MASARYK UNIVERSITY

FACULTY OF INFORMATICS

Analysis of Security-as-a-Service solutions for SOHO

Master's Thesis

BC. ADAM HLAVÁČEK

Brno, Spring 2024

MASARYK UNIVERSITY

FACULTY OF INFORMATICS

Analysis of Security-as-a-Service solutions for SOHO

Master's Thesis

BC. ADAM HLAVÁČEK

Advisor: Mgr. Vít Bukač, Ph.D.

Department of Computer Systems and Communications

Brno, Spring 2024

FACULTAS ARTIS INFORMATICÆ • UNIVERSITAS MASARYKIANA •

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Bc. Adam Hlaváček

Advisor: Mgr. Vít Bukač, Ph.D.

Acknowledgements

I am sincerely grateful to my advisor, Mgr. Vít Bukač, Ph.D., for his invaluable guidance and support throughout the development of this thesis. I would also like to extend my gratitude to my consultant, RNDr. Václav Lorenc, whose practical insights into the subject were essential in grounding my research in real-world applications. Your contributions were critical in enhancing the depth and quality of my work.

Additionally, I must thank my girlfriend, family and friends for their support and understanding. Your encouragement has been a source of strength and motivation.

To all of you, I offer my heartfelt thanks for the everlasting support that has been indispensable and cherished.

Abstract

Cybersecurity presents significant challenges, particularly for individuals and small organizations that often lack the expertise and resources necessary for effective defense. This gap has led to the emergence of Security-as-a-Service (SaaS) tailored for Small Office / Home Office (SOHO) environments.

This diploma thesis investigates the relevancy of SaaS solutions for SOHO environments, as offered by major cloud providers. Focusing on various real-life-like scenarios, ranging from individual users to small businesses, the thesis identifies specific cybersecurity requirements and assesses how different SaaS products meet these needs. A comparative analysis methodology is developed to explore the strengths and weaknesses of each solution, providing insights that will assist SOHO users in making informed cybersecurity decisions. This analysis aims to determine which SaaS offerings effectively balance security, cost, and ease of use for diverse SOHO contexts.

Keywords

cybersecurity, SOHO, cloud, Digital Competence, security, privacy, data retention, physical safety

Contents

List of Tables

List of Figures

Abbreviations

AP Access point. 19

CD Continuous development. 27, 37

CI Continuous integration. 27, 37

DigiComp Digital Competence Framework. ix, 9, 11, 12, 13, 14, 15, 16, 17, 18

E2EE End to end encryption. 26, 33, 51, 53, 55, 56, 83, 106

IoT Internet of things. 21

ISP Internet service provider. 20, 29, 30, 75

LAN Local area network. 27, 28, 59, 107

MFA Multi-factor authentization. 22, 23, 24, 25, 28, 32, 34, 48, 53, 61, 76, 77, 78, 85, 106

NAS Network-attached storage. 35, 59, 86, 106

OIDC Open ID Connect. 38, 61, 85

OS Operating System. 5, 19, 29, 35, 39, 42, 54, 55, 77, 78, 108

P2P Peer to peer. 25, 33, 107

SaaS Security-as-a-Service. v, 7, 42, 51, 53, 55, 69

SOHO Small Office / Home Office. v, 6, 8, 95

SSO Single sign-on. x, 30, 34, 48, 49, 53, 54, 55, 61, 70, 73, 84, 85

TLS Transport Layer Security. 29, 84, 85

TOTP Time-based one-time password. x, 50, 51, 53, 55, 76, 77

VPN Virtual private network. 25, 28, 34, 51, 54, 60, 79, 81, 83, 84, 85, 91, 107, 108

VPS Virtual Private Server. x, 44, 80, 82, 91, 107, 108

Introduction

Cybersecurity is a crucial part of everyday life. Be it an individual user with only an email address accessed monthly through a library computer or an international company with thousands of employees, everyone is facing risks. Be it self-inflicted dangers from reckless usage of their own devices, having been selected by automated mass phishing email, or password spraying against their online account, or being specifically targeted; everyone is still at risk of losing their data or privacy to a malicious actor or for good. Even though most people are aware of these ever-looming threats, only some know about relevant security best practices for data protection and retention, as even once-good advice and lessons learned may have aged with the transition to a more internet-connected environment in the last two decades.

With the higher connectivity, new services have arisen, one of the types being security-as-a-services cloud applications that offer to solve the users' cybersecurity needs, while significantly streamlining their security workflow in the process. Instead of having all passwords written on post-it notes around the room or inside an encrypted file on the computer, the users can use a cloud-based password manager that automatically synchronizes between all their devices and auto-fill their passwords whenever needed. Even better, the regular user may not need any password manager at all, as they have a single account with a password-less login, which they use to authenticate against all other applications with a single sign-on. Students no longer have to worry about losing their draft of a lengthy paper just a week before deadline due to accidental deletion of the document or laptop's disc failure because they can simply log in to their friend's computer and download the latest version from a trashbin of their cloud storage provider. A company will not cease to exist because a water main break caused the server room to flood, as they have all their websites distributed around the globe in various data centers managed by their cloud provider. These are just a few examples of how security-as-a-service cloud applications can simplify everyday operations.

In this thesis, I first compare what advice regarding computer security is available and what a general user may stumble upon together with their counter-examples in security best practices. As this thesis is being tailored to a broad audience with different skill sets and levels in their IT backgrounds, in the second chapter, I present and quantify what knowledge can be expected by expressing existing publications in a unified international standard. Afterwards, in Chapter 3, I set forth selected profiles demonstrating standard settings of a combination of a person's IT knowledge and their needs, ranging from a family with minimal technical knowledge to a small technology start-up company. Next, in Chapter 4, I explore selected large general security-as-a-service solutions and their capabilities, together with a small set of solutions tailored for a specific tasks. Finally, in Chapter 5, I showcase the methodology for deciding which solution best fits the needs of the before-mentioned profiles. In Chapter 6, I describe the best possible solutions for each profile in detail.

1 Related work

Related to security in general, numerous publications exist on how to perform day-to-day operations with best practices. However, they often concentrate more on the business side of the user population.

One notable example can be found in a book *Information Security Best Practices: 205 Basic Rules* [1], which, despite being published in 2002, is still being sold and may contain typical advice that today's adults may have heard while first trying online services. The book covers a wide range of best practices that everyone, according to the book, should follow. These practices do include typical advice like:

- ″Use an automatic password generator to help the user with password creation.″
- ″Use a virus scanner on every computer.″
- ″Keep up to date with newly released security software that may enhance security.″
- ″Use a firewall to separate your internal network from the internet.″

Three of the latter are nowadays trivially solved by using Windows Operating System (OS). To highlight the more business-oriented focus of this book, there are often mentions of employees and their security training to reduce the risk of human error leading to possible security breaches. However, some of the best practices presented in this book may be considered severely outdated, such as ″To stop mailings from a known source, send mail to the source with instructions to remove you from their mail list.″, which is presently replaced by the mandatory Unsubscribe button [2][1] included in mass email. Another already outdated example may be ″If you are in the process of being spammed, stop your post office process on the mail server.″, where ideally, the mail server should handle a higher load of messages by itself or should be hosted by a third party is capable of managing such load. The administrator accepts the risk of losing legitimate email communication by shutting down the mailing server.

[1] Large freemail providers like Google and Yahoo are mandating the option to unsubscribe easily

By moving from business-oriented publications towards the SOHO networks, a well-known regularly updated[2] textbook *Guide to Computer Network Security* [3], includes a chapter specifically about home local area network. That chapter, similar to the previous source, provides advice such as

- ”Use virus protection software.”
- ”Use a firewall.”

These rather generally obvious propositions are followed with

- ”Disable Java, JavaScript, and ActiveX if possible.”
- ”Disable scripting features in e-mail programs.”

To abide the first advice may cause issues with many websites that nowadays require JavaScript for proper functioning, putting aside that Java was entirely disabled by browsers like Google Chrome in 2015. [4] Furthermore, the second advice may not be feasible for regular users who rely on web-based email interfaces provided by their email providers, as even Google is turning off its original basic HTML view [5]. As for the recommendation to ”Make a boot disk in case your computer is damaged or compromised.”, this may be above the skill level of a regular user, who may instead use the help of a professional, which is thankfully also recommended in ”Consult your system support personnel if you work from home.”. In ”Make regular backups of critical data.”, the textbook correctly points out that backups are essential for protecting critical data from loss or damage. However, as for the last advice, it can be challenging for a regular user to determine which backup solution is secure and reliable without proper guidance. Additionally, in a section about local network of a family, this publication from 2020 needs to mention the latest security solutions available today, such as WPA3. Another suggestion from the guide is to ”Turn network name broadcasting off”, which hides the SSID of the wireless network and, according to the book, should increase the network security, while the opposite may be true. By hiding the network’s SSID, it is necessary to manually configure every device to connect to it, which the devices do by broadcasting the names of known networks, compromising the device owner’s privacy, as the broadcasts are not encrypted and could lead to a fingerprinting and

[2] The newest published version is from 2024, this thesis is citing from its previous version published in 2020

tracking of the user. Next, the textbook proposes to ″Use the MAC address filter″ to prevent unauthorized devices from accessing the network. Because the MAC addresses can generally be easily spoofed, the security improvement of this advice is relatively low. Ultimately, the general user following this advice will face a much more significant overhead than necessary when setting up any new device.

As cybersecurity is almost always a tradeoff between security and convenience, it needs to be put into perspective of a user who is supposed to use the system. For some users, the convenience or lack of skill to properly manage may outweigh the need for the most secure solution, putting the users at unnecessary risk. With SaaS, one of the advantages is the ability to outsource most of the technical parts to a specialized team behind the SaaS solution while still gaining the security that the solution provides.

To step one step closer to the level of an individual user, we may draw inspiration from a bachelor thesis titled *Selected open tools supporting security and privacy protection for regular end-users* [6], which focuses on the security and privacy needs of regular users. The author defines two user categories: beginners and intermediate users. Beginners have a ″lack of information security and privacy knowledge″ and require ″their system needs to be secured by default″. In contrast, intermediate users ″are aware of basic threats they might encounter″ and ″are confident with adjusting some system properties and trying new features and applications″, while to ″solve problems, they can search for, read and understand standard documentation″. Although the definition of these user profiles may be relatively straightforward, our thesis takes a different approach by basing the user definitions on existing research and international scales, as shown in Chapters 2 and 3. The thesis emphasizes using open-source tools for data security and privacy protection rather than commercial software, which regular users more commonly use. Commercial software also includes widely used tools like Microsoft's operating system, a freemail web client, and a Microsoft Office suite for performing basic document and spreadsheet tasks, which are omitted from this thesis.

When continuing in the direction of commercial operating systems, it is worth mentioning another bachelor thesis called *Password managers: a survey* [7]. This thesis examines various password managers with the condition that they can run on the Windows operating system.

This presents an opportunity for us to compare different software that can be used by or recommended to a general user. The thesis also strongly focuses on usability, which is essential for the general audience who may not have extensive security knowledge. The software selection in this thesis is similar to a previous bachelor thesis about open tools, which included KeePass password manager in some variation, PasswordSafe and Bitwarden. The main difference may be that, in this thesis, the KeePass is its original product, whereas, in the previous thesis, the more modern-looking KeepasXC was presented [6]. While this thesis mainly focuses on analyzing password managers, which is only a very narrow part of the overall security pallet, it can provide valuable insights into what services may be recommended to the users.

Moving away from password managers and focusing more on the data retention aspect of computer security, it may be interesting to mention a paper called *Personal & soho Archiving* [8], which discusses the differences between storing data for archival and personal purposes. The paper presents a unique solution for data archiving that should be specifically tailored to SOHO needs. Although the software used in the paper is not widely adopted, it provides valuable insights into existing solutions and challenges that a SOHO user may face when trying to archive data for long-term storage.

2 Digital Competence Framework

The Digital Competence Framework (DigiComp) "... provides a common framework to assist European citizens and workforce in self-evaluating their skills, setting learning goals, identifying training opportunities, and reaching more and better career opportunities." [9] It is an international tool for evaluating each person's technology readiness. Multiple versions of this framework exist, with the newest being version 2.2, published in 2022 [10]. This version replaces version 2.1, which was published in 2017. [11]. The main difference between version 2.1 and 2.2 is that "The 2.2 update focuses on "Examples of the knowledge, skills and attitudes applicable to each competence" [10], which does not break backwards-compatibility with the previous version and related sources are referring to either of these versions. For this thesis I will use the version interchangeably.

DigiComp comprises five areas and eight proficiency levels. Each of the areas covers a different aspect of working with IT systems, while levels assigned to the areas quantifying the skills of the user in the range from 1 (least-skilled, foundation) to 8 (highly specialized) [10, 11]. The DigiComp areas, together with examples of tasks, can be seen in Table 2.1. The levels are outlined in Table 2.2 [10, 11].

As this framework is supposed to be used on an international level and presents well-defined scales together with examples and explanations, I will use this framework as a reference point for the abilities discussed in user profiles that we can reasonably expect to be present based on existing research and publications. This should make putting this thesis in context with other publications using this scale or directly expanding upon this thesis easier as opposed to developing a custom scale just for this thesis.

Table 2.1: Areas of Digital Competence v2.2 with examples of tasks for each area [10]

Area	Example
Information and data literacy	Browsing, searching, filtering data, information and digital content; Evaluating data, information and digital content; Managing data, information and digital content
Communication and collaboration	Interacting through digital technologies; Sharing through digital technologies; Engaging in citizenship through digital technologies; Collaborating through digital technologies; Netiquette; Managing digital identity
Digital content creation	Developing digital content; Integrating and re-elaborating digital content; Copyright and licenses; Programming
Safety	Protecting devices; Protecting personal data and privacy; Protecting health and well-being; Protecting the environment
Problem solving	Solving technical problems; Identifying needs and technological responses; Creatively using digital technologies; Identifying digital competence gaps

Table 2.2: Proficiency levels of Digital Competence v2.2 with described properties [10, 11]

Level	Description	Cognitive domain	Autonomy
1	Foundation	Remembering	With guidance
2	Foundation	Remembering	Autonomy and with guidance where needed

Continued on next page

Table 2.2: Proficiency levels of Digital Competence v2.2 with described properties [10, 11] (Continued)

Level	Description	Cognitive domain	Autonomy
3	Intermediate	Understanding	On my own
4	Intermediate	Understanding	Independent and according to my needs
5	Advanced	Applying	Guiding others
6	Advanced	Evaluating	Able to adapt to others in a complex context
7	Highly specialized	Creating	Integrate to contribute to the professional practice and to guide others
8	Highly specialized	Creating	Propose new ideas and processes to the field

2.1 Mapping to other scales

DigiComp can be considered bulky because it requires providing several scores for several categories. In practice, various available sources often present their own scales, which are not directly related to DigiComp levels but are simplified to just one overall score. Because of that, I have decided to, instead of presenting levels for each of the areas of the DigiComp, specify only one number, which represents a person's average DigiComp level. This simplification does not necessarily mean a significant loss of accuracy. Especially on lower average levels, it can be expected that the individual person has very similar values in all areas, whereas in company settings, multiple employees should specialize in different areas, collectively gaining the final higher level. With that, it should be possible to map level specifications from other sources into the simplified DigiComp. In the sections below, I provide examples of the general public, employees in service and manufacturing companies, and a Czech high school graduate based on existing publications.

2.1.1 General public proficiency levels

In 2016 [12, 13] and 2019 [14], the OEDC has published a report including the population information and communication technologies (ICT) readiness. This readiness is represented as a portion of a country's population falling into three proficiency levels. The levels on the OECD scale and their best-match mappings into the DigiComp proficiency levels are described [14] in Table 2.3.

For this thesis, I will be using the OECD average level as a point of reference, so this thesis is tailored for a broader audience. In the 2015 policy brief, it is shown that roughly 20 % of adults have reached OECD level 2 (DigiComp 3) and 5 % level 3 (DigiComp 6) [12]. The 2019 publication differentiates between young adults (aged 25-34) and older adults (aged 55-65), where approximately 35 % of younger adults fall into OECD level 2 and 10 % level 3, while for older adults, these numbers are 8 % and 2 % adults respectively. With that, we expect a general audience to be within the DigiComp level range of 2-3, meaning that most adults can perform tasks with which they are familiar on their own.

Table 2.3: Mapping of OECD proficiency levels [14] into DigiComp levels

OECD Level	OECD Description	Digi-Comp level	Explanation
Level 1	Complete tasks in which the goal is explicitly stated and for which the necessary operations are performed single and familiar environment. Solve problems in the context of technology-rich environments whose solutions involve a relatively small number of steps, and a limited amount of monitoring across a large number of actions	2	Is able to autonomously perform operations, but in a familiar environemnt
Level 2	Complete problems that have explicit criteria for success, a small number of applications, and several steps and operators. Can monitor progress towards a solution and handle unexpected outcomes or impasses.	3	Is able to performs tasks on their own, but needs to have the goals expicitly stated

Continued on next page

Table 2.3: Mapping of OECD proficiency levels [14] into DigiComp levels (Continued)

OECD Level	OECD Description	Digi-Comp level	Explanation
Level 3	Complete tasks involving multiple applications, a large number of steps, impasses, and the discovery and use of ad hoc commands in a novel environment. Establish a plan to arrive at a solution and monitor its implementation as they deal with unexpected outcomes and impasses.	6	Is able to select a solution in a complex previously unknown environment.

2.1.2 Industry and service workers' levels

To obtain a reference point of competencies of employees of a service company profile presented in later chapters, I will use a 2021 paper [15], which has explored and compared the digital competencies of employees of manufacturing and service-related companies. Furthermore, the author represents their abilities for multiple area dimensions on a 1 to 4 scale of maturity levels, where ”the lowest maturity level (Level 1) describes a lack of the focused digital competence and the highest level (Level 4) describes a state of completed development compared to the current state-of-the-art.” [15] As the levels presented inside this article cover almost the same scale as the levels from DigiComp, the mapping of the four levels from this publication into the eight levels of DigiComp can be approximated by multiplying the level by two. Next, by averaging the presented maturity levels, we get to level 2.925 for the service company and 1.875 for the manufacturing company, resulting in 5.85 and 3.75 on the DigiComp scale, respectively. This means that we may expect a relatively high ability of service workers to perform even more complex tasks and for manufacturing workers to use their devices independently.

2.1.3 Czech high-school absolved level

The Czech Ministry of Education has provided a list of things a high-school insolvent should be capable of regarding their virtual activity [16]. Even though they do not directly provide numbered DigiComp levels, it is possible to assign the most probable DigiComp level to each of the separate items, and take the average level as the overall high school absolvent's DigiComp proficiency level. The items and the assigned closest-match proficiency levels from DigiComp can be seen in Table 2.4.

The resulting overall rounded proficiency level is 4, which can be translated to a person who is independent in using technologies and can adapt them according to their needs.

Table 2.4: Abilities of Czech high school absolvent [16] with assigned DigiComp proficiency levels

Absolvent's ability	Assigned Level	Explanation
... is proficient with the necessary set of digital devices, applications and services, using them in school work and in public life; adjusts and changes digital technologies and their use as available options evolve and as their own needs change	4	Independent in usage of technologies
... acquires, assesses, manages, shares and communicates data, information and digital content in a variety of formats; to do so, chooses processes, strategies and methods that are appropriate to the specific situation and purpose	5-6	Evaluates the best solution
... creates, enhances and connects digital content in different formats; expresses themselves using digital means	4-5	Is able to creatively apply knowledge for personal tasks
... proposes solutions through digital technologies to improve processes or technologies; can advise on technical problems	5	Is able to guide others in non-professional settings
... deals with the variability of digital technologies and assesses how developments in technology affect different aspects of individual and societal life and the environment, weighing up the risks and benefits	4	Is able to customize the new technologies to their needs

Continued on next page

Table 2.4: Abilities of Czech high school absolvent [16] with assigned DigiComp proficiency levels (Continued)

Absolvent's ability	Assigned Level	Explanation
... avoid situations that threaten the security of equipment and data, and situations that threaten their physical and mental health; act ethically, with consideration and respect for others when collaborating, communicating and sharing information in a digital environment	3	Does understand learned methods of data security and protection on their own

3 Profiles

For this thesis, I have prepared four profiles on which possible security, privacy and data retention threats may be presented. Each of the profiles represents a typical user archetype. All of the profile characteristics and the proposed solutions in later chapters are based on the DigiComp levels shown in the previous chapter. Additional data from which the profiles were created, such as their settings, needs and problems, was obtained from discussions with relevant parties and personal experience. For the creation of each of the profiles a number of real-life samples ranging from 5 to 33 were collected. The exact numbers together with questions and discussed areas can be found in section A.1. During the constructions of profiles, the focus was more laid on the negative patterns observed to better highlight solutions to the issues existing in the wild. This means that no profile is a direct representation of one party, but rather a worst-case scenario of combination of frequently occurring malpractices.

