Security at Affinity

Relationships are the backbone of the world's most vital industries but managing them is far from a perfect science. Affinity is on a mission to revolutionize the underlying tools and processes to better help your business manage its relationships. To do so, we need to make sure your data is secure; protecting it is one of our most important responsibilities. Affinity has designed platforms and applications to meet these requirements as well as exceeded relevant industry security protocols and standards.

We're committed to being transparent about our security practices and helping you understand our approach.

affinity

People security

All Affinity employees are required to understand and follow internal policies and standards. Background checks are performed to screen all employees. Security training is mandated as part of the onboarding process. Topics covered include device security, acceptable use, preventing spyware/malware, physical security, data privacy, account management, and incident reporting, among others.

Application security

Secure software development lifecycle

Standard best-practices are used throughout our software development cycle from design to implementation, testing, and deployment. All code is checked into a permanent version-controlled repository. Code changes are always subject to peer review and continuous integration testing to screen for potential security issues. All changes released into production are logged and archived, and alerts are sent to the engineering team automatically. Access to Affinity source code repositories requires strong credentials and two-factor authentication.

Secure by design

All features are reviewed by a team of senior engineers as soon as they are conceived. Members of the Affinity team have substantial experience working with and building secure technology systems. We believe in secure by design, hence we plan all functionalities with security in mind to protect the platform against security threats and privacy abuses.

We leverage modern browser protections, such as Content Security Policy (CSP) and security HTTP headers to prevent Cross-Site Scripting (XSS), Clickjacking and other code injection attacks resulting from the execution of malicious content in the trusted web page context.

Security testing

Once features are implemented, we perform internal security testing to verify correctness and resilience against attacks. We follow the leading Open Web Application Security Project (OWASP) Testing Guide methodology for our security testing efforts. Discovered vulnerabilities are promptly prioritized and mitigated. In addition, we regularly engage top-tier third-party security companies to independently verify our applications.

Authentication

Affinity allows users to login with Google accounts using OAuth 2.0, the industry standard for authorizing secure access to external apps without exposing their account credentials. Affinity does not receive or store user passwords when using OAuth. We implement the most secure version of the OAuth 2.0 authorization code grant to mitigate attacks that could leak the user’s access token. Both access tokens and refresh tokens are encrypted at rest using AES-128 encryption.

Affinity can also integrate with any SSO provider that supports OpenID Connect or SAML 2.0 as an authentication method. This includes but is not limited to Okta, OneLogin, Azure, Ping Identity, ADFS, etc. An impersonation or service account can then be used to give Affinity access to email and calendar data.

Affinity also allows users to login directly with their Microsoft Exchange account. We encrypt the credentials at rest using AES-128 encryption and in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.2). The credentials are only used to verify login and when communicating with the customer's Microsoft Exchange server using Microsoft's Exchange Web Services API.

All of the above authentication flows have been extensively tested against common attacks including but not limited to Cross-Site Request Forgery (CSRF) and misconfigurations of the redirect url by an independent security testing company. Users can further revoke access from Affinity at any time and request all their data in Affinity to be deleted.

Network security

Encryption in transit

To protect data in transit between Affinity's apps and our servers, Affinity uses SSL/TLS during data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. SSL/ TLS is further used to encrypt the traffic between Affinity servers and Affinity databases within the same datacenter. Affinity monitors the changing cryptographic landscape and upgrades its cipher suite settings as the risks change.

In our web application, we flag all authentication cookies as Secure and enable HTTP Strict Transport Security (HSTS) with "includeSubDomains" and "preload" enabled. Our web domain is included in the HSTS Preload list for all major browsers which is maintained at https://hstspreload.org/ Together with SSL/TLS and Affinity public certificates, HSTS prevents man-in-the-middle attacks and ensures that Affinity apps only communicate with Affinity servers.

Network isolation

Affinity divides its systems into separate networks using logically isolated Virtual Private Clouds in Amazon Web Services data centers. This setup protects sensitive data by providing isolation between machines in different trust zones. Systems supporting testing and development activities are hosted in a separate network from systems supporting Affinity's production website. Customer data only exists and is only permitted to exist in Affinity's production network, its most tightly controlled network.

Network access to Affinity's production environment from open, public networks (the Internet) is significantly restricted. Only network protocols essential for making Affinity's service work are open at Affinity's perimeter. All network access between production hosts is restricted using security groups to only allow authorized services to interact in the production network.

Our infrastructure and applications are monitored using standard health checks and log watchers. This helps detect systems that are malfunctioning as well as potential intrusions. Our on-call engineering team is responsible for investigating and addressing issues as they emerge.

Physical security

Data center security

Affinity leverages Amazon Web Services (AWS) data centers for all production systems and customer data. AWS offers state-of-the-art physical protection for the servers and complies with an impressive array of standards. For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Office and digital equipments security

A set of policies and procedures have been implemented to address the security posture of our workstations and laptops. All employee computers comply with these standards for device security. We require computers to have strong passwords, full disk encryption and automatic lock when idle. Even though no data is stored on employee computers or servers located in our office, Affinity's premises are protected with locked building entrances, deadbolted doors, CCTVs, and intrusion detection alarms.

