**THE TOP 10 SECURITY RECOMMENDATIONS WE SHOULD CONSIDER WHILE WORKING FROM HOME!**

* Mobile working is a standard, today.
* Companies are not longer protected by their infrastructure in their corp-environment.
* Crucial document data is moving away from centralized systems because it’s easier to work on them on our own document systems.
* The irrelevance of bombastic systems in corporate environment is holding collaboration down.
* Does it sounds familiar?

**the 10 security recommendations we should consider while working from home!**

1. Identity Security / [MFA](https://jasperbernaers.com/the-multi-factor-authentication-struggle-and-the-solution/)
2. Install the latest patches and updates
3. Passwords and management
4. Build real-time reports of security risks
5. Create automated and intelligent alerts
6. Install antivirus on all endpoints
7. Secure devices and corporate devices (+ personal phones)
8. Evaluate regularly which users have access to data, devices and networks
9. Track, change and block access for temporary projects and when employees are leaving your company
10. Use [information protection](https://jasperbernaers.com/tag/information-protection/)solutions to protect your data everywhere.

**1. Identity protection**

* Some facts: 1.2 million of all Office 365 or [Microsoft 365](https://jasperbernaers.com/tag/microsoft-365/) accounts (each month) are compromised. This represents 0.5% of all accounts in your environment. Source: [theregister-co-uk](https://www-theregister-co-uk.cdn.ampproject.org/c/s/www.theregister.co.uk/AMP/2020/03/05/microsoft_12_million_enterprise_accounts_are_compromised_every_month/" \t "_blank)

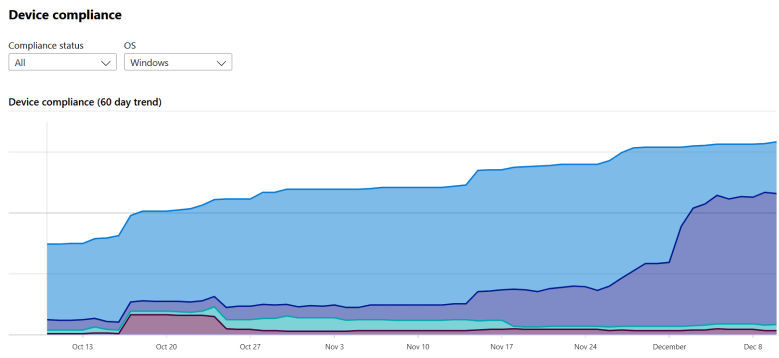
**Multi-factor authentication prevents 99.9% of all attacks.**

* [Activate MFA](https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide), It’s easy.
* Run a [Microsoft Attack Simulator](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide). It cost 2 hours. And will show the potential risk.
* See which account has most likely been compromised through [risky sign-ins.](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins)
* IMAP, POP3 disablement and implementation of MFA in 1 click? Enable [Azure AD Security Defaults](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults)



**2. Patching & updates**

* Take control of all devices in your organisation with [Microsoft EndPoint Manager](https://www.microsoft.com/en-us/microsoft-365/microsoft-endpoint-manager).
* Take control of Mobile Devices, or at least use [Mobile Aplication Management](https://docs.microsoft.com/en-us/mem/intune/apps/app-management) and protect your corporate data. (iOS, Android, W10, MacOSX,..)

