affinity

Affinity Security Practices

Introduction

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, and protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

People Security

All Affinity employees are required to understand and follow internal policies and standards. 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 by design

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.

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.

Affinity encrypts Microsoft Exchange credentials at rest using AES 256-bit encryption and in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS). Credentials are only accessed when communicating with the customer's Microsoft Exchange server, which happens either during the standard IMAP authentication process or when connecting to an exchange server using Microsoft's Exchange Web Services API.

Users can 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 the cipher suite choices as the landscape changes.

Additionally, on the web, 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/. HSTS, together with SSL/TLS and Affinity public certificates, 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 better protects sensitive data by providing isolation between machines. 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 restricted. Only network protocols essential for delivery of Affinity's service to its users are open at Affinity's perimeter. All network access between production hosts is restricted using firewalls to only allow authorized services to interact in the production network.

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 security

All employee computers comply with our standards for security. These standards require all computers to have strong passwords, encrypt data on disk and lock when idle. Even though no data is stored on employee computers or servers in the office, Affinity's office itself is protected with locked building entrances, deadbolted doors, CCTVs, and intrusion detection alarms.

Data Security

Encryption at rest

All data at rest in Affinity's production network is encrypted using 256-bit Advanced Encryption Standard (AES). The most sensitive customer data such as email bodies is further encrypted in our database such that the plaintext never exists on Affinity database servers at any point in time. Affinity uses the 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. To ensure the security of our database, encryption keys are rotated regularly.

Employee access

The Affinity Privacy Policy can be viewed at https://affinity.co/privacy and is strictly adhered to by all Affinity employees. No customer data persists on employee laptops. 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 employee are logged. Upon termination of work at Affinity, all access to Affinity systems is immediately revoked.

Audits

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 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 a combination of strong passwords, passphrase-protected SSH keys, a Virtual Private Network (VPN), and two-factor authentication.

Server hardening

Servers deployed to production, as well as bastion hosts used to access production servers, are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying Affinity's custom configuration settings before use.

Vulnerability Management

Affinity works with third-party vendors to perform automated vulnerability tests on the production environment. We also tap into the broader security community via a 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.

Penetration testing

Affinity engages independent third-party entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with our security team as well as with Affinity management, and all findings are reviewed, prioritized, and tracked to resolution, including third-party verification of resolution.

Compliance

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.

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.

Conclusion

We take security seriously at Affinity, because every customer using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust. If after reading this whitepaper you have any further questions, please don't hesitate to contact us at security@affinity.co.