3.1 Low-tech skilled family

The first introduced profile is of a family with middle-aged parents and two young children (aged 12 and 8). Any family member is expected to have a non-IT related education and occupation and, as such, a small technology skill set, ranging on an average Digital competence level 3 [14]. Both parents work in accounting and were issued a laptop from their employer; the kids use a second-hand laptop with a shared account.

3.1.1 Hardware settings

As mentioned above, both parents were provided with a laptop from work, while the kids received a single Windows laptop shared between them. Each family member also possesses an older, lower-to-mid-range Android smartphone (priced under 7,000 CZK). The family has purchased a single 8 TB external HDD as a backup solution for their most important data. Other than that, the family has one large-screen

TV with Tizen OS. All devices are connected to a WiFi router with a single Access point (AP) running.

3.1.2 Software settings

All their laptops run Windows OS, while admin-level permissions are available only on their shared laptop. The family does not (intentionally) use any cloud service to store data. Their family chat is primarily on Viber, whereas children use Instagram as their primary application to stay in touch with friends. For their personal office work and children's school purposes, they use a Microsoft Office 2010 suite, which they have previously paid for. They use default web browsers for each platform, meaning Chrome for their Android phones and Edge on their laptops.

3.1.3 Digital hygiene

As their technological knowledge is in the level 3 range, they are susceptible to adverts and recommendations for software, resulting in multiple antivirus software and computer-cleaning programs being installed superfluously. They are also not bothered by any pop-up dialogues or warnings, as they simply select continue on anything. During the early days of the internet, it was common knowledge that anything uploaded to it would forever stay on it. For that matter, they are reluctant to intentionally (e.g. Viber uses Google Drive in the background for message backups) use any cloud service. They have started with a Seznam.cz accounts for freemail services, but with the arrival of Android phones, they have added a Google account for everyone. Nowadays, they have multiple accounts on various social media platforms (Facebook, TikTok, Instagram), hobby sites, and so on. They use two passwords, one *"strong"* for critical accounts (online banking and primary email account) and one easy-to-remember for all other accounts.

3.1.4 Already solved problems

The family has already solved, or partially solved, some of the possible issues that may arise from their everyday operations. Perhaps most importantly, the family does perform backups in some form. This is true for their shared data (on external HDD) and Android phones, which have backup to Google Drive as the default option. Next, the users are at least aware of basic security practices, so they use antivirus software and multiple passwords. Finally, because their Internet service provider (ISP) set up their home network, it can be considered resilient and properly configured.

3.1.5 Problems with current approach

There are numerous problems with the current approach that can be divided mainly into categories of privacy and computer security. To start with the security related issues, because their Android smartphones are older and are in the lower-to-mid price range, there is a good chance that they no longer receive any security updates, meaning that any known security vulnerability may be exploited. This makes these devices inappropriate for use with any personal data, especially baking applications with financials. As for their shared laptop, Office 2010 is no longer supported[1], which in combination with their low digital competence may make them vulnerable to severe phishing attacks. The severity of this issue is also reinforced by using only two different passwords, where a breach of at least one of them will result in a possible breach of multiple accounts. They also cannot use the password manager built into the web browser, as they use a different browser on every platform. Lastly, depending on their ISP, they were issued an outdated router without relevant security patches, which may be an issue mainly with smaller ISPs within less-densely populated areas.

As for privacy, the most notable issue can be found within the shared laptop, where issues may arise from one of the children forgetting to log out of their session without the web browser. On the other hand, the parents are using work laptops for personal agendas, which may be closely monitored by their employer (depending on the policy deployed by the company). The third risk for privacy is their smart TV, which may record audio of their conversation and send it for analysis

[1] <https://support.microsoft.com/en-us/office/end-of-support-for-office-2010-3a3e45de-51ac-4944-b2ba-c2e415432789>

to third parties without the knowledge of the family. A final privacy risk may be linked with the end-to-end encrypted chatting application Viber, which lists privacy as an important aspect of this service (”Our mission is to protect your privacy so that you never have to think twice about what you can or cannot share when you are using Viber.” [17]), but still stores a large collection of metadata on its servers. [18]

A third category of problems consists of data retention and recovery. Even though the disc used for backup provides a basic level of redundancy, it can still be easily destroyed, e.g., by dropping it, mistakenly deleting wrong files, or simply connecting it to an infected device. Furthermore, this solution cannot be performed automatically, which may result in the backups being outdated. A thought must also be put into backing up their family conversation on Viber, where all messages are lost after onboarding on a new device unless backup is explicitly enabled. [19]

3.1.6 Needs not covered

Some of the needs that needed to be covered were already outlined in the current problems, namely a redundant backup solution prone to accidental or malicious deletion, with the automatic schedule set to prevent backups from being outdated. Next, the family must be aware of basic privacy settings for handling smart devices. As the last part of privacy and security combined, the family would benefit from setting up an isolated guest-only WiFi network for the security reasons of isolating untrusted Internet of things (IoT) devices or for privacy reasons (guests).

Finally, there is a clear need for some form of password management.

Moreover, the parents are also interested in the physical security of their children. Ideally, the parents would want to have the ability to check the real-time position of a child and manage its online activity to prevent any abuse.

3.2 Low-tech skilled university student

The second profile is of a 20-year-old university student in a non-technical program. This student is a Czech high-school absolvent, which, according to the expected level of high-school graduates, would place them on level 4 of the Digital competence scale. [16]

3.2.1 Hardware settings

The student profile is more straightforward regarding hardware settings because they use devices and networks they do not manage at their dormitories or at their parent's home. Nonetheless, the students possess an iPhone 11 smartphone as their primary device and a Windows laptop for note-taking and school-related office work.

3.2.2 Software settings

As their primary device is an iPhone with iOS, most of their software settings are centred around the Apple ecosystem – all their photos and videos are automatically saved to iCloud, as these are default settings of iOS, together with the complete system backup. Because the free storage limit of iCloud is set to 5 GB [20], they need to use the paid plan to fit into the limit. While using their smartphone as their primary device, they create most of their online accounts there, credentials to which they save to the built-in Apple KeyChain.

To work with documents and note-taking, they use the Office 365 suite provided by the university with a linked Microsoft account.

3.2.3 Digital hygiene

For their accounts, they do use Seznam as their main email provider without any Multi-factor authentization (MFA). However, they were issued a school-issued Microsoft account with Outlook for university-based operation and communication. They also have an Apple account, social media accounts and many common accounts for multiple e-shops and hobby sites. Because iCloud is not preinstalled on Windows, they are not aware that it is possible to use this application to synchronize files and passwords [21], so instead, they connect their phone using cable every time they need to copy photos and videos from their iPhone and retype all passwords manually when on desktop.

3.2.4 Problems with current approach

Security-wise, the most critical problem with the current set-up is the Seznam account missing MFA, as up to 200 thousand people lose access to their Seznam account every year. [22] Next, because they are retyping all passwords manually on the desktop, for convenience's sake, they cannot be expected to use as complex passwords as if entirely random and long passwords were used.

Regarding data retention, there is a lack of backup from their Windows laptop, as it is not handled automatically by the Apple ecosystem.

3.2.5 Already solved problems

Because data backup is enabled on iOS by default, the student can recover all their data quickly in case of a lost device. This includes a good password policy, where all passwords are securely stored inside Apple KeyChain, protected by Face ID or fingerprint.

3.2.6 Needs not covered

Even though the Apple ecosystem solves multiple common issues for its users, its closeness produces new ones when interacting with systems outside of it. It makes it harder to interact with Windows PCs and requires the iCloud for Windows software to run on the PC for features like password sync with Google Chrome or Microsoft Edge. [21]

3.3 Individual tech-skilled user

The third profile is again of a 20-year-old student, but with more IT-related experience and knowledge. It is safe to place them at least on level 6 of the digital competence scale, as they are expected to be ”able to adapt to others in a complex context” [11]. As a student with lower income, they are reluctant to pay for software and services if they are able to find a cheaper alternative, even if it requires some level of tinkering.

3.3.1 Hardware settings

As they can configure their devices to an advanced degree and prefer to save financials, they use a mid-range Android phone as their primary mobile device. They also possess a gaming laptop with Windows 11 running on it. Again, as this is a second profile of a student, there is little hardware device to be owned.

3.3.2 Software settings

Software-wise, this profile differs significantly from the profile of low-tech student. As for an Android phone a Google account is a requirement[2], it is the primary account that the student uses. Because the Google ecosystem provides a multitude of services, including a mail service and file storage service, Google Drive, the student heavily utilizes these. Android devices often come preinstalled with the Google Photos application, which, in the past, offered unlimited backup storage [23]; the student uses this application to automatically back up all their photos and videos. Next, as Google offers a free online office suite, they also use Google Drive to store all their documents and notes. In the past, when finding the most fitting file synchronization and sharing service, they have also used Dropbox and Ulož.to but have since forgotten about their accounts on this service.

For web browsing, they use the Google Chrome web browser on both their laptop and Android phone, and the built-in password manager synchronizes their passwords across all platforms. They have also set up an MFA for all their accounts as additional protection where applicable. For Google, their Android smartphone with the Google app installed works as an MFA agent, and for Microsoft and Steam accounts, they have a separate application for each. They have printed the recovery codes on paper to keep access to the accounts in case the smartphone with MFA applications is unavailable.

[2] Unless the user is using a de-Googled variant of Android, which is out of the scope of this thesis.

For communication with peers, they mostly use the Telegram application on smartphones and laptops as an installable application.

They are hosting a Minecraft server on their gaming laptop to play with their friends. Since they do not have a public IP address, they are using LogMeIn Hamachi software to create a Peer to peer (P2P) Virtual private network (VPN).

3.3.3 Digital hygiene

The student is aware of some of the security threats they may become the victim of, so they are using an MFA whenever the service offers them and deploying randomly generated long passwords on other accounts. Furthermore, given that the recovery codes for their accounts are printed only once, it is possible that they need to remember where they have put the codes and may not be able to locate them again if needed.

Because of their student status, they often travel from and to their university, connecting to public WiFi networks on trains, buses, and trams.

3.3.4 Already solved problems

Thanks to a single web browser capable of password synchronization across multiple platforms, the user can have unique strong passwords for every account. Furthermore, on Windows, Google Chrome can protect access to the passwords with the Windows account password, which may serve as a basic level of protection against an attacker with physical access. Next, the user will be notified if there is a reported breach of their account. [24]

Even if (only) the password is leaked for one of their most critical accounts, there may not be any direct risk of account compromise thanks to the deployment of MFA on these accounts.

3.3.5 Problems with current approach

As the student takes security into account when managing login credentials, the biggest security threat may be the need to log into their Google account every time they need to access their passwords. If they perform the login operation on an infected machine, their session may be stolen and used to extract data (passwords, browsing history) from their account. Secondly, there may be threats from other devices connected to the same LogMeIn Hamachi network or the public network in public transportation.

The most significant possible privacy issue is connected to the forgotten legacy account on Dropbox and Ulož.to, which may not be sufficiently protected and still contain personal data. The next possible privacy issue may be with Telegram – a messenger that calls itself "... more secure than mass market messengers like WhatsApp and Line" [25]. The main issue may be that the messenger itself does not have End to end encryption (E2EE) enabled unless a unique feature is used ("Telegram's special secret chats[3] use end-to-end encryption" [25]), but in mainstream media is still being presented as if everything on Telegram was using E2EE [26, 27] or the detail that a particular feature must be turned on is omitted [28, 29], which may confuse or deceive any user into believing that every message on Telegram is protected with E2EE.

Regarding data retention, the student is backing up all their important data on Google Drive, which may be further improved by having a separate backup copy on another service. Not only because an account compromise could lead to the saved files being deleted by a malicious party but also because the service itself can break, and the student could lose some of their files [30, 31].

3.3.6 Needs not covered

Even though the student has covered much of their needs, there may still be room for improvement with malware protection for their smartphone and endpoint protection on untrusted WiFi networks for all their devices.

3.4 Small technology company startup

The final profile is for a small technology company that is currently in its startup phase. As this is a technology company, most of the people

[3] `<https://telegram.org/faq#secret-chats>`

employed will be working directly as a member of the IT/development team or will have service-related jobs, so they can be expected to have an average digital competence level of at least 6 [15].

The company currently consists of approximately 20 employees meeting in a hybrid co-working centre, so a portion of them can be expected to connect remotely from their home offices.

3.4.1 Hardware settings

All employees are provided with a company's MacBook laptop and iPhone smartphone for their employment-related tasks. Next, the company has a self-managed Windows laptop in their office that works as a dedicated server.

3.4.2 Software settings

The company was provided with a static public IPv4 address assigned to their MikroTik router, which acts as an OpenVPN and DNS server. Their laptop server runs Windows with Hyper-V, providing multiple virtual servers for development and production purposes, while itself natively hosts Jenkins[4] software to perform Continuous integration (CI)/Continuous development (CD) jobs. Local area network (LAN) is considered to be fully secure in the rationale that all devices on LAN have to be already authorized to be there in a first place, Jenkins does not need any further login when accessing from a LAN address. All these virtual servers are remotely accessible through shared accounts created on them via SSH for Linux-based or RDP for Windows-based machines. Passwords for said accounts are shared using a document hosted on Google Drive.

In order for the employees to not have to remember the respective IP addresses of all their machines, they have set up static DNS records on their MikroTik router that resolve addresses in the format `xxxx.company.internal`. To have valid HTTPS certificates, they have created a custom certification authority with a root certificate installed on all company devices.

[4] <https://www.jenkins.io/>

All their project files are stored inside private repositories on central GitLab instance[5], but larger files (e.g. large binary files, promotional videos) are being transferred using USB flash discs.

3.4.3 Digital hygiene

As this is a technology startup, most employees know that computer security should be implemented on some level. However, though as they are roughly aware what security contains, they may be unreasonably confident in detecting and avoiding all threats.

Next, as there is no central company monitoring software enforcing company device usage policy, employees also use the devices for personal matters.

3.4.4 Problems with current approach

The most immediately notable security threat is a file with plain-text shared passwords, as its leak may lead to a compromise of multiple devices. The second problem may be with the OpenVPN server on the MikroTik router not supporting any form of MFA, meaning that a compromise of a single VPN account password could compromise the whole company's internal network. This issue is linked to the Jenkins build server, which does not require any additional login when accessing from LAN, which is fully accessible in case of the local network compromise and could lead to failed automation jobs or malicious build being published. An additional issue is linked to the company using its top-level domain name for internal purposes, as not only does this approach introduce a single point of failure in case of the company's local DNS server malfunction, but the installation of a custom company's CA on all of its devices introduces two security threats:

1. As the company does not have any centralized ways to install the CA certificate on all of their devices, it may be possible that some of the employees will not have it installed properly into their system, and rather than spending time on resolving the issue, they will only ignore browser warning about unknown

[5] `<https://gitlab.com/>`

certificate. With that, the user may need help distinguishing between a man-in-the-middle attack and a missing legitimate CA certificate.

2. If the private certificate of the company's internal CA is not stored correctly and is stolen, the attacker may then impersonate any website by simply generating a new certificate for it and launching a man-in-the-middle attack, which the user will not notice unless they analyze which organization has issued a certificate for every website, which is unlikely. This attack effectively removes practically any advantage of using Transport Layer Security (TLS) for communication, as the attacker could intercept and analyze any data sent.

Furthermore, as there is no centralized device management or monitoring software and the employees are using them for personal tasks, there is a risk of employees unintentionally bringing malware into the company or for insider threats to remain undetected.

Regarding data retention, as large files are transferred via unencrypted flash discs, this may lead to company-internal data being leaked in case of flash disc theft or data loss, as there is no direct system for the backup of larger files.

Lastly, having all company servers running as virtual servers on a single Windows laptop poses a significant single point of failure, either from the laptop and its OS being used in different ways than was designed for or by simply having connectivity loss caused by ISP, company's router or the laptop applying new updates. Depending on the length of the outage, this could lead to severe reputation damage for the company.

3.4.5 Already solved problems

Even though it is not done securely, there is a centralized way to manage credentials and secrets. Next, as the code is versioned in a git repository hosted by a reputable service, it may be considered safely backed up.

3.4.6 Needs not covered

The company would benefit from a scaleable virtual machine management that is not dependent on the current state of its ISP. Next, the company should implement some form of least-privilege separation between users accessing the virtual machines, which would streamline the onboarding and offboarding of employees, perhaps best with an SSO from a single identity provider. Lastly, a more robust solution for sharing larger files should be implemented to prevent data loss or data leak.

3.5 Shared needs and problems

A pattern exists among the profiles, which can be categorized as a list of shared problems or needs that any user of any category may encounter. These problems or needs include:

- passwords or secret sharing and synchronization
- backing up important data
- malware endpoint protection
- sharing of documents.

Notably, the requirement for backing up data differs between storing the data for personal use or long-term data preservation dictated by law for companies. Despite these differences in scale, it is observed that every presented user profile does include these needs in some form. Finding a single solution that addresses these needs would be beneficial, as the lower number of used services would lower the risk of setting them up incorrectly or insecurely. It is important to note that when discussing password management or sharing secrets, this thesis also considers identity management services that can be used as single sign-on sources on the reasoning that not having to input any password is generally more secure than having a specifically generated password for each account. This is because the user does not need to have the necessary capacity, knowledge, or skills to manage their passwords securely in the long term. By preferring services that provide a single sign-on service, the user does not need to keep more than a few passwords, mainly for the service itself and other services that do not support single single single single single authentication.

3.6 Summary of problems and needs

To provide more straightforward navigation within this thesis, a bullet point summary of current problems with and needs of all the profiles can be found in Table 3.1.

Table 3.1: Summary of profiles' needs and problems

Profile	Problems	Needs
Low-tech skilled family	• unsupported office suite • possibly outdated router • no guest network separation • complex chat history backup • company laptops used for personal agenda	• password managment • children account separation • resilient personal data backup • physical and virual security of children
Low-tech skilled university student	• main mail account missing MFA • having to re-type passwords on desktop	• sychronization of passwords with desktop • automatic backup of desktop data

Continued on next page

Table 3.1: Summary of profiles' needs and problems (Continued)

Profile	Problems	Needs
Individual tech-skilled user	• sharing the account for password managment and for mail • having P2P connections with untrusted parties • forgotten accounts with leftover data • using Telegram without E2EE	• having backup on multiple services • smartphone malware protection • more secure public WiFi usage

Continued on next page

Table 3.1: Summary of profiles' needs and problems (Continued)

Profile	Problems	Needs
Small technology company start-up	• plain-text shared password • no MFA on VPN server • custom top-level domain & CA • centralized device managment	• scaleable virtual machine managment • least-privilege access • secure file sharing • SSO zero-trust authentication

4 Services

In this chapter, I will explore various existing services that can help address the problems outlined in the previous chapter, with a preference for those solutions that can effectively solve most of the user needs at once. This chapter contains well-known examples that may cover most user requirements while also examining smaller-scale solutions focusing on a specific subset of tasks. Lastly, in later chapters, I will introduce a unique solution that involves self-hosting everything on a Synology Network-attached storage (NAS) device as a control group for the other solutions.

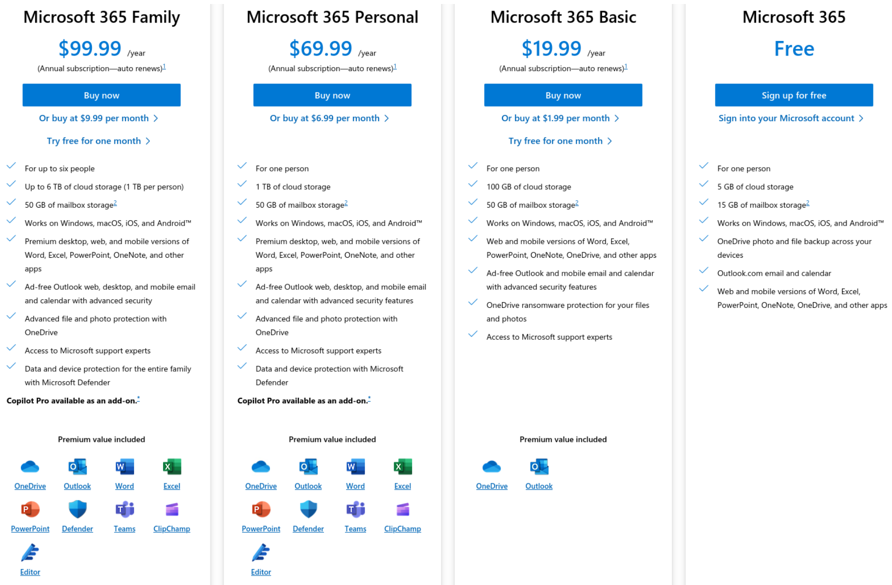
4.1 Microsoft

The first large security provider as a service that we will introduce in this thesis is Microsoft. Microsoft's most well-known product is Windows, currently available in version 10 or 11, dominating the desktop OS market. Besides that, Microsoft also provides a large spectrum of cloud-based services for individuals and company-based use.

