Petri IT Knowledgebase Resource
A BWW Media Group Brand

Petri IT Knowledgebase

Microsoft Office 365 Security for the Busy Administrator

Sponsored by
Quadrotech

Microsoft Office 365 Security for the Busy Administrator

Presenter: Doug Davis, Reporting & Analytics, Quadrotech

Moderator: Brad Sams, Petri IT Knowledgebase, Executive Editor at Petri.com

Overview

When organizations move to the cloud, security is almost always among the top concerns and challenges to overcome. Luckily for users and tenant administrators, Microsoft Office 365 offers many robust security features. However, due to the vast amount of data and multiple security portals, it can be hard to tell if you've implemented the right security best practices for a truly secure environment.

Context

In this webinar, you will learn what is considered a 'secure' Office 365 tenant, what tools can determine the security of your Office 365 tenant, why tools often give a false sense of security, what Microsoft Secure Score is and what it really means for your organization, how to determine if your tenant is truly secure, how to mitigate risk and lock down your Office 365 Tenant, and how to prevent a secure tenant from creeping back to insecurity.

Key Takeaways

How do you define secure Office 365?

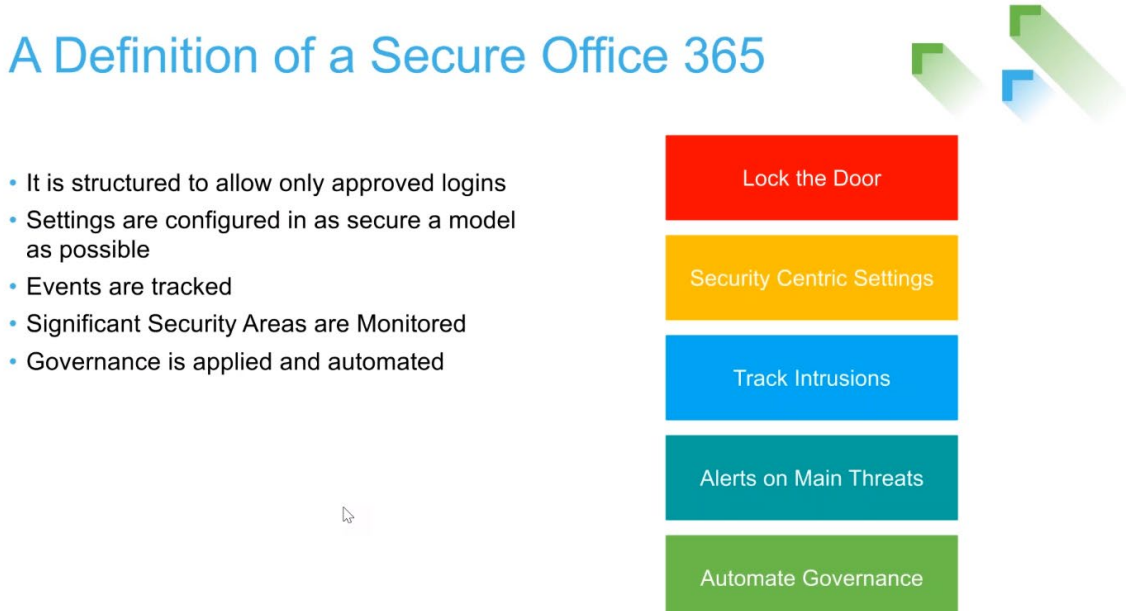
In an Office 365 world, which is by design hosted and available on the web, security isn't directly related to physical access. Instead, it is tied to the currently estimated 50 billion access points; anything that can connect to the web, can try to access your Office 365 tenant.

Knowing this, you can't manage the access points, which means that you need to control the entry points. Therefore, all possible available doors need to be covered, but unfortunately there is not a definitive list of Office 365 settings that define security.

Your first and main line of defense will be your logins or authentication credentials and locations.

Definition of secure Office 365

In the webinar, Doug details his five steps to defining a secure Office 365 environment. These five steps will help to make sure that you are protected at the authentication step, have the ability to track anyone who does get in through the front door, and the ability to automate the process. By following these steps, as outlined in this webinar, you will be able to improve the security of your environment.



How do you get to the secured state?

