



NTNU GJØVIK

Windows Security Baselines

Group 107:
Mats Nerhagen
Mads Reneflot Moe

May, 2022

Date: 20.05.2022

Title: Windows Security Baselines

Authors: Mads Reneflot Moe, Mats Nerhagen

Supervisor: Erik Hjelmås

Employer: NTNU SOC

Contact Person: Christoffer Vargtass Hallstensen

Keywords: Windows 10, Windows 11, Built-in security, NSM, Security baselines

Pages: 41

Attachments: 3

Availability: Open

Studypoints 22,5

Abstract: In the field of cyber security the malicious actors and the security threats they exploit are constantly evolving to find new and creative ways of gaining unauthorized access to IT systems. As these threats evolve the IT security technologies are evolving with them in response. The starting point of this thesis is what security features NTNU should implement if they look to transition over to a Windows 11 based IT-system. To provide a basis for this decision, we provide a detailed description of the different security features of Windows 10/11, we test selected security features and provide an evaluation of how they may affect user experience for NTNU employees and students. Based on our analysis we recommend that NTNU SOC upgrade to hardware that supports Windows 11, especially TPM 2.0. Further, Windows 11 has a lot of security features enabled by default that should stay enabled as they have little impact on performance and high security value. Finally, modernizing NTNU's user authentication system with Windows Hello and moving away from the use of passwords will also help NTNU adopt the security standards and concepts that Windows 11 introduces. These recommendations may be an important stage in the planning process to create a seamless transition when performing a large scale system change such as this, with minimal impact on productivity and operational disruption.

Preface

This thesis is a collaborative work between Mads Reneflot Moe and Mats Nerhagen. However, this thesis would not have been possible without the support and advice from our advisor Erik Hjelmås. We would like to thank him for providing us with constructive and inspiring feed-back through our weekly meetings on the campus.

We would also like to thank NTNU SOC and our contact person Christoffer Vargtass Hallstensen for giving us a theoretical thesis just like we wished for, and advice along the way. We would also like to thank some of our fellow students, Emil, Kristian, Kjetil, Martin, Anders, Marius, Halfdan, Jørgen and Torstein.

Your social and academic company through this three year bachelor study have been invaluable.

Table of Contents

Preface	ii
Table of Contents	v
List of Figures	vi
Acronyms	vii
1 Introduction	1
1.1 Background	1
1.2 Thesis definition	1
1.3 Framework	2
1.4 Competence	2
1.5 Target audience	2
1.6 Roles	2
1.7 Setup of report	3
2 NSM ground principles	4
3 Windows Security Concepts	6
3.1 Zero Trust model	6
3.2 Root of Trust	6
4 Windows security - Hardware features	7
4.1 Hardware root of trust	7
4.2 Pluton security technology	7
4.3 Trusted Platform Module	7
5 Windows security - operating system features	9
5.1 Secure boot and trusted boot	9
5.2 Device health attestation and conditional access	10
5.3 BitLocker	10
6 Windows security - Software features	11
6.1 Windows Defender	11
6.1.1 Features	11
6.1.2 Protection	11
6.2 Windows Firewall	11

6.2.1	Features	12
6.2.2	Protection	12
6.3	Microsoft SmartScreen	13
6.3.1	Features	13
6.3.2	Issues	14
6.3.3	Protection	14
6.4	Windows Event Viewer	14
6.4.1	Features	14
6.4.2	Issues	15
6.4.3	Protection	15
6.5	Sysmon	15
7	Group Policies	16
7.1	Local Group Policies	16
7.2	Relevant NSM principles	16
8	Passwordless Authentication	17
8.1	Windows Defender Credential Guard	17
8.2	Windows Hello For Business	17
8.3	FIDO and FIDO2 Security Key	18
9	Windows Security - Application	19
9.1	Windows Defender Application Control (WDAC)	19
9.2	User Account Control (UAC)	19
9.3	Application isolation and Microsoft Defender Application Guard	20
10	Testing & user experience evaluation	22
10.1	Introduction	22
10.2	Limitations	22
10.3	Software and test-setup	22
10.3.1	SkyHiGh	22
10.3.2	Windows Remote Desktop	22
10.4	Testing of Microsoft Defender Application Guard	23
10.4.1	Microsoft Defender Application Guard for Microsoft Edge - Testing	23
10.4.2	Microsoft Defender Application Guard for Microsoft Office 365 - Testing	26
10.4.3	Microsoft Defender Application Guard - User experience evaluation	27
10.5	Windows Hello - User experience evaluation	28

10.5.1 PIN	28
10.5.2 Biometrics	29
10.6 Windows Event Viewer - User experience evaluation	29
10.7 Windows Defender - User experience evaluation	29
10.7.1 Windows Firewall - User experience evaluation	30
10.7.2 Microsoft SmartScreen - User experience evaluation	30
10.8 User Account Control (UAC) - User experience evaluation	31
10.9 BitLocker	31
11 Conclusion & Recommendations	32
11.1 Hardware	32
11.2 Operating systems	32
11.3 Software & Application	32
11.4 Passwordless authentication	33
11.5 Summary	34
12 Thesis conclusion	36
12.1 Results compared to goals	36
12.1.1 Task requirements	36
12.2 Limitations	37
12.3 Further work	37
12.4 Evaluation of our work	37
References	39

