

Microsoft Security Risk Assessment (MSRA)



Assess

Comprehensive and practical guidance for optimizing your IT security program

Microsoft Services Security Risk Assessment offering (MSRA) is designed to help determine the security risks in an application and the infrastructure supporting it. Using a formal methodology, the offering helps organizations understand their risk of exposure to security breaches in critical applications and measure their security controls and processes against industry practices, thereby establishing a security baseline from which to measure progress.

Overview

There are headlines almost every day about massive loss of data via a hacker, Government or insider. A recent [Microsoft Security Intelligence Report](#) points out that even more data is lost by negligence. All this is happening more rapidly as we move forward into the Cloud. This is why the very first question customers usually and increasingly ask is about security. In today's global business environment, the profile of any large organization includes custom-built, multi-tiered applications accessible on the network, and many times the Internet, powering databases and fueling collaboration. The more complex the environment, however, the greater the security risks to its infrastructure, applications, operations and organizational components. Microsoft Services Security Risk Assessment offering is designed to adapt your security strategy to help reduce risk across the entire enterprise. Specifically, the MSRA provides:

- A proactive approach to security that identifies breakdowns in people, processes, and technologies before they affect operations
- A threat model against a critical application and the infrastructure that supports it
- Clear insight into how the organization compares against industry standard controls
- A remediation roadmap that prioritizes findings into tactical and systemic recommendations that can be acted upon immediately

Why Perform an MSRA?

As organizations' environments are increasingly complex, validation of configurations, and testing against common vulnerabilities does not always occur for every application. The MSRA examine application architecture and design, the infrastructure, and the operational management process to identify key risk areas related to the application.



How the Offering Works

The MSRA Service is delivered by experienced security consultants from Microsoft Services. Each consultant has received required training in performing assessments using Microsoft's tools and methodologies.

The Microsoft Security Risk Assessment (MSRA) is a two-week engagement that helps to gauge the efficacy of your security strategy by evaluating the implementation of the defense-in-depth concept – layering technical, organizational, and operational controls.

Using on-site, in-person interviews and technical examination, MSRA results in the creation of a roadmap customized for your business. This roadmap takes into account your organization's resources and tolerance for change, and harnesses planned IT upgrades wherever possible. MSRA also captures opportunities for security to contribute to new business areas and reduce the cost of compliance. MSRA is focused on your need to protect important data and systems, mitigate threats, support business priorities, and address ever-evolving attack techniques – while keeping cost under control and minimizing any disruption to the business.

Key Benefits

- Gain a comprehensive and consolidated view of your existing security programs
- Improve your overall security posture by implementing an actionable roadmap with specific steps to meet your business and security needs
- Enhance your program by working with experienced Microsoft specialists to learn up-to-date policies, practices, and technologies

2 Days Kick-Off Planning	 Review objectives, identify customer focus areas, and schedule on-site interviews
3 Days Data Collection	 Conduct on-site interviews to gather goals, policies, technologies, and practices across your security program(s)
3 Days Analysis	 Analyze interview results and compare against Microsoft Cybersecurity Infrastructure Optimization Maturity Model. Prepare your roadmap based on criticality and impact of the findings.
2 Days Reporting	 Create written report and provide Executive Briefing summarizing findings and roadmap <i>Deliverables – Tailored Security Program Recommendations, Executive Briefing, Roadmap, Plan and Associated Estimate</i>