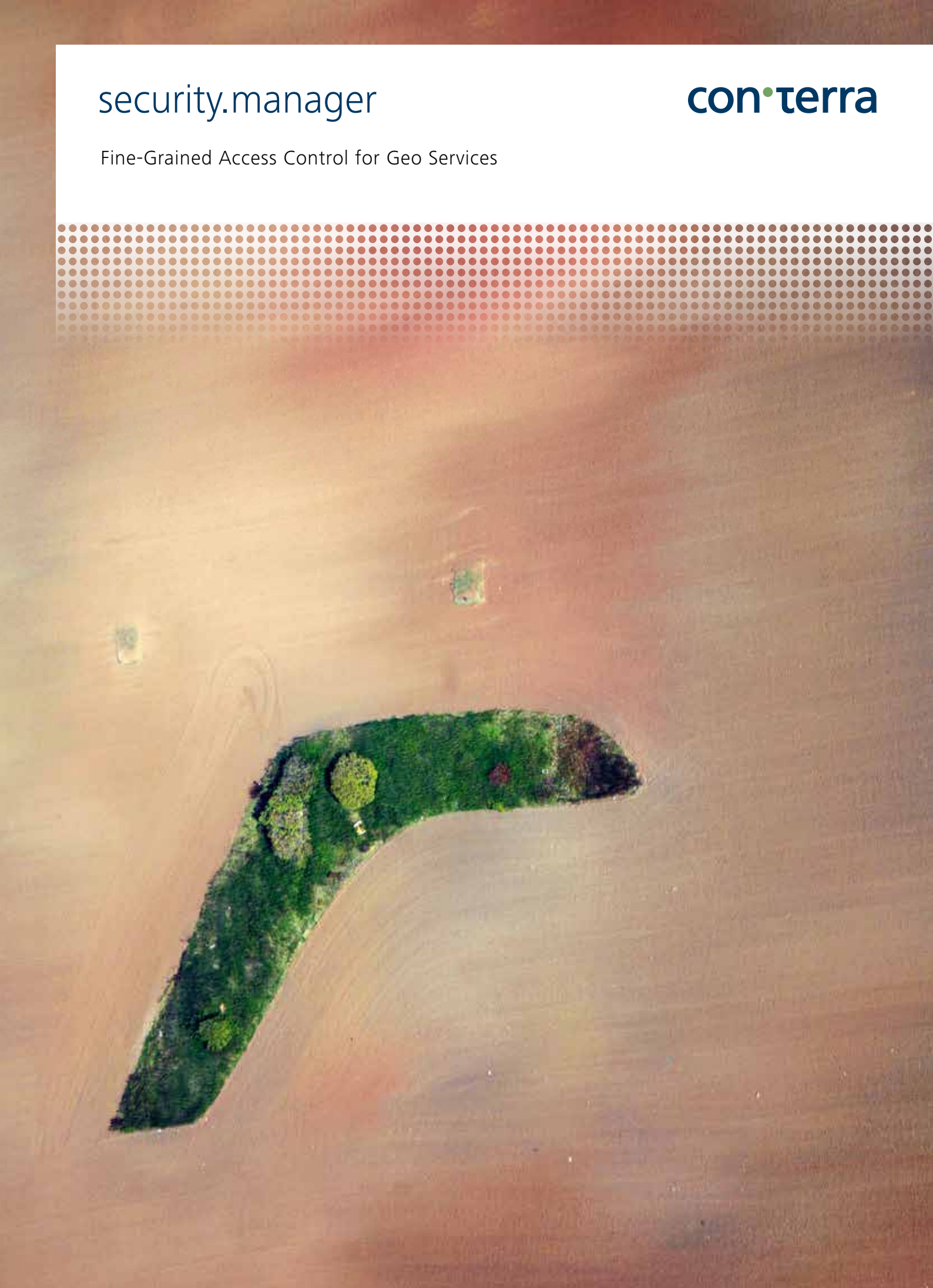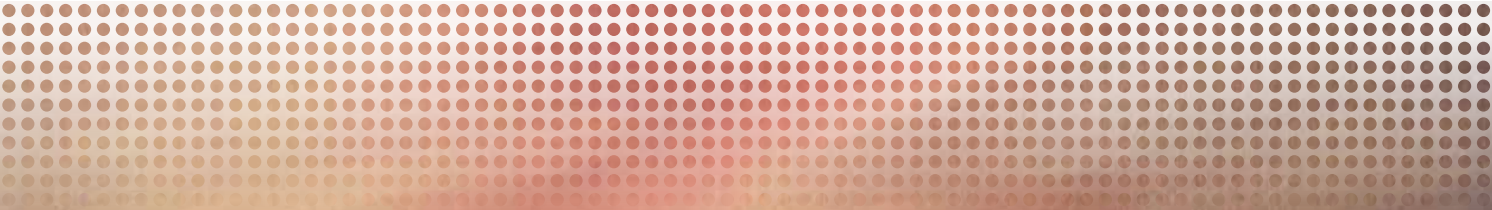# security.manager