List of Figures

1	<i>The NSM ground principles four categories, inspired by image from NSM website: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/hva-er-nsms-grunnprinsipper-for-ikt-sikkerhet/</i>	4
2	<i>A TPM 2.0 chip. Received 25.04.2022 from https://upload.wikimedia.org/wikipedia/commons/thumb/b/be/TPM.svg/1280px-TPM.svg.png</i>	7
3	<i>Basic Firewall overview in Windows 10. Screenshot taken 03.05.2022</i>	12
4	<i>Microsoft SmartScreen pop-up message, where SmartScreen has detected a file with low reputation. Retrieved 02.05.2022 from https://www.soft8soft.com/docs/files/creating-desktop-apps/windows-protected-your-pc.jpg</i>	13
5	<i>Difference between explorer interface with Microsoft Defender Application Guard compared to explorer interface without. Retrieved 09.05.2022 from https://commons.wikimedia.org/wiki/File:ApplicationGuard_for_Microsoft_Edge.png</i>	20
6	<i>Windows Defender Application Guard interface in the group policy editor. Screenshot taken 02.05.2022</i>	23
7	<i>Network Isolation interface in the group policy editor. Screenshot taken 02.05.2022</i>	24
8	<i>The interface for the enterprise resource domains in the group policy editor. Notice that google.com is set as allowed domain. Screenshot taken 02.05.2022</i>	25
9	<i>The upper window is the normal Microsoft Edge browser, while the one at the bottom is Microsoft Edge with Application Guard which opened automatically. Screenshot taken 02.05.2022</i>	25
10	<i>The interface for the Microsoft Defender Application Guard in Managed Mode, showing option "2" being applied. Screenshot taken 02.05.2022</i>	26
11	<i>Two different Microsoft Word files opened. The top one has been opened in Application Guard. Screenshot taken 02.05.2022</i>	27
12	<i>Process for removing application guard in word file. Screenshot taken 02.05.2022</i>	28
13	<i>Process for removing application guard in word file. Screenshot taken 02.05.2022</i>	28
14	<i>Two different Microsoft Word files opened. The top one has been opened in Application Guard. Screenshot taken 02.05.2022</i>	30

Acronyms

AD Active Directory. 16

FIDO Fast Identity Online. 18

GPO Group Policy Object. 16

GUI Graphical User Interface. 30

LGP Local Group Policies. 16

MDM mobile device manage. 22, 37

NSM Nasjonal Sikkerhetsmyndighet. 4, 11–16, 32, 33

OS Operating system. 9, 10, 32, 33, 36

PSP Pluton Security Processor. 7

SDK Software Development Kit. 19

TPM Trusted Platform Module. 7, 8, 10, 17, 18, 22, 28, 32

UAC User Account Control. 19

VBS Virtualization Based Security. 17, 18

1 Introduction

1.1 Background

To be able to evaluate which security mechanisms are essential to provide NTNU with the best possible security coverage on all areas, it is important to have a good understanding of the cyber security threat landscape. This includes knowing what the biggest threats are both currently and what might become important in the future.

Companies today have a plethora of cyber security threats that they need to be aware of and actively mitigate against. Phishing, ransomware, and compromised passwords are examples of some of the most common security threats that we face today. These threats have become especially more prevalent today considering how working from home has become the new normal for many employees around the world. Now that companies have invested so much to make it easy for workers to work from home, this will probably not go away after the pandemic is over.

This thesis is commissioned by the Digital Security Operations Center (SOC) of NTNU. The section is responsible for the digital security of NTNU. NTNU is a Norwegian University localized with campuses in Trondheim, Ålesund and Gjøvik. The headquarters is in Trondheim. NTNU has about 42 000 registered students and 9000 employees. The university specializes in science and technology but it also covers disciplines like economics, medicine, social sciences, educational science, architecture and art. NTNU has several strong research environments and some are ranked as world leading.

All though this expansion of remote and hybrid workplaces has brought new opportunities and made productivity a lot easier for the workforce, it also has brought with it a set of new cyber security challenges. According to data from the Microsoft commissioned security signals report[1]; “75% of security decision-makers at the vice-president level and above feel that the move to hybrid work leaves their organization more vulnerable to security threats”.

1.2 Thesis definition

The task is to analyse the different security functions within Windows 10 and 11 together with Microsoft Office, and examine how these security functions protects against specific threats. The information that is gathered here will be used to come up with an assessment for measures that NTNU can use to protect their user base against malware. What specific threats the different security functions protects against will also be focused on.

The tasks requirements:

1. To map out the built in security mechanics in Windows 10 and 11.
2. To map out the built in security mechanics in Microsoft Office and explain how these can complement the ones already in Windows.
3. To analyse the different threats the built in security mechanics protects against, and how these can detect attacks.
4. To come up with a professional assessment of what features NTNU should use in their systems now and in the future for best possible security.
5. To investigate if these security features can have a negative impact on the user experience in the NTNU systems.

1.3 Framework

The project will primarily focus on built in features in Windows 10 and Windows 11. We will not look at the Windows Server operating systems, due to a group split the 16th of February. Our "new" task is therefore only to focus on Windows 10 and 11, together with the built-in security in Microsoft Office. Due to how the NTNU servers are set up, we will not be able to look at all of the features in Windows 11 fully. This is because NTNU's servers are missing an important hardware component. More on this in chapter 4, "Windows security - Hardware features".

The project will last from the middle of January to the middle of May in 2022. We have made a Gantt-schedule to keep track of our goals, and we use a Kanban board as a to-do list.

We will limit the task to the most important built in security components in Windows 10 and 11. To explain and analyse every single security feature would be too time consuming of a task, and we have therefore chosen to focus on the most important ones. We will not look at cloud features that Microsoft and Windows provides. This therefor excludes programs like Microsoft OneDrive and security around this.

1.4 Competence

Both of us writing the thesis have 2,5 years of education in the information security field, more precisely digital infrastructure and cyber security. We have not had any specific subjects focused specifically on security in Windows, other than "DCSG1005 - Infrastruktur: sikre grunntjenester" in the spring of 2020, which had a lot of focus on powershell. Due to this, we have spent much time researching during the whole project. Much of the research comes from Microsoft's technical documentation on different parts of their systems. We also had to learn how to setup a few security softwares using powershell in our test environment, but most of our time went towards research.

Other subjects that are especially relevant to our thesis include "IDATT2202 - Operativsystemer" which gave valuable insight into the inner workings of operatingsystems, and "DCST2005 - Risikostyring" where we learned about risk management and security standards such as NSM ground principles and ISO:27001.

1.5 Target audience

The target audience for the thesis other than the NTNU SOC will mainly be people who have a medium to high understanding of the Windows operating system, who wishes to learn more about its different security mechanics and features. IT administrators who are seeking to upgrade their systems to Windows 11 or implement new and more modern security features from Windows can also use this thesis as a guide to learn more about Windows 10/11 security and how they should be implemented.

