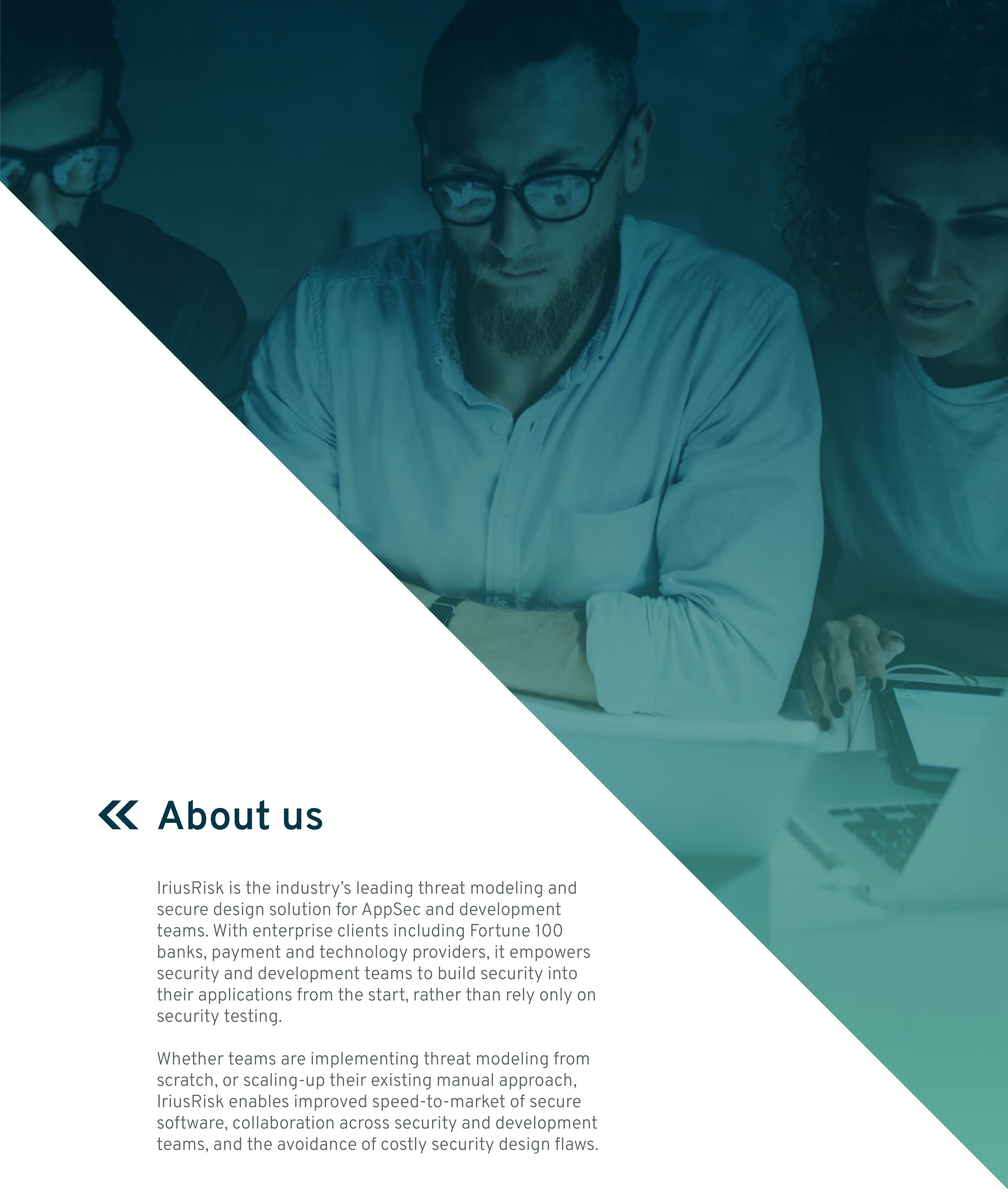
Secure Design at scale

IriusRisk



« About us

IriusRisk is the industry's leading threat modeling and secure design solution for AppSec and development teams. With enterprise clients including Fortune 100 banks, payment and technology providers, it empowers security and development teams to build security into their applications from the start, rather than rely only on security testing.

Whether teams are implementing threat modeling from scratch, or scaling-up their existing manual approach, IriusRisk enables improved speed-to-market of secure software, collaboration across security and development teams, and the avoidance of costly security design flaws.