4.1.1 Cloud services

Microsoft cloud service services called Microsoft 365, range from its freemail account to OneDrive cloud storage together with a full-featured browser-based office suite. Although, the freemail account is not a requirement, when creating a new Microsoft account, the user may decide if they do want to reuse their existing email account or create a new mail account. For Windows, the preinstalled OneDrive client supports virtual files. Virtual files are shown as regular files while browsing directories on the disc but are downloaded from the cloud only when explicitly requested, saving space on the local machine. In free version of OneDrive, the user has the capacity of 5 GB for cloud storage and 15 GB for mail storage, if they have chosen also to create a mail account. [32]

This storage can be extended to 50 GB or 1 TB in paid plans (Figure 4.1). The business plans start with 1 TB shared or 1 TB per employee (Figure 4.2). [32]



Microsoft 365 Family

$99.99 /year

(Annual subscription—auto renews)[1]

- For up to six people
- Up to 6 TB of cloud storage (1 TB per person)
- 50 GB of mailbox storage[2]
- Works on Windows, macOS, iOS, and Android™
- Premium desktop, web, and mobile versions of Word, Excel, PowerPoint, OneNote, and other apps
- Ad-free Outlook web, desktop, and mobile email and calendar with advanced security
- Advanced file and photo protection with OneDrive
- Access to Microsoft support experts
- Data and device protection for the entire family with Microsoft Defender

Copilot Pro available as an add-on.[*]

Premium value included

Microsoft 365 Personal

$69.99 /year

(Annual subscription—auto renews)[1]

- For one person
- 1 TB of cloud storage
- 50 GB of mailbox storage[2]
- Works on Windows, macOS, iOS, and Android™
- Premium desktop, web, and mobile versions of Word, Excel, PowerPoint, OneNote, and other apps
- Ad-free Outlook web, desktop, and mobile email and calendar with advanced security features
- Advanced file and photo protection with OneDrive
- Access to Microsoft support experts
- Data and device protection with Microsoft Defender

Copilot Pro available as an add-on.[*]

Premium value included

Microsoft 365 Basic

$19.99 /year

(Annual subscription—auto renews)[1]

- For one person
- 100 GB of cloud storage
- 50 GB of mailbox storage[2]
- Works on Windows, macOS, iOS, and Android™
- Web and mobile versions of Word, Excel, PowerPoint, OneNote, OneDrive, and other apps
- Ad-free Outlook and mobile email and calendar with advanced security features
- OneDrive ransomware protection for your files and photos
- Access to Microsoft support experts

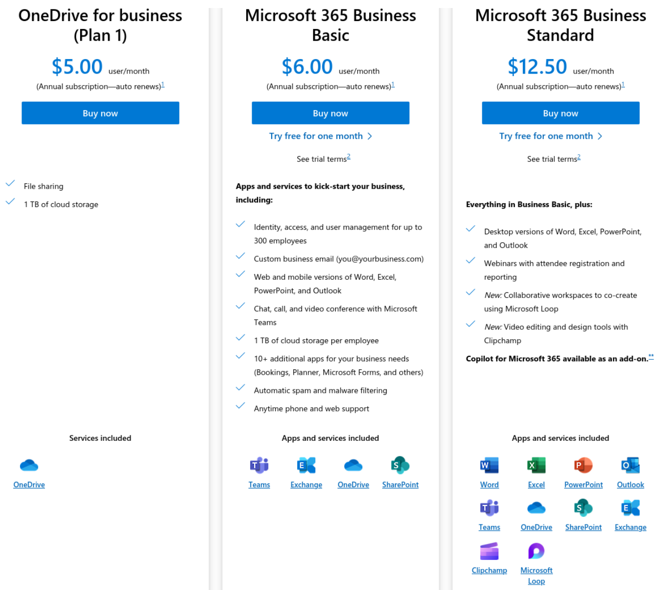
Premium value included

Microsoft 365

Free

- For one person
- 5 GB of cloud storage
- 15 GB of mailbox storage[2]
- Works on Windows, macOS, iOS, and Android™
- OneDrive photo and file backup across your devices
- Outlook.com email and calendar
- Web and mobile versions of Word, Excel, PowerPoint, OneNote, OneDrive, and other apps

Figure 4.1: Pricing and feature comparison for Microsoft 365 individual subscription



OneDrive for business (Plan 1)

$5.00 user/month

(Annual subscription—auto renews)[1]

- File sharing
- 1 TB of cloud storage

Services included

Microsoft 365 Business Basic

$6.00 user/month

(Annual subscription—auto renews)[1]

See trial terms[2]

Apps and services to kick-start your business, including:

- Identity, access, and user management for up to 300 employees
- Custom business email (you@yourbusiness.com)
- Web and mobile versions of Word, Excel, PowerPoint, and Outlook
- Chat, call, and video conference with Microsoft Teams
- 1 TB of cloud storage per employee
- 10+ additional apps for your business needs (Bookings, Planner, Microsoft Forms, and others)
- Automatic spam and malware filtering
- Anytime phone and web support

Apps and services included

Microsoft 365 Business Standard

$12.50 user/month

(Annual subscription—auto renews)[1]

See trial terms[2]

Everything in Business Basic, plus:

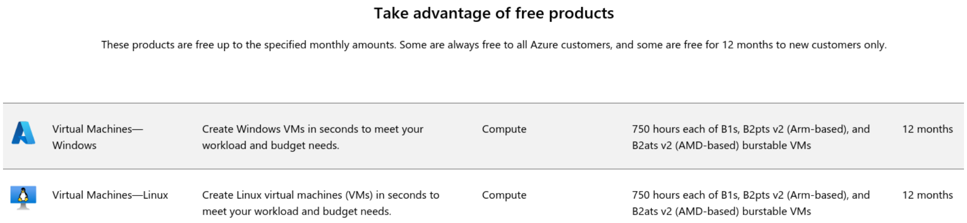
- Desktop versions of Word, Excel, PowerPoint, and Outlook
- Webinars with attendee registration and reporting
- *New:* Collaborative workspaces to co-create using Microsoft Loop
- *New:* Video editing and design tools with Clipchamp

Copilot for Microsoft 365 available as an add-on.[**]

Apps and services included

Figure 4.2: Pricing and feature comparison for Microsoft 365 business subscription

For more business-related use cases, Microsoft provides a cloud hosting service Azure. New customers are presented with a 30-day $200 free credit and popular services free for 12 months. These popular services also include Linux or Windows virtual machines (Figure 4.3). Other than that, there is also a range of always-free services (with some limitations), such as Functions or Azure DevOps, a service for hosting Git repos and performing CI/CD.[1] [33]



Take advantage of free products

These products are free up to the specified monthly amounts. Some are always free to all Azure customers, and some are free for 12 months to new customers only.

Virtual Machines—Windows	Create Windows VMs in seconds to meet your workload and budget needs.	Compute	750 hours each of B1s, B2pts v2 (Arm-based), and B2ats v2 (AMD-based) burstable VMs	12 months
Virtual Machines—Linux	Create Linux virtual machines (VMs) in seconds to meet your workload and budget needs.	Compute	750 hours each of B1s, B2pts v2 (Arm-based), and B2ats v2 (AMD-based) burstable VMs	12 months

Figure 4.3: Azure provided 12 months free for virtual machines

4.1.2 Identity management

After its creation, the Microsoft account can be used as a single sign-on source for other applications. For more technical users and complex scenarios, the accounts can be assigned to groups within the Microsoft Azure portal. For companies, Microsoft also provides advanced security features such as data loss prevention for filtering documents and email messages for company-confidential data or specifying labels assigned to assets together with policies that can apply encryption to the data and prevent its accidental leakage [34]. To help manage multiple company-owned devices and assure compliance with company policies (such as password complexity policies), Microsoft provides Intune, available for all major desktop and smartphone OSs. [35]

One of the options that Microsoft provides is to use the account in a passwordless manner, where the user, instead of typing password, uses a smartphone application to confirm login attempts with their biometric. [36] Because no password is involved, the user does not have to worry about remembering any complex sequence, which is crucial

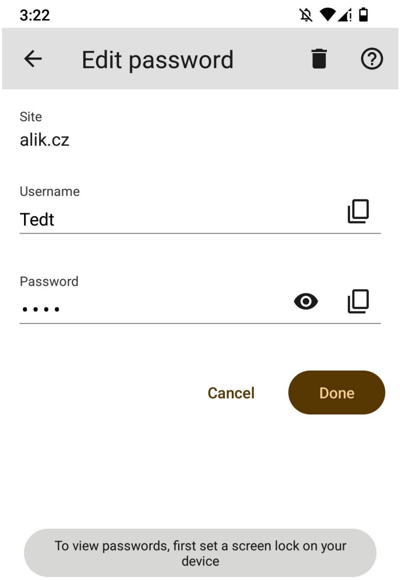
[1] Microsoft does provide a much more extensive range of cloud-based services, such as databases, but these services are out of scope of this thesis and as such are not included

for a user with low password hygiene. Next, as the Microsoft account can be used as an identity source on multiple other web services utilizing OAuth or Open ID Connect (OIDC) protocol, the user can further minimize the number of used passwords while benefiting from password-less authentication even on third-party servers.

4.1.3 Smartphone services

Using the default web browser Microsoft Edge, it is possible to use the Microsoft account to synchronize passwords across all user's devices. The saved passwords are automatically filled into web pages. There is no option to look up saved passwords from a web UI; instead having always to log-into the Edge browser to view the saved passwords. Every time the user wants to show or copy the password manually, they first need to fill in their device login information. [37] The passwords cannot be copied nor shown if the device has no lock-screen protection set, as shown on Figure 4.4. On Android, the Edge browser offers to generate a strong password when creating a new account, while on Windows, this feature needs to be explicitly turned on first inside browser's settings. [38] Lastly, the Edge browser on Android can be set as a service for filling login credentials for all other system applications that support automatic field recognition.

The OneDrive application is also available for Android, where it offers automatic backups of taken photos and video. [39] As OneDrive offers versioning, trashbin and ransomware protection, it is an valid solution to guard against accidental or even malicious data loss. [40]



Site
alik.cz

Username
Tedt

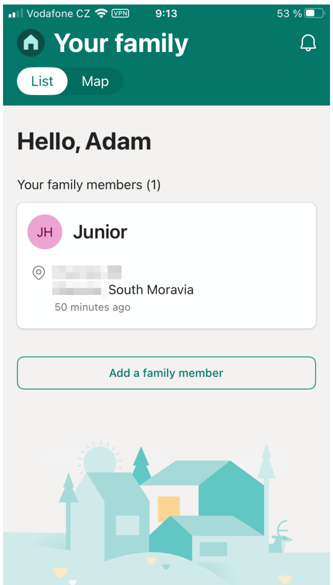
Password
••••

To view passwords, first set a screen lock on your device

Figure 4.4: Password in Edge cannot be shown without a lock-screen in place

4.1.4 Family services

For the Android OS, Microsoft provides a Family Safety application. After installing this application on both the parents and the children's phones, the parents gain the ability to take a look at the children's position (Figure 4.5), be notified when children reach specific locations such as their school or home, or they can impose limits on how much of applications for which time the child can use per day (Figure 4.6). There is also a possibility of recording all their strokes to protect the children against cyber-bullying. [41] Furthermore, when using the Microsoft Edge browser on the smartphone or desktop, the parent can monitor all visited sites and create an allowlist of allowed sites for the child (Figure 4.7). As the application is installed on the smartphone as an administrator of the device, it has the authority to prevent launching of third party web browsers that do not have the same controls and safeguards in place (Figure 4.8).



Hello, Adam

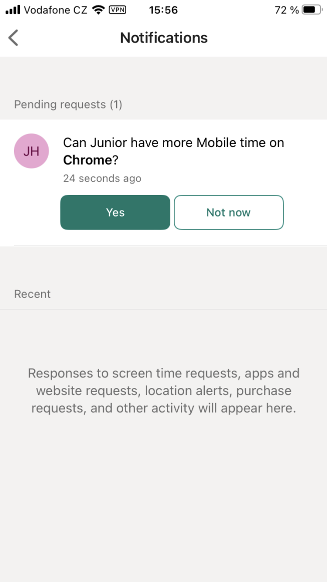
Your family members (1)

JH Junior

[redacted] South Moravia

50 minutes ago

Figure 4.5: Microsoft Family Safety showing position of children

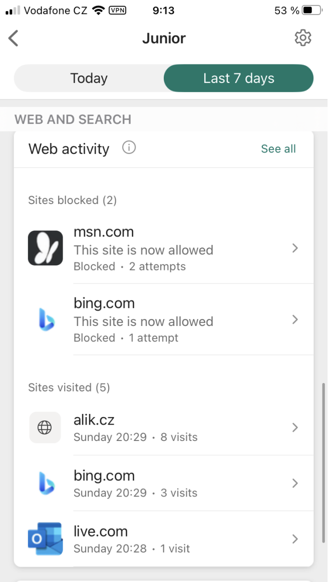


JH Can Junior have more Mobile time on Chrome?

24 seconds ago

Responses to screen time requests, apps and website requests, location alerts, purchase requests, and other activity will appear here.

Figure 4.6: Microsoft Family Safety asking parent to allow access to application



Vodafone CZ 9:13 53 %

Junior

Today | Last 7 days

WEB AND SEARCH

Web activity See all

Sites blocked (2)

msn.com
This site is now allowed
Blocked · 2 attempts

bing.com
This site is now allowed
Blocked · 1 attempt

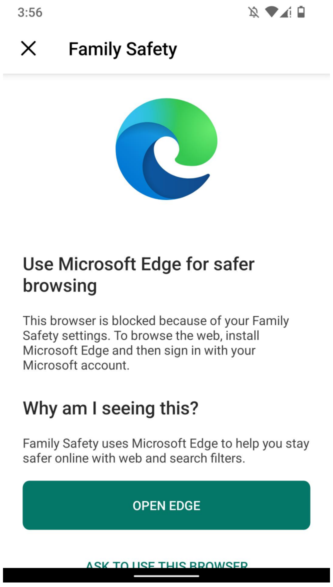
Sites visited (5)

alik.cz
Sunday 20:29 · 8 visits

bing.com
Sunday 20:29 · 3 visits

live.com
Sunday 20:28 · 1 visit

Figure 4.7: Microsoft Family Safety activity overview



3:56

Family Safety

Use Microsoft Edge for safer browsing

This browser is blocked because of your Family Safety settings. To browse the web, install Microsoft Edge and then sign in with your Microsoft account.

Why am I seeing this?

Family Safety uses Microsoft Edge to help you stay safer online with web and search filters.

OPEN EDGE

ASK TO USE THIS BROWSER

Figure 4.8: Microsoft Family Safety preventing launch of other web browser than Microsoft Edge

4.1.5 Desktop integration

As an operating system from Microsoft, Windows seamlessly integrates with the company's services ecosystem. Windows comes preinstalled with the OneDrive application or Microsoft Defender, an endpoint malware protection program. The operating system features also contain a Microsoft Smart Screen, which verifies the authenticity of applications before launching them. This security measure ensures that only trusted applications are allowed to run on the computer unless explicitly disabled. When using a BitLocker-encrypted hard drive, Microsoft also provides an option to recover encryption keys from the online portal if needed.

4.2 Google

Google is the second largest SaaS provider introduced in this thesis. Unlike Microsoft, which has a large portion of the desktop market, Google has extensive smartphone market coverage with its Android OS. New devices with this system often come with preinstalled Google applications.

Google is also well-known for its web browser, Google Chrome. One of the security benefits of using this browser is its built-in phishing protection. [42] Next, like the Microsoft Edge, the Chrome browser has an inbuilt password manager. On the desktop, the password manager works similarly to the Edge browser, offering the option to be notified when any saved passwords are found within the list of known breached passwords. The main difference is that, when signed into the account, the passwords can also be shown within the Google passwords web portal[2], making accessing the passwords on any device easier.

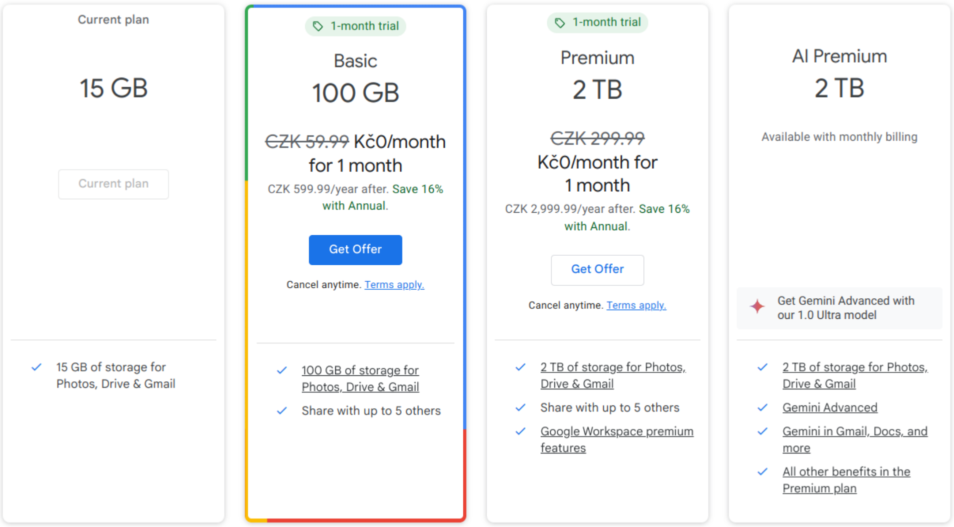
4.2.1 Cloud services

Google provides various publicly available free services, perhaps most importantly, its free mail service, Gmail, and cloud storage, Google Drive. These services include a shared free 15 GB of storage and a full

[2] <https://passwords.google.com/>

web-based office suite. With a Google One subscription plan, the storage can be extended to up to 2 TB, which can be shared with up to 5 others (Figure 4.9). [43] When in company settings with more than six people, Google offers its Google Workspace solution, which provides company mail hosting solution, video conferences via Google Meet and storage for Google Drive ranging from 30 GB to 5 TB per user, or more with undisclosed pricing (Figure 4.10). [44] Google Drive offers a trash bin and version control, with a detailed differentials version history for the office documents. To further strengthen the security of the files stored on Google Drive or received to a Gmail account, Google scans all files for malware or possible phishing documents. [45]

To access files stored on Google Drive on Windows, the user may download the Google Drive application to access and synchronize stored files. All supported platforms, including smartphone apps, can make specific files available even when not connected to the internet. Though, if the user wants to edit documents within the web office suite, they need to install a Chrome extension to edit documents offline. [46]



Current plan

15 GB

Current plan

✓ 15 GB of storage for Photos, Drive & Gmail

1-month trial

Basic

100 GB

~~CZK 59.99~~ Kč0/month for 1 month

CZK 599.99/year after. Save 16% with Annual.

Get Offer

Cancel anytime. Terms apply.

✓ 100 GB of storage for Photos, Drive & Gmail

✓ Share with up to 5 others

1-month trial

Premium

2 TB

~~CZK 299.99~~

Kč0/month for 1 month

CZK 2,999.99/year after. Save 16% with Annual.

Get Offer

Cancel anytime. Terms apply.

