Auth0 Platform Security

auth0.com

Security Drives Auth0 Culture, Value and the Platform

Auth0 customers trust us for a crucial part of their business. As one customer put it, “Identity is Tier 0 mission critical service.” We understand that if we go down, you go down — and your job and your company’s success hangs in the balance. We also understand that Identity is the key to your business’ crown-jewels. Because of the significant stakes involved, we go above and beyond normal industry best practices to ensure an effective security posture.

We believe that the most effective posture is one that addresses the classic trifecta of people, process, and technology. But attackers are more sophisticated than ever, making it essential to also have an agile, secure-by-design, defense-in-depth approach engineered into our offering from the ground up. So we focus on embedding security at the beginning of key processes, into core engineering teams, and at an executive level as a strategic function that is responsible for critical, company-wide policies, decisions, and activities.

This means that we are more agile in response to risks and attacks and more aware of ways in which we can enhance security across every aspect of the business, while at the same time remaining effective for our customers. At Auth0, security enables our business. We embrace it as a company-wide mission and value.

As your trusted business partner, we not only believe in, but also act on, a policy of transparency and responsible, timely communications. We also hold others in our ecosystem to the same high security standards; ensuring that working with Auth0 means working with a vetted, secure solution and partner who understands that you expect a return on your security investment.

> The cost to build the identity solution ourselves would have been significant. We’re getting at least 50% ROI on the investment just for security alone.
>
> **Sung Ho Choi**
> fuboTV Co-Founder — Case Study

> We hadn't expected to be able to find a partner like Auth0 who would be so focused on security, proper authentication, and yet create a platform that's incredibly well-documented, easy to test, and is HIPAA compliant.
>
> **Narath Carlile**
> Chief Medical Information Officer, Act.md

Compliance

> Auth0's adherence to best-in-class compliance frameworks demonstrates our dedication to information security best practices across the board.
>
> **Joan Pepin**
> Auth0 CISO and VP of Operations

Auth0 commits to compliance as a way of transparently communicating our security posture to our customers. We maintain a dedicated compliance group within the Security organization who works closely with stakeholders across Auth0.

Auth0 has the following attestations and certifications:

- SOC 2 Type 2
- ISO 27001 and 27018

We are also compliant with the following regulations:

- HIPAA Compliant
- GDPR Compliant

People

At Auth0 we recognize that our employees are the cornerstone of our security posture, and security controls are most effective when they are supported by a robust security culture. As such, we engage our employees (and contractors) in a culture of security for the entire employee lifecycle, from the time they apply and throughout their time at Auth0. This culture includes:

- Background checks
- Training (Starting on day 1)

- Mobile Device Management
- Security as a dedicated, integrated function (the CISO and VP of Operations reports directly to the CEO as a peer to our CRO, CTO, CMO, etc.)

Product Security

Auth0's Secure Systems Development Life Cycle (SSDLC) ensures that security is incorporated from the inception of a new project and continued throughout the entire life of the system. The security of services and applications is important to maintain the reliability and integrity of data under the stewardship of Auth0. This has become increasingly important in recent years as applications become more complex, and the cost of remediating a vulnerability after release is often magnitudes higher than if it had been detected during the early stages of development. We write secure-by-design software, embedding product security engineers to work with engineering from ideation through release.

Auth0's SSDLC provides a single comprehensive risk-based process model that governs how engineering projects are planned, implemented and delivered to ensure the system functions securely and is fit for its intended use.

The scope of the SSDLC includes all systems development and integration projects used for and in support of the Auth0 service. Further, the process is applied to all project efforts associated with the development, implementation and maintenance of new and existing systems.

Security Monitoring

A core component of Auth0's security program is Security Monitoring. Auth0 has made strategic investments in our monitoring infrastructure to collect data from our services and infrastructure to our central SIEM for analysis and application of integrated machine learning and detection. Our Security Operations team are specialists in detection and responsible for acting on all security events.

To further ensure we review all critical security alerts, Auth0 has invested in a 24x7x365 eyes-on-glass Security Operations Center to monitor our SIEM and provide real time alerting to the Auth0 Security Operations team.

Incident Response

Auth0's Security Operations team maintains our Digital Forensics and Incident Response (DFIR) function. This includes an on-call rotation for responding to Security Incidents. Our Incident Response Process details a clear process for handling incidents, contains clear escalation paths to senior and executive staff members and is tested annually.

Vulnerability Management

Once software is released, we do automated vulnerability scanning on a weekly schedule of all our servers and instances.

Daily: All new instances are scanned as they are added to the production environment

Weekly: We have automated vulnerability scans for everything

At least every 6-months: We have third-party penetration tests

All new features: We perform end-to-end third-party penetration tests

Whitehat program: We have a Responsible Disclosure Program that encourages researchers to investigate the company's services and products.

Privacy and Personal Data

See our privacy policy

Learn more information about how Auth0 complies with GDPR

Learn more about how Auth0 helps its customers with GDPR

Access Control

At Auth0, we follow the principle of least privilege and its logical conclusion Zero Trust (providing employees with the minimal access necessary for their job functions, as well as applying that philosophy to software and infrastructure, such that no component of the system has more access than it requires to do its job). This is an important component of how we deliver defense-in-depth. Existing access is audited on a regular basis to ensure that employees only have the permissions necessary to perform their duties.

Secrets Management

The practices stated below only apply to Auth0's public cloud.

Auth0 follows best practice around secrets management, using a combination of tools that has proved to be scalable securely and effortlessly:

- AWS Key Management Service (KMS)
- CredStash

Data and Media Disposal

A customer may export customer data from the Auth0 Platform at any time during the subscription term, using the Auth0 Platform's then existing features and functionality. The customer is solely responsible for its data retention obligations with respect to customer data.

On customer's request or otherwise following termination of the subscription services, if and to the extent a customer cannot delete customer data stored on Auth0's systems using the then existing features and functionality of the Auth0 Platform, Auth0 will destroy the customer data in Auth0's custody or control.

Endpoint Protection

Auth0 employs specific endpoint protection tools depending on system type. Auth0 employs a broader philosophy around ‘defense-in-depth’ where multiple protections are in place and no single control is relied on to provide adequate protection.

Data Encryption At-rest and In-transit

Auth0 helps you prevent critical identity data from falling into the wrong hands. We never store passwords as clear text — they are always hashed and salted securely using bcrypt.

Certain data-at-rest and in-motion is encrypted — all network communication uses transport layer security (TLS) with at least 128-bit advanced encryption standard (AES) encryption.

The connection uses TLS, and it is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

DDoS protection

All Auth0 services have built-in rate limiting and automated blocking features to mitigate advanced denial-of-service or authentication attacks. The Auth0 network infrastructure is protected against volumetric attacks by their cloud providers, in addition to a dedicated DDoS mitigation service. Also, to protect the platform, the Auth0 system imposes rate limits on APIs and database calls.