Meeting the needs of security and development

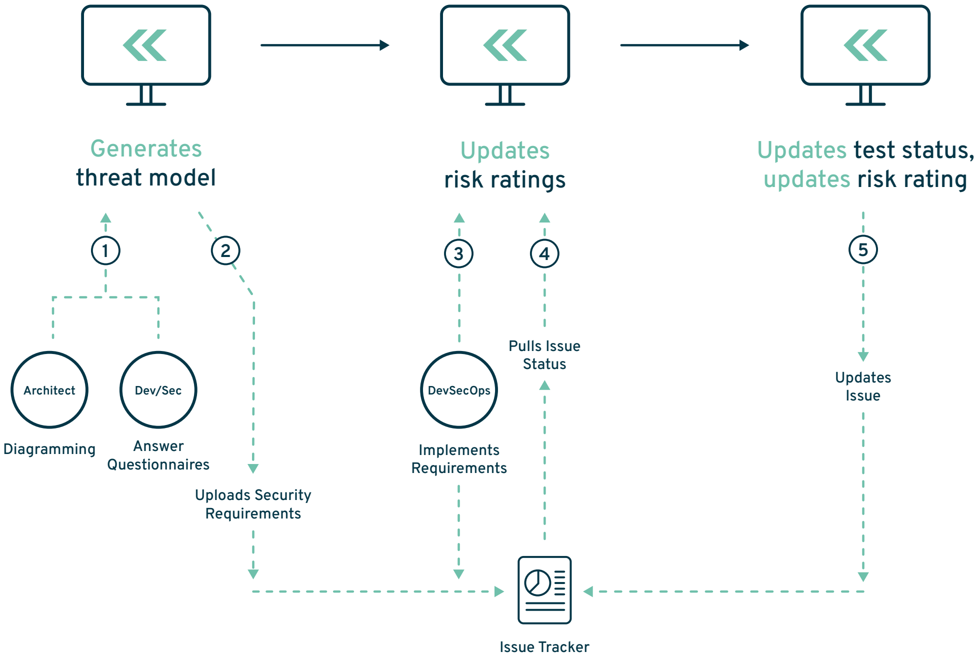
Keen observers will have noted an uptick in activity around threat modeling within the information security community. With new tools being introduced, strategies, and methodologies being discussed, what are the implications for the architectural, development and security teams within your organization?

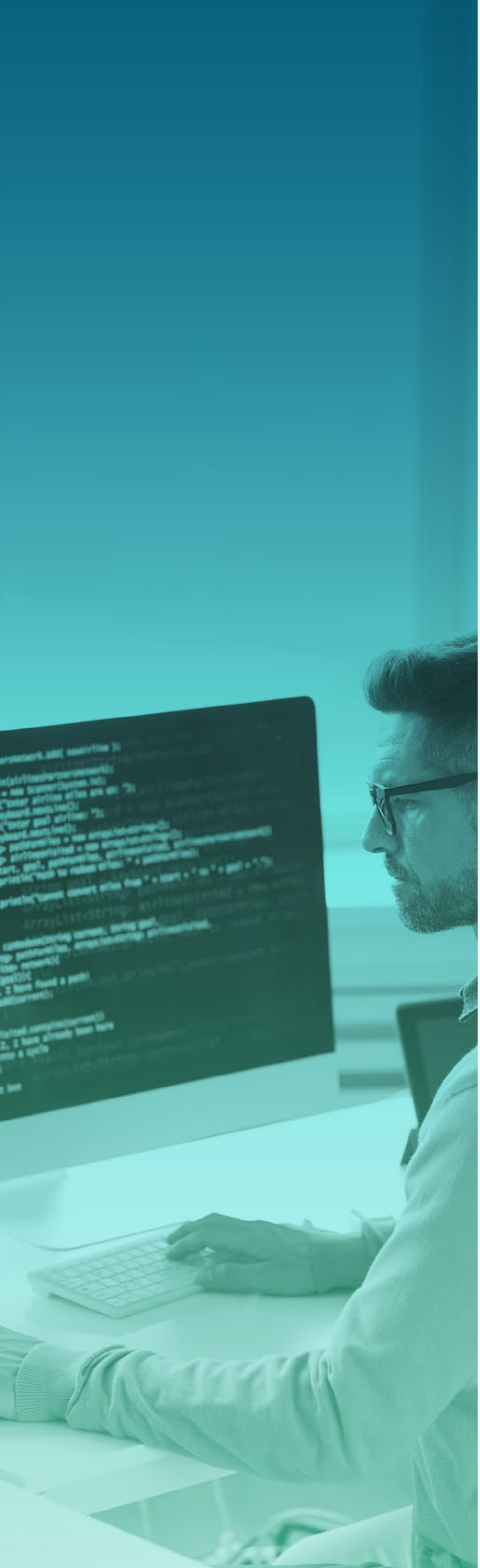
As a **Security Manager**, you need your team to scale. Demands placed on you are more intense than ever before, and you need to help every development team understand how to build security into their applications from the start.

For the **Security Team**, IriusRisk provides a single point to define secure design patterns and manage Threat Models throughout the entire development process. You can quickly define diagrams using draw.io, generate threat models and push security tasks to ALM tools.

As a **Development Manager**, you need to be sure that security doesn't become a bottleneck for your projects. The business isn't willing to wait for delivery. You need to build secure apps – but build them faster.

