RESULTICKS

# Cloud security and Governance


## Standards and protocols

## Audits, certifications, and compliance

## Data security

**Regulating data access, storage, and transmission**

### Transmission

Use of 256-bit SSL encryption during Internet transfer, secure web service, and controlled VPN connections restricting direct exposure of Resulticks environment

### Encryption

Multilayered 256-bit encryption using a combination of registry key, DLL key, and an account-specific encryption key

### Authentication

Multi-factor authentication including user credentials and OTP verification to download data files from the system

### Obfuscation

Key profile data that is masked on storage as well as on display to maintain confidentiality

## Application security

**Ensuring authenticated and authorized access to the Resulticks platform**

### Authentication

Secure login after multi-factor authentication that includes individual user credentials, encrypted passwords, and captcha mechanisms

### Data hosting

Customer data is hosted on servers with non-routable IP addresses (private), which combine with next-gen firewall and NAT to eliminate potential vectors of internet attacks

### Authorization

Multiple user roles with access control to leverage modules, features, and data

### User logging

Automated capture of all user activity, exceptions, errors with time, activity type, source IP, and other transactional information

## System security

**Protecting the software modules, resources, and configuration**

### Geo-fencing

Ensuring storage of data within respective physical zones (e.g., APAC, EMEA, the Americas)

### Disaster recovery

Tested business continuity plans that includes a data center physically remote from the primary center with restoration services

### Network security

Enabling network access protection, segmentation, and encrypted communication to prevent unauthorized access

### Activity logging

Documentation of activity around system components providing date/time, activity type, source IP, and other transactional information

### Segmentation

Resulticks network is segmented as a single protected entity to increase safety

## Infrastructure Security

Securing the physical servers and data devices that enable the platform at the backend

### Controls

Strong firewall, restricted IP access for administration and notifications from servers, authorized personnel access only

### Protection

Powerful anti-spam, anti-virus controls, and network-based intrusion detection mechanisms

### Data centers

SOC 1 and SOC 2 certified, SSAE 16/ISAE 3402 attested, biometric protected data centers with 100-percent power backup facility

### Established workflows

Established workflow and streamlined prevention procedures activated for newly detected threats across devices and channels to avert unauthorized access

**Learn what Resulticks can do for your brand.**

REQUEST A DEMO