1.6 Roles

The different roles for the project is the following:

- Student - Mats Nerhagen. Main responsibility for LaTeX and OverLeaf setup, together with SkyHiGh and remote desktop.
- Student - Mads Reneflot Moe. Main responsibility for report-structure and contact with supervisor and employer (contact person).
- Supervisor - Erik Hjelmås
- Employer - NTNU SOC
- Contact Person - Christoffer Vargtass

1.7 Setup of report

The report will be written using Overleaf, which is an online editor for text documents where real-time collaboration is integrated [2]. The whole thesis will be written using LaTeX style, since LaTeX is the de facto standard for publishing scientific document [3]. The default article setup for Overleaf from NTNU thesis will be used, with the "Computer Modern" default font. The margins of the thesis is a bit wider than the default one from NTNU's template. This is to fit screenshots and pictures better.

The report will include a list of acronyms, together with a list of figures used. There will be an included list of references at the end. Each page will have a page number at the bottom.

The report will be split into three parts. The first part will be listing all the different security features of Windows 10/11 from hardware to application level. We will be providing a detailed description of:


- What the features are
- How they work
- What security threats they protect against
- Requirements for using these features
- How they tie in with the NSM ground principles

Part two of the report will focus on testing the security features that we can test with the resources available to us, as well as evaluating how these different security features might affect user experience for NTNU employees or students. Part two will then end with a discussion and final conclusion.

Part three will be focused on the conclusion to our thesis as a whole. This includes evaluation of the thesis, our work as a group, and discuss possibilities for further work that can be done by building on this report.

2 NSM ground principles

The NSM ground principles is a set of guidelines for how to protect IT-systems from unauthorized access or tampering[4]. These principles were developed by Nasjonal Sikkerhetsmyndighet (NSM) in corporation with both public and private organizations to establish the building blocks of how to create a secure IT-security system. These guiding principles are divided into four categories as illustrated in the image below.



1. Identify and mapping	2. Protect and maintain		3. Detection	4. Incident management and restoring
1.1 Map out governing structures, deliveries and underlying support systems.	2.1 Maintain security in acquisition- and development-processes.	2.2 Establish a secure IT-architecture.	3.1 Detect and remove known vulnerabilities and threats.	4.1 Improve organisations ability to handle incidents.
1.2 Map out deviced and software.	2.3 Maintain a secure configuration.	2.4 Protect organization network.	3.2 Establish security monitoring sytem.	4.2 Analyse and categorize incidents.
1.3 Map out users and necessary access privileges.	2.5 Control data flow.	2.6 Have a complete overview of identities and access privileges.	3.3 Analyse data from the monitoring system.	4.3 Control and manage incidents.
	2.7 Protect data in storage and the channels it is transported through.	2.8 Protect e-mails and web-browser.	3.4 Perform penetration testing.	4.4 Evaluate and improve from incidents.
	2.9 Establish ability of restoring data.	2.10 Integrate security in processes for change management.		

Figure 1: *The NSM ground principles four categories, inspired by image from NSM website: <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/hva-er-nsms-grunnprinsipper-for-ikt-sikkerhet/>*

We will be using these ground principles throughout this report as a foundation for our evaluation of the different Windows 10/11 cyber security functions, as well as our final conclusion and configuration recommendation. All though these categories are all integral to a complete IT-security strategy, we will mainly be focusing on category two and three as they are the categories that are most relevant to our client-side security. "Identity and mapping" is not as relevant as we were instructed by NTNU SOC not to look at how the systems are like today. Our thesis will touch on category four "Incident management and restoring", as it is important when creating a configuration recommendation for NTNU clients that there is laid a foundation for good incident response and recovery.

Part 1: The Security features

Description:

This part of the thesis will delve into the different security features in Windows10/11 from hardware to application level.

3 Windows Security Concepts

Windows 11 introduces new ways of thinking when it comes to tackling cyber-security threats with the rapid changes in today's hybrid work environment. Microsoft has used these security concepts to design the Windows 11 security strategy and based each security feature around these concepts, from hardware to cloud technology.

3.1 Zero Trust model

The Zero Trust model is developed for security in today's environment. The principles goes as following:

- Verify explicitly - Authentication should always be based on all available methods (user identity, location, workload etc.)
- Least-privileged access - User access should be limited, so that the user always has just enough privileges and just enough time.
- Assume breach - A breach should always be presumed. This is to minimize potential damage to data. Privileged roles, end-to-end encryption and threat detection are key factors here.

The zero-trust model moves away from a system where any user or device is assumed trustworthy. Instead users must now constantly earn trust by proving their identity and the integrity of their device[5]. This is achieved through technologies and metrics like; device health attestation, secure boot and certificates which we will be elaborating more about later on.

3.2 Root of Trust

Root of Trust is a physical hardware source that always can be trusted within a system. Hardware RoT is secure by design and cannot be tampered with[6]. Since computer systems use cryptography to encrypt and decrypt data, a way to check that this data is authentic and authorized is required. Hardware RoT is therefor the foundation for all security functions when it comes to digital signatures and encryption/decryption of data. It is "the root" of what can be trusted.

4 Windows security - Hardware features

Most security features in Windows 10 and Windows 11 uses both software and hardware. They are equally important. This cooperation between software and hardware makes attacks much harder, since the hardware itself is hard to tamper with without physical access. Making hardware a part of security also reduces the load on the software itself, which leads to increased performance and security.

4.1 Hardware root of trust

Windows operates using a root-of-trust system, where the goal is to maintain integrity of the system as the hardware itself turns on. When firmware is loaded and the operating system is launched, root-of-trust uses hardware to check the firmware and operating system code that boots[6]. This is done to easily see if the boot code is malicious. This also builds on the zero trust principle described earlier[5].

The hardware root-of-trust does not only do this, but also provides an isolated and secure area. This area is separated from the operating system itself, and is used for storing cryptographic keys, data and code. Sign-on tokens, Windows Hello biometric and BitLocker uses this storage space, and is required for them to work as securely as possible.

4.2 Pluton security technology

Microsoft Pluton security is security at the CPU-chip itself. This builds on the hardware root-of-trust described earlier. The Pluton Security Processor (PSP) works like the TPM-chip, but can be seen as an extra security measure. PSP is primarily produced by AMD where the goal is to integrate the motherboard and the OS[7]. This might sound a lot like the TPM, and that is because many of the features are the same. Pluton security technology can be viewed as an extension of the TPM-technology. This thesis will mainly focus on TPM, and not so much on PSP.