✓ 2 TB of storage for Photos, Drive & Gmail

✓ Share with up to 5 others

✓ Google Workspace premium features

AI Premium

2 TB

Available with monthly billing

Get Gemini Advanced with our 1.0 Ultra model

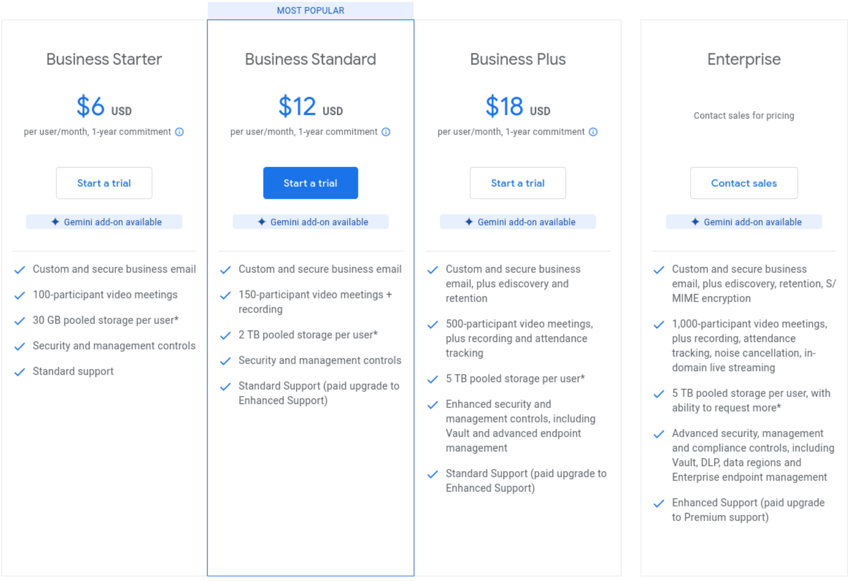
✓ 2 TB of storage for Photos, Drive & Gmail

✓ Gemini Advanced

✓ Gemini in Gmail, Docs, and more

✓ All other benefits in the Premium plan

Figure 4.9: Google One Subscription plans



MOST POPULAR

Business Starter

$6 USD

per user/month, 1-year commitment

Start a trial

✦ Gemini add-on available

- ✓ Custom and secure business email
- ✓ 100-participant video meetings
- ✓ 30 GB pooled storage per user*
- ✓ Security and management controls
- ✓ Standard support

Business Standard

$12 USD

per user/month, 1-year commitment

Start a trial

✦ Gemini add-on available

- ✓ Custom and secure business email
- ✓ 150-participant video meetings + recording
- ✓ 2 TB pooled storage per user*
- ✓ Security and management controls
- ✓ Standard Support (paid upgrade to Enhanced Support)

Business Plus

$18 USD

per user/month, 1-year commitment

Start a trial

✦ Gemini add-on available

- ✓ Custom and secure business email, plus ediscovery and retention
- ✓ 500-participant video meetings, plus recording and attendance tracking
- ✓ 5 TB pooled storage per user*
- ✓ Enhanced security and management controls, including Vault and advanced endpoint management
- ✓ Standard Support (paid upgrade to Enhanced Support)

Enterprise

Contact sales for pricing

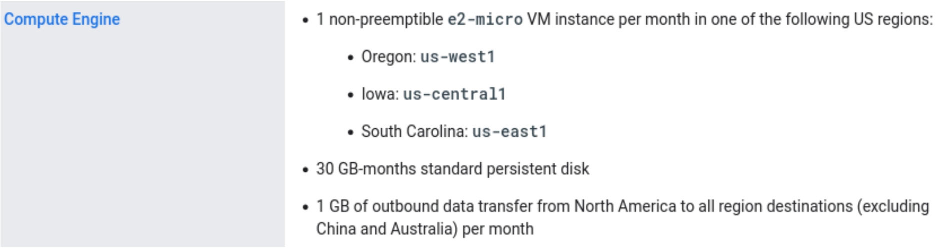
Contact sales

✦ Gemini add-on available

- ✓ Custom and secure business email, plus ediscovery, retention, S/MIME encryption
- ✓ 1,000-participant video meetings, plus recording, attendance tracking, noise cancellation, in-domain live streaming
- ✓ 5 TB pooled storage per user, with ability to request more*
- ✓ Advanced security, management and compliance controls, including Vault, DLP, data regions and Enterprise endpoint management
- ✓ Enhanced Support (paid upgrade to Premium support)

Figure 4.10: Google Workspace subscription plans

For more advanced use cases, Google offers its cloud hosting solution, Google Cloud. This cloud provides standard features such as VPS hosting, functions, containers, databases and more. One of the specifics of the Google Cloud is that it provides a 90-day $300 free trial and also a range of always-free services, including a always-free VPS with specifications as shown on Figure 4.11. [47] With company settings, Google offers device management and support for all major desktop and smartphone OSs. [48]



Compute Engine

- 1 non-preemptible e2-micro VM instance per month in one of the following US regions:
  - Oregon: us-west1
  - Iowa: us-central1
  - South Carolina: us-east1
- 30 GB-months standard persistent disk
- 1 GB of outbound data transfer from North America to all region destinations (excluding China and Australia) per month

Figure 4.11: Free VPS specifications provided by Google Cloud

4.2.2 Smartphone services

When installing new applications through Google Play, the applications have already been processed by Google Play Protect and are deemed non-malicious. [49] Next, because of sometimes slow rolling out of security updates for Android devices by third-party manufacturers, Google has introduces a feature to the preinstalled Google Play Services, that can be used to apply security patches on its own. [50] To recover a misplaced device, Google offers a web portal that can contact the device and show its real-time location on the map or force the device to start ringing. On Android, Google also offers the ability to perform a backup and restore all apps supporting it on a fresh or new device. [51] Next, Google offers to save and auto-fill saved passwords by default, making the process frictionless.

4.2.3 Family services

Similarly to Microsoft's Family Safety, Google presents its service called Family Link. After linking parent and children accounts, this service allows for seeing the child's physical location in real-time or specifying which applications and sites they can access while optionally imposing time limits. The controls can be more granular on per-Google-app basis, meaning that the parent can currently configure control restrictions for:

- Google Play Store
- YouTube
- Google Chrome
- Google search
- Google Assistant
- Google Photos

These restrictions are applied whenever possible, e.g. YouTube and Google search options are enforced whenever the child logs in with their account, while Google Chrome settings are used on all platforms.

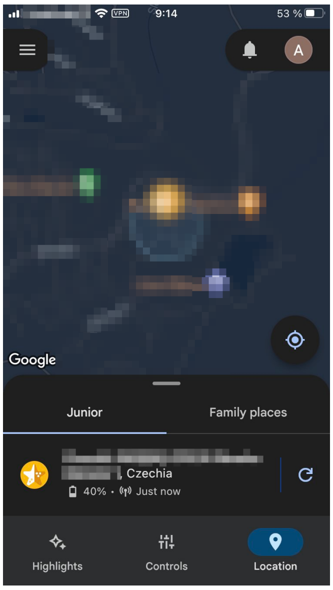
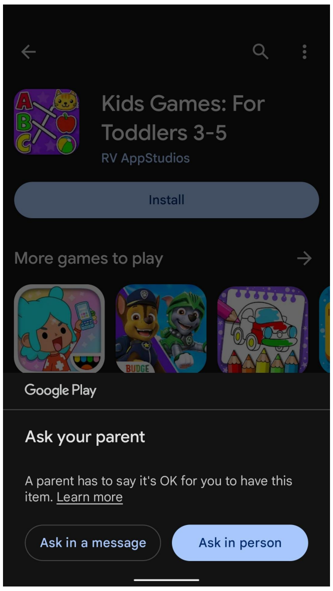


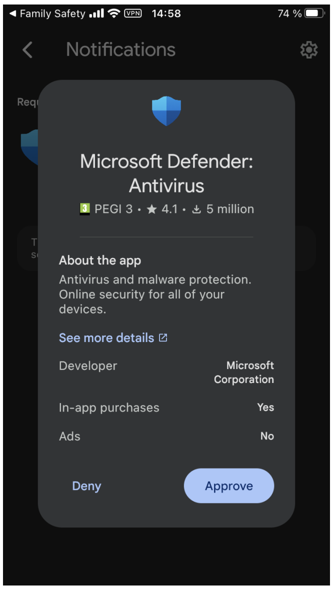
Figure 4.12: Google Family Link showing the position of children



Ask your parent

A parent has to say it's OK for you to have this item. Learn more

Figure 4.13: Child attempting to install application requires approval form Google Family Link



Microsoft Defender: Antivirus

PEGI 3 • ★ 4.1 • 5 million

About the app

Antivirus and malware protection. Online security for all of your devices.

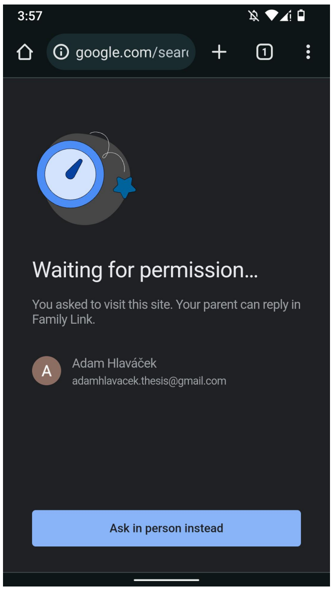
See more details

Developer: Microsoft Corporation

In-app purchases: Yes

Ads: No

Figure 4.14: Google Family Link asking parent to approve installation on child's device



Waiting for permission...

You asked to visit this site. Your parent can reply in Family Link.

Adam Hlaváček
adamhlavacek.thesis@gmail.com

Figure 4.15: Google Family Link preventing the child from accessing disallowed site in Google Chrome

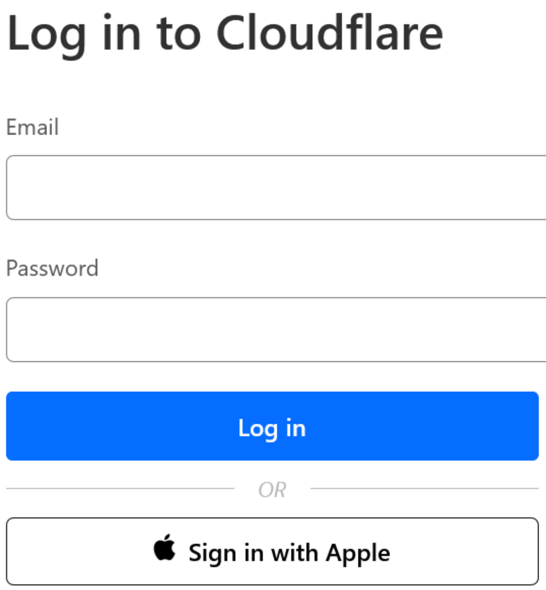
Furthermore, the parent can control the whole device more closely; they can remotely lock the device, turn on or off installation of applications outside Google Play, turn developer options on or off or directly manage permissions of each application – e.g. removing the microphone permission from a web browser and checking an option that only the parent can allow the application to access the microphone on the child's device. Next, the parent has detailed control of the child's Google account – they can set the required parent's approval on every sign-in attempt to the child's account or when the child uses their Google account to sign into a third-party app. They can also change the child's password directly or delete the account.

4.3 Apple

Another ecosystem that provides security as a service is the Apple ecosystem. Even though all of Apple's services are mostly closed for devices produced by the company, it provides a wide range of services for them.

4.3.1 Identity management

Apple provides an option to create a new free account, called Apple ID, for its products. This account is essential for the correct working of Apple-produced devices, as currently, it is needed to be able to install new software from the Apple store. With this account, the user may also create a new mail account on the icloud.com domain. This account can be subsequently used as an identity source for other services, e.g., the only SSO login option to the Cloudflare Dashboard (Figure 4.16). The login process to the Apple account itself can be set to require login confirmation in a form of MFA on the user's existing device.



Log in to Cloudflare

Email

Password

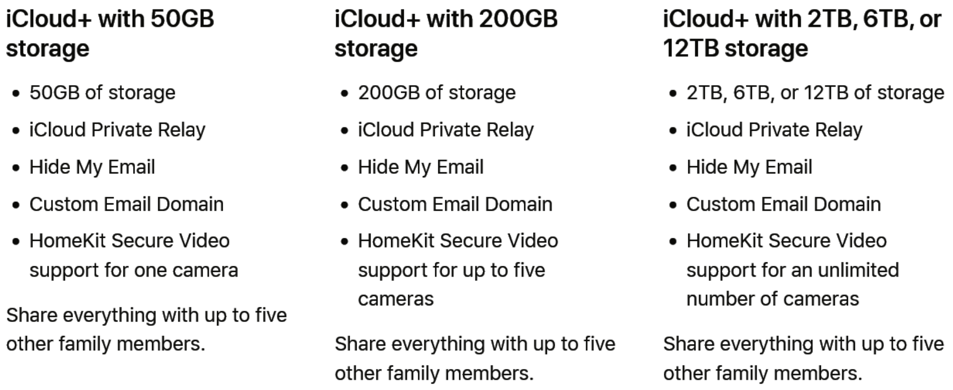
Figure 4.16: Login form for a Cloudflare Dashboard portal with Apple ID as the only SSO option

4.3.2 Cloud services

Apple's main point of cloud services for general consumers is its cloud storage, iCloud Drive. With a free Apple ID account on an Apple device, the user gets only 5 GB of storage. However, this storage can be extended with a paid subscription. By default, Apple automatically backs up all photos taken and the whole device to the iCloud Drive. As this does not require any action to be taken by the user, it can be considered a secure-by-default solution. On the other hand, it can quickly drain the available free storage, pushing users to the paid subscription. Unlike other cloud storage providers, Apple does not support versioning files, but only allows of restoration of deleted files from the trash bin. [52] The paid subscription is priced monthly at [20] (Figure 4.17):

- 25 CZK for 50 GB
- 79 CZK for 200 GB
- 249 CZK for 2 TB
- 749 CZK for 6 TB
- 1490 CZK for 12 TB

Other than these tiered subscriptions, the possibility exists to use so-called Web-only access to iCloud, which offers only 1 GB of space. [53]



iCloud+ with 50GB storage

- 50GB of storage
- iCloud Private Relay
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for one camera

Share everything with up to five other family members.

iCloud+ with 200GB storage

- 200GB of storage
- iCloud Private Relay
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for up to five cameras

Share everything with up to five other family members.

iCloud+ with 2TB, 6TB, or 12TB storage

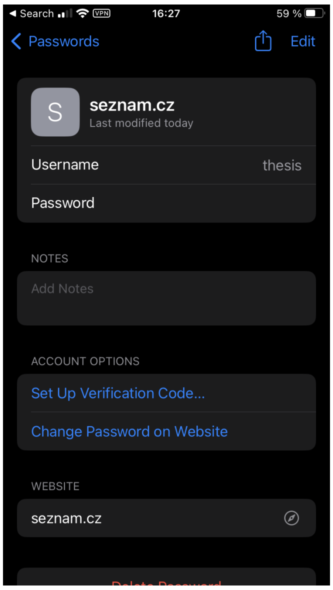
- 2TB, 6TB, or 12TB of storage
- iCloud Private Relay
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for an unlimited number of cameras

Share everything with up to five other family members.

Figure 4.17: Payed subscription plans for iCloud

Apple also provides a complete office suite for all Apple-produced devices and web access using iCloud.

Another security feature that is available on Apple devices by default is its password manager, iCloud Keychain. This manager is set to auto-fill on iOS by default and is protected by the same measures as the device's lock screen. It is possible to access the passwords stored within the Keychain on Windows with the dedicated iCloud application and browser extension. [21] App Keychain can generate TOTP codes, as shown on Figure 4.18.



seznam.cz
Last modified today

Username thesis

Password

NOTES

Add Notes

ACCOUNT OPTIONS

Set Up Verification Code...

Change Password on Website

WEBSITE

seznam.cz

Figure 4.18: Apple KeyChain providing the option to add TOTP

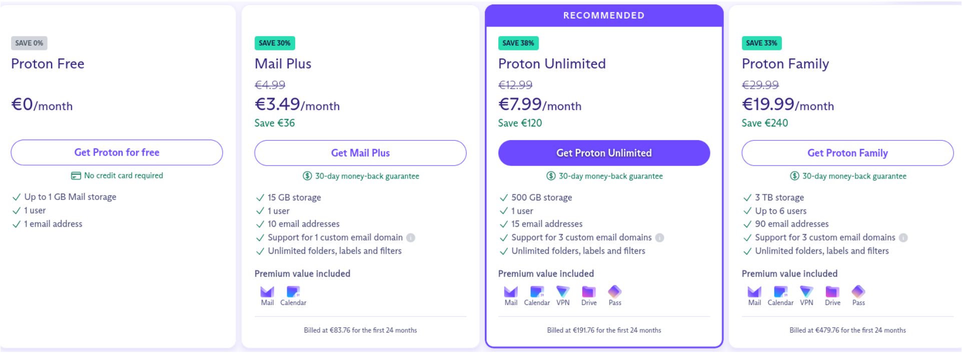
4.3.3 Smartphone services

For Apple devices, Apple provides an E2EE communication service called iMessage. However, as with many Apple products, this service cannot currently be used outside the Apple ecosystem.

For families, it may be helpful that iOS provides a location-sharing feature, where one person can select contacts and see the position updated in real-time. As with Google and Microsoft, there is a web UI for locating a misplaced device.

4.4 Proton

Proton is a Swiss-based company providing SaaS focused primarily on privacy. Its services include an E2EE mail account, Proton Mail with contacts manager, cloud storage Proton Drive and calendar Proton Calendar. Proton also offers a no-log VPN service, ProtonVPN. The free version of the account includes 1 GB of storage for mail, 5 GB of storage for Drive and one connected device to VPN. This can be upgraded to 500 GB of storage shared between mail and Drive for individuals or 3 TB for family tariff (Figure 4.19). Furthermore, paid tariffs allow the addition of custom domains for Proton Mail. [54] For the purposes of this thesis, I will consider the Mail Plus plan the same as the free plan, as it primarily focuses only on the mail-services portion of Proton services and, as such, does not have many of the features of other paid subscriptions. For business plans, the offered storage is 15 GB or 500 GB, while a customizable enterprise plan can be arranged (Figure 4.20). [55]



Proton Free

€0/month

No credit card required

- ✓ Up to 1 GB Mail storage
- ✓ 1 user
- ✓ 1 email address

Mail Plus

~~€4.99~~

€3.49/month

Save €36

30-day money-back guarantee

- ✓ 15 GB storage
- ✓ 1 user
- ✓ 10 email addresses
- ✓ Support for 1 custom email domain
- ✓ Unlimited folders, labels and filters

Premium value included

Billed at €83.76 for the first 24 months

Proton Unlimited

~~€12.99~~

€7.99/month

Save €120

30-day money-back guarantee

- ✓ 500 GB storage
- ✓ 1 user
- ✓ 15 email addresses
- ✓ Support for 3 custom email domains
- ✓ Unlimited folders, labels and filters

Premium value included

Billed at €191.76 for the first 24 months

Proton Family

~~€29.99~~

€19.99/month

Save €240

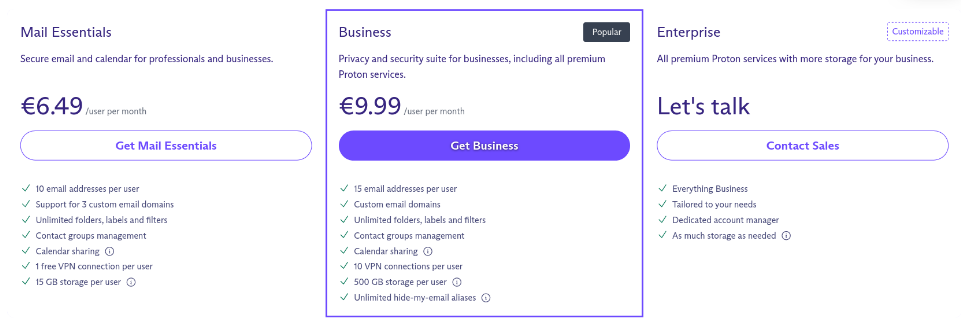
30-day money-back guarantee

- ✓ 3 TB storage
- ✓ Up to 6 users
- ✓ 90 email addresses
- ✓ Support for 3 custom email domains
- ✓ Unlimited folders, labels and filters

Premium value included

Billed at €479.76 for the first 24 months

Figure 4.19: Proton invidual pricing plans



Mail Essentials

Secure email and calendar for professionals and businesses.

€6.49 /user per month

- ✓ 10 email addresses per user
- ✓ Support for 3 custom email domains
- ✓ Unlimited folders, labels and filters
- ✓ Contact groups management
- ✓ Calendar sharing
- ✓ 1 free VPN connection per user
- ✓ 15 GB storage per user

Business

Privacy and security suite for businesses, including all premium Proton services.

€9.99 /user per month

- ✓ 15 email addresses per user
- ✓ Custom email domains
- ✓ Unlimited folders, labels and filters
- ✓ Contact groups management
- ✓ Calendar sharing
- ✓ 10 VPN connections per user
- ✓ 500 GB storage per user
- ✓ Unlimited hide-my-email aliases

Enterprise

All premium Proton services with more storage for your business.