For the **Development Team**, IriusRisk automatically generates a threat model with recommended and required countermeasures and adds them to your issue tracker, like Jira and Microsoft TFS/Azure DevOps, so you can address security just like any other task. Whether you're in development or security, IriusRisk helps you design security into your software and applications from the start.





« Adaptable to your process

IriusRisk supports flexible workflow definition and automation, so that it can adapt to your existing processes:

The Security Team

Reviews and modifies the threat model and decides on the risk treatment. Then they upload the security requirements to the issue tracker for assignment to the development team.

Developers

Define the architecture by drawing a draw.io diagram, complete a questionnaire, and IriusRisk automatically generates the security requirements and adds them to an issue tracker. This lets developers identify and implement important security work without involving the security team.

Or a combination of both

Developers focus on implementing requirements and the security team continuously monitors and adjusts the risk response, pushing new requirements to issue trackers as needed.

How does it work?

Workflow for the Security Team:

- Security Champion reviews the threat model that IriusRisk generates. They can add new threats, weaknesses or countermeasures; or remove those that are not applicable.
- A security standard is then applied to the model – either based on the provided OWASP ASVS, PCI DSS, EU GDPR standards, or a customized standard, specific to the organization
- They decide on the risk treatment for any untreated risks. IriusRisk provides guidance on risk treatment by highlighting the countermeasures with a high return on investment: Low cost countermeasures that mitigate high risk threats.
- Finally, they can push the requirements to Jira (or other issue trackers), or manage them from within IriusRisk.
- As the development team works, IriusRisk continuously monitors the counter measure state from the issue tracker and adjusts the level of risk accordingly. The security team monitors the countermeasures and risks through IriusRisk to decide whether actions should be taken.

Workflow for Developers:

- Development team answers questions in a questionnaire to define the architecture and security context of the application. The questionnaire is tailored for each application and only displays relevant questions.
- When the questionnaire is completed, IriusRisk automatically generates a threat model with recommended countermeasures.
- Developers apply a security standard, which turns the recommended counter measures into requirements. This can be a bespoke standard developed by the security team, or one of the bundled standards like the OWASP ASVS and PCI DSS.
- The Developer specifies the issue tracker project details and IriusRisk uploads the new requirements to the issue tracker.
- From here, countermeasures are just like any other project feature, and developers continue using their normal workflow in the issue tracker.

Workflow for Testers

IriusRisk provides two types of tests: tests for the presence of countermeasures – important for auditing purposes - and tests for the presence of weaknesses – important for penetration testers or red teams.

- Auditors and functional testers can use the list of tests for countermeasures
- Penetration testers can use the list of weakness tests to test for the presence of weaknesses, in addition to their usual testing methodologies. This provides them with a checklist of tests to run.

Customize and extend

IriusRisk generates its threat model based on the content of the following data sets:

The architectural diagram and dataflows

Information provided by the answers to the questionnaires

The rules that determine which Risk Patterns are applicable

Libraries of Risk Patterns that contain the threats, weaknesses, countermeasures and tests

All of the datasets are configurable and editable in the system. This allows a completely customizable threat model to be generated. Both the questionnaire and risk rules use the JBoss Drools rules engine to allow complex questionnaires and rules to be created.

IriusRisk also includes a built-in graphical rules editor that provides an even easier way for users to create common rules. The data for all components: Diagrams, Questionnaires, Rules and Libraries - can be imported and exported from the system in an open format (Draw.io, JBoss Drools and XML respectively).

FAQ

Does IriusRisk only generate security requirements?
In addition to security requirements, IriusRisk also generates the threat model that justifies those requirements. This provides a more complete view of the security context so that the security team can make informed decisions about how to treat the risk.

Is a risk rating a static measure?
No. IriusRisk manages security risks and plans risk mitigation while continuously adjusting the risk rating based on the status of implemented countermeasures and the results of security tests. This gives security teams constant feedback on which risks and countermeasures to prioritize.

How is IriusRisk licensed?
IriusRisk is licensed per managed application. The number of users is unlimited for all editions, so every member of your organization who cares about security can participate in making your software more secure.

Can IriusRisk be customized for my organization?
Yes. All the threats, countermeasures, questionnaires and rules are 100% editable and customizable. You can even export all this content in open formats, so that your investment in customization is never trapped in a proprietary format.

Do threat models only exist for a single application?
No, threat models can be stored as Templates for easy re-use by other applications, and changes to these templates can be propagated to all applications that use that template.

How does user security work?
Permissions-based access control system. This allows teams to use a granular user permission system to assign only the required permissions to required users.

Can IriusRisk fit into our existing security workflow/ process?
Yes. A highly customizable workflow system allows teams to map security activities onto the development workflow, and to filter applications based on their workflow state.

Does IriusRisk support my issue tracking system?
Yes. IriusRisk integrates with multiple issue trackers such as Jira, Servicenow, Microsoft TFS and Azure DevOps. We regularly expand our list of supported integrations, too. If the system you use is not currently supported, let us know and we will work with you to add support for it.