The journey begins with understanding the settings and tools that ship with Office 365. The challenge is that there are thousands of settings with more being added all the time.
While some of these settings are very important, others can be de-prioritized. The challenge is knowing which to treat as 'nice to haves' and which settings are critical to securing your environment.

In addition, these settings are evergreen, meaning Microsoft can change them and update them at any time.

Get to know your admin tools

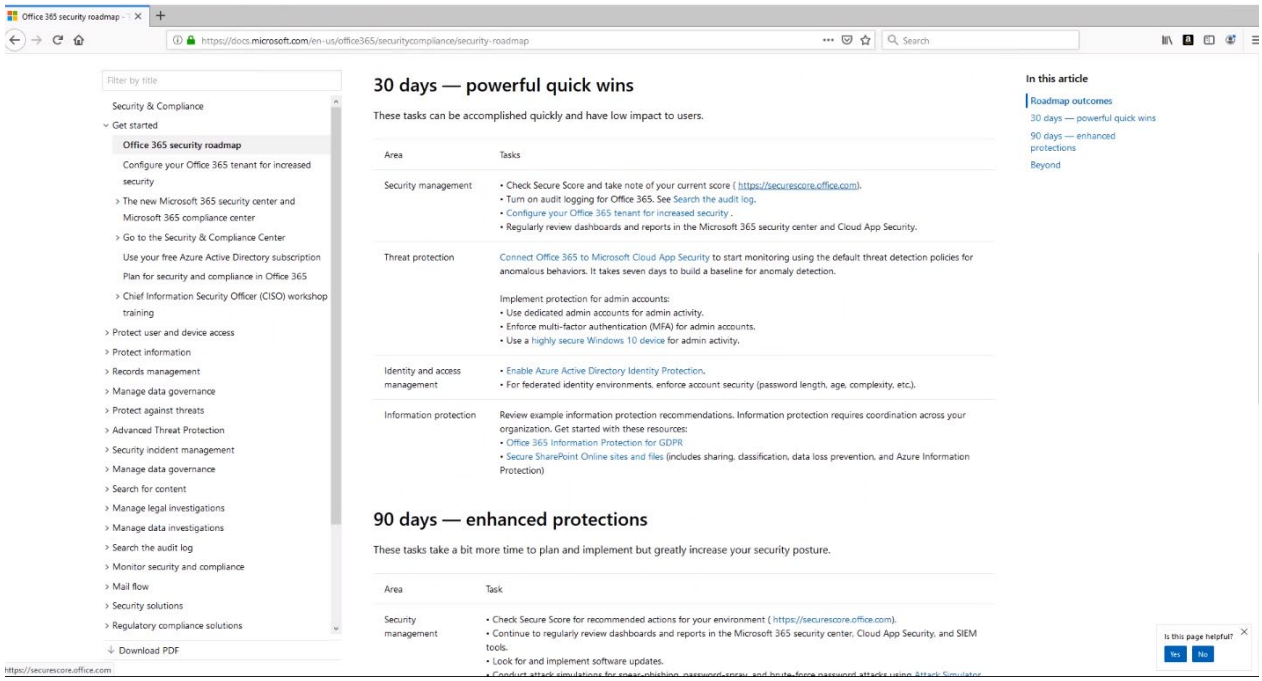
One of the challenges of managing Office 365 is that there is not a tool called 'Settings'; there are multiple sections for configuration that are defined by your role or tier.

Because there are so many different options, you have two paths: learn everything or learn the important options.

Where to start – educate yourself

Microsoft knows that the configuration of your environment can be complex, and the company outlines what to do in the first 30 days and beyond.

The two Microsoft security roadmaps you will want to follow are the first 30 days and 90 days of documentation. This information will help you identify the key settings that will set a baseline configuration for security and governance.