Let's talk

- ✓ Everything Business
- ✓ Tailored to your needs
- ✓ Dedicated account manager
- ✓ As much storage as needed

Figure 4.20: Proton business pricing plans

Unlike Google or Microsoft, Proton Drive does not offer an office suite, so all files must be edited externally. For Windows and Mac, Proton Drive provides desktop applications, while Linux can be integrated with software such as rclone[3], where the user can open their

[3] <https://rclone.org/protondrive/>

files in a local editor of their choosing. The mobile application on Android can automatically upload all taken photos. All deleted files stay inside the trash bin until it is manually emptied. For a paid subscription, Drive keeps up to 200 versions of files for up to 10 years. The E2EE is preserved even when sharing files through links, and the shares can be password-protected with an optional expiration date.

Proton Pass password manager is structured into so-called vaults, which can be shared with others. In the free version, the user can create up to 2 vaults and share them with up to 2 other accounts. For payed plans, the user can create up to 50 vaults, share them with ten other accounts, and use the manager as a time-based one-time password (TOTP) generator. The passwords stored inside the manager can be accessed either through web UI, an extension for popular web browsers, or a native application for smartphone OSs and Windows, with macOS and Linux applications coming soon. [56] On smartphones, the Proton Pass can auto-fill passwords throughout the system.

4.5 Cloudflare

Cloudflare SaaS solutions target companies or IT enthusiasts more than regular individuals, as its central core of services is providing secure web application hosting. However, Cloudflare's range of services is broad so that I will focus only on those relevant to the solutions in this thesis. [57] As for pricing, all of the services discussed in this thesis are free with limits set such as a single person or start-up should not reach them, with some exceptions.

With a Cloudflare account, the user can use R2 – a cloud storage service with S3-compatible API, free for up to 10 GB of stored data [58]. For most services to function, the users first need to link a domain with their Cloudflare account, either by registering it directly on Cloudflare or pointing domain DNS servers toward Cloudflare. After that, the user gains access to a Cloudflare Zero Trust dashboard.

Within the Zero Trust dashboard, it is possible to configure the following services:

- Access – enforces policies, such as users having to authenticate via SSO with MFA enabled until they are allowed to access the application itself (Figure 4.21) [59]

- Routes – after installing a connector on an endpoint device, it is possible to set IP address ranges that should be forwarded through [60]
- Tunnel – after installing a connector, can specify which subdomain should be forwarded through to a specific IP address and port combination [61]

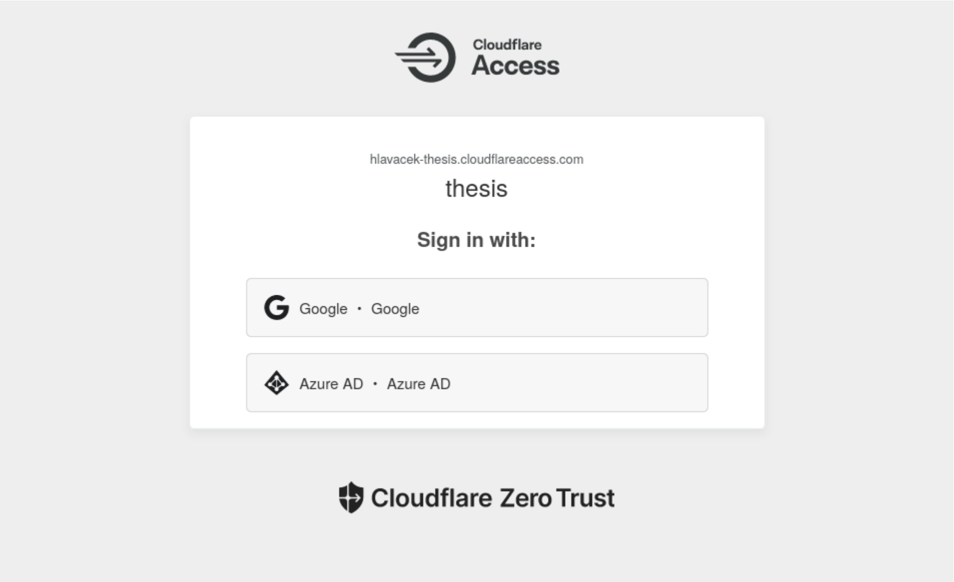


Figure 4.21: Cloudflare Access requiring sign in with two configured SSO providers before allowing access to the application

For HTTP-only or HTTPS-only tunnels, there is no additional software required, while for non-HTTP applications, additional software is required to be installed on the machine that tried to access the resource – WARP client for desktop, Cloudflare One Agent app for iOS and Android. The user logs in to the additional software before any access is allowed so that policies can be enforced correctly.

Other than that, Cloudflare offers a free VPN service called 1.1.1.1 for all major smartphone and desktop OS. This VPN service can switch between functioning as a DNS resolver only or forwarding all data through it, optionally blocking malware or adult sites. [62]

4.6 Bitwarden

As a special solution for SaaS that does not cover a wide range of needs but instead focuses only on one specific area, I would like to introduce Bitwarden. This solution can be found in [7] and [6]. Bitwarden is an open-source password manager that is available as an extension to the web browser and a native application on the most popular platforms. It supports standard features such as auto-filling of passwords but also advanced features where it can pose as a virtual WebAuthn token. Another service available with a free Bitwarden account is the so-called Bitwarden Send[4], capable of sending E2EE text as a link with an expiration date and optional password protection.

Bitwarden also provides paid subscription tiers for individuals, families and businesses, where the added features are the option to share saved credentials, send arbitrary files through Bitwarden Send or use the Bitwarden client as a TOTP keychain. There is an option for business plans to set up login through SSO. Individual plan costs are set at $10 per year, family $40 per year for up to 6 users. Business plans start at $4 per month per user, with SSO included with a plan priced at $6 per month per user. [63]

4.7 BackBlaze

BackBlaze is a cloud-archiving solution focusing on file versioning and deletion prevention. It offers two products:

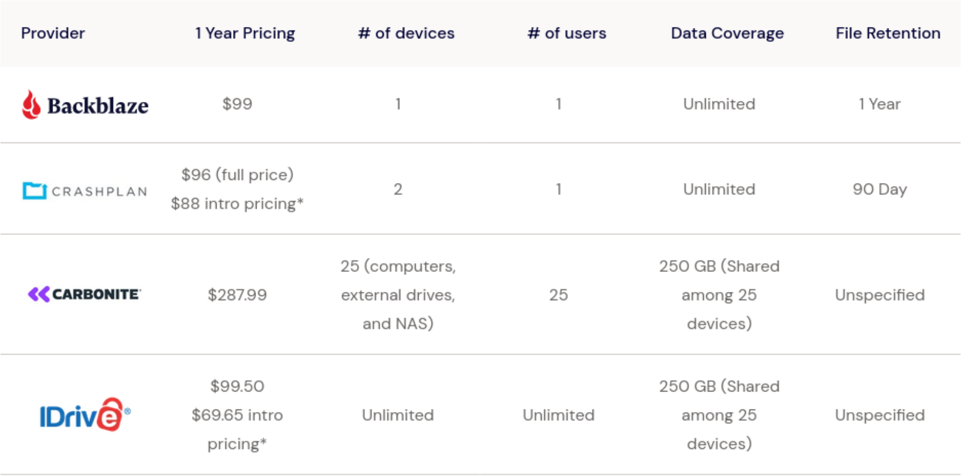
- Computer Backup for backing up personal computers with unlimited storage (Figure 4.22) [64]
- B2 Cloud Storage with S3-compatible API with pay-as-you-go pricing (fixed pricing is available for purchases of 20+ TB, Figure 4.23) [65]

Computer Backup is supported for Windows and Mac OS, while its default setting is to perform a backup of all data across all user profiles. Its unlimited storage for a fixed price makes it a perfect service when the user wants to ensure everything is properly stored. [66]

B2 Cloud Storage works by creating buckets into which the data is uploaded. Except for standard features like versioning of files, B2

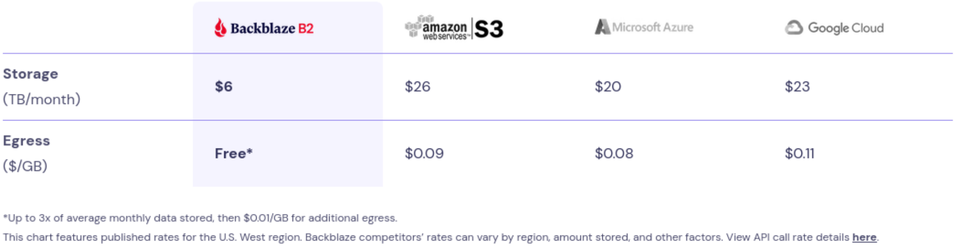
[4] <https://bitwarden.com/products/send/>

offers to set a so-called Object Lock, which prevents modification or deletion of files for a given period, which is useful for protecting against ransomware attacks or compliance with local laws. [67]



Provider	1 Year Pricing	# of devices	# of users	Data Coverage	File Retention
Backblaze	$99	1	1	Unlimited	1 Year
CRASHPLAN	$96 (full price) $88 intro pricing*	2	1	Unlimited	90 Day
CARBONITE	$287.99	25 (computers, external drives, and NAS)	25	250 GB (Shared among 25 devices)	Unspecified
IDrive	$99.50 $69.65 intro pricing*	Unlimited	Unlimited	250 GB (Shared among 25 devices)	Unspecified

Figure 4.22: BackBlaze Computer Backup pricing comparison



	Backblaze B2	amazon web services S3	Microsoft Azure	Google Cloud
Storage (TB/month)	$6	$26	$20	$23
Egress ($/GB)	Free*	$0.09	$0.08	$0.11

*Up to 3x of average monthly data stored, then $0.01/GB for additional egress.

This chart features published rates for the U.S. West region. Backblaze competitors' rates can vary by region, amount stored, and other factors. View API call rate details here.

Figure 4.23: BackBlaze B2 Cloud Storage pricing comparison

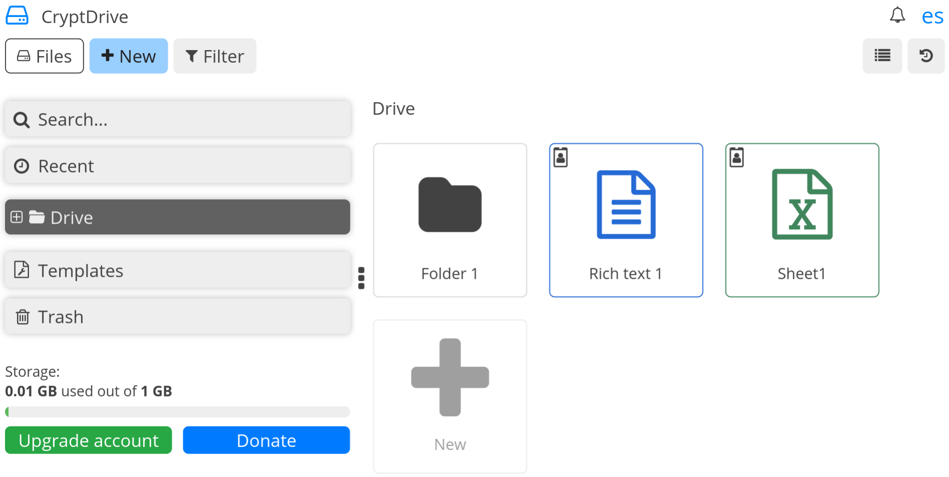
4.8 CryptPad

CryptPad is a service that focuses mainly on E2EE cloud storage. It is similar to Proton Drive but with the addition of an entire office suite contained inside the web UI. The user can either self-host their CryptPad instance, use the official CryptPad[5] instance, or use one of

[5] `<https://cryptpad.fr/>`

third-party instances[6]. When using the official instance, any registered user obtains 1 GB of free storage, while with a paid subscription, it can be upgraded to 50 GB. Every stored file can be shared with other users or by a link. A specific feature is the ability of a document to self-destruct after being opened, e.g. by the recipient of the shared link to it, and a permanent chat for every document. Additionally, in the office suite, CryptPad integrates a calendar and the ability to create virtual teams with multiple users.

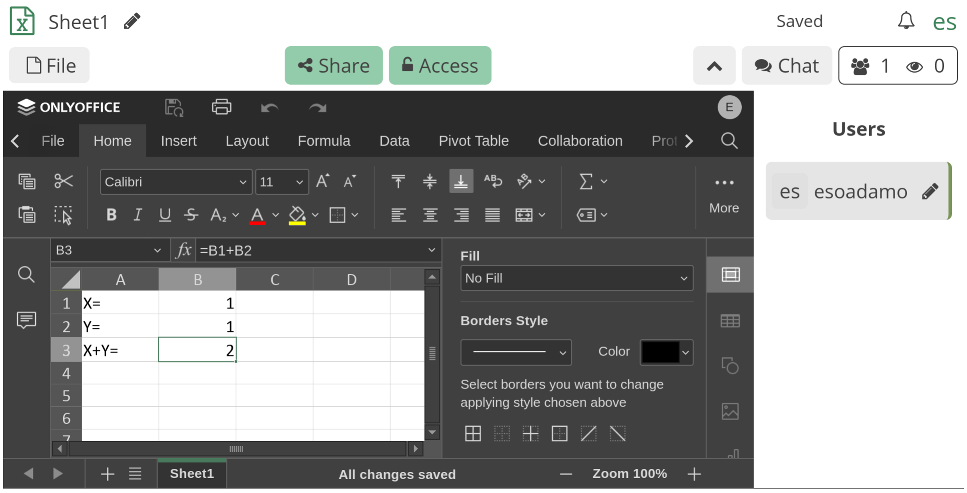
For this thesis, the main downside of the CryptPad is the inability to integrate with other systems. To quote directly from the documentation: ”The way encryption is currently used in CryptPad does not allow syncing with the local file system.” [68] This limitation severely decreases the ease of usage as any user must either keep all their document directly in the cloud or export them manually to the local drive. The second most significant obstacle, at least for the official instance, is that the maximum size of each file is only 25 MB for free accounts and 150 MB for the highest tier of paid accounts.



Storage:
0.01 GB used out of **1 GB**

Figure 4.24: The main menu of CryptPad with folder and files selection

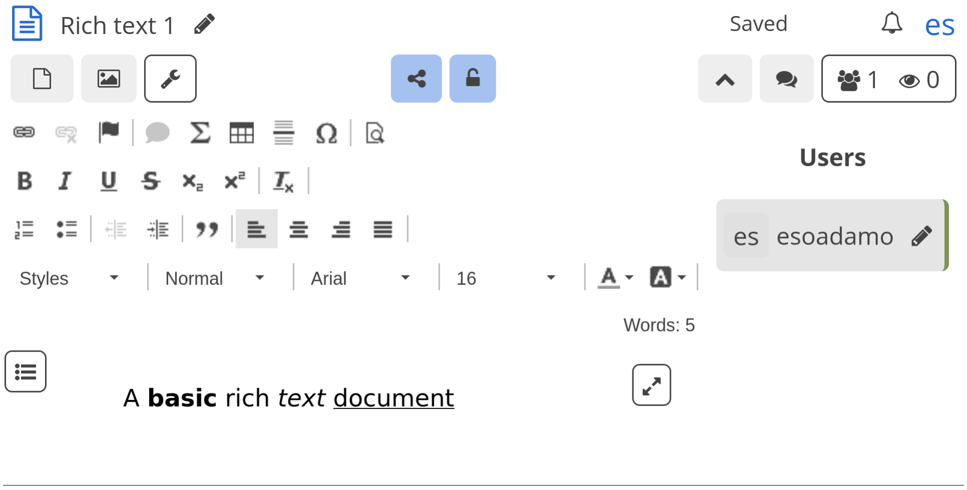
[6] <https://cryptpad.org/instances/>



B3 =B1+B2

	A	B	C	D
1	X=	1		
2	Y=	1		
3	X+Y=	2		
4				
5				
6				

Figure 4.25: Modifying sheet on CryptPad with simple formula



A **basic** rich *text* document

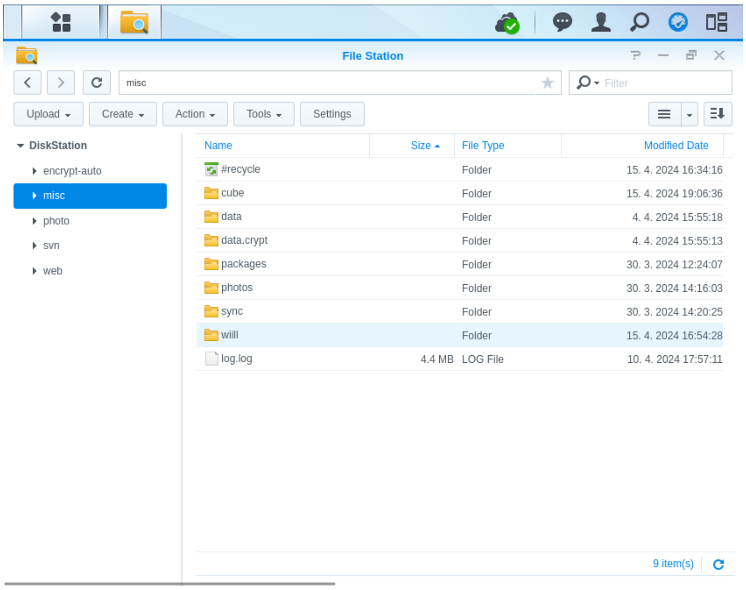
Figure 4.26: Modifying rich text document on CryptPad

4.9 Synology

All of the before-mentioned services share the property of being hosted in the cloud. As some of the services require a monthly subscription to function properly, I am presenting a local solution that should be capable of handling the needs of the users in a similar manner.

Synology NAS is a standalone embedded devices with CPU, RAM and empty disc slots. The discs are supposed to be purchased and installed by the user separately, giving the user full control over how much storage is available. The models differ in CPU performance, RAM size or the number of available disc slots. The primary purpose of the Synology NAS is to be connected to the LAN and easy to configure.

After the separate disc are inserted, the device boots into the DiskStation Manager operating system. Initially, the system consists of a simple web UI for creating an administrator account and setting up the actual topology of drives. The default options are to use Btrfs as a file system, taking advantage of the native support of extent checksum and RAID. After that, the administrator can create additional volumes, and users can then access said volumes through services enabled by the administrator, such as web UI, SMB, FTP, WebDAV, and more. The most prominent disadvantage of using Synology devices is that, unlike cloud-based services, they can reach their end-of-life and may be cut off from all security updates. The second disadvantage that needs to be considered is that with a physical device, the administrator needs to take care of its physical security and protect it from accidental damage or theft.

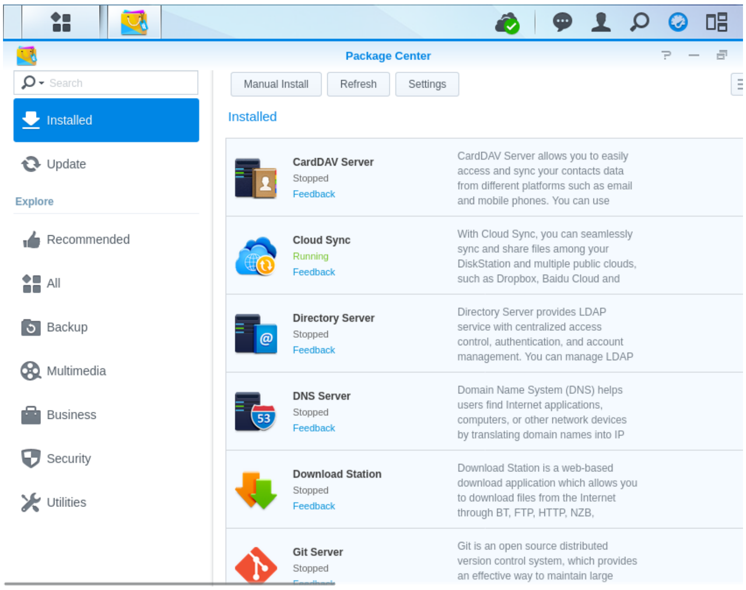


Name	Size	File Type	Modified Date
#recycle		Folder	15. 4. 2024 16:34:16
cube		Folder	15. 4. 2024 19:06:36
data		Folder	4. 4. 2024 15:55:18
data.crypt		Folder	4. 4. 2024 15:55:13
packages		Folder	30. 3. 2024 12:24:07
photos		Folder	30. 3. 2024 14:16:03
sync		Folder	30. 3. 2024 14:20:25
wiill		Folder	15. 4. 2024 16:54:28
log.log	4.4 MB	LOG File	10. 4. 2024 17:57:11

Figure 4.27: Synology DSM Web UI with opened file manager

4.9.1 Provided services

Even though initially, the system supports only file sharing, a wide range of packages exists that can be directly installed to extend the system's functions. These packages include CardDAV for contact synchronization, CloudSync for synchronization with other storage providers (with the option to encrypt the remote content, which may be helpful for backup of local data), VPN server, RADIUS server and many more. Some devices allow the execution of arbitrary docker images or entire virtual machines via Virtual Machine Manager, making it easy to run practically any service.



