

Acushnet Company

SMP's singular focus is

IT security audit and assessment professional services. Our vendor-neutral, in-depth IT Assurance consulting approach leverages best practice and compliance expertise from hundreds of engagements. SMP will reduce your company's vulnerabilities, brace operational and network infrastructure security, and facilitate compliance with evolving government regulations. We provide concrete, actionable recommendations to help you identify, achieve, and maintain the right level of security.

Industry: Manufacturing

Company Bio: Industry: Manufacturing

Company Bio: Acushnet Company, comprised of the Titleist®, FootJoy®, and Pinnacle® golf brands, is the world's leading manufacturer and marketer of golf equipment. A \$1.4 billion company, Acushnet's brands own the number one market share in balls, shoes and gloves on each of the worldwide professional golf tours and in golf shops. Acushnet's distribution channels include: on course pro shops; off course golf shops; sporting goods stores; mass merchants; and the corporate custom channel for logo golf balls.

World Headquarters: Fairhaven, Massachusetts

Locations: Over 45 locations worldwide including U.S., Canada, Europe, Africa, and Asia.

“**SECURITY MANAGEMENT PARTNERS** brought the application security expertise we needed to complement our own internal efforts. SMP's automated and manual approach both validated Acushnet's own efforts while providing suggestions and remediation efforts we hadn't thought of. We have not only utilized SMP's application expertise but their external and internal penetration testing, and security infrastructure assessments as well. SMP has exceeded our expectations on every project.”

— PETER MARSHALL
Vice President, Technology Services
Acushnet Company

Objective

Cybercriminals are finding holes in web applications and exploiting them with relative ease. Acushnet Company engaged Security Management Partners (SMP) to:

- execute an application penetration test of five of its e-commerce applications
- ensure that existing security controls in the applications are effective.

Testing

First, SMP's penetration tests using actual hacker and industry leading tools identified any configuration deficiencies and security vulnerabilities. Next, targeted application testing was performed from an authenticated user's perspective to determine if an individual could gain access to other users' accounts or the application's administrator functionality. Finally, SMP conducted an assessment of common exploits resulting from input validation problems such as script injection, cross site scripting, SQL injection, request forgeries, directory transversals and buffer overflow checks.