4.3 Trusted Platform Module

Trusted Platform Module (TPM) technology[8] is designed to provide security-related functions to the operating system. In most cases, Trusted Platform Module is done using a physical chip that is integrated on to the motherboard, which communicates with the rest of the system using a hardware bus. This chip is then used to generate and store cryptographic keys securely, which makes it very hard to tamper with for malware due to it being a physical chip.



Figure 2: A TPM 2.0 chip. Received 25.04.2022 from <https://upload.wikimedia.org/wikipedia/commons/thumb/b/be/TPM.svg/1280px-TPM.svg.png>

Most computers and laptops produced in the last decade has been produced with either TPM version 1.2 or TPM version 2.0. The main differences between these two versions is the algorithm they use for cryptography. As an example, TPM 1.2 only allows for the use of RSA and SHA-1 algorithms, while TPM 2.0 has a far longer list of algorithm options. TPM 2.0 is also much more consistent, since the operating system takes full ownership over it. TPM 1.2 varied in policy settings, since parts of it could be configured manually. TPM 2.0 on the other hand does not need to be configured manually at all[8].

An advantage of using TPM is that it is built on the root-of-trust principle. The operating system has full ownership over the TPM, and verifies it when the machine is turned on. The boot code is then loaded into the TPM, where it is measured. This integrity measurement is used as evidence to show that the system starts with the correct software. This boot code, together with other software, is securely stored in the TPM rather than in the main memory. This separation means that the operating system always can trust the TPM-chip. In practise, this also means that malware targeting boot-code and memory is essentially useless, since it is not accepted via the TPM.

This Trusted Platform Module technology is required for many key features when it comes to security in Windows 11. The chip itself is also a requirement for the client machine to be able to update from previous versions of Windows to Windows 11. When the computer is booted in Windows, the boot code is loaded into the TPM where it is measured and loaded.

The TPM does not need to be configured manually in neither Windows 10 or 11. The operating system takes full ownership of the TPM. There are two different versions of TPM. We have version TPM 1.2 and version 2.0. Either one works with Windows 11. TPM 1.2 started getting produced in laptops in 2006, while TPM 2.0 were released in the 2016-2017 era. Both TPM 1.2 and TPM 2.0 has the same features, but TPM 2.0 has more options[9].

TPM can be connected to principle 2.7 of the NSM ground principles. Principle 2.7 is "Protect data in storage and the channels it is transported through". This principle is mostly about encryption and cryptography[10]. TPM stores cryptographic keys securely so no software or components can tamper with it, other than the hardware bus which transfers it. Therefor, both the data in storage and the channel it is transported through is considered safe. TPM protects mainly against attacks where the goal is to steal data such as passwords.

5 Windows security - operating system features

With more secure hardware and software it is important that the operating system that is the glue between the two is just as, if not more reliable and protected. Windows 11 introduces enhanced data protection with advanced data encryption and validation technologies. This chapter is dedicated to describing those OS security features and technologies.

5.1 Secure boot and trusted boot

Secure boot is a windows security tool that functions to keep your device secure from malware during the boot process until your anti-malware software is activated. Secure boot makes sure the device boots using only bootloader software that has been pre-approved by the original equipment manufacturer. Computers without secure boot would just load the bootloader that is on the PC hard drive and trust that this is not a rootkit[11][12].

Rootkits are a type of malware that run in kernel mode. Rootkits have the same privileges as the Operating system (OS) itself and starts before the OS. The rootkit can therefore hide itself and other applications completely. There are different rootkits for the different phases of the boot process. They are:

- Firmware rootkits
- Bootkits
- Kernel rootkits
- Driver rootkits

The PC will begin the boot phase by ensuring that firmware is digitally signed, confirming that it has not been tampered with and is not loading any firmware rootkits. The secure boot then verifies all code that is run before the OS before checking the OS bootloader itself and that it is also digitally signed and trusted by the secure boot policy[11].

This is where the trusted boot process takes over for secure boot. At this point of the boot phase the windows bootloader confirms the digital signature of the windows kernel before it can load. From here it is the kernel's job to verify every other component of the windows start-up process. The kernel confirms the digital signatures of boot drivers, startup files, ELAM (early launch anti malware) driver etc. If secure boot or trusted boot detects any malware in a corrupted component, it will refuse to load this component. This component will also often be fixed automatically by windows by restoring the old and verified version[12].

NSM principle 2.2 is especially relevant for secure and trusted boot. This is to establish a secure IT-architecture[13]. This is done physically by the use of secure and trusted boot through the operating system. As mentioned above, the attacks this defends best against is rootkits attacks and attacks that targets the kernel. This means that unauthorized software cannot take control over the system during boot.

5.2 Device health attestation and conditional access

Device health attestation and conditional access are two useful tools that builds on the zero trust concept to control access to resources within an organization. Before it is granted access a device must prove it's identity and "health" to be able to access organization resources. Device health attestation is provided through data that is encrypted and stored in the TPM to prove the health of the device. This data includes information about the firmware, boot process and software. With this information the device health attestation policy controls[1]:

- That the device booted correctly, which is a vulnerable stage where security risks may occur.
- That the TPM is enabled and in attestation flow.
- That the operating system has all the required security settings.

This data is evaluated to confirm the device has not been tampered with and that it is a device with the right privileges to access these resources.

NSM ground principle 2.6 is the most important principle when talking about device health attestation. This principle is "Have a complete overview of identities and access privileges"[14], which is what device health attestation helps with specifically.

5.3 BitLocker

BitLocker Driver Encryption is an IT security feature designed to help protect your data and protect you from exposure to lost, stolen or improperly decommissioned devices[15]. BitLocker integrates with the OS and offers the most protection to the operating system system drive with the help of the TPM. It will help protect user data as well as make sure the computer is safe from offline attacks.

One of the ways BitLocker does this is by offering the option for the user to input a pin or a USB drive with an encryption key before the computer will initialize the start-up process. Windows will not start up until this PIN or USB drive has been entered and is separate from the users login credentials which they will also have to provide after Windows has booted up. This helps provide further verification steps before the computer will wake up from hibernation and making the contents of the system drive accessible[16].

