AUGMENTT

How MSPs can leverage Microsoft Secure Score to help build their own security standards

Instead of overreliance on the handy catch-all value of Microsoft Secure Score, MSPs should use it as a foundation for building their own security standards that will help them more effectively protect their customers.

What is the Microsoft Secure Score?

For organizations and MSPs, the Microsoft Secure Score is a widely known analytics tool that provides a snapshot of an organization's IT security standing from a Microsoft perspective

Along with a numerical score of up to 1,188, the tool produces a host of recommendations to improve the score and boost the organization's security from within a Microsoft environment

What is the Microsoft Secure Score?

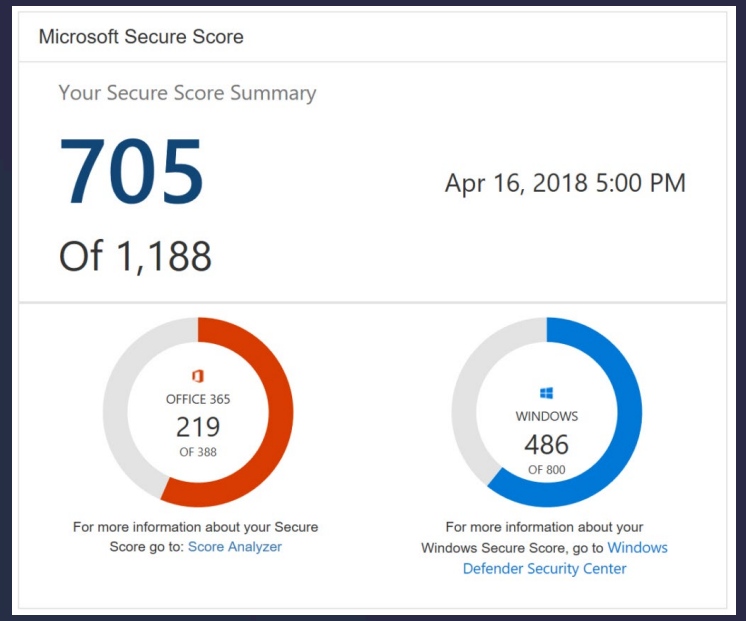
Organizations can view their score in the Microsoft 365 Defender portal. The higher the score, the stronger the Microsoft security practices in place.

Products that are currently factored into the Microsoft 365 Secure Score:

- Azure Active Directory
- Microsoft Office 365
- Teams
- Microsoft Defender for both Endpoint and Identity
- Defender for Cloud Apps

What is the Microsoft Secure Score?

The Secure Score is calculated in real time and is broken down into separate evaluations for Microsoft 365 and Windows security



How can organizations improve their Microsoft Secure Score?

Each calculation of the Secure Score includes a listing of the most relevant actions for improvement, including:

- Require MFA for administrative roles
- Turn on Firewall in macOS
- Turn on MS Defender Antivirus PUA
- Use advanced protection against ransomware
- Block execution of potentially obfuscated scripts

What are the limitations of the Microsoft Secure Score?

For Microsoft, the Secure Score is primarily a sales tool used to encourage the purchase of additional Microsoft technology and services

Despite its popularity, many MSPs struggle to determine the true value of the Secure Score when it comes to protecting clients with non-Microsoft technology

What are the limitations of the Microsoft Secure Score?

Industry observers say that reaching a 100% Secure Score would necessitate 100% adoption of the Microsoft technology stack

But MSPs often rely on third-party services that are not recognized in Secure Score analysis

What are the limitations of the Microsoft Secure Score?

Even with 100% Microsoft adoption, unrecognized third-party antivirus, antispam, and tooling for multi-factor authentication (MFA) would result in low Secure Scores

It’s theoretically possible to manually specify use of third-party tooling in the MS portal to improve a Secure Score, but that process would be tedious and time-consuming for the already busy MSP

What are the limitations of the Microsoft Secure Score?

MSPs often use the Secure Score automatically captured by Augmentt to encourage customers to add more security services, but such encouragement is based on a very limited analysis

For instance, Secure Score doesn't address security-related compliance requirements such HIPAA, NIST, and privacy regulations

A better way to leverage Microsoft Secure Score

Rather than simply adhere to Microsoft's generic standards that factor into the Secure Score, MSPs and organizations should use the score to help develop their own security standards

An impressive Secure Score is nice to have, but ultimately the only security controls that matter are the ones that MSPs put in place and keep in place

A better way to leverage Microsoft Secure Score

Augmentt has taken core elements of the Secure Score (MFA, legacy authentication, file sharing options, etc.) and enabled a much deeper audit

This audit can show, for instance, precisely which users don’t have MFA enabled and lets MSPs configure alerts to be triggered if MFA is ever disabled

A better way to leverage Microsoft Secure Score

Rather than chase a high Secure Score, MSPs should use it to obtain a better understanding on the standard security baseline they will consistently put in place.

Aside from MFA, does that MSP standard include legacy authentication? Blocking sign-ins from risky countries? Default data sharing/guest invitations? Additional core security measures?

The MSP “score” for keeping customers safe

Secure Score can be a helpful part of the picture, but foundational security standards implemented across customer sites can provide MSPs with vital standardization and measurable protection methods

Developing and adhering to their own “security score,” can make life easier for MSPs when keeping customers safe from the ever-growing security threats out there

Augmentt can provide expert guidance

Contact your Augmentt representative today for more about the Secure Score as a springboard for better security services.

Contact sales@augmentt.com

AUGMENTT