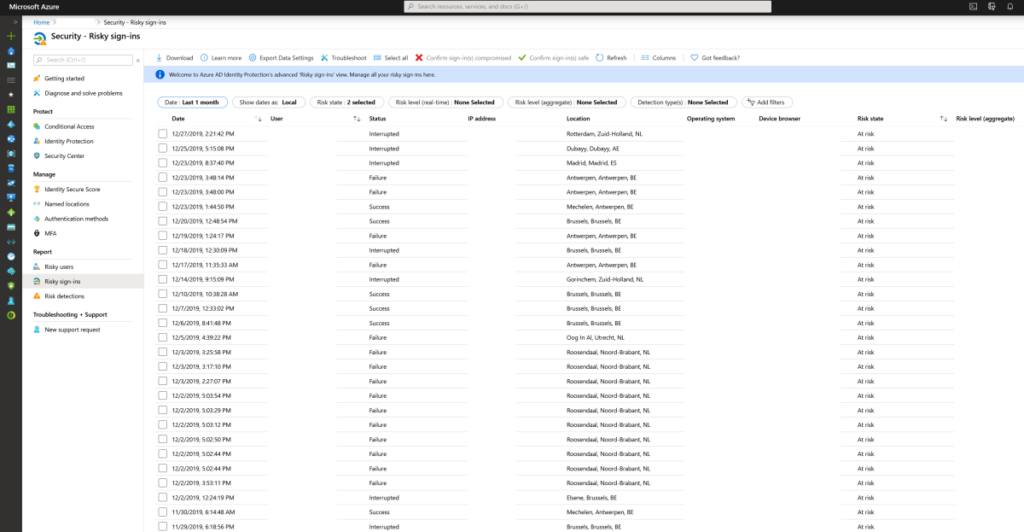
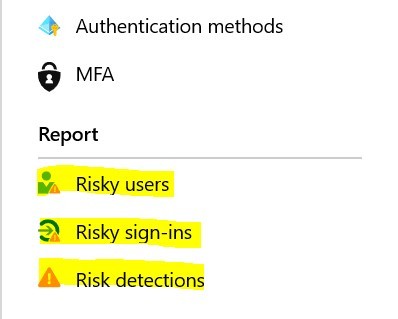


**3. Passwords and management of authentication**

* Create a password policy. Check if 100% is during renewals. Enable [MFA](https://jasperbernaers.com/the-multi-factor-authentication-struggle-and-the-solution/) for everyone. In case you don’t do it create policy for example: IF not with [MFA](https://jasperbernaers.com/the-multi-factor-authentication-struggle-and-the-solution/) than set password +100 characters. (for applications, not users) etc..
* Microsoft has advised to disable password renewals [in this article](https://docs.microsoft.com/nl-nl/archive/blogs/secguide/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903). I think it’s possible IF you are doing multiple other steps of this article.
* [Start using Windows Hello For Business](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification)
* Start using [Passwordless Authentication](https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3YNUl" \t "_blank)
* Start using [Self-Service Password Management](https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr)

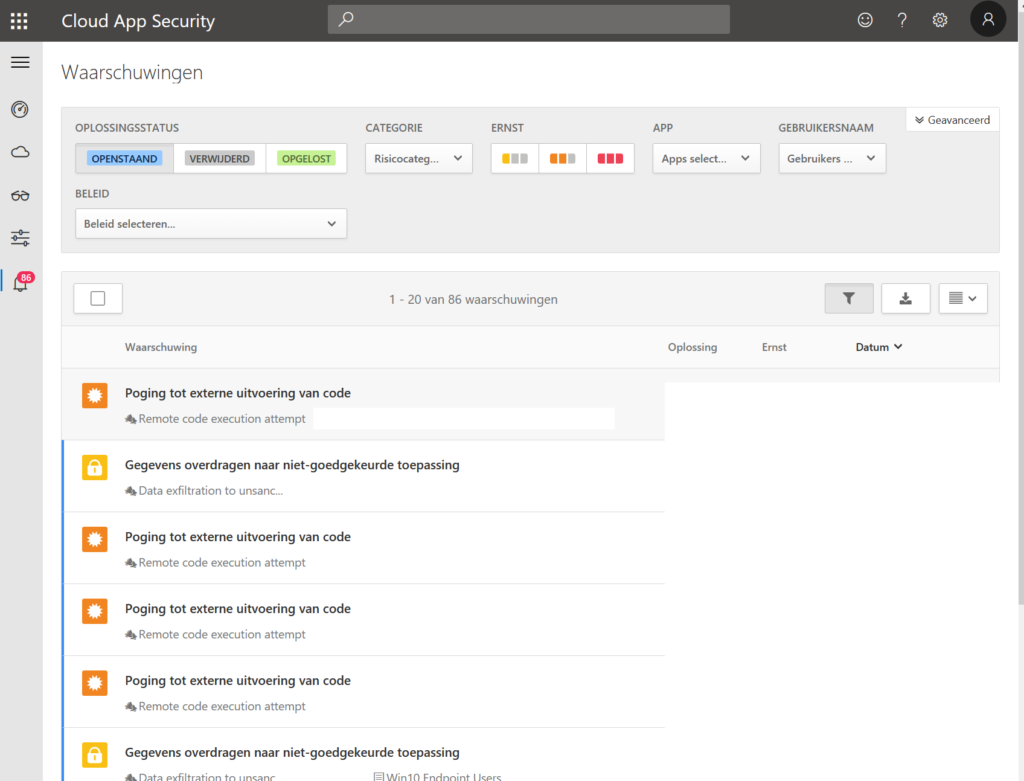
**4. Create real-time reporting of security vulnerabilities**