TPM is not a must have for BitLocker to work but it improves the quality of service significantly. BitLocker can only offer pre-startup system integrity verification with the help of TPM.

NSM ground principle 2.7 is relevant for BitLocker. Ground principle 2.7 is about protecting data in storage and the channels it is transported through. More specifically, point 2.7.3 of the principle is about encrypting confidential data that easily can be compromised[10]. This is exactly what BitLocker does. The way BitLocker works can remind of the way TPM works, which builds on the same ground principles. Offline attacks is the best way to describe the attacks BitLocker defends against[17]. If someone steals your harddrive and connects it to another device, it is virtually impossible to decrypt this and harvest the data due to BitLocker.

6 Windows security - Software features

The software features of the Windows system is equally important as the hardware features. The hardware collaborates with the software to create a secure platform. Below are the most important software security features of Windows 10 and 11. Almost all of these are standard in Windows, with the exception of one towards the end of the chapter.

6.1 Windows Defender

One of the most basic built in software security features in Windows 10 and 11 is Microsoft Defender. It has been shipped with Windows since 2006 in Windows Vista, but was not a big part the operating system until Windows 8. Until Windows 8, Microsoft Defender was only used as an anti spyware software, instead of a full antivirus program that it is today. Windows Vista and Windows 7 had used another software called Microsoft Security Essentials where Microsoft Defender was a small program on the side. Microsoft Defender eventually replaced Microsoft Security Essentials, which is now the standard and ships with all new Windows versions[18].

6.1.1 Features

Until Windows 8, Microsoft Defender was only used to detect spyware. These early versions only checked certain parts of the disk for changes in files, which did not give much protection against other malware than spyware. Back then, Windows Defender also had a report function for reporting and flagging files that users considered to be spyware. When Windows 8 released, Microsoft Security Essentials anti-malware engine and virus recognition were transferred over to Microsoft Defender for a complete software[18].

Real-time protection is one of the advanced features that Microsoft Defender provides, and the most important one. The software is built around real-time protection, to protect the system 24/7. The real-time protection part of Microsoft Defender is enabled by default in Windows 10 and 11, but can be turned off if the user really wants to. This feature checks all downloaded files and software against a threat database, and removes the file if it seems malicious. This feature is called "block at first sight", and is done by machine learning and the use of large threat databases. The real-time protection feature also performs periodical scans of the system in the background to always check for malware[19] and verify that the system is safe.

6.1.2 Protection

Since Microsoft Defender has various built in functionality in Microsoft Edge, NSM principle number 2.8 is relevant here. This is "Protect e-mails and web browser"[20]. Microsoft Defender collaborates with both e-mail and web browser defence with other functions down, which fills out the principle. Examples on attacks that Microsoft Defender prevents is phishing attacks and malicious files, where block at first sight as mentioned above is relevant.

6.2 Windows Firewall

The built in Windows Firewall (officially named Windows Defender Firewall) has been a built in security feature since Windows XP back in 2001. Windows Defender Firewall works by checking inbound and outbound network traffic connected to the system, based on a set of rules which filters out and blocks the unsafe packets. Its job is therefor to protect the home network and computer from malicious software, hackers and intruders by checking the traffic and creating a barrier between the user's system and the external environment [21].

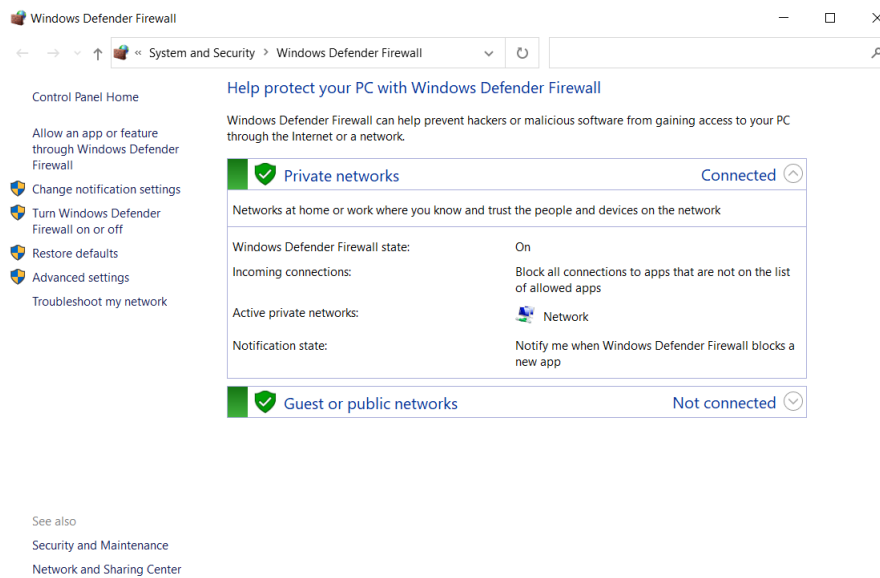


Figure 3: *Basic Firewall overview in Windows 10. Screenshot taken 03.05.2022*

6.2.1 Features

This feature is turned on by default in all versions of Windows, and has both a basic and an advanced user interface. The advanced interface has the ability for the user to create custom made rules, which makes custom filtering available. Filtering in this case is letting specific traffic through or blocking specific traffic based on a set of characteristics. These advanced features are rarely used by your standard user, since they are not aware of its existence. This advanced interface also automatically logs all network traffic into a default file for extra security [21]. For domain networks, the Windows firewall can also be set up using group policies to make sure all of the users are running the same setup.

6.2.2 Protection

The Windows Firewall primarily protects against threats that attacks through network traffic. Examples here are malware that are downloaded from specific sites, which the firewall will detect and block. This downloaded malware might give an attacker an opportunity for an access via a backdoor. Backdoors are security holes or bugs the system might have which gives an extra access point for the attacker[22]. These backdoor attacks are stopped using the Windows Firewall, since the packet is sorted out[23]. Windows Firewall also has a function to stop source routing. Since packets are routed through multiple routers and networks before reaching their destination, attackers may take advantage of this creating packets that seem trustable. Due to this, Windows Firewall has the ability to disable source routing[23].

