Seerist Platform Security Overview

Seerist (“we”) provides Seerist CORE for our clients (“you”). It provides incisive analysis and forecasting on geopolitical and security issues, a series of country risk ratings and an extensive database of incidents. Coupled with visualization and analytics tools, these help you make informed business decisions and plan operations in confidence.

This document explains what information we hold and how we secure the information.

The information we hold about your users

Personal data is collected direct from a data subject when they create their own profile and account for the purpose of accessing Seerist CORE content through the website or mobile application.

Login process

Our preferred method for your users to log in to Seerist CORE services is to use Single Sign-On. We implement SSO (Single Sign-On) using SAML version 2 (Security Assertion Markup Language). In simple terms, it works as follows:

- When a user attempts to log on to our service, the user’s browser session is redirected to your domain to be authenticated.
- If the user is not already logged on to your domain in that browser instance, your authentication service will prompt them to log on by their usual method.
- If successful, or if already logged on, your domain will send back a secure message which the browser then passes to our online systems, to confirm that the user in question has authenticated. We ONLY see the user’s email address as a default, although you can optionally also include first name and last name in the response message if you choose to.

Note: In SSO, we do not have internal access to your network or directory service. We do not extract a list of valid usernames or email addresses – we only receive an email address when a user logs in successfully. The user’s password is not visible to our systems.

We also support hosting accounts for your users within the Seerist service. Accounts that are hosted within the Seerist service enforce strong passwords (better than 8-character with complexity), and lockouts after repeated failed attempts to log in we also monitor lists for compromised accounts.

How we secure your information

Our strong set of security measures covers the people, process and technology required to assure the confidentiality, integrity and availability of information. It includes policies; screening and training of our people; defined and audited processes; and extensive technological controls such as encryption, segmented data stores, data backups, firewalls, network and communication security, two-factor authentication, and continuous monitoring.

We have well defined security policies that include analysis of risks and legislative requirements, and assessment and implementation of appropriate mitigations on an ongoing basis.

Hosting

- Our Seerist Platform is hosting in Amazon Web Services, which maintains 140+ security standards and compliance certifications. These establish adherence to strict security controls and procedures. AWS staff are security-screened as standard. Further information on AWS security is available at: https://aws.amazon.com/compliance/.
- We manage Seerist Platform in AWS through a private cloud ensuring the service is self-contained.
- Physically, we utilize AWS regions in Northern Virginia, Ohio and Oregon in the United States.
- Physical access to the data center locations by tenants is not permitted. Only AWS data center technicians are able to access the data halls where the infrastructure is located. Access to physical data center facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations center. Premises are also protected by fire alarms and fire suppression systems.

Seerist Platform Security Overview

Infrastructure and security

- Seerist Platform has various technologies to protect the services, such as web application firewalls, DDOS protection, malware protection and monitoring agents.
- Seerist Platform is only hosted over HTTPS providing end-to-end encryption in transit between the client browser or mobile application and the Online application service.
- All components of the Seerist Platform housing customer data are encrypted at rest.
- Seerist Platform is penetration/vulnerability tested at regular intervals by third-party testing companies.
- Security patches are applied on a regular defined schedule each month ensuring that the latest vendor security patches are implemented.
- Out of band security patches that are released outside of vendors' normal release schedule is assessed and applied as required.
- Software changes are peer-reviewed and security scanned before deployment.
- Remote management access to Seerist Platform infrastructure is restricted to a defined list of employees, each with individual access accounts audited on a regular basis. No use of generic access accounts is permitted. Accounts are MFA protected.
- All components of Seerist Platform are highly available, providing redundancy at all layers in the event of individual service/system failures.

Access controls - your end users

- Access control for your employees is explained in the Login Process section above.
- Users have one level of access – All users can access to view content and edit their searches and notification settings.

Access controls - our users

- Access control for our own employees is via SSO to our directory service with Multi Factor Authentication (MFA) which allows for central control and management. Access is at two possible levels:
  - **End-user** – All Seerist employees have this access by default, to enable them to access our own research. This level gives them the same access as your users, but not to any of your data.
  - **Administrator** – Can manage End-users and their profiles across all clients.
- Our directory service enforces strong passwords and lockouts after repeated failed attempts to log in.

If you have any further questions with regards to the security of Seerist Platform, please do not hesitate to contact your Seerist account manager or reach out to us at help@seerist.com