the eventual Series A. We recommend BVP make this investment.

© Bessemer Venture Partners