Like all of the other mentioned security features, the Windows Firewall builds on the NSM ground principles mentioned earlier in the text. The firewall mainly protects data going in and out, in other words data flow. This connects closely to principle 2.5 under "Protect and Maintain" which is "control data flow". The goal of this principle is to control the information flow between different parts of a bigger system, like NTNU's system. This means that even if a malicious packet gets into the system and passes a firewall, it will likely get stopped elsewhere[24]. Controlling the flow of data also reduces the risk that the whole system gets infiltrated if an attacker gets access through a weak client machine, which protects against attacks targeting active directory. An example here is a Kerberos Golden Ticket attack. Simply put, the goal for the attacker here is to get a "golden ticket" in the means of taking over the Active Directory Key Distribution Service Account and granting themselves admin rights[25].

NSM ground principle 2.4 is also very relevant here. This principle is about protecting the organization network. Since the Windows Firewall controls packets passing through both inside and outside of the organizational network, it can be used to detect if an unwelcome guest is in the system and spreading dangerous data[26].

6.3 Microsoft SmartScreen

Microsoft SmartScreen is a built in cloud-based software in Windows 8 and newer versions, where the goal is to protect the system and user against phishing-attacks and malware via downloads[27]. It is controlled via the Windows Defender Security Center, and is also built into various Microsoft products such as Microsoft Edge, Outlook and Internet Explorer. It is activated by default in both Windows 10 and 11, as well as in Microsoft Edge.

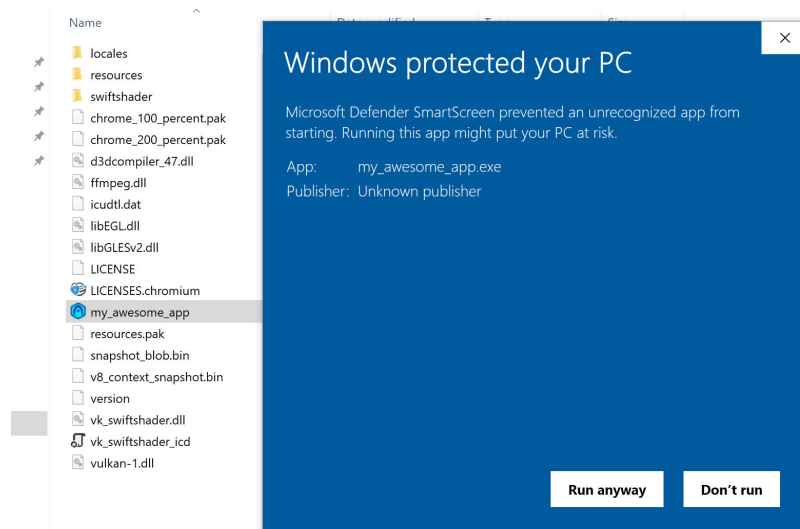


Figure 4: *Microsoft SmartScreen pop-up message, where SmartScreen has detected a file with low reputation. Retrieved 02.05.2022 from <https://www.soft8soft.com/docs/files/creating-desktop-apps/windows-protected-your-pc.jpg>*

6.3.1 Features

Microsoft SmartScreen uses machine learning and statistics to verify downloads. When downloading a file from the web, SmartScreen checks the reputation this file has in the cloud. If this program has a bad reputation, the user will get a warning suggesting that the downloaded file may be harmful. All Windows users can report if a file is safe or not via the Windows Security Center, which ultimately decides the total reputation of a file[28].

On paper, this is especially effective against phishing attacks where the user has to download files or click on links. When SmartScreen scans the downloaded file, it will have a very low reputation, which increases the chance of the user not running this file at all and deleting it. If the user also uses Outlook as an email service, SmartScreen will mark the email as an attack and therefore automatically delete it and mark it as spam, together with giving the user a warning. This is done by machine learning and user reports, meaning that junk mail and phishing attempts will be sorted out more often as more users register them as spam. However, there are some issues with SmartScreen presented below[28].

6.3.2 Issues

The reputation system is built upon code signing certificates that identify the author of the software. Because of this, new versions of the same file will have the same reputation as the old one during the certificates lifetime. This raises a problem: if a file creator releases a safe file, they can later release one with malware that can pass through SmartScreen safely and infect the system, due to a good reputation score. These certificates needs to be renewed every two years, meaning that the reputation will have to be rebuilt from zero relatively rarely. Microsoft has gotten much criticism because of this, and many users refuse to use SmartScreen due to inaccurate scans of files.

As of right now, some of the functions SmartScreen has is only built into Microsoft Edge. Examples here are if you click on a dangerous link in Microsoft Edge, you will automatically get stopped if the web page has been reported several times and has a low reputation. This becomes an issues for users that does not use Microsoft Edge as their primary browser.

6.3.3 Protection

Microsoft SmartScreen protect against threats that is downloaded onto the computer, such as malware, worms and other malicious downloadable files. The attackers goal here can vary from taking over the machine or system to destroying files and applications.

Microsoft SmartScreen touches a few different of the NSM security principles. The most important ones here are principle 2.4 and principle 2.8.

Principle 2.4 is designed to protect the organization network. Microsoft SmartScreen does this by detecting threats through phishing attempts and warning the user about malicious files, preventing these from spreading further into the network[26].

Principle 2.8 is about protection of the web browser and e-mails[20]. Microsoft SmartScreen does both of these when used in Microsoft Edge. For example, Microsoft SmartScreen warns you if you try to enter a dangerous domain.

6.4 Windows Event Viewer

Windows Event Viewer is utility software developed by Microsoft. It has been around since Windows Vista, and the main use for Event Viewer is to let users and administrators see the event logs it generates. The event logs are log files which keeps track of running events, system failures, security, configurations and more[29]. These files can for example be used to backtrack and analysed to determine whether something has happened or not, or if the operating system is running without errors. Another example is reporting of applications refusing to start, or applications failing to complete an action. This centralized application allows other programs and software to use its interface, which leads to better usability for the end user since all the logs are collected at the same place.