* Identity risks are in every organisation. Don’t think that your changes are low. Check the facts.
* It is very easy to use ‘[risky users](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins)‘, ‘risky-sign’ ins and ‘risk detection’ to find out real risks.
* Integrate with [Microsoft Defender ATP](https://jasperbernaers.com/tag/advanced-threat-protection/)and ATP Sensors to have all intelligence in the Microsoft cloud.



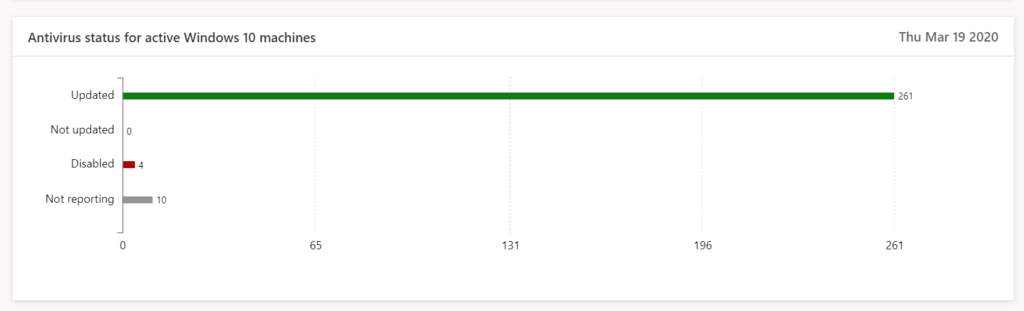
**5. Create automated and intelligent alerts**

* There is only 1 answer. Microsoft Cloud App Security.
* Create alerts when 100 files are deleted. Copied to Dropbox for example.



**6. Install antivirus on ALL endpoints + go beyond antivirus**

* [Microsoft Defender ATP](https://docs.microsoft.com/en-us/windows/security/threat-protection), sentinel-one, Norton, McAfee, it doesn’t really matter. As long as you are able to protect all endpoints.
* The second factor is to make sure that your antivirus is enabled. Use a single console. OR use [MDATP](https://docs.microsoft.com/en-us/windows/security/threat-protection). Set security alerts so you know when you are at risk.
* [Use EDR monitors](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-endpoint-detection-response) to detect and respond to advanced attacks in real time.



