

# SECURE APPLICATION DEVELOPMENT SERVICES FOR MICROSOFT PLATFORMS

## Trying to Develop Secure Microsoft Applications? Watch Your Step.

Developing applications that can effectively withstand today's malicious hacker attacks can be scary. It does not have to be. At least not when you have the Impacta Secure Application Development services team on your side.

Email [info@impactalabs.com](mailto:info@impactalabs.com) to find out how.



*Innovations That Inspire™*

### GO WITH THE CLEAR EXPERTS

Developing applications for Microsoft platforms that can withstand today's malicious hacker attacks requires an intimate knowledge of secure development best-practices, tools and processes, such as the **Microsoft Secure Development Lifecycle (SDL)**. Why not augment your current development team with expert secure application developers from Impacta? Our secure application development services team is comprised of former Microsoft senior security developers, published authors and recognized industry innovators. This means that whether you are developing your applications in C, C++ or with the .NET Framework, your applications will always be closely aligned with Microsoft's own internal secure development best-practices and recommendations. That's the Impacta advantage!

### WE ARE HERE FOR YOU

Companies like Microsoft and Big 4 auditing firms have recognized Impacta for its security research contributions and for helping them better protect their customers from online attacks. Let Impacta also help you protect yours!

Your questions are important to us. Please email [info@impactalabs.com](mailto:info@impactalabs.com) for more information about this service and a representative will respond shortly.

### THREE THINGS YOU CAN DO NOW TO MAKE YOUR MICROSOFT APPLICATIONS MORE SECURE

Here are three easy things you can do right now to improve the overall security of your Microsoft applications, and reduce your exposure to online attacks:

1. Compile C/C++ applications with automated compiler protection features, such as GS and DYNAMICBASE
2. Use publicly available analysis tools, such as Microsoft FxCop and PReFast to quickly identify common code vulnerabilities
3. Use Microsoft's Secure CRT Secure Template Overloads to automatically convert unsafe function calls to safer function calls