

DeflectorShield™

External Vulnerability Management System

WatSec, Our Company

WatSec is transforming the traditional security vulnerability assessment into a complete, continuous, cybercrime prevention program for companies around the globe.

Our unique approach for ongoing vulnerability management offer practical solutions to a growing menace.

Products

Find security problems

DeflectorShield™

Multi-Point Site Assessment (MPSA)™

SafetyNet™

Improve security stature

WatSmart™ Education

WatSmart™ Policy

WatSmart™ Business Continuity

Solutions

The Ultimate Firewall (TUF)™

“Last year, our network was compromised. Today DeflectorShield provides us with the confidence that our network is secure.”

-Paul Young, Skybound Software, Co.-Founder

We Do Security. You Focus on Your Bottom Line.

Finding your security holes is only half the battle.

There are over 65,000 potential entry points (ports) into your confidential data even when being “protected” by anti-virus. Like leaving your door unlocked, an unprotected entry point gives cyber criminals a fast path to your critical corporate data and to a potentially devastating financial loss.

But how can you determine which entry points are vulnerable?

Assessing Your Exposures, So You Don't Have To.

Introducing DeflectorShield; an external assessment of your exposures

DeflectorShield™ checks for known security holes, identifies the ones which really matter, and provides your IT advisor with up-to-date and unbiased cybercrime protection knowledge.

WatSec's product is fully backed by certified security specialists, who will craft a custom remediation roadmap for your organization, and keep your management team regularly updated with plain language management reports.

SecureGrade™ Illustrates Your Current Security Level

Overall Security Grade: F
External Assessment: A - B - C - D - E
Internal Assessment: N/A (Has not been completed)

Summary
On the basis of WatSec's external tests, your organization has weak security over your network. WatSec has identified security flaws that allow a hacker to infiltrate your systems. To improve your security configuration review the following vulnerabilities:

1. Vulnerability in Server Service Could Allow Remote Code Execution
An attacker who successfully exploits this vulnerability could take complete control of the affected system.
2. Microsoft SMB Remote Code Execution Vulnerability
An attacker who successfully exploits this vulnerability could install programs view, change, or delete data; or create new accounts with full user rights. Successful exploitation also results in denial of service which causes the affected system to crash and stop responding.

Recommendations

1. Fix vulnerability 1: download and install the appropriate patches; see [Microsoft's Security Bulletin MS08-067](#)
2. Fix vulnerability 2: block TCP ports 139, 445 and install the corresponding patches;

Powerful Monthly Audit Trail

Plain Language Management Reporting



University of Waterloo Research & Technology Park
295 Hagey Blvd, Waterloo, Ontario, Canada N2L 6R5
Phone: 519. 747. 2549 Email: info@watsec.com
www.watsec.com

Take Control of Your Network Before The Hackers Do. **Contact WatSec Today!**