Fine-Grained Access Control for Geo Services

con·terra

Fine-Grained Access Control for Geo Services

security.manager allows the assignment of individual access permissions to different user groups, thereby ensuring that everyone gets access only to what they are entitled to.

Decide who shall see what

security.manager controls access to services, right down to feature and attribute level. While a service is published only once, security.manager can enable different views for different users, by limiting access according to a user's rights. In doing this, security.manager provides a consistent user experience together with a holistic security approach. This means, users will not get any information about the existence of content they are not entitled to, and permissions need to be explicitly expressed in the system. Everything that is not allowed by a policy is automatically forbidden, to ensure that access cannot be granted by accident.

Security at your fingertips

The administration process for security.manager relies on a browser-based rights editor that allows for the definition of rights, easily and fast. It takes just a few clicks to assign permissions for resources, and a few more clicks to create additional filters on feature, attribute or spatial level. Once a right is created, it is already active, and access is granted accordingly.

Seamless integration

The beauty of a good security system lies in its transparency. A user working with a service protected by security.manager will not even realize that security measures are in place. Adding security.manager to a service will not change the user experience, nor will it have a noticeable impact on performance. Users will work as they do with every other service, just in a limited way.
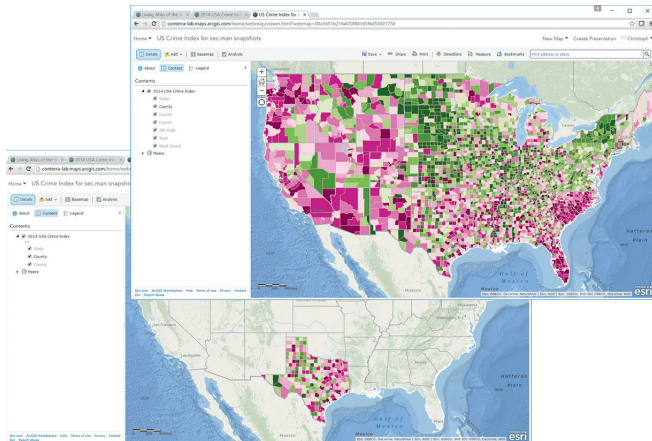

Two editions, one concept

con terra security.manager is shipped in two editions:

- security.manager Enterprise Edition
  The Enterprise Edition has been in the market for more than ten years. During this time, it has grown to a mature and widely used GIS security system, offering a full set of capabilities. Besides controlling access to services, it provides many integration possibilities for enterprise IT landscapes. It can connect to existing user repositories, provides cross-application and cross-domain single-sign-on based on SAML 2.0, supports multiple authentication methods up to the Windows log-in and can protect different service implementations, including ArcGIS and OGC services, etc.

- security.manager – ArcGIS Edition
  ArcGIS Edition works right in ArcGIS for Server. Being implemented as a Server Object Interceptor (SOI), security.manager – ArcGIS Edition is not added to, but is integrated into a service. Deployed as an extension, it also integrates seamlessly into the ArcGIS Server Manager application, in order to extend the authorization capabilities of ArcGIS for Server.
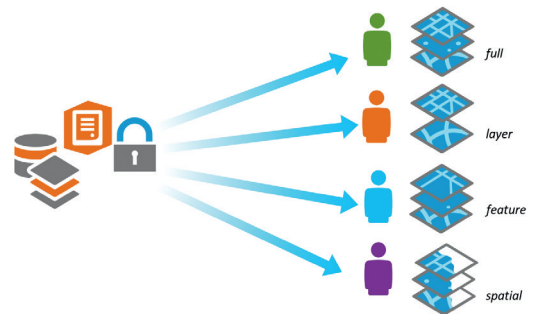
Benefits

- Extend GIS systems with enhanced security options
- Provide individual views without deploying several services
- Embed security easily into existing infrastructures
- Manage permissions conveniently in the browser
- Incorporate existing user repositories
- Rely on mature technology