Microsoft Best Practices Analysis (MBPA) Check

axis BUSINESS SOLUTIONS

Trying to keep up with best practices in your Microsoft Network gets more difficult every year. The Axis MBPA check analyzes your Microsoft server environments, providing network and security analytics, specifically designed to keep your infrastructure up to date with industry known best practices.

MBPA Proactive Network and Security Health Check

- **Comprehensive check will outline all risks found in your environment**
  Includes deliverable reports with high level detail
- **All risks will be presented in a weighted system and assessed as high, medium or low**
  High risk is presented with mitigation action items
- **Multiple deliverable reports available from both Network and Security aspects of infrastructure**
  A sample of the reports include Asset Detail, External Vulnerability Analysis and Share Permission reports
- **Learn about all aspects of your infrastructure and use the active report data to help manage it**
  The comprehensive reports make managing your Microsoft systems easier
- **Use Microsoft Best Practice Standards to effectively secure your network**
  The MBPA check will let you know if your network has any risks according to the best practices standards
- **Be proactive and not reactive to failures or threats**
  Eliminate issues before they happen
- **Keep up with constantly changing Microsoft Best Practice Standards**
  Use the MBPA check to implement procedures that will keep your infrastructure framework current
- **Our MBPA security analysis will alert you for deeper issues in your environment**
  Use MBPA analysis to see if a full security audit is warranted

Step 1: Interview

We ask you about your network. What are your challenges with your infrastructure? Which systems are critical to operations? What is the basic structure of your Active Directory? What is the primary managed Antivirus system? How has your password policy been implemented? What is responsible for internal patching for MS updates?

Step 2: Gather Scan data and analyze reports

We perform a complete Microsoft Network and Security Check. This check collects data about your entire network infrastructure and performs an external penetration test. Our team reviews the findings and analyzes the data. Finally, we compile a comprehensive report outlining potential risks found on your infrastructure in terms of Microsoft Best Practices.

Step 3: Follow-up

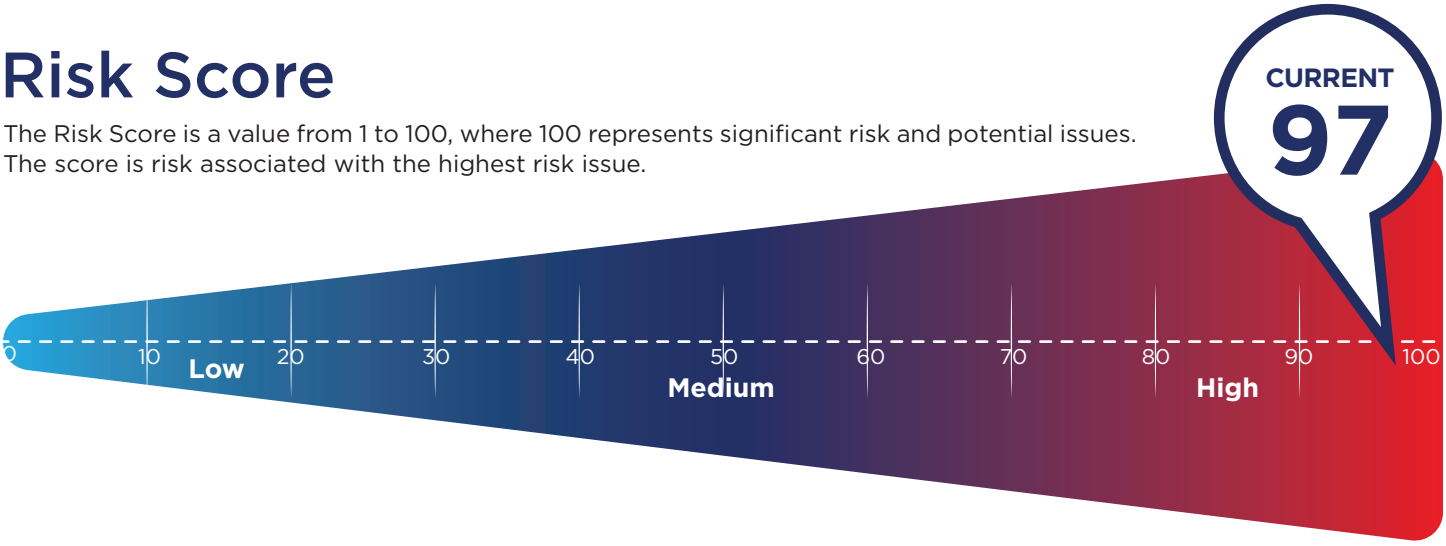
Within a day or two of the interview, we deliver all reports and schedule a follow-up meeting with you and your technical team. We give you an action plan to mitigate the risks and we will walk you through the management plan, making sure you understand the weighted priorities to resolve. Once mitigation is complete we re-scan and provide change reports which identify how the risk levels have changed.

What to Expect

Axis' Microsoft Best Practices Analysis Check generates findings based on data about your network and infrastructure. Our team reviews the findings and creates a comprehensive report that outlines the potential risk found on your infrastructure with a summary of issues detected during the Analysis, and an "Overall Issue Score" that grades the level of risk in your environment.

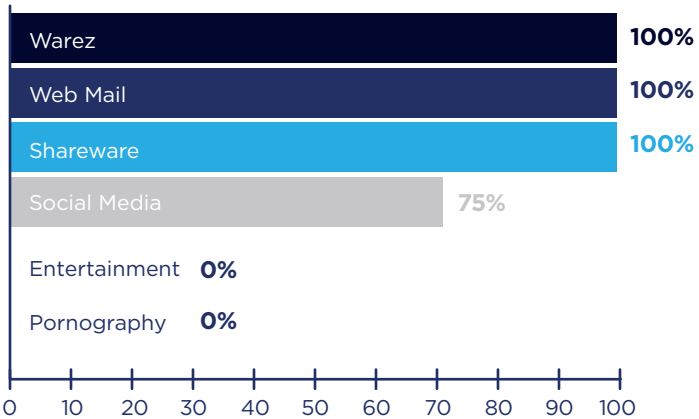
Risk Score

The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Internal Vulnerabilities

Content Filtering Assessment



Local Security Policy Consistency

% Policy Consistency