PreEmptive Solutions

PreEmptive Privacy & Security
Fact Sheet

Application owner and end-user security and privacy have been a central theme of PreEmptive Analytics design and development since its inception. The following is a summary of PreEmptive Analytics security and privacy capabilities and safeguards.

Data Collection

Application Instrumentation:

Activation: No "accidental" or "inadvertent" application monitoring. Application instrumentation is typically accomplished through post-compile injection. The default setting is "off." This capability must be manually activated avoiding "accidental" application instrumentation.

Configuration: No data, other than what is explicitly requested by development, is ever transmitted. Once "activated," each individual data component must then be explicitly identified for data capture.

Opt-in

PreEmptive Analytics "opt-in" requires a Boolean "True" value to be set before any data monitoring functionality is initiated (which is prior to transmission). The default value of this setting is "False" and must be explicitly reset by the application at the start of every application session. There are, in fact, two opt-in settings.

- **Application usage:** opt-in covers session, feature and system data previously identified by development prior to deployment.
- **Exception monitoring:** opt-in covers unhandled, caught and thrown exception data previously identified by development prior to deployment.

Privacy Policy

PreEmptive Analytics permits development to encode a link to the company's own privacy policy that can be communicated to an end-user prior (or during) a request for an informed opt-in.

Data Transmission

SSL Encryption: by default, all data transmitted from an application to an endpoint is first encrypted before transmission. This can only be overridden by development prior to the release of the application.

Data Storage and Access

In every case, runtime data collected for management and analysis is owned by the development organization. PreEmptive Solutions has no access (other than is required to ensure the proper functioning of the managed service) and no rights to reuse runtime data – either in part or in aggregate.

On-premises: Endpoints that are "on-premises" or "client-managed" are completely under the development organization's control.

Managed service: Data managed by endpoints owned by PreEmptive Solutions are managed solely for our clients' benefit. There is no other access or use authorized or permitted.

Application Security

In addition to the thorough, "end-to-end," approach to information security and privacy, PreEmptive Solutions also provides technology and associated controls to minimize the risk of application reverse engineering or tampering that may lead to the disclosure of application vulnerabilities that can be exploited or the tampering (modification) of applications to alter its behavior (to introduce exploitable vulnerabilities where none had previously existed). These include:

- **Preventative controls:** Obfuscation prevents reverse engineering and recompilation.
- **Detective controls:** Tamper detection and defense provides real-time defense and alert notification when application tampering (modification post-compile) has been detected.

Taken as a whole, PreEmptive Analytics provides the industry's most complete and comprehensive application analytics security and privacy solution – built to encode and enforce the wide variety (and ever-evolving) application and information security and privacy policies, mandates and controls.

PreEmptive Solutions
Visit us at www.preemptive.com

Worldwide Headquarters
767 Beta Drive, Suite A
Mayfield Village, OH 44143
Phone +1 440.443.7200
solutions@preemptive.com

European Headquarters
140 bis rue de Rennes
75006 Paris, France
Phone +33 01.83.64.34.74
eurosolutions@preemptive.com

Find us: f in You Tube