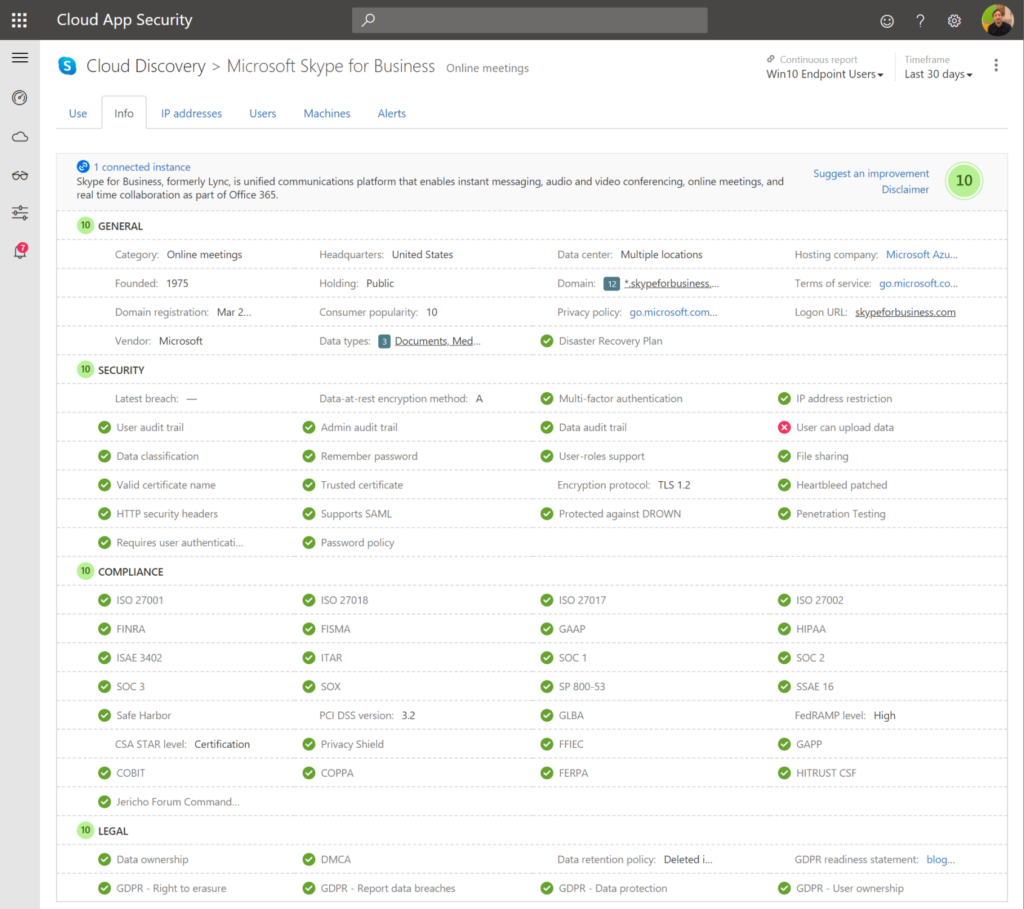
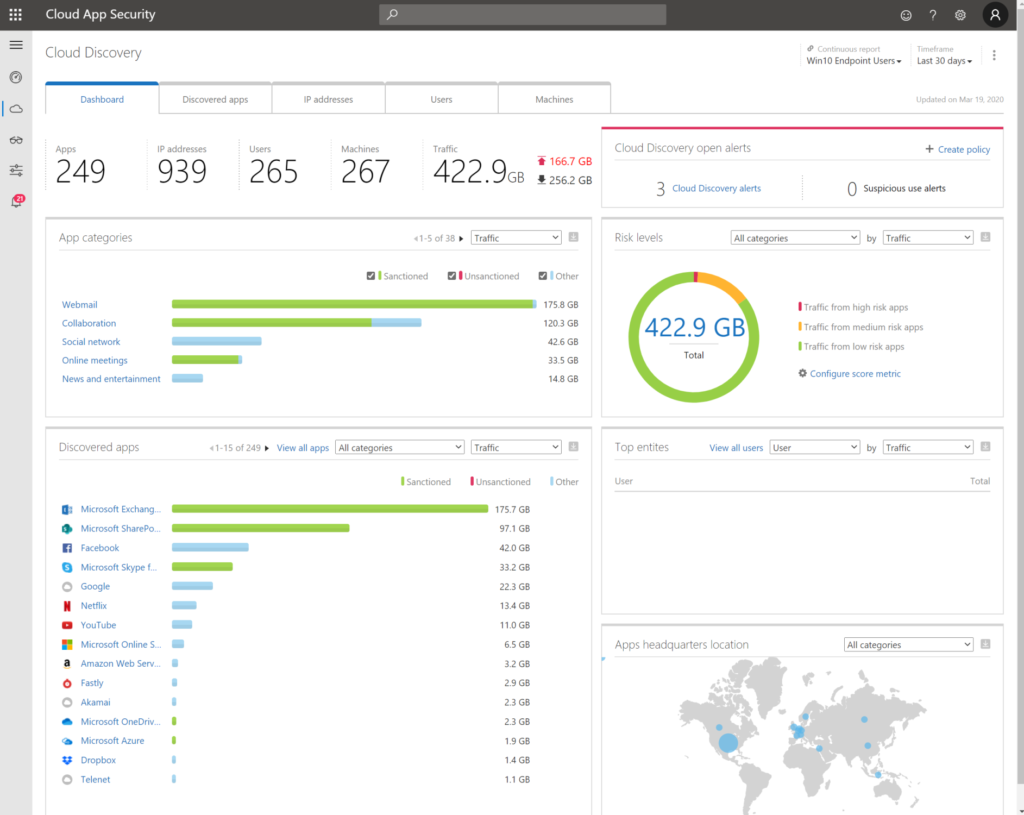
**7. Secure private(personal) devices and corporate devices**

