Product Sheet

Security and Architecture

Your data is one of the most important assets of your business. You need to trust that it is handled securely and is available to you whenever you need it. We understand this and have implemented technologies, processes and procedures that are designed to ensure your data is protected when you use Act-On.

Here's how we do it:

Architecture

The Act-On solution is a Software-as-a-Service (SaaS) based web application served from a hybrid cloud infrastructure. It is built using industry standard components which provide security and resiliency with minimum downtime. All connections within the application, between its components and stored credentials are protected via encryption and firewalls. Our API access is achieved through secure REST calls. All customer account data is isolated and protected from access by other multi-tenant accounts. All multi-tenant data is partitioned logically and isolated to prevent unauthorized access.

Data Centers

We host our application (and your data) in toptier data centers located in the United States, Germany and Ireland. These data centers implement the highest standards of security including:

- Maintaining accepted security certifications such as ISO 27001, SSAE 16/SAS 70 or similarly recognized standards
- Restricted access leveraging biometric scanning
- On-site security personnel
- Security camera monitoring and intrusion detection
- Redundant HVAC (Heating Ventilation Air Conditioning) units to ensure that temperature and humidity remain consistent
- Monitoring, alerting and suppression systems in the event of smoke, fire, water or similar threats
- Back-up power with immediate failover
- Distributed Denial of Service (DDoS) mitigation services

Administrative Controls

Act-On implements and maintains stringent controls on accessing our customers' environments and data. This includes:

- Limited access to customer data to authorized personnel only and according to documented processes
- Logging and tracking access to our SaaS servers to enable auditing
- Ensuring that all employees who are provided access have passed extensive background check as a condition of employment and are bound to protect our customers and their data

Act-On customers designate which of their employees will have access to the organization's instance of Act-On. Customers can designate permission levels based on log-in credentials. By default, only the administrator and all designated marketing users share full access to all creative assets and content within Act-On.

Email Authentication

Act-On sends all mail with DomainKeys Identified Mail (DKIM) authentication. DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication. This is an industry best practice to establish sender identity.

Backups and Redundancy

Act-On applies a daily automatic backup that is maintained with daily snapshots for recovery offsite for 30 days. To satisfy data privacy requirements, backups are never sent out of the country in any of our data centers. Act-On applies automatic HA fail-over for data storage and network fabric.

Our infrastructure is redundant meaning that there is a back-up component for each piece of hardware that stores data. All network devices, including firewalls, load balancers, and switches are fully redundant and highly-available. High availability for Internet connectivity is ensured by multiple connections in each data center to different ISPs.