CardDAV Server
Stopped
Feedback
CardDAV Server allows you to easily access and sync your contacts data from different platforms such as email and mobile phones. You can use

Cloud Sync
Running
Feedback
With Cloud Sync, you can seamlessly sync and share files among your DiskStation and multiple public clouds, such as Dropbox, Baidu Cloud and

Directory Server
Stopped
Feedback
Directory Server provides LDAP service with centralized access control, authentication, and account management. You can manage LDAP

DNS Server
Stopped
Feedback
Domain Name System (DNS) helps users find Internet applications, computers, or other network devices by translating domain names into IP

Download Station
Stopped
Feedback
Download Station is a web-based download application which allows you to download files from the Internet through BT, FTP, HTTP, NZB,

Git Server
Stopped
Git is an open source distributed version control system, which provides an effective way to maintain large

Figure 4.28: Some of the existing Synology DSM packages

For basic cloud-storage-like functionality, installing the Synology Drive Client on the desktop is possible, which will then synchronize the user's local files with Synology drive and vice versa. [69] On a smartphone, the user may install the DS Photo application and set up an automatic upload of newly taken media. [70, 71] For editing documents, Synology does offer its web-based office suite as a downloadable package for some of its models. This office suite works similarly to the Google Drive office suite, as it employs its storage format and, as such, requires importing and exporting when working with third-party office suites. [72] When files are modified or deleted, Synology provides both trashbin and restoring old versions, with the office package providing an convenient user interface for the view of performed changes.

For more business-related usage, Synology can perform full-system backups of endpoint devices [73], work as a web-mail client or server, host web pages and more.

4.9.2 Account management

If an SSO Server package is installed, the local Synology account can be used as an SSO source. Other applications can be configured to accept this service with OIDC protocol, including the Cloudflare Zero Trust. [74] Or, the administrator can enable and set up the Directory Server package for LDAP. The accounts may be protected with an MFA using supported methods, such as approved sign-in, OTP code, or hardware security key. [75]

4.9.3 Remote connection

Synology itself provides a feature called QuickConnect, that, after creating a public Synology account, allows to create a device ID that will make the device accessible through the internet without the need to set any port forwarding. The administrator can select which services they want to route publicly through the QuickConnect. [76] Another option may be to set up a Cloudflare tunnel that will route a custom subdomain to a specific port on the local Synology device through the ability to run arbitrary docker images.

5 Methodology for solution

To select and formulate which solutions best fit the needs of every profile, it is necessary first to formulate a methodology for evaluating those solutions. Each service is compared with a set of 9 criteria. Each criterion is formulated as a question with a single-choice answer. Every answer is then awarded up to 6 or 8 points, where scores for each answer were defined after consultation with the thesis supervisor. The final score of the solution is equal to the sum of scores for each criterion. The scores are balanced to prefer solutions that provide higher convenience for the user and their ability to adjust the solution to their needs if they hit an obstacle over fully understanding the underlying inner workings. For example, a low-tech skilled student's understanding of how iCloud Drive performs encryption of the data provides a lower overall benefit over their ability to set up synchronization of files between their iPhone and Windows laptop in a time under a few hours. Similarly, if the solution does solve almost all of the family's problems and needs, it is more valuable, even if not completely free, over a larger number of smaller but free solutions that would need to be set up and managed independently, increasing spent overhead along the way.

The criterion questions that this thesis asks are:

- How long does it take to set the solution up?
  - Under half an hour – 8 points
  - Under one hour – 6 points
  - Under three hours – 4 points
  - Under six hours – 2 points
  - More than six hours or not applicable – 0 points
- Can the user repair it if there is a problem?
  - Without any issues or external sources – 8 points
  - With a simple internet search – 5 points
  - With the help of a peer or professional – 2 points
  - Not likely or not applicable – 0 points
- Does the user understand the solution?
  - They fully understand how the solutions work – 6 points
  - They understand almost all aspects of the solution – 4 points

  - They can remember how to operate the solution without understanding it – 2 points
  - Unlikely they will be able to understand or operate the solution or not applicable – 0 points
- Is it affordable?[1]
  - Free – 6 points
  - Small investment – 5 points
  - Considerable investment – 2 points
  - Over the budget – 0 points
- Does it solve the user's problems and needs?
  - It solves all problems and needs – 8 points
  - It solves most of the problems and needs – 5 points
  - It solves some of the problems and needs – 2 points
  - It does not solve any of the user's problems or needs — 0 points
- Does the solution integrate well with other systems?
  - Integration is a crucial part of the solution – 6 points
  - It is possible to integrate the solution with a reasonable amount of work – 4 points
  - It is possible to integrate the solution with significant work or workarounds – 2 points
  - It is impossible to integrate the solution – 0 points
- Does the solution support importing data?
  - Importing data is a crucial part of the solution – 6 points
  - It is possible to import data to the solution with a reasonable amount of work – 4 points
  - It is possible to import data to the solution with a significant amount of work or data loss – 2 points
  - It is not possible to import data into the solution – 0 points
- Does the solution support exporting data?
  - Exporting data is a crucial part of the solution – 6 points
  - It is possible to export data from the solution with a reasonable amount of work – 4 points

[1] As there is a considerable difference between what a student and what a company considers a small investment, these answers are defined on a per-profile basis in the tables below.

    - It is possible to export data from the solution with a significant amount of work or data loss – 2 points
    - It is not possible to export data from the solution – 0 points
- Is this solution relevant to the profile?
    - It is essential to fulfil the problems and needs – 8 points
    - It is an important part of the solution – 6 points
    - The service brings some advantages but is not necessary – 2 points
    - This service is fully out of scope for this solution – 0 points

Results of questions for each profile can be found in a form of a table with answer points. If there are any special considerations, they are listed in footnotes below respective table:

- Low-tech skilled family in Table 5.1
- Low-tech skilled university student in Table 5.2
- Individual tech-skilled user in Table 5.3
- Small technology company start-up in Table 5.4

Table 5.1: Low-tech skilled family solutions

Question	Mst	Ggl	Apl	Prt	Clf	Bwa	BaB	Crp	Syn[2]
How long to set solution up?	4	4	4	2	0	4	4	6	2
Can the user repair it?	5	5	2	0[3]	0	0	2	0	2
Does the user understand the solution?	4	4	4	2	0	4	2	2	2
Is it affordable?[4]	5	2	2	2	6	6	2	2	5[5]
Does it solve user's problems and needs?	5	5	5	2	0	2	2	2	2
Does the solution integrate well?	4	4	0	2	0	6	4	0	4
Does the solution support importing data?	6	6	6	6	0	6	6	4	6
Does the solution support exporting data?	6	6	6	6	0	6	4	4	6
Is this solution relevant to the profile?	8	8	2	2	0	6	2	2	6
SUM	**47**	**44**	31	24	6	40	28	22	35

[2] Microsoft, Google, Apple, Proton, Cloudflare, Bitwarden, BackBlaze, CryptPad, Synology

[3] Forgotting password equals losing encryption keys

[4] Free, < 200 CZK/m, < 500 CZK/m, > 500 CZK/m

[5] When used for 5 years

Table 5.2: Low-tech skilled university student solutions

Question	**Mst**	**Ggl**	**Apl**	**Prt**	**Clf**	**Bwa**	**BaB**	**Crp**	**Syn**[6]
How long to set solution up?	6	4	8	4	0	6	6	6	2
Can the user repair it?	5	5	8	2	0	2	5	2	2
Does the user understand the solution?	6	6	4	4	0	4	4	4	2
Is it affordable?[7]	2	0	2	2	6	6	2	0	2
Does it solve user's problems?	8	8	8	5	0	2	0	0	2
Does the solution integrate well?	6	6	6	6	0	6	2	0	4
Does the solution support importing data?	6	6	6	6	0	6	6	4	6
Does the solution support exporting data?	6	6	6	6	0	6	4	4	6
Is this solution relevant to the profile?	8	8	8	6	0	2	2	0	2
SUM	**53**	49	**56**	41	6	40	31	20	28

[6] Microsoft, Google, Apple, Proton, Cloudflare, Bitwarden, BackBlaze, CryptPad, Synology

[7] Free, < 100 CZK/m, < 250 CZK/m, > 250 CZK/m

Table 5.3: Individual tech-skilled user solutions

Question	Mst	Ggl	Apl	Prt	Clf	Bwa	BaB	Crp	Syn[8]
How long to set solution up?	4	4	6	6	4	6	4	6	2
Can the user repair it?	8	8	8	5	5	8	5	5	5
Does the user understand the solution?	6	6	6	4	4	6	6	4	6
Is it affordable?[9]	0	2	2	2	6	6	5	2	2
Does it solve user's problems?	5	5	2	2	5	2	2	0	5
Does the solution integrate well?	6	6	6	6	0	6	2	0	4
Does the solution support importing data?	6	6	6	6	0	6	6	4	6
Does the solution support exporting data?	6	6	6	6	0	6	4	4	6
Is this solution relevant to the profile?	8	8	2	2	6	6	6	2	6
SUM[10]	**49**	**51**	44	39	30	52	40	27	42

[8] Microsoft, Google, Apple, Proton, Cloudflare, Bitwarden, BackBlaze, CryptPad, Synology

[9] Free, < 175 CZK/m, < 375 CZK/m, > 375 CZK/m

[10] As this profile works with multiple services, solution can be also a combination of them – e.g. Cloudflare with Synology

Table 5.4: Small technology company start-up solutions

Question	**Mst**	**Ggl**	**Apl**	**Prt**	**Clf**	**Bwa**	**BaB**	**Crp**	**Syn**[11]
How long to set solution up?	2	2	2	2	2	4	4	2	4
Can the user repair it?	5	5	2	5	5	5	8	5	5
Does the user understand the solution?	4	4	6	6	6	6	6	6	6
Is it affordable?[12]	0	0	2	2	6	2	0	2	5
Does it solve user's problems?	6	6	2	2	5	2	2	2	5
Does the solution integrate well?	6	6	6	6	0	6	2	0	4
Does the solution support importing data?	6	6	6	6	0	6	6	4	6
Does the solution support exporting data?	6	6	6	6	0	6	4	4	6
Is this solution relevant to the profile?	8	8	2	2	6	2	2	2	6
SUM	**43**	**43**	34	37	30	39	34	27	**47**

[11] Microsoft, Google, Apple, Proton, Cloudflare, Bitwarden, BackBlaze, CryptPad, Synology

[12] Free, one-time payment, fixed price, dynamic price

6 Recommended solutions for profiles

In this chapter, I present selected solutions for all of the profiles. These solutions that fit the profile best are described in more detail and accompanied by the possible solution of using a self-hosted Synology device instead of a cloud service. Even though all solutions try to map to the needs and problems of the presented profile as best as possible, in natural settings, it can be expected that the implemented solution will be a combination of all the presented ones, together with smaller SaaS products tailored for specific needs.

6.1 Low-tech skilled family

As mentioned, the most prominent issues faced were their somewhat outdated and mixed knowledge of best practices. As they do not possess an adequate skill set for completing complex tasks, the solutions for this profile will focus mainly on usability, with a slight compromise on privacy and security. Some of the issues, though, can only be solved by training the user on the best security practices, such as not installing multiple malware protection programs.

6.1.1 Microsoft

They are already using Windows on their work laptops and have bought a shared one for their kids, so they are already familiar with this environment. This is a significant advantage thanks to the fewer new things to learn. Microsoft provides two services directly tailored for families, which complement each other:

- Microsoft 365 Family subscription that can be shared for up to 6 people and includes access to the up-to-date versions of classical end-user software from Microsoft
- Microsoft Family Safety, which provides an assortment of tools for monitoring the well-being of a child

Security

As for malware protection, Microsoft offers their Defender for both operating systems utilized by the family. On Windows, Defender is provided without cost and enabled by default. On Android, the Defender needs to be installed separately on every device, together with a valid Microsoft 365 subscription. As this subscription also comes with the newest version of the Microsoft Office suite, it makes the currently used and insecure Office 2010 obsolete, consequently remediating the security threat of opening a maliciously crafted document that exploits known vulnerabilities of the old software.

As a password manager, the Microsoft Edge can be used. Though, if all of the passwords are saved inside Microsoft Edge, the breach of the Microsoft account could lead to a possible breach of all other accounts. For that matter, it is imperative to secure the Microsoft account itself. Here, the ability to use the Microsoft account in a passwordless manner can be fully utilized to protect this account and all accounts that the family will sign into using SSO at once.

Privacy

With the main privacy concern for children being that they use shared account on their laptop, the best possible solution would be to implement five distinct account – one with regular permissions for each child and parent and one with elevated administrator permissions for parents. This will mitigate privacy dangers:

- for children who no longer have to worry about their browsing history being shared or forgetting to log out
- for parents to separate their activity and data from their company-issued laptops

Having a separate administrator account will also improve the overall security standing of the device, as one user cannot simply install a system-wide malicious application. Next, for communication applications, Viber can be replaced by Signal, which focuses on security without compromise and ease of use. On the other hand, neither Signal does persist messages after logging into a new device, unless additional steps are performed.

Data retention

To solve the problem with non-redundant backup, the Family 365 subscription offers every member 1 TB of OneDrive storage, which should be enough for the critical data. Furthermore, as OneDrive is integrated into Windows from the installation, it provides a seamless experience to set up and use. For Android, the family may set up the application to automatically upload taken photos to mitigate problems of lost of damaged device.

Another data loss can currently happen when the Viber application is used as a primary means of communication. Microsoft Teams, part of the Office Suite, may step in as a replacement service. Even though it is a step down in terms of privacy, as it does not provide any form of end-to-end encryption, I would suggest using a service that can archive messages without any user interaction, as losing messages may pose a more significant discomfort to the family than storing the messages on a server with a somewhat reputable company in the plain text.

Child safety

A specific category for this profile is the need to keep children safe in the virtual and physical worlds. For that matter, Microsoft's Family Safety provides those features, just as explained in previous chapters. By linking parents' and children's accounts, the parents can set up parameters for their children's devices.

6.1.2 Google

The family already has a Google account for their Android smartphones, so it will not require them to create any new ones. Like Microsoft, Google provides a dedicated service for the security of children. The disadvantage is that neither the Chrome browser nor Google Drive client is installed on Windows devices by default and needs to be downloaded separately.

Security

On desktops, the most essential part of security for users may be the Google Chrome web browser, together with its phishing protection and password manager. As with Microsoft accounts, when all passwords are being stored within the same account, e.g. email, a simple breach of this account could result in a breach of all accounts for which the user has saved credentials.

As for the vulnerable office suite, the Google provided full-web-based office suite within Google Drive could be used as a replacement. As all documents are edited within the web browser, this solution should not possess any security vulnerabilities that are not present inside the browser itself. On the other hand, this suite may pose some compatibility problems that are explored more within the Data retention section.

Privacy

To solve the most notable privacy problem – the children sharing the same account on their shared laptop – Google provides an option to define multiple Google Chrome profiles, each with its own settings and active accounts. In contrast to creating multiple user accounts, this solution works more on a trust-based approach in that the other child will not internationally launch another child's profile. However, it is easier to set up than creating a new Windows account.

The user may use Google Duo for calls to replace Viber, but no suitable replacement for text messages exists.

Data retention

As Google Drive can be upgraded to up to 2 TB of available storage with the shared Google One subscription, this should still be enough for the family data. However, it is a several step down from the total of up to 6 TB of storage for Microsoft's One drive.

Given that Google has its storage format for the Office suite, and even though it offers most of the features that the user may need, it may only partially support some features available in Microsoft Office. Conversion from the Microsoft Office format into the format used by

Google Drive may not maintain some special formatting, resulting in partial data loss.

Child safety

In addition to similar features in Microsoft Family Safety, the Google Family Link provides more direct control over children's accounts. By allowing the parent to allow the child to use SSO only for applications that do not require permissions except for name, email, and profile picture, the child can safely log into any application without worrying about giving too much access to the account.

6.1.3 Synology

Given that Synology requires an initial setup, it may be necessary for the family to consult with a professional to perform it for them. Even after that, Synology does not provide easy solutions to all outlined problems, and the family will need to keep care of the device – e.g., monitoring that the device is not after its end of life and still receives regular security updates.

Security

To replace the vulnerable Microsoft Office suite, the family can use the Synology web-based office suite. Though, as it uses its own storage format, this approach again presents the possible problem of some features not being fully supported by the Synology office.

Next, Synology does not offer any password manager directly. Of course, it is possible to self-host a password manager such as BitWarden using the generic Docker container feature of some of the Synology models. However, I advise against that, as the family members cannot be expected to maintain a self-hosted password manager in a secure and safe manner.

Even though Synology can be used as an SSO source, it first needs to be configured as such with any application that should support it, making it unfeasible for the family.

Privacy

Except for the obvious advantage that the data does never leave family-owned devices, the most prominent way how Synology may improve privacy is if all the users keep most of their files only stored there, as then they are protected by their account credentials as opposed to having the files synchronized with the shared computer account. The Viber can be replaced by a Synology Chat package that allows basic chatting while outsourcing video and audio calling to third-party applications such as JumpChat and Jitsi. [77]

Data retention

Given that Synology works with the hard drives that the user directly supplies, they significantly impact how resilient the system will be. As the storage is a single-time investment, the hard drive is expected to have more capacity than the 6 TB offered by the Microsoft O365 family subscription. Furthermore, we can probably expect the user to have only one hard drive or set up RAID 0 to maximize the available storage, so the failure of one disc may mean an unrecoverable loss of stored data. To combat this, the user may set up a secondary backup solution, e.g., CloudSync or an in-built Amazon Glacier backup. However, both options require additional setup, possibly too complex, while inquiring more costs.

On the other hand, users may synchronize files from their computers automatically or have their taken media uploaded from their smartphones to store the original data directly on the user's device.

Child safety

As there is no direct control over what content children can access or directly monitor the child's online activity, the options for the child's safety are severely limited. A third-party application may be recommended to monitor at least the children's position. As an example, the family can install an application called Find My Device (FMD) [78], which is capable of responding to commands sent over SMS, so it does not need to rely on any specific service.

6.1.4 Unsolved problems

Unfortunately, not all problems can be solved directly by these services, as they are too complex or out of scope. The first example of this may be the use of outdated Android devices, where the best option may be to buy new devices with a declared duration of security updates. As for an outdated router from the ISP, the best course of action may be to ask the ISP to replace it, as the family cannot be expected to manage their router securely. Related to their router is creating a WiFi network for guests, where a router with a user-friendly web interface may help. Creating a separate WiFi network would also help with moving less-trusted devices into the more isolated network.

As for the possible privacy concerns of using the company-provided laptop for personal activities, here the user needs to consult their company laptop usage policy or contact their IT department. The last need that was not covered is performing a backup of the cloud storage service, such as when the account is compromised and all data falls victim to, e.g., a ransomware attack, there is an option to restore said data. Solving this problem would increase the complexity of the solution, while the currently proposed solutions have already severely increased data security.

6.1.5 Final recommendations

For the profile of a family, out of all the services presented, the services provided by Google and Microsoft are the most fitting and almost interchangeable in terms of solving needs and problems and pricing. Microsoft may be preferable, as it provides higher overall storage space at a slightly lower price. Next, it also comes with an up-to-date version of the Microsoft Office suite, which has no compatibility problems. On the other hand, if 2 TB of shared storage is enough and a more granular control over the child's account is preferable, with only the web-based office suite being sufficient for the user's needs, Google services are a viable solution.

6.2 Low-tech skilled university student

The specificity of low-tech skilled university students is in the closeness of the Apple ecosystem combined with a Windows laptop.

6.2.1 Apple

As the student is already using their smartphone as their main device, they are already used to services provided by Apple by default. Furthermore, as the services are well integrated into iOS, it would be helpful to have a solution that uses the same services on other platforms.

Security

The most crucial security aspect to cover for this profile is the missing MFA for the primary mail account hosted on Seznam. For this, there exist three solutions:

- moving away from Seznam to iCloud mail, which has integrated MFA confirmation into the iOS
- install a separate Seznam application[1] to approve login
- utilize Apple KeyChain as a TOTP code generator

The first solution is time-consuming and, as some services do not allow changing email addresses after account creation, potentially impossible. The second solution is the most secure, as the user can review every login login and act accordingly, but it requires additional application installation.

The third solution may be the most viable, as it uses an application that the user is already comfortable with. This solution also contributes to the user's need to synchronize the password to their desktop, as all the user needs to do is install iCloud for Windows and a web browser extension.

Privacy

By default, iCloud Drive offers encryption in transit and at rest, which should be enough for regular use. Furthermore, when combined with

[1] <https://apps.apple.com/us/app/seznam-cz/id950278657>

the MFA-protected Apple ID account, no unauthorized party should be able to access the stored data.

Data retention

If the users purchase at least 2 TB of storage, it should be enough to store all their critical data. Though the inability of iCloud to properly version files can become a disadvantage if the users accidentally rewrite their files, e.g., when using an external office suite and saving an empty document instead of an existing one. The taken photos are uploaded automatically from iOS by default, while for synchronization with a Windows computer, the user needs to download and install the iCloud application.

6.2.2 Microsoft

Microsoft's main advantage over services provided by Google is its already present integration of Microsoft Edge and OneDrive into the Windows OS. Its solutions are also slightly cheaper than comparable products. Furthermore, as the student is already using O365 via its university subscription, they already have all services free of charge for the length of their studies.

Security

As with Apple, there is an option to use the TOTP secret in the Microsoft Authenticator application, which users should already use if they have MFA enabled for their Microsoft account.

As already stated, Microsoft Edge can hold and synchronize saved passwords to multiple sites. Same as on Android, Microsoft Edge can be changed as the default auto-fill source inside the iOS settings, solving the password management and synchronization between different platforms and systems.

Privacy

Same as the default settings of iCloud Drive, the data is encrypted both in transit and at rest. The protection of the Microsoft account with MFA enabled using Microsoft Authenticator is comparable to the security of Apple ID account.

Data retention

As more than 100 GB of storage may be needed for all documents and photos, the next available tier has a storage size of 1 TB. Compared to iCloud Drive, OneDrive offers support for file versioning.

As OneDrive is already included in the Windows OS, users do not have to install anything new. On iOS, they need to download the OneDrive application, which can automatically upload photos and videos.

6.2.3 Synology

For the individual student with low-tech skills, purchasing a Synology device may be too expensive and overly complex to set up. Furthermore, as the student can be expected to be travelling between their home, dormitory and school, they need to think about the device's physical placement in case of the device or power failure.

Security

As there is no direct option to perform password management or storing MFA tokens instead of directly hosting Docker containers, I conclude Synology as unsuitable for this profile.

Privacy

As with the family profile, Synology's main advantage in terms of privacy is that the data are stored on the user-owned device. Other than that, for the purposes of this profile, there are no significant privacy features.

Data retention

For the purposes of this profile, there is no significant difference in terms of features when compared to the Microsoft OneDrive. The most crucial difference is that the user is now responsible for managing the storage device.

6.2.4 Unsolved problems

As every one of the problems or needs was solved by at least one of the presented solutions, there are no leftover unresolved problems.

6.2.5 Final recommendations

Because the student uses the iPhone as their primary device and already interacts with the Apple ecosystem, it is most convenient for them to use the same services on their laptop. On the other hand, OneDrive from Microsoft provides the additional benefit of restoring an older version of files, which may be preferable if the user is working on longer documents, as this would prevent accidental overwriting. However, this comes at the cost of having only half the storage (1 TB for OneDrive, 2 TB for iCloud Drive) at a comparable price.

6.3 Individual tech-skilled user

As this user is more experienced, we can expect them to be able to understand or create their own even more complex solutions. First, as this profile is more interested in privacy, they may consider switching from their main Google account to Proton, which offers features similar to those the user currently uses. A second advantage of Proton is that it offers a private VPN service that solves the need to protect their device when connecting to untrusted networks.

Next, one of the needs of this profile is to create a distinct account for password management and for other actions. As a separate account for password management, the user may consider BitWarden password manager. This manager is available for all user platforms, can be accessed through web UI so that the user does not need to install additional software, e.g. on university computers, and can also be used to auto-fill on smartphones and web browsers via extensions.

6.3.1 Google

The student already uses a Google account for their daily tasks, so they do not need to create any new accounts for this service. Its main advantage over Microsoft is its always-free tier with VPS, so the student does not need to worry about checking when their free starting credit will run out.

Security

For hosting the Minecraft server for their friends, it is possible to set up the free Google VPS, which is doable either with experience or by following some online hosting tutorials. By default, as the Google VPS's shell can be accessed directly through web UI and the firewall allows only a limited number of ports, this leaves out the need to manage SSH keys or restrict access with a manual firewall configuration, simplifying the process. Furthermore, by moving the hosting away from the student's device, they achieve higher uptime and, in case of compromise of the Minecraft server, security for the data on the student's device.

Data retention

To solve the double-backup problem, which could serve as a last resort in case a malicious party gains access to the currently used cloud storage and purges original files even from the trash bin, Google offers an S3-API compatible solution called Google Storage. With only 5 GB of free storage, the user must change to a paid subscription. The user may set up a system schedule to copy all their local files or whole Google Drive into this remote storage with a program such as rclone[2]. As this setup setup is more complicated, it can be severely simplified with the usage of Synology, as shown below.

[2] <https://rclone.org/googlecloudstorage/>

6.3.2 Cloudflare

Even though Cloudflare is more business-oriented, it may prove usable for the student due to its provided hosting and tunnelling solutions, data storage and VPN.

Security

Even though Cloudflare does not allow it to host the Minecraft server directly, its ZeroTrust network can replace the currently used LogMeIn Hamachi. It can be configured as a direct replacement, where the routes are configured to point to the friend group devices, providing no additional benefit.

The second option requires configuring a tunnel pointing to the student's device and selecting which port should be forwarded. This approach provides additional security because only required ports are exposed, decreasing the possible attack surface.

Privacy

To solve the issue of privacy and security threats of connecting to untrusted networks, the student may use the free VPN software 1.1.1.1.

Data retention

Similarly to Google, Cloudflare provides its S3-API-compatible storage called R2. As the provided free storage is only 10 GB of space, it is reasonable to expect that the user will be required to pay a monthly fee for the stored data. The storing procedure may be the same as outlined for the Google solution.

6.3.3 BackBlaze

As BackBlaze is a service specializing only in data backup, it cannot cover most of the user's needs, except for the double backup. The first option that BackBlaze offers is its B2 Cloud Storage, which has an S3-compatible API and can be used in the same way as Google Storage or Cloudflare R2.

The second option is the unlimited personal backup for $99 per year, which the user may install on their Windows laptop to perform a full backup of their data, together with versioning.

6.3.4 Synology

For this profile, Synology may solve many needs alone or with other presented services.

Security

Like a VPS, Synology can run arbitrary software as a docker container. This means that Synology can host the Minecraft server, achieving a higher uptime than on a laptop and security for the same reasons shown within the Google solution. Remote access to Synology can then be provided by Cloudflare or through a third-party virtual network provider with a step-by-step guide such as ZeroTier[3].

Data retention

Synology provides an option to perform a backup to Amazon Glacier via an official package. Another option may be to use a CloudSync package capable of synchronizing with a remote endpoint and optionally encrypting data on the remote side. Two of the previously shown solutions for this profile – Google Cloud Storage and BackBlaze B2 – are directly supported, so setting them up for backup is relatively straightforward. To use Cloudflare R2 as a backup endpoint, the CloudSync package supports a generic S3-compatible API endpoint.

6.3.5 Unsolved problems

One of the current problems that cannot be solved easily is the deletion of forgotten accounts, as no presented service currently automates this process. The first step to deleting old accounts is to find out which accounts exist. This can be significantly simplified if the user has already used password management software so that they can search

[3] <https://docs.zerotier.com/synology/>

for saved accounts there. Otherwise, they may need to determine if the email address for every service in question is used. After the services and accounts are identified, they may use a service such as Just Delete Me[4] that lists many services and steps or direct links to delete accounts for them.

The second unresolved problem is for the E2EE chat application, where the user uses Telegram. One option to achieve E2EE for one-to-one conversations would be to turn on the Secret chats feature, but another application must be used for group conversations. Here, an alternative could be presented Signal, which uses E2EE by default for everything or WhatsApp, which does collect and store some data about user's communication unencypted [18].

A third unresolved issue is the smartphone endpoint protection, where, in addition to the already used-by-default Google Play Protect, the student may install additional applications, such as Microsoft Defender, if provided by the university.

6.3.6 Final recommendations

Even though Google or Microsoft services can handle most of the problems and needs, they may not be the best solution overall. The main drawback is that it would require a complex cloud environment setup and may become costly, which could become a problem for a student with limited income. Instead, a solution consisting of more specialized services can be recommended, as these services have lower pricing for the solved needs. Bitwarden can be used for separate password management, BackBlaze can be utilized for double-redundant backup, and Cloudflare can create a VPN among friends and browse public networks more safely. A viable solution is to outsource server hosting to Synology, which can be connected in the same way as stated above.

6.4 Small technology company start-up

The specificity of the small-technology start-up profile is that when services are unavailable, it may lead to revenue loss. As the start-up has a higher budget than students and is staffed with IT professionals, it is

[4] `<https://backgroundchecks.org/justdeleteme/>`

possible to present more complex solutions that may take a significant amount of time to set up.

6.4.1 Microsoft

As Microsoft provides a range of services for cloud management for companies, it is possible to resolve the needs of this profile by moving the infrastructure to the cloud. However, given the volume of different services and configuration options, the administrator may require some training before securely setting up the whole system.

The company IT administrator may start by creating a new Microsoft Entra ID (previously known as Azure Active Directory) instance, with which the company gains the possibility to structure company employees into groups, making the process of moving into the least-privilege access philosophy easier. With a Microsoft account, employees are now able to use the account as an SSO source for multiple applications. Furthermore, suppose a web application is not configured to support SSO login (such as companies Jenkins). In that case, it can be placed behind Azure's built-in authentication mechanism, which will first require the user to authenticate against it before any request is left to pass to the target application.

Azure directly supports managing VMs, solving the need for a more scaleable approach. Next, the company can directly register a new domain name with an automatic generation of a TLS certificate, making the internal custom top-level domain with custom DNS obsolete. When everything is moved into the cloud, there is no longer any need for a VPN server to be used on the internal company network.

For secure storage and sharing of files, employees may use their OneDrive subscription, which offers 1 TB per employee, which should be enough for generic company data. To share secrets that should not be stored directly on OneDrive, the company may use Azure Key Vault, which offers secure storage and management of secrets and certificates.

The last need is centralized device management, which can be solved by Microsoft Intune, which directly supports enrolling macOS and iOS devices.

6.4.2 Google

Google offers services similar to Microsoft's, though under different product names. To secure access to the web application with the Zero Trust access model, the administrator may use the Identity-Aware Proxy. Like Microsoft, Google offers automatic setup and renewal of TLS certificates. For secure sharing of files, the users may use Google Drive to share secrets with the Secret Manager. Device management can be done with the Google device management software.

Where Google differs from Microsoft is the storage space available to the users. In Google's case, the storage is set at 2 TB, but it costs roughly double the price of Microsoft's solution. Furthermore, O365 for business offers a Microsoft Teams subscription capable of performing video and chat messaging, while Google Workspace offers only video conferences. The second difference is that Google no longer offers domain registration, as it was outsourced to Squarespace on September 7 2023. [79]

6.4.3 Synology + Cloudflare

Even though Synology itself does support a wide range of needs for this profile, it lacks the option to create a VPN server with MFA, purchase a custom domain, or protect hosted applications with zero trust. To solve this, the administrator can set up a Cloudflare tunnel on the Synology device to connect it to the Cloudflare Zero Trust. As the Synology account offers MFA protection and can be used as an OIDC-compatible SSO source, by exposing the Synology DSM interface either via QuickConnect or via the publicly accessible tunnel, the Cloudflare Zero Trust can be set to perform authentication via the local Synology accounts.

By using the Cloudflare WARP clients on the company devices, the employees can connect to the hosted Synology device after logging in through the SSO. The advantage of connecting the company device via the WARP client is that the Cloudflare administrator can see basic information about connected devices and linked users, posing as a basic form of centralized device management.

Even when connecting via the public internet, Cloudflare offers to set up zero trust authentication before letting the requests pass through, similar to the Google and Microsoft solutions. Cloudflare does offer domain registration, with all tunnels having a valid HTTPS certificate for their subdomains, regardless of whether the target service uses HTTP or HTTPS.

Synology has to ability to run arbitrary docker containers or whole virtual machines, so hosting company's services is simple and managable. Synology also offers per-user or per-group permissions, making it easy to implement least-privilege access. As a NAS device, sharing files is one of its core features, mainly when combined with the encryption of data on rest, which Synology natively supports.

The obvious drawbacks of this solution still persist, where Synology still poses as a single point of failure in case of power outage or connectivity downtime. Next, the physical security of this device is more important than with other profiles, as accidental dropping or theft of the device could lead again to service unavailability or company-confidential data leakage. Lastly, there is a need for a password manager or secret-sharing software capable of sharing passwords and secrets, where, like for other profiles, an external service such as Bitwarden needs to be used.

6.4.4 Unsolved problems

As every one of the problems or needs was solved by at least one of the presented solutions, there are no leftover unresolved problems.

6.4.5 Final recommendations

All of the problems and needs can be solved by migrating to a cloud environment from Google or Microsoft. Both of these companies offer similar services and both offer a possibly higher uptime than by continuing to self-host. Though, there are some smaller differences in auxiliary services, where Microsoft supports a direct registration of domain names and provides its Microsoft Team application for both text and video communication, while Google Meet supports only video conferences. Next, Google Drive pricing for business plans relevant to this profile provide double the storage space compared to Microsoft plans, but for double the price.

Though, if the company does want to have a fixed pricing for its services, instead of pay-as-you-go pricing of cloud environments, the company may achieve similar results by connecting self-hosted Synology services with Cloudflare ZeroTrust. Nevertheless, the company needs to know about and accept the risks that arise from hosting on their own hardware.

6.5 Summary of selected solutions

To provide more straightforward navigation within this thesis, a bullet point summary of each profile's selected solution and its advantages and disadvantages can be found:

- for low-tech skilled family in Table 6.1
- for low-tech skilled university student in Table 6.2
- for individual tech-skilled user in Table 6.3
- for small technology company start-up in Table 6.4

Table 6.1: Low-tech skilled family's summary of selected solutions

Solution	Advantages	Disadvantages
Microsoft	• integrated chatting application • password-less login • Microsoft Office suite • larger available storage space	• missing web UI for accesing passwords
Google	• more granular control over child account • simple to set up multiple user profiles within Google Chrome • web UI for accessing passwords	• missing chatting application • custom office file formats

Continued on next page

Table 6.1: Low-tech skilled family's summary of selected solutions (Continued)

Solution	**Advantages**	**Disadvantages**
Synology	• one-time payment • adjustable storage space • intergated chatting applicaiton	• complex to set up • custom office file formats • no children physical protection • no password manager

Table 6.2: Low-tech skilled university student's summary of selected solutions

Solution	Advantages	Disadvantages
Apple	• pre-integrated within iOS	• no file versioning on iCloud Drive
Microsoft	• file versioning	• smaller storage space for comparable price
Synology	• one-time payment • adjustable storage space	• **too complex to set up** • no password manager

Table 6.3: Individual tech-skilled user's summary of selected solutions

Solution	Advantages	Disadvantages
Google	• free VPS for hosting	• complex cloud environment • costly data backup service
Cloudflare	• free VPN for both acccessing internet and friends' machines	• software needs to be installed to on every endpoint
BackBlaze	• cheap data storage for high volumes • simple data recovery and retention	• limited scope of solved problems and needs

Continued on next page

Table 6.3: Individual tech-skilled user's summary of selected solutions (Continued)

Solution	Advantages	Disadvantages
Synology	• one-time payment • adjustable storage space • integrable with other solutions for data backup	• only partial solution, needs to be integrated with other services

Table 6.4: Small technology company start-up's summary of selected solutions

Solution	Advantages	Disadvantages
Microsoft	• outsourced hardware managment • direct domain name registration	• smaller storage space per user • dynamic pricing
Google	• outsourced hardware managment • larger storage space per user	• missing chat applicaiton • dynamic pricing

Continued on next page

Table 6.4: Small technology company start-up's summary of selected solutions (Continued)

Solution	Advantages	Disadvantages
Synology + Cloudflare	• direct domain name registration • fixed pricing	• basic employee device managment • no secrets sharing • single point of failure

7 Conclusion

In this thesis, I have first shown what existing publications exist on the subject of SOHO cybersecurity and what advice the SOHO users may already know regarding computer security and safety. I have put this advice in context with current practices and shown that not all of the advice is still relevant, that following them may come at the cost of highly decreased user comfort, or that the recommendation is over the skill level of the users.

Next, I have identified four distinct user archetypes as profiles – low-tech skilled family, low-tech skilled university student, individual tech-skilled user, and small technology company start-up – where every profile has a specific set of cybersecurity requirements, with some shared between all the profiles. These requirements were based on questionnaires, hands-on discussions, and personal experience with people matching the profile specifications, representing the displayed profiles' problems and needs as a mixture of real-life examples. I have put the profiles in context with current publications and the Digital Competence Framework to provide a baseline of the user's level of technical skills.

After profiles were defined, I have presented services provided by a range of security-as-a-service products that either cover a broad spectrum of user needs – Google, Microsoft, Apple, Proton – or are specialized in solving a specific area – Cloudflare for hosting web services, Bitwarden for storing passwords, BackBlaze for data backup and retention, CryptPad for an end-to-end encrypted web-based office suite.

To evaluate which service solves the needs and problems of each profile to the highest degree, I have formulated a methodology. The methodology focuses on the usability aspects of the solution, price, integration with other systems and user understanding of the inner workings via a point system that awards the most points to the services that fit specific criteria concerning the profiles.

I have described the services evaluated as best for each profile in more detail, along with the advantages and disadvantages over other services. I have shown that nowadays, even a single or a small number of services may solve a large area of cybersecurity needs while simultaneously making the user's life easier and increasing their security posture, e.g. by mitigating simple-to-break passwords by not using passwords at all. I have presented that these services that solve threats to the user's security, privacy or data retention can be used either free of charge or at a reasonably low cost. I have concluded that with these services, even users with little digital competence can take advantage of the increased security they provide.

Bibliography

1. STEFANEK, George L. *Information security best practices: 205 basic rules*. Butterworth-Heinemann, 2002.
2. KUMARAN, Neil. *New Gmail protections for a safer, less spammy inbox* [online]. 2023 [visited on 2024-01-10]. Available from: `https://blog.google/products/gmail/gmail-security-authentication-spam-protection/`.
3. KIZZA, Joseph Migga. *Guide to computer network security*. Cham, Switzerland: Springer Nature, 2020.
4. ORACLE. *How do I enable Java in my web browser?* [Online]. 2024 [visited on 2024-02-12]. Available from: `https://www.java.com/en/download/help/enable_browser.html`.
5. DAVIS, Wes. *Gmail's basic HTML view will go to the Google graveyard in 2024* [online]. 2023 [visited on 2024-04-10]. Available from: `https://www.theverge.com/2023/9/25/23889791/gmail-basic-html-view-discontinued-2024`.
6. ČIERNIKOVÁ, Tamara. *Selected open tools supporting security and privacy protection for regular end-users*. Brno, 2022. Available also from: `https://is.muni.cz/th/h7qfk/`.
7. PECUCH, Daniel. *Password managers: a survey*. Brno, 2021. Available also from: `https://is.muni.cz/th/sm620/`.
8. STRODL, Stephan; MOTLIK, Florian; STADLER, Kevin; RAUBER, Andreas. Personal & Soho archiving. *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*. 2008. Available from DOI: `10.1145/1378889.1378910`.
9. MISHEVA, Galina. *The Digital Competence Framework (DigComp)* [online]. 2021 [visited on 2024-01-13]. Available from: `https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/digital-competence-framework-digcomp`.

10. COMMISSION, European; CENTRE, Joint Research; VUORIKARI, R; KLUZER, S; PUNIE, Y. *DigComp 2.2, The Digital Competence framework for citizens – With new examples of knowledge, skills and attitudes*. Publications Office of the European Union, 2022. Available from DOI: doi/10.2760/115376.