* workstations and portables (With W10 for example) are in control in most of the companies. Mobile devices are left unmanaged because we don’t know the options.
* With Intune (EndPoint Manager) you can isolate and segment applications without having to manage the device. The corp. applications is under control. The organization’s data is protected. The most important thing is done!
* Choose a fingerprint, faceID worst-case pincode in app protection.
* Below you may find an example of the Outlook application which is protected by [Mobile Application Management](https://docs.microsoft.com/en-us/mem/intune/apps/app-management). In case organisations are not the owner of these devices this is a great option. And simple to implement.



**8) Evaluate regularly which users have access to data, devices and physical network**

* Cloud App Security shows you exactly whether data is passing on all endpoints.
* Document data, lateral movements, usage of applications, global traffic, count of applications in use in your organisation. Risk levels, GDPR proof applications..
* Bring network devices logging in CASB to have more insights.

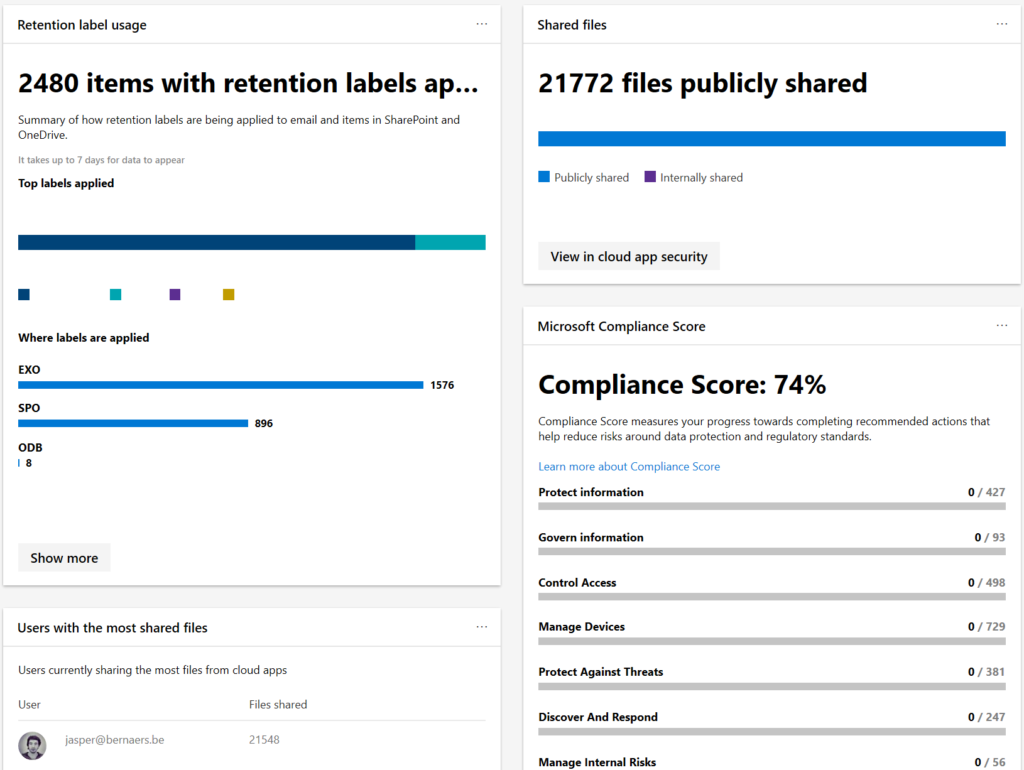
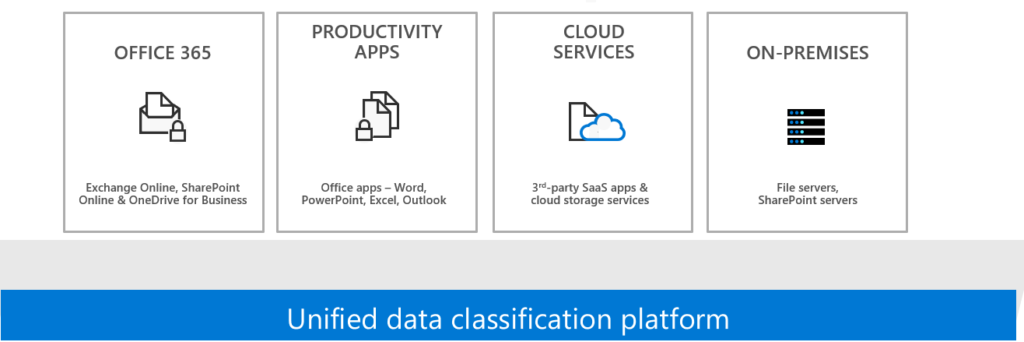