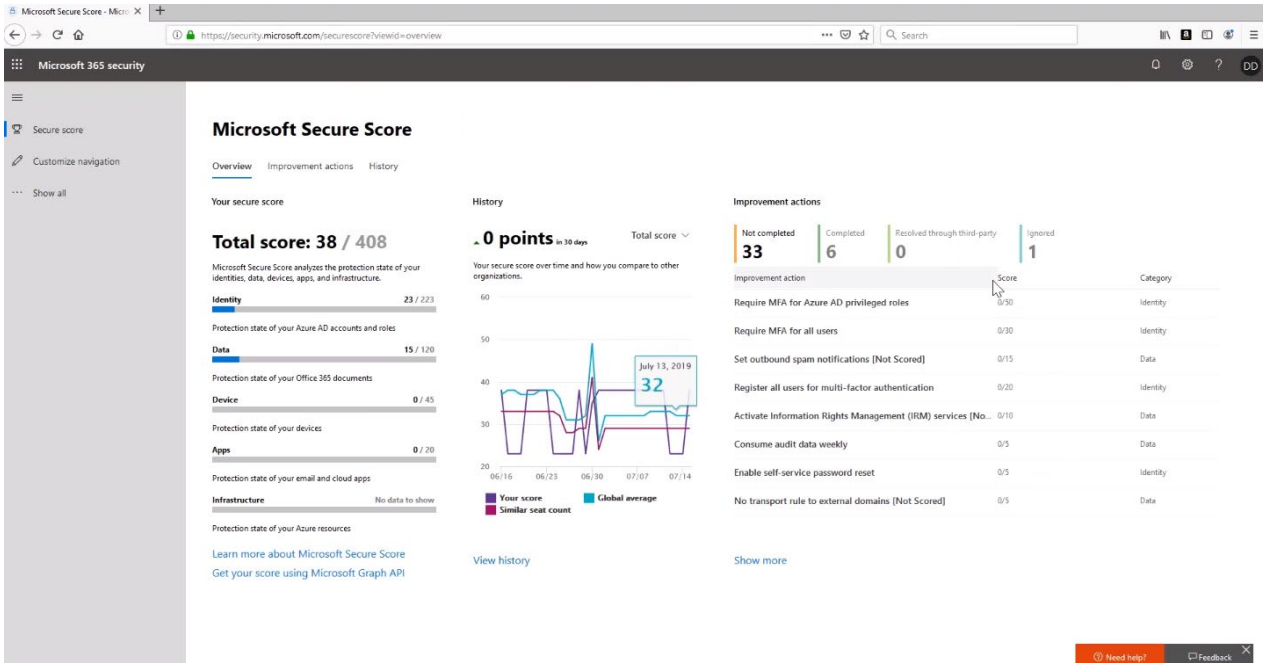


The documentation provided by Microsoft will help you land quick wins, but it can also be overwhelming too. It's important to fully understand that changes you will enable or disable and how that will impact your users.

Microsoft Secure Score

Microsoft provides a tool called Microsoft Secure Score and while the name makes it sound like it should tell you if your content is secure, it's a bit misleading. A high score does not mean that you are secure, and a low score doesn't mean that you aren't secure.

What you need to do with Secure Score is to review each of the settings and set them appropriately for your environment. As Doug notes in the webinar, you are only as secure as your weakest entry point and that just because you have a high Secure Score because you reviewed all the settings, your data can still be exposed to significant risks.