Data security

We are committed to the goals of confidentiality, integrity, and privacy of our customer data by employing a multifaceted approach to data security.

Encryption at rest

All data at rest in Affinity's production network is encrypted using 256-bit Advanced Encryption Standard (AES). Affinity leverages AWS Key Management Service (KMS) to manage encryption keys. Keys are never stored on disk, but are delivered at process start time and retained only in memory while in use. The most sensitive customer data such as email bodies and access tokens are further encrypted in our database and in-memory storages such that the plaintext never exists on Affinity databases at any point in time. To ensure the security of our database, encryption keys are rotated regularly.

Employee access to customer data

No customer data persists on employee laptops. We apply the principle of least privilege in all operations to ensure confidentiality and integrity of customer data. All access to systems and customer data within the production network is limited to those employees with a specific business need. A best effort is made to troubleshoot issues without accessing customer data; however, if such access is necessary, all actions taken by the authorized employee are logged. Upon termination of work at Affinity, all access to Affinity systems is immediately revoked.

Audit trails

All actions taken to make changes to the infrastructure or to access customer data for specific business needs are logged for auditing purposes. In order to protect end user privacy and security, only a small number of senior engineers on the infrastructure team have direct access to production servers and databases.

Employee authentication

Every Affinity employee is provided with a secure password manager account and is required to use it to generate, store, and enter unique and complex passwords. The use of a password manager helps avoid password reuse, phishing, and other behaviors that reduce security. All access to the production servers and data is protected using network isolation and strong authentication mechanisms. A combination of strong passwords, passphrase-protected SSH keys, a Virtual Private Network (VPN), and two-factor authentication is used to shield mission critical systems.

Server hardening

Servers deployed to production, as well as bastion hosts used to access production servers, are hardened by disabling unnecessary and potentially insecure services, removing default passwords, and applying Affinity's custom configuration settings before use. We setup our systems following the Center for Internet Security (CIS) Benchmark recommendations. CIS Benchmarks are consensus-based configuration guidelines developed by experts in US government, business, industry, and academia to help organizations assess and improve security.

Vulnerability management

Affinity works with third-party independent vendors to perform automated vulnerability tests and manual pentesting on the production environment. We also tap into the broader security community via a private bug bounty program and offer incentives for researchers to responsibly disclose software bugs and centralize reporting streams. This involvement of the external community provides an independent scrutiny of Affinity applications to help keep users safe. Engineers are always on call to immediately address any discovered threats to our network.

We support vulnerability disclosure by taking responsibility for addressing product vulnerabilities in a timely manner. To encourage this practice, we provide the following Responsible Disclosure Guidelines: https://www.affinity.co/bounty.

Compliance

Compliance with applicable regulations, standards and industry best practices protect us and our customers' sensitive information in ways that are testable and verifiable. The following security-related audits and certifications are applicable to Affinity services:

- **Service Organization Control (SOC2):** Affinity has undergone a SOC 2 audit, and a copy of the most recent report is available upon request.
- **General Data Protection Regulation (GDPR):** Affinity has introduced tools and processes to ensure our compliance with requirements imposed by the GDPR. Our Data Protection Impact Assessment (DPIA) report is available upon request.

Affinity is hosted in Amazon Web Services (AWS) data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. More information can be found at https://aws.amazon.com/compliance/.

Privacy features

Affinity is built upon being able to view and understand how your team interacts with other people and companies. As such, Affinity provides various visibility features with conservative defaults that allow users to control how much information is shared with their team. Below is a small sample of such features:

Hidden persons

Users can choose to hide, from their entire team, all email and event interactions between their team and any person(s) as well as all profile information about that person(s).

Email visibility

By default, email bodies are only viewable by users who sent or received those emails. Email subjects, email recipients, event titles, and event invitees are viewable by all team members. However, users can choose to hide these from all team members as well.

List sharing

By default, a new list created by a user is only visible to that user (also known as the owner of that list). The owner can choose to let specific team members or the entire team view and manage the settings for that list.

The Affinity Privacy Policy can be viewed at https://www.affinity.co/legal/privacy-policy.

Disaster recovery and business continuity

Affinity customer data is regularly backed up each day to guard against data loss scenarios. All backups are encrypted both in transit and at rest using strong industry encryption techniques. All backups are also geographically distributed to maintain redundancy in the event of a natural disaster or a location-specific failure. Affinity uses third-party monitoring services to track availability, with engineers on call to address any outages.

Affinity is setup to operate from geographically distributed locations. By leveraging cloud resources, Affinity infrastructure and customer support teams can support your business at any time.

Conclusion

We take security seriously at Affinity. Customers using our service expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have, and we work hard to maintain that trust.

If after reading this whitepaper you have any further questions, please don't hesitate to contact our security team at security@affinity.co.