**9. Track and block access for temporary projects or employees leave the company**

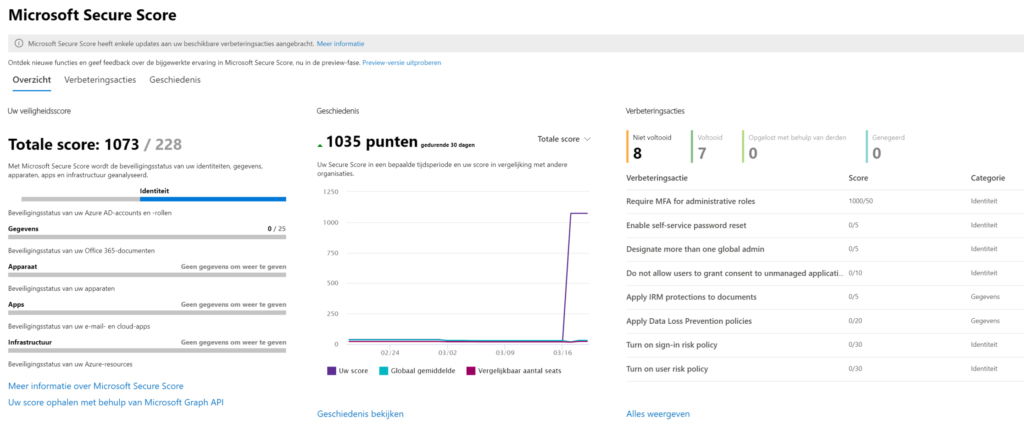
* governance without enforcement is just good advice.
* Create simple written policies, enforce policies.
* Create retention policies for example in a Microsoft Team that removes the team after 180 days.

**10. Use**[**information protection**](https://jasperbernaers.com/tag/information-protection/)**to protect your data everywhere**

* Use[Information protection](https://jasperbernaers.com/tag/information-protection/) to protect document data. Even if you lose the document “physically”. There are still options to block this from opening and keep in secure from distribution, opening, editing,..
* Create document data insights from on-premises and cloud solutions with Microsoft [Information Protection](https://jasperbernaers.com/tag/information-protection/) Policies.



**Conclusions**



* Security priorities are difficult. However, I would always start with [MFA](https://jasperbernaers.com/the-multi-factor-authentication-struggle-and-the-solution/) becasue this is fundamental identity security. Afterwards document and device security. Because companies are moving to Teams during Covid-19. And you don’t want data leakage during this time.
* If your identity is not secure, and compromised, there is no point in doing [information protection](https://jasperbernaers.com/tag/information-protection/). Because a ‘hacker’ will use your accounts to access your corporate data.
* Use Microsoft [Securescore.microsoft.com](https://securescore.microsoft.com/) as a guidance. Extract your priorities.
* Let’s do it!