11. CARRETERO, Stephanie; VUORIKARI, Riina; PUNIE, Yves. *DigComp 2.1. The digital competence framework for citizens with eight proficiency levels and examples of use*. 2017. Available from DOI: 10.2760/38842.

12. OECD. *Policy Brief on the Future of Work, Skills for a Digital World* [online]. 2016 [visited on 2023-12-30]. Available from: https://www.oecd.org/els/emp/Skills-for-a-Digital-World.pdf.

13. OECD. Skills for a Digital World. 2016, no. 250. Available from DOI: 10.1787/5jlwz83z3wnw-en.

14. OECD. *Skills matter - Additional results from the survey of adult skills* [online]. 2019 [visited on 2023-11-30]. Available from: https://www.slideshare.net/OECDEDU/skills-matter-additional-results-from-the-survey-of-adult-skills.

15. STEINLECHNER, Markus; SCHUMACHER, Andreas; FUCHS, Benedikt; REICHSTHALER, Luisa; SCHLUND, Sebastian. A maturity model to assess digital employee competencies in industrial enterprises. *Procedia CIRP*. 2021, vol. 104, pp. 1185–1190. ISSN 2212-8271. Available from DOI: 10.1016/j.procir.2021.11.199. 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0.

16. MŠMT ČR; NPI ČR. *Digitální kompetence v uzlových bodech vzdlávání* [online]. 2023 [visited on 2023-12-30]. Available from: https://revize.edu.cz/digikompetence-uzlove-body.

17. VIBER MEDIA S.À R.L. *Home | Viber* [online]. 2024 [visited on 2024-03-13]. Available from: https://www.viber.com/en/.

18. ARNTZ, Pieter. *Here's what data the FBI can get from WhatsApp, iMessage, Signal, Telegram, and more* [online]. 2021 [visited on 2023-11-30]. Available from: https://www.malwarebytes.com/blog/news/2021/12/heres-what-data-the-fbi-can-get-from-whatsapp-imessage-signal-telegram-and-more/.

19. VIBER MEDIA S.À R.L. *Transfer Your Chat History From One Phone to Another* [online]. 2023 [visited on 2023-11-30]. Available from: `https://help.viber.com/hc/en-us/articles/9173905938845-Transfer-Your-Chat-History-From-One-Phone-to-Another`.

20. APPLE INC. *iCloud+ plans and pricing* [online]. 2024 [visited on 2024-03-13]. Available from: `https://support.apple.com/en-us/HT201238`.

21. APPLE INC. *Set up iCloud Passwords on your Windows computer* [online]. 2024 [visited on 2024-03-13]. Available from: `https://support.apple.com/en-gb/guide/icloud-windows/icw2babf5e03/icloud`.

22. DRTINA, Martin. *Až 200 tisíc lidí ročně přijde o svůj e-mailový účet, spočítal Seznam* [online]. Internet Info, s.r.o., 2023 [visited on 2023-12-30]. Available from: `https://www.lupa.cz/aktuality/az-200-tisic-lidi-rocne-prijde-o-svuj-e-mailovy-ucet-spocital-seznam/`.

23. BEN-YAIR, Shimrit. *Updating Google Photos' storage policy to build for the future* [online]. 2020 [visited on 2024-03-17]. Available from: `https://blog.google/products/photos/storage-changes/`.

24. GOOGLE. *How chrome protects your passwords* [online]. 2024 [visited on 2024-03-17]. Available from: `https://support.google.com/chrome/answer/10311524`.

25. TELEGRAM. *Telegram FAQ* [online]. 2024 [visited on 2024-03-17]. Available from: `https://telegram.org/faq`.

26. HESSE, Brendan. *The Best WhatsApp Alternatives* [online]. 2021 [visited on 2024-03-17]. Available from: `https://lifehacker.com/the-best-whatsapp-alternatives-1832064581`.

27. ANNA, Křenková. *WhatsApp mění pravidla. Kterými bezpečnými aplikacemi ho nahradit?* [Online]. 2021 [visited on 2024-03-17]. Available from: `https://tn.nova.cz/zpravodajstvi/clanek/435392-whatsapp-meni-pravidla-kterymi-bezpecnymi-aplikacemi-ho-nahradit`.

28. JAMES, O'Malley. *WhatsApp alternatives: the best messaging apps for Android and iPhone* [online]. 2021 [visited on 2024-03-17]. Available from: https://www.techradar.com/best/whatsapp-alternatives.

29. KILIÁN, Karel. *Čím nahradit WhatsApp: Vyberte si z 10 alternativních komunikátorů* [online]. 2023 [visited on 2024-03-17]. Available from: https://www.zive.cz/clanky/cim-nahradit-whatsapp-vyberte-si-z-10-alternativnich-komunikatoru/sc-3-a-207956/default.aspx.

30. TOULAS, Bill. *Google Drive users angry over losing months of stored data* [online]. BleepingComputer, 2023 [visited on 2023-12-30]. Available from: https://www.bleepingcomputer.com/news/google/google-drive-users-angry-over-losing-months-of-stored-data/.

31. GATLAN, Sergiu. *Google shares "fix" for deleted Google Drive files* [online]. BleepingComputer, 2023 [visited on 2023-12-30]. Available from: https://www.bleepingcomputer.com/news/google/google-shares-fix-for-deleted-google-drive-files/.

32. MICROSOFT. *Compare cloud storage pricing and plans* [online]. 2024 [visited on 2024-04-16]. Available from: https://www.microsoft.com/en-us/microsoft-365/onedrive/compare-onedrive-plans.

33. MICROSOFT. *Create Your Azure Free Account Today | Microsoft Azure* [online]. 2024 [visited on 2024-05-07]. Available from: https://azure.microsoft.com/en-us/free/.

34. MICROSOFT. *Apply encryption using sensitivity labels* [online]. 2024 [visited on 2024-04-16]. Available from: https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels.

35. MICROSOFT. *What is device enrollment* [online]. 2024 [visited on 2024-05-08]. Available from: https://learn.microsoft.com/en-us/mem/intune/user-help/use-managed-devices-to-get-work-done.

36. MICROSOFT. *How to go passwordless with your Microsoft account* [online]. 2024 [visited on 2024-03-18]. Available from: https://support.microsoft.com/en-us/account-billing/how-to-go-passwordless-with-your-microsoft-account-674ce301-3574-4387-a93d-916751764c43.

37. MICROSOFT. *Edit your passwords in Microsoft Edge* [online]. 2024 [visited on 2024-03-18]. Available from: https://support.microsoft.com/en-us/topic/edit-your-passwords-in-microsoft-edge-38ef988f-5a65-4c6a-9db8-937995d3ae31.

38. MICROSOFT. *Password generator* [online]. 2024 [visited on 2024-03-18]. Available from: https://www.microsoft.com/en-us/edge/features/password-generator.

39. MICROSOFT. *Automatically save photos and videos with OneDrive for Android* [online]. 2024 [visited on 2024-03-18]. Available from: https://support.microsoft.com/en-us/office/automatically-save-photos-and-videos-with-onedrive-for-android-66605e54-48b8-4f55-bcff-34159702e344.

40. MICROSOFT. *Ransomware detection and recovering your files* [online]. 2024 [visited on 2024-03-18]. Available from: https://support.microsoft.com/en-au/office/ransomware-detection-and-recovering-your-files-0d90ec50-6bfd-40f4-acc7-b8c12c73637f.

41. MICROSOFT. *Phone monitoring apps and protecting your family in the digital age - Microsoft 365* [online]. 2021 [visited on 2024-04-22]. Available from: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/protect-your-family-how-to-select-a-phone-monitoring-app.

42. JONATHAN LI, Jasika Bawa. *Browse safely with real-time protection on Chrome* [online]. 2024 [visited on 2024-05-04]. Available from: https://blog.google/products/chrome/google-chrome-safe-browsing-real-time/.

43. GOOGLE. *Upgrade Your Cloud Storage - Google One* [online]. 2024 [visited on 2024-05-08]. Available from: https://one.google.com/about/plans.

44. GOOGLE. *Compare Flexible Pricing Plan Options | Google Workspace* [online]. 2024 [visited on 2024-05-08]. Available from: https://workspace.google.com/pricing.html.

45. GATLAN, Sergiu. *Google Drive now warns you of suspicious phishing, malware docs* [online]. 2024 [visited on 2024-05-04]. Available from: https://www.bleepingcomputer.com/news/google/google-drive-now-warns-you-of-suspicious-phishing-malware-docs/.

46. GOOGLE. *Use Google Drive files offline - Computer - Google Drive Help* [online]. 2024 [visited on 2024-05-04]. Available from: https://support.google.com/drive/answer/2375012?hl=en.

47. GOOGLE. *Free cloud features and trial offer | Google Cloud Free Program* [online]. 2024 [visited on 2024-05-07]. Available from: https://cloud.google.com/free/docs/free-cloud-features.

48. GOOGLE. *Overview: Manage users' computers & smart home devices - Google Workspace Admin Help* [online]. 2024 [visited on 2024-05-08]. Available from: https://support.google.com/a/answer/9453479?hl=en.

49. KAFKA, Steve. *How we fought bad apps and bad actors in 2023* [online]. 2024 [visited on 2024-05-01]. Available from: https://security.googleblog.com/2024/04/how-we-fought-bad-apps-and-bad-actors-in-2023.html.

50. NAMERAH, Fatmi. *Google Play Services: What is it, and how does it keep your Android phone safe?* [Online]. 2024 [visited on 2024-05-01]. Available from: https://www.androidcentral.com/apps-software/google-play-services.

51. GOOGLE. *Back up or restore data on your Android device - Android Help* [online]. 2024 [visited on 2024-05-01]. Available from: https://support.google.com/android/answer/2819582?hl=en.

52. WINSC1. *Version History in iCloud Drive - Apple Community* [online]. 2024 [visited on 2024-05-06]. Available from: https://discussions.apple.com/thread/254911251?sortBy=best.

53. APPLE INC. *Web-only access to iCloud - Apple Support* [online]. 2024 [visited on 2024-05-06]. Available from: https://support.apple.com/en-us/102447.

54. PROTON AG. *Create a free email account or choose a paid plan* [online]. 2024 [visited on 2024-05-01]. Available from: https://proton.me/mail/pricing.

55. PROTON AG. *Proton for Business plans and pricing* [online]. 2024 [visited on 2024-05-01]. Available from: https://proton.me/business/plans.

56. PROTON AG. *Download Proton Pass for your Browser or Mobile Device* [online]. 2024 [visited on 2024-05-01]. Available from: https://proton.me/pass/download.

57. CLOUDFLARE, INC. *Everywhere Security | Unified Security Platform* [online]. 2024 [visited on 2024-05-07]. Available from: https://www.cloudflare.com/cybersecurity/.

58. CLOUDFLARE, INC. *Pricing · Cloudflare R2 docs* [online]. 2024 [visited on 2024-05-07]. Available from: https://developers.cloudflare.com/r2/pricing/.

59. CLOUDFLARE, INC. *Enforce MFA · Cloudflare Zero Trust docs* [online]. 2024 [visited on 2024-05-07]. Available from: https://developers.cloudflare.com/cloudflare-one/policies/access/mfa-requirements/.

60. CLOUDFLARE, INC. *Private networks · Cloudflare Zero Trust docs* [online]. 2024 [visited on 2024-05-07]. Available from: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/private-net/.

61. CLOUDFLARE, INC. *Create a remotely-managed tunnel (dashboard) · Cloudflare Zero Trust docs* [online]. 2024 [visited on 2024-05-07]. Available from: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/get-started/create-remote-tunnel/.

62. CLOUDFLARE, INC. *1.1.1.1 — The free app that makes your Internet faster.* [Online]. 2024 [visited on 2024-05-07]. Available from: https://one.one.one.one/.

63. BITWARDEN, INC. *Bitwarden Password Manager Pricing & Plans* [online]. 2024 [visited on 2024-05-07]. Available from: `https://bitwarden.com/pricing/`.

64. BACKBLAZE. *Computer Cloud Backup Pricing Comparison* [online]. 2024 [visited on 2024-05-07]. Available from: `https://www.backblaze.com/cloud-backup/pricing`.

65. BACKBLAZE. *Cloud Storage Pricing Comparison: Calculate Your Costs* [online]. 2024 [visited on 2024-05-07]. Available from: `https://www.backblaze.com/cloud-storage/pricing`.

66. BACKBLAZE. *Supported Operating Systems* [online]. 2024 [visited on 2024-05-07]. Available from: `https://www.backblaze.com/computer-backup/docs/supported-operating-systems`.

67. BACKBLAZE. *Cloud Storage Object Lock* [online]. 2024 [visited on 2024-05-07]. Available from: `https://www.backblaze.com/docs/cloud-storage-object-lock`.

68. TEAM, CryptPad. *Frequently Asked Questions - CryptPad 2024.3.0 documentation* [online]. 2024 [visited on 2024-04-17]. Available from: `https://docs.cryptpad.org/en/FAQ.html%5C#can-cryptpad-sync-documents-to-my-local-filesystem`.

69. SYNOLOGY INC. *How to sync files between Synology NAS and your computer using Synology Drive Client - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: `https://kb.synology.com/en-us/DSM/tutorial/How_to_sync_files_between_Synology_NAS_and_your_computer_using_Drive_desktop`.

70. SYNOLOGY INC. *DS photo | Android - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: `https://kb.synology.com/en-us/DSM/help/DSphoto/Android?version=6`.

71. SYNOLOGY INC. *DS photo | iOS - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: `https://kb.synology.com/en-us/DSM/help/DSphoto/iPhone?version=6`.

72. SYNOLOGY INC. *Synology Office* [online]. 2024 [visited on 2024-05-05]. Available from: https://www.synology.com/en-us/dsm/feature/office.

73. SYNOLOGY INC. *How do I back up an entire computer or server using Active Backup for Business? - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: https://kb.synology.com/en-us/DSM/tutorial/How_back_up_PC_physical_server_with_ABB.

74. SYNOLOGY INC. *Service | SSO Server - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: https://kb.synology.com/en-us/DSM/help/SSOServer/sso_server_service?version=7.

75. SYNOLOGY INC. *2-Factor Authentication | DSM - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: https://kb.synology.com/en-global/DSM/help/DSM/SecureSignIn/2factor_authentication?version=7.

76. SYNOLOGY INC. *QuickConnect | DSM - Synology Knowledge Center* [online]. 2024 [visited on 2024-05-01]. Available from: https://kb.synology.com/en-us/DSM/help/DSM/AdminCenter/connection_quickconnect?version=7.

77. SYNOLOGY INC. *Synology Chat* [online]. 2024 [visited on 2024-05-05]. Available from: https://www.synology.com/en-global/dsm/feature/chat.

78. NULIDE. *Find My Device (FMD) | F-Droid - Free and Open Source Android App Repository* [online]. 2024 [visited on 2024-05-05]. Available from: https://f-droid.org/packages/de.nulide.findmydevice/.

79. GOOGLE. *Google Domains | Official Site – Google Domains* [online]. 2024 [visited on 2024-05-08]. Available from: https://domains.google/.

A An appendix

A.1 Profile data collecting

During the writing of this thesis, I have sent the following questions to students (n=5) of non-it universities:

- Do you consciously back up your photos/videos?
- Do you consciously back up documents/school notes?
- Do you use a password manager? For example, Apple Key-Chain?
- Do you use email on your iPhone? Possibly through their Mail app or some other app?
- Do you use some form of multi-level login/MFA/PassKeys?
- Do you use the iCloud app for Windows? Possibly for what?

Next, I performed a discussion about password practices with (n=27) high-school students and high-school teachers (n=33), with questions such as:

- Do you have more than three complex passwords that you remember?
- Do you use passphrases instead of passwords?
- Do you use a password manager?
- Did you ever used some form of password-less login?

With students (n=27), I have also performed a discussion about data retention, backups and privacy with instant messaging applications:

- Do you know how to back up data?
- Do you use some form of backup?
- Have you ever heard of or used cloud storage?
- Do you know what a NAS device or Synology is?
- Which messaging applications do you use?
- Could you order them in terms of privacy?
- Do you know what E2EE is?
- Which of these applications utilize E2EE?

A.2 Author's solution

To stress why selecting a simple-to-manage solution from the beginning is essential, I am including the approach and history of what solution I implement. This solution is currently far from perfect, and as such can show how technical debt can be quickly created when learning to achieve hosting goals on the go.

I started self-hosting stored files using a dedicated Windows XP device with Windows folder sharing. My initial reasoning for self-hosting most of the software was the cost of cloud storage, though now the privacy aspect has already surpassed it. As this solution was not very stable in the long term, I have moved to a dedicated Linux machine with an Apache web server with ownCloud[1]. For some time, I have experimented with P2P VPN software such as N2N[2] to access my ownCloud instance even when not within the same LAN. I abandoned this solution because it required the N2N to be installed and properly configured on all devices, making it impossible to access the site on devices I did not own. For that, I bought my first domain with the cheapest Czech-based VPS I could find. On that VPS, I have installed a reverse-proxy tool HAProxy[3] and an OpenVPN server to forward requests to specific subdomains to the server on my LAN.

Since then, I have bought more VPS, moved away to my apartment with a new machine, and started managing LANs with own routers. I have accumulated much technical debt while learning how to do all of this. My current solution is:

- one cheap VPS dedicated to hosting a WireGuard VPN that connects all my other VPSs and home servers
- second cheap VPS serving as an entry point to my network, with HAproxy that forwards requests to the relevant servers
- one more powerful but cheap VPS that hosts most of the publicly accessible docker containers and static websites

[1] <https://owncloud.com/>

[2] <https://github.com/ntop/n2n>

[3] <https://www.haproxy.org/>

- refurbished laptop in my apartment that acts as a file-storage server with NextCloud[4] running in docker
- refurbished desktop PC in my parent's house that acts as a hypervisor for virtually running images of the old servers that I had used before and did not have enough time to migrate yet

This solution has certain drawbacks, mainly that multiple single points of failure exist. For example, if the VPN VPS fails, it cuts all connections between any two of my servers. If the entry VPS fails, none of my services are publicly available through internet. Alternatively, if the more powerful VPS hosting most of my websites fails, it may again disturb multiple services. Due to my cost-saving selection of hosting providers, these outages happen quite often – some weeks, my services have less than 50 % uptime. Next, as the number of devices I manage grows over time, keeping everything well-maintained becomes more and more time-consuming.

For these reasons, I have slowly started to migrate to more cloud-based solutions – beginning with transferring my mail self-hosting to a paid Proton Mail subscription, moving my static websites to free Cloudflare pages and the most critical dynamic web apps to a free Google Cloud Compute Engine VPS. These three changes should vastly improve the uptime of my most critical services, such as my personal webpage, status monitoring tool UptimeKuma[5] and privacy-friendly web analytics software Plausible[6].

As for the physical servers, the current settings with virtual servers running on top of another Linux server encounter decreased performance. To solve this issue, I have begun transferring services from the virtual machines into docker containers that run directly on the bare-metal OS. In addition to increasing performance, I now keep the configuration of my docker containers inside a git-versioned docker-compose file, simplifying the overall configuration management.

My automated backup routine for my physical servers consists of replicating all shared data via `rclone` bi-directional sync. Data not supposed to be shared or from my VPSs is backed up using borg[7]

[4] <https://nextcloud.com/>

[5] <https://github.com/louislam/uptime-kuma>

[6] <https://plausible.io/>

[7] <https://borgbackup.readthedocs.io/en/stable/>

to a single server with the largest attached storage. Borg provides compression and deduplication of data with authenticated encryption. Furthermore, it can be executed over SSH in so-called append-only mode, where, even if the data was mistakenly deleted from the original storage, it cannot be deleted from the remote storage. As to have multiple backups in case of a e.g. power surge, the encrypted backup data is copied to a remote location using rsync[8].

As most devices interacting with local networks are either Linux, Windows or Android, the self-hosted NextCloud works flawlessly for file synchronization and automatic upload. The issues are with a few iOS devices, where the automatic upload to NextCloud only sometimes works, and the app needs to be opened manually to start the upload process. On the other hand, thanks to the direct support of CalDav and CardDav inside iOS, the synchronization of tasks, calendar events and contacts is practically effortless. The physical security is handled by a NextCloud application PhoneTrack[9]. This application can be configured as a remote endpoint of multiple position-tracking applications. After that, the position of a device is recorded in configured intervals and can be shared with other NextCloud users. This solution was chosen as it is privacy-respecting, multi-platform and can generate GPX files as an output, which is helpful for further data manipulation.

[8] <https://github.com/rsyncproject/rsync>

[9] <https://apps.nextcloud.com/apps/phonetrack>