6.4.1 Features

Event Viewer is not a security feature in itself, nor does it detect any threats on its own. However, the utility lets you detect threats and potential security risks in your system yourself. The ability other software has to build their own log system integrated into Event Viewer proves it to be a important component for threat reduction, also when using other software than the ones built into Windows.

Event Viewer logs each event with its' own unique event ID, meaning that if your system crashes during boot, this will have another ID than if user authentication fails. This makes sorting and filtering different events from each other much easier for the client. The Windows logs themselves which comes directly from the operating system also have their own tags based on how critical they are[29]. There are not just automated events that are logged, such as booting or system crashes, but also events done manually by the user. This means that you can backtrack easily if someone has had physical access to your computer, provided that they have used applications that logs these types of events.

6.4.2 Issues

Even though Event Viewer is a very practical tool, it is not without it's issues. The fact that Event Viewer logs all Windows events by default means it can be difficult to find whatever you are looking for if you do not know the correct ID for the event. Looking for the correct ID can also prove time consuming, since there are so many different ones. Much of the information provided in the description tag for each event is also often complicated, even for technical personnel. This can make Event Viewer tricky for first time users to get into.

6.4.3 Protection

As mentioned above, Windows Event Viewer does not protect against any threats specifically, but makes finding attackers and intruders easier. It is therefor widely used in collaboration together with other security tools. Event Viewer therefor applies to mainly section 3 of the NSM principles, more specifically point 3.1 through 3.3. These principles in depth are:

- 3.1 - Detect and remove known vulnerabilities and threats[30].
- 3.2 - Establish security monitoring system[31].
- 3.3 - Analyse data from the monitoring system[32].

This is exactly what Event Viewer is: a monitoring system that saves activity in the system.

6.5 Sysmon

Sysmon (System Monitor) is a security software developed by Mark Russinovich and Thomas Garnier for Windows. This assignment will focus on Sysmon version 13.33.

Sysmon acts as a Windows system service and device driver. When installed, it monitors and logs systems activity even between reboots. Sysmon specifically focuses on process creations, network connections and file creation. Events generated by Sysmon can be viewed using the built in Windows Event Viewer. It is important to note that Sysmon does not provide any protection or defense against system threats, it simply monitors and logs them. By using Sysmon you can more easily analyse the activity in the system and detect malicious activity or other anomalies[33]. Sysmon is also a useful tool during system recovery and clean-up after a cyber security incident as it can help track the attackers footprints in the system and map out what parts of the system they might have had access to.

Since Sysmon is essentially an extension of Event Viewer with added functionallity, we can apply the same NSM ground principles as the ones relevant for Event Viewer. This is 3.1, 3.2 and 3.3 which are described in chapter 6.4.3, Protection.

7 Group Policies

A big part of the advanced security in Windows is Group Policy. This is a way for network administrators to set up account rights and privileges using Active Directory (AD). The goal of Group Policy is to provide centralized management where you can control many users or user groups from one location. A domain controller which controls the network is used for this. Group Policy Object (GPO) is the name of a set of group policy configurations. In practice the GPO controls what a user can and cannot do inside the computer system. This means that you can set up a GPO for all NTNU-machines, which makes all the users and computers in this group them have the same rights and privileges[34].

Some examples on what GPO can be used for:

- Not allow users to change certain settings.
- Set a fixed character length for passwords.
- Restrict users from accessing specific folders and files.

All Windows versions updates its group policies every 90 minutes by default, with a 30 minute offset. The policies are also updated when you restart the computer. While using a domain computer (centralized control unit), the policies are updated every 5 minutes[34]. This will be the case for computers on the NTNU network.

GPOs are updated in this fixed order:

1. Local - This means any settings in the computers local policy.
2. Site - This means any computers connected to the AD.
3. Domain - This means any policies linked to the domain controller.
4. Organizational Unit - This means any policies connected to the AD organizational unit.

7.1 Local Group Policies

Local Group Policies (LGP) is a more basic version of group policies, meant for controlling standalone computers. This works by using the domain controller to specify special rules for specific computers or groups. Local Group Policies (LGP) is also used for backing up GPO setups, where you can copy a specific computers policies and back this up. This has been in use since Windows Vista[34].

7.2 Relevant NSM principles

The most relevant NSM principles for Group Policies are principle 2.6, 2.4 and 3.2. This is "Have a complete overview of identities and access privileges"[14] which is much of what Group Policies are for. Access privileges is something the system administrator of a organizational network sets up, which decides who has access to what. Group policies also lets the administrators see who is connected to the network, with for example enabling of logging tools like Event Viewer. This is principle 3.2: establishing of a security monitoring system[31]. This prevents attacks from inside the system. All in all this results in better protection of the organization network, which is principle 2.4[26].

8 Passwordless Authentication

Passwords is perhaps one of the biggest security weaknesses in IT-systems today, and the most common point of entry for hackers. Brute force, phishing, reuse of passwords and weak passwords are some of the easiest and most common ways that malicious actors might gain unauthorized access to a company's systems. As we can see, passwords leave a lot of room for human error which makes this much easier to exploit for potential hackers. People are expected to create passwords that are strong, unique, random enough so they can't be guessed, all while being able to remember these passwords and not use the same password twice.

For these reasons Windows 11 has put a lot of emphasis on creating a passwordless future. Windows 11 provides passwordless access using a variety of different tools and technologies such as; Windows Hello, Biometrics, PIN-codes, Microsoft Authenticator App and FIDO2. All the while protecting the users credentials with robust software and hardware protection like TPM 2.0, Windows Defender Credential Guard and Virtualization Based Security (VBS).

8.1 Windows Defender Credential Guard

Windows Defender Credential Guard is a security feature that isolates user credentials from the rest of the operating system using virtualization based security. It does this by storing the credential information in separate containers, only granting access to certain privileged software. The data is therefore kept safe from malicious software even if the network becomes infected[35]. Windows Defender Credential Guard requires TPM 2.0, Hyper-visor and Secure boot to run.

8.2 Windows Hello For Business

Windows Hello For Business is a useful tool meant to replace passwords as a means of authentication. Instead of passwords Windows Hello requires the user to use a PIN-code as well as biometric authentication such as face, fingerprints, and iris recognition. It can be used to log into your Microsoft account, Active directory, Microsoft Azure active directory, and other identity provider services that rely on and are FIDO certified [36].