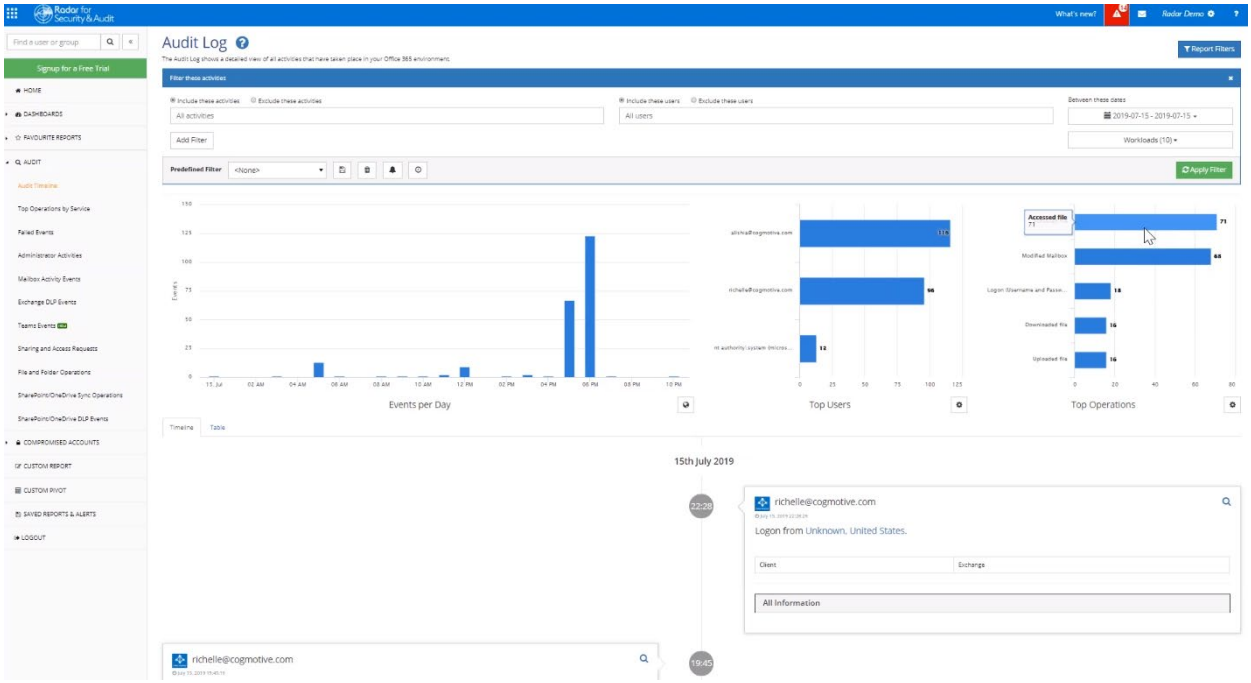
A demonstration of Secure Score is shown during the webinar that identifies how you can learn more about each setting and where to find the relevant sections of the admin environment to improve your Secure Score.

Reviewing the Quadrotech Audit Log

While Microsoft's settings can help you secure your environment, it's not a perfect solution and threats to your organization can be from malicious or accidental employee activity. It's important to keep tabs on internal activity for this reason.

Quadrotech has an Office 365 Reporting & Auditing tool that identifies unusual activity inside your environment through a dashboard experience – including insights like who has modified a mailbox, failed events, and many more bits of helpful investigative information. While reviewing the Quadrotech Audit Log sounds cumbersome, Doug provides a few tips and tricks to streamline the process.

Some more obvious scenarios to look into are users who went on a download binge, odd changes to their usage, and trends for the user that are outside their normal use-case. Unfortunately, most breaches are uncovered in non-conventional ways. Microsoft's automation tools are good for finding outside threats, but internal threats are much harder to detect with automation tools. This is where a third-party solution like Quadrotech's can help bridge that gap.



Insecurity creep

Once you have taken all the steps to secure your environment, you need to review settings occasionally to make sure that it doesn't creep back into being unsecure.

The creep can happen when user permissions access is changed to allow everyone to access a directory or file for a temporary project, multi-factor authentication becomes annoying, so it is turned off, or simply time pressure where the approval processes take too long and are removed.

Many times, we revert to a non-secure setup for a temporary fix and then never return to the secure configuration; this is where governance comes into play.

Settings are not governance

While setting up your environment correctly is critical, maintaining that configuration is an on-going effort. Governance is adopting your own set of rules or policies and then governing them to ensure they are adhered to.

There are many frameworks out there to help you get started, like COBIT, ITIL, ISO 17799 but the best place to start is with your own list.

Doug has a few simple suggestions to get you started including MFA for logins, policies that enforce complex passwords that need to be changed every 30 days, guest access is purged frequently, don't allow auto forwarding, SharePoint/OneDrive settings are locked down, restrict shared mailboxes and disable/delete accounts that are no longer needed.

Later this year, Quadrotech will ship a Governance dashboard that will help you monitor and maintain compliance to your framework.

Use a Data Driven Governance Tool

Security isn't all that hard

The idea of being secure may seem complex but with the right tools and mindset, it doesn't have to be hard.

With a few simple tips like use Microsoft Secure Score, follow an established set of guidelines, spend time reviewing audit logs, and start with simple governance and ramp up over time, you can keep your Office 365 environment protected.