Auth0's Approach to Information Security

Introduction

Auth0's commitment is to provide the best identity security solution possible to every enterprise subscriber. As a security company, every one of our employees understands their personal role in keeping our subscribers and Auth0 safe from security compromises, and every employee understands that our subscribers rely on us every day to protect their most sensitive data. We've built this trust over years through a defense-in-depth approach to security that both layers protections throughout our entire application stack and includes regular security training and exercises for every employee.

In this white paper, we will detail our approach to security so that our subscribers can better understand how their data is protected. The content in this document applies to both our multi-tenant cloud service and to Auth0 Appliance, unless otherwise noted.

Dedicated Security Team

Auth0 has a dedicated information security team, led by a director of security with nearly two decades of experience at organizations such as AT&T, Amazon.com, and the US Department of Defense. The team includes specialists in application security, infrastructure security, and cloud security—they are the "tip of the spear" whose sole responsibility is 24/7 vigilance and security process improvement to keep Auth0's subscribers safe.

People and Processes

All members of Auth0's workforce, including regular employees and independent contractors, are required to comply with internal security policies and standards designed to ensure compliance with law and with best security practices.

Background Checks

Auth0 has partnered with a third-party company to conduct background verification of the professionals who help the company achieve its mission. Employees, job candidates, and contractors have their identity, address history, professional standing, work history, educational history, qualifications, and criminal records scanned to determine eligibility for employment or ongoing employment with the company. We renew these background checks every five years.

Security Awareness

We institute a company-wide culture of security, starting from day one. During on-boarding, new employees and contractors are provided a set of documents and training videos that instruct them about Auth0's security policies, procedures, and recommended best practices. The workforce has to acknowledge reading and understanding the company policies at the time of hire, and then confirm this annually. Security awareness training is also conducted annually. To provide a reminder of the security threats that employees should be aware of, Auth0 conducts periodic phishing assessments that include an educational aspect.

Access Requests

Additionally, we've developed an internal access request and provisioning tool to handle and automate resource requests. Employees submit requests (via web app or a Slack bot) for various resources as needed to perform their duties. Each resource has an associated approval workflow which kicks off upon submission. Requests are only fulfilled once all approvers have signed off.

This system allows all access requests to be tracked and provides a reliable audit trail. For any employee at any given time, the system shows what resources they have access to, why they requested them, who approved it, and when. We follow the principle of least privilege and existing access is audited on a regular basis to ensure that employees only have the permissions necessary to perform their duties.

Security Policies

Auth0 has a comprehensive set of security policies, standards, and guidelines to ensure compliance and to guide our employees in making sound security decisions. Examples include:

- **Password Protection Policy:** Establishes a standard for how the workforce makes use of strong passwords, the protection of those passwords, and the frequency of change
- **Encryption Policy:** Provides guidance on the use of encryption to protect Auth0 information resources that store, process, or transmit Auth0 Confidential and Auth0 Restricted information
- **Monitoring Policy**: Describes the methodology and procedures for Auth0's monitoring of systems and data
- **Server Security Policy:** Specifies the system security requirements necessary to protect Auth0 information, computing, and network resources, and minimize susceptibility to attack

Privacy

Auth0 limits the private data we collect, and what we do collect is detailed in our Privacy Policy. Personal information is requested only when it is required to deliver expected services and to ensure that the company site and solutions run properly. When we analyze our subscribers' data, we use aggregated data pools to protect the privacy of individual subscribers.

For Auth0 Appliance—i.e., private SaaS running on the subscriber's premises—we collect telemetry and user activity metrics. This information is required to inform subscribers about subscription compliance.

In addition to the Privacy Policy, Auth0 is also certified and follows the rules laid out in the EU-US Privacy Shield. Privacy Shield allows compliant companies to transfer personal data from the European Union to the US. Among its principles, this system enforces that Auth0 must:

- Make clear to individuals what type of data is collected, and for what purposes
- Inform individuals of any third parties to whom their data will be transferred, their right to access their data, and the means for limiting the use and disclosure of their personal data
- Enable individuals to opt out of any disclosure of personal data to a third party or the use of data for a purpose other than the one for which it was initially collected
- Specify, in third-party contracts, that transferred personal data may only be processed for limited and specified purposes consistent with the data subject's consent
- Take reasonable and appropriate measures to protect data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Secure Product Development

Auth0 believes in the value proposition of zero-friction identity management that is both secure and reliable. For this reason, Auth0 has built a development process that requires minimal manual intervention, is constantly monitored, allows rapid response to issues, and encourages efficient software testing. The deployment of our products is done with common industry standard tools and follows best practices.

Specification Compliance

Auth0 implements proven, common, and popular identity protocols used in both consumer-oriented web products and in enterprise identity infrastructures.

The following are the specifications that Auth0 currently complies with:

- **OAuth 2.0:** an authorization framework that enables a third-party application to obtain limited access to resources the end-user owns
- **OpenID Connect:** an identity layer, built on top of the OAuth 2.0 framework, that allows third-party applications to verify end-user identity
- **SAML**: an XML-based framework for authentication and authorization between a service provider and an identity provider
- **WS-Federation:** a piece of the WS-Security framework that extends the WS-Trust functionality
- **LDAP:** an application protocol used for accessing and maintaining distributed directory information services over an internet protocol (IP) network.

Authentication Experts

Auth0 was founded and built by some of the foremost security and identity experts in the world: Matias Woloski, Eugenio Pace, and Jared Hanson. Matias and Eugenio have extensive security and identity backgrounds, including implementing federated identity projects for Fortune 500 companies, and are published authors. Jared is the author of the most popular authentication framework for Node.js: passport.js.

Code Review

All components developed at Auth0 are peer-reviewed by the workforce to ensure security, performance, and adherence to the company's principles and commitments. Also, a significant part of Auth0 source code is built on standard open-source components that are inherently subject to security review by the community of experts and software engineers who also use them. Auth0 contributes patches back to open-source projects whenever possible, but maintains custom forks if necessary to correct security flaws.

External contributions to the core of Auth0 are thoroughly reviewed by the Auth0 engineering team before being accepted and are subject to our network of automated test harnesses. This network verifies that the components are behaving as expected, through the use of unit tests, and that

systems are running and responding properly to our subscribers' needs, with the help of acceptance tests.

Development Tools

We provide tools to our developers to avoid common development mistakes and misconfigurations, including:

- A credential scanner to search our source code repositories for secret value leakage. The tool marks the change as problematic and alerts the responsible engineering team, who then respond and rotate credentials as necessary.
- An additional scanner that checks our applications for the use of vulnerable or outdated third-party modules and packages. Engineers are immediately notified so that they can complete the upgrade process.

Secret Management

The practices stated below apply to Auth0's public cloud and to private SaaS hosted by Auth0.

Software systems often need access to shared credentials. For example, a web application might need a database password to read and write some data, or an API key to communicate with a third-party service. Auth0 uses a combination of tools that has proved to be scalable securely and effortlessly:

- **AWS Key Management Service (KMS):** provides seamless, centralized control over encryption keys
- **CredStash:** a system that uses KMS and DynamoDB to safely store, distribute, and manage credentials in the cloud

White Hat Program

Auth0 has a Responsible Disclosure Program that encourages researchers to investigate the company's services and products. We encourage responsible vulnerability research and testing on the Auth0 services to which they have authorized access.

When a potential security vulnerability is discovered, the company works with the researcher to solve the issue before publicly announcing it. This practice helps guarantee that the entire community around Auth0—subscribers, partners, and employees—are not put at any risk while we address any potential security issues.

OWASP Compliance

The Open Web Application Security Project (OWASP) is an online community that creates freely available articles, methodologies, documentation, tools, and technologies in the fields of web application security. It was started in 2001 as a nonprofit organization and since its foundation has contributed a wide range of publications.

Auth0 has embraced most of the OWASP recommendations with regard to authentication and related topics. In order to comply with OWASP practices, the security engineering team has instituted a task force to conduct a detailed review of the current status of the company's solutions and to determine features that can be improved or added. As a high-level overview, Auth0 is addressing topics such as:

- Input Validation
- Whitelist Input Validation
- Client-Side vs Server-Side Validation
- File Upload Validation
- Email Address Validation
- Transport Layer Protection
- Protection with SSL/TLS
- Application Security Verification Standard

Deployment Process

Auth0's software engineers have crafted a mature deployment process that is based on proven open-source tools–like NPM, Puppet, and Jenkins–and reliable third-party solutions–like GitHub.

This process has enabled the company to:

- Control access to deployment processes and code per team
- Easily deploy and roll back service enhancements and patches
- Implement automated iterative deployment to limit blast radius
- Provide a clear audit trail of changes to code and deployment processes

Whenever a member of our workforce submits a change to our systems, the deployment process starts by running a "Build & Testing" phase. Handled by Jenkins, this phase validates if the change behaves as expected. Changes that passes the behavioral tests are then sent to our Continuous Integration (CI) tool that performs integration tests and security checks. Proposed changes that get validated by the entire deployment process are then made live through an application of our configuration management tool.

Auth0 Appliance subscribers, with solutions running on premises, also benefit from these updates. The difference is that this type of subscriber gets updates through packaged releases, which occur roughly once a month. These releases are applied at a time coordinated with subscribers. Appliances are updated from aprivate, secure Auth0 mirror that can be whitelisted through subscribers' firewalls.

Third-Party Compliance

At Auth0, we believe that independent organizations must review an organization's processes to determine that their solutions comply with specific standards for security, quality, and performance. This helps the company improve its practices, making them more mature with the oversight of external experts while also ensuring subscriber trust.

SOC II Type 2

A Service Organization Controls (SOC) 2 audits how SaaS companies like Auth0 manage their subscribers' data on five Trust Principles: Security, Availability, Processing Integrity, Confidentiality, and Privacy. A SOC 2 report may include just one of these principles or all five. Auth0 has been audited on the Security and Availability trust principles since 2014, when we conducted a Type I audit. Since 2015, we have been conducting Type II audits.

We are committed to maintaining our SOC 2 compliance in the future and to adding additional compliance regimes over time. Our SOC 2 reports are available to subscribers under NDA.

External Security Assessments

To ensure that Auth0 is shipping safe, secure products, we engage with trusted third-party consulting firms staffed by experts in application security and cryptography to review specific Auth0 products and components on a quarterly basis. We work to quickly mitigate any potential security issues that may be discovered. These assessment reports are also available to subscribers under the NDA.

Infrastructure and Data Security

Cloud Security

Auth0 depends on the public cloud, and securing the management of our cloud services is one of the security team's primary focuses. We monitor the use of management APIs, raising the alarm upon detecting suspicious activity. We limit the administrators who have access to our production environment and enforce the use of MFA. We regularly scan our accounts for configuration errors and continually make improvements to monitoring and controls.

Infrastructure as Code

Infrastructure as code, or programmable infrastructure, means writing code to manage configurations and automate the provisioning of infrastructure in addition to deployments. This approach enables faster response times to horizontal scalability and to unavoidable server issues. At Auth0, we adhere to this practice by using tools such as Puppet—a tested and proven system that manages various stages of the IT infrastructure lifecycle, including provisioning, patching, configuration, and management of operating system—to create and deploy new servers when needed.

Network Security

Our production networks are segmented to separate public services from internal services. Access to our production networks is controlled through a VPN with multifactor authentication (MFA). We also divide our services by geographical region with controls on what can move between them. We monitor and remediate any potentially unsafe network configurations, such as open security groups.

Security Monitoring

Security monitoring is the foundation of our security program at Auth0 and we monitor all of our infrastructure for security events. We collect logs from our internal server infrastructure and the external cloud services that we use. We centralize and analyze this data to detect potential security incidents, and any suspicious activity triggers an alert and is responded to by a security engineer.

Authentication

We mandate multifactor authentication (MFA) on all systems that support it. MFA is enforced for all tasks that require administrative or elevated privileges. Whenever available, solutions provided by third parties use MFA as well, preferably within Auth0's Single Sign-On infrastructure.

Data Encryption

Auth0 protects all confidential data using strong encryption. We never store passwords in clear text—they are always hashed and salted securely using bcrypt. Bcrypt is a proven algorithm and is considered one of the best choices for password storage. Both data at rest and data in motion are encrypted—all network communication uses TLS with at least 128-bit AES encryption. Qualys SSL Labs scored Auth0's TLS configuration A+ on their SSL Server test, and we regularly monitor this score.

Laptop and Mobile Device Security

All devices used by Auth0 employees, such as laptops and mobile devices, are encrypted and password-protected, which is enforced through a computer management solution. This solution enforces best-practices security settings such as screen lock, disk encryption, and a strong password policy.

Disaster Recovery and Backup

The Auth0 service has been designed from the beginning with redundancy at multiple levels, allowing it to adapt automatically to a number of different disaster scenarios, such as the sudden unavailability of a particular data center. The Auth0 service also makes use of established hosting providers, with sophisticated redundancy, to mitigate risks arising from individual server or disk failures.

The act of failing over from one data center to another, as well as any necessary Domain Name Service (DNS) updates, is automated and based on rules that make use of health checks.

Business Continuity Plan (BCP)

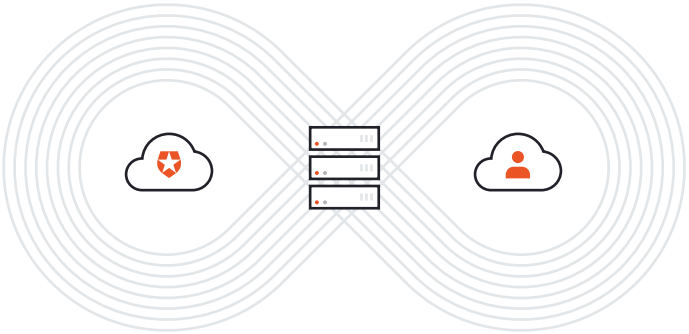
Emergency and nonemergency conditions can happen to any business, no matter how large and stable. At Auth0, we have developed a Business Continuity Plan that covers these conditions to ensure that the company will be able to continue supporting subscribers.
There are a wide variety of threats that could interrupt Auth0's ability to conduct its business. While it is impossible to predict every possible threat, they can be categorized and reduced into a finite set of potential impacts, allowing Auth0 to plan mitigations for each of these issues.

At a high level, the Business Continuity Plan approach to these threats is:

- Use SaaS solutions and hosting providers that provide continuity and redundancy of service locations and data backups
- Geographic dispersal of staff with flexibility to work anywhere with laptop and phone
- Cross-training of staff to ensure depth of skills and no single points of failure
- Ensure at least two known people have admin access to each SaaS service
- All critical data is stored in cloud services, rather than on individual laptops
- Redundant backups of critical data

Backup Strategy

There is always a risk that systems and procedures may fail, resulting in loss of access to information, data, and systems, despite the implementation of best practices. Auth0 has defined a mature approach to ensure that its information and data is backed up securely and frequently, and that its restoration occurs in the most timely and efficient manner possible.



The practices stated below apply to Auth0's public cloud and to private SaaS hosted by Auth0. Auth0 Appliance subscribers must maintain their own backup strategy.

Extensive documentation regarding backup and recovery procedures exists, and is updated periodically,. As a summary, these procedures outline that:

System engineers provide system support and data backup tasks to ensure adequate backup and system recovery practices

- All backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and system backup and recovery
- All infrastructure state data and supporting system configuration files are backed up systematically
- Access to backups is restricted to authorized personnel
- Regular tests are carried out to establish the effectiveness of the backup and restore procedures
- Records are maintained for any failures, detailing the backup job failure including any actions taken via an incident publication on Auth0's website

Vendor security

While the use of external service providers allows for increased efficiency, it also creates an additional responsibility to understand the security and compliance policies of the service providers. To guarantee that Auth0 complies with its certifications, like the EU-US Privacy Shield, and obligations to subscribers, the security team reviews vendor agreements that involve sharing sensitive data to ensure the vendor will respect our Privacy Policy and our subscribers' best interests.

Security Team Review

Any tools, projects, or vendor agreements that involve sharing sensitive data (intellectual property, proprietary source code, or subscriber data) must go through a security review before being implemented. When employees and/or contractors of the company need to use external solutions, they must fill out a form that thoroughly specifies all the details of the solution. For example, they must input:

- Why this solution and this vendor is needed
- The members of Auth0's workforce who will use the solution
- The list of Auth0's data and/or access that will be shared

With this information, the Security Team reviews the objectives, the members involved in the solution's usage, and what data will be exchanged with the vendor before deciding on whether to proceed with its implementation.

Privacy Considerations

As stated in our Privacy Policy, Auth0 may disclose personal information to certain types of third-party companies but only to the extent needed to enable them to provide their service. All third-party agents, performing services at our instruction and on our behalf pursuant to contracts, are required to provide at least the same level of privacy protection as Auth0 itself.

Subscribers may opt out of having their personal information transferred to any or all categories of agents by contacting us at privacy@auth0.com.

Summary

At Auth0, we have built state-of-the-art security into our products and processes so that subscribers can take advantage of cutting-edge features designed to make protecting users and businesses worry-free. We have based the entire company, its features, and its processes, on security best practices. Our systems and practices are compliant with industry standards, clearly demonstrating to our subscribers our ongoing commitment to security and privacy.