A PIN might sound like it's just a shorter and less complex version of a password and would therefore be less secure. But there are in fact several factors that make PINs the better option of the two. The PIN is bound to the device, meaning that it is bound to that specific hardware and would be useless to any malicious actor unless they physically stole your device as well [37]. Password phishing attacks is as a result not a threat with Windows Hello for Business. The PIN is also therefore only stored in the device's hardware, more specifically in the TPM. Passwords on the other hand, even if they are only stored locally will on Windows 10 not be linked to the TPM and will for that reason be much more exposed to tampering.

Even though a PIN might have less complexity than a password the TPM will also protect against attempts at brute-forcing the PIN as the device will get locked after a certain amount of incorrect PIN's. And even if one does not find that reassuring enough, an IT administrator can also add more requirements of complexity to the PIN in Windows Hello's policy settings. There an IT administrator can demand that users create PIN's with special characters, lower and upper case letters, and numbers. This will make the PIN more complex and similar to a password, but it will still be a PIN-code.

Windows Hello For Business uses a cryptographic private/public keypair that is stored in the TPM and the public key is sent to the identity provider during the initial Windows Hello registration. This public key is then mapped to the users account. By entering the PIN or providing biometric authentication the user unlocks access to these keypairs which are then validated in combination with the PIN/biometric signature by the identity provider. The user is then granted an authentication token and access to the desired resources [36].

Just like so many other security features in Windows 11 2.0 is a requirement for Windows Hello. Windows Hello also require the device to support biometric hardware that complies with the Microsoft Windows Hello biometric requirements. Most of the new hardware from the major OEMs complies with these requirements. Windows Hello also supports Enhanced Sign-In Security which is something that creates an additional layer of security using VBS and TPM 2.0 to protect the users biometric credential data. The VBS and TPM is used to isolate the data and the channels through which that data is communicated.

8.3 FIDO and FIDO2 Security Key

Above we mentioned that Windows Hello is FIDO certified. Fast Identity Online (FIDO) is widely considered to be the leading standard for what a secure, simple, and quick authentication solution should look like and function[38]. It has been developed by The FIDO Alliance with the goal to replace passwords and eliminate security threats such as phishing. FIDO2 Security keys is a key, typically a USB, that can be used as authentication as an alternative to passwords.

9 Windows Security - Application

Windows 11 provides multiple layers of application security to keep devices safe from unsecure applications. Hackers often use applications with bad security as a way to infect systems with malicious code [1]. In Windows 11 Microsoft has improved application security from an applications development, all the way to after the application has been deployed. By providing a Windows Software Development Kit (SDK) that is up to date with today's security standards and protocols, Windows can help developers make more secure and protected application. To protect systems from applications Windows 11 have several layers of protection. The implementation of the zero trust concept is the first line of defence to keep compromised application from gaining access to data that it should not have access to. Applications now need to earn trust as opposed to in the past when all applications the user decided to run was deemed trustworthy by default.

9.1 Windows Defender Application Control (WDAC)

Application control is an effective tool to create restrictions of what material applications can access as well as which applications are allowed to run in the system[39]. This widely considered an integral security strategy to mitigate against executable file-based malware. WDAC is a technology available on both Windows 10 and Windows 11 that can perform this sort of task. WDAC can create policies based on:

- Attributes of the codesigning certificate(s) used to sign an app and its binaries.
- Attributes of the app's binaries that come from the signed metadata for the files, such as Original Filename and version, or the hash of the file.
- The reputation of the app as determined by Microsoft's Intelligent Security Graph.
- The identity of the process that initiated the installation of the app and its binaries (managed installer).
- The path from which the app or file is launched (beginning with Windows 10 version 1903).
- The process that launched the app or binary.

(This list is retrieved (23.05.2022) from: <https://docs.microsoft.com/en-us/Windows/security/threat-protection/Windows-defender-application-control/wdac-and-applocker-overview>)

9.2 User Account Control (UAC)

If the user device should get infected with malware it is important to limit the spread of that malware as much as possible. User Account Control (UAC) is a feature that is integral to reduce the impact of any malware that might inadvertently enter the system. UAC enforces the concept of "least privilege" by making sure users operate at the lowest privilege needed for the task they are performing. This will help preventing malicious actors or malware from gaining administrative rights to access sensitive data or performing changes to the device[40].

Windows protects a process by giving it an integrity level. A process with a high integrity level is a process that is performing higher privilege tasks like modifying system data. While a process with a low integrity level is a process with higher likelihood of compromising system security. All apps and tasks run with the privilege of a standard user by default. If a standard user wishes to run an application that needs an administrator access token it must provide proper administrator credentials to do so. All apps that need an administrator access token must request permission. Child processes on the other hand inherit the access token from the parent process so long as the child and parent process both have the same integrity level[40].

All users as well as administrators consequently operates on a standard user level from logging in. Users will get a consent- or credential prompt when attempting to run an application that requires an administrative access token. Administrators in Admin approval mode will usually get the consent prompt where they can give permission for an app to elevate it's privilege. And a standard user will get a credential prompt where they have to give valid credentials to run the application.

9.3 Application isolation and Microsoft Defender Application Guard

Phishing is one of the biggest cyber security threats we see today. Especially for larger organizations the impact of a sophisticated phishing attack can be catastrophic. Phishing can have consequences like loss of data, operational disruption, damaged reputation etc. Hackers use social engineering to try and bait users into clicking a malicious attachment in e-mails or enter a compromised website. And these sorts of attacks are getting more and more convincing, especially to an untrained eye. This is exactly why application isolation is pivotal in the future of combating phishing. This builds upon the concept of zero trust and least privilege access.

By treating every web browser session and application as untrustworthy and keeping them isolated from the rest of the system, Windows 11 makes it significantly harder for any attacker to breach system integrity. This is what Microsoft Defender Application Guard is designed to do. By utilizing hyper-V virtualization technology, Application Guard can isolate applications and websites that are deemed as unsafe by administrators[41]. By running these applications and browser sessions in an isolated Hyper-V container any possible malicious code is contained within that container and the host-OS remains unaffected.

Application Guard mainly works for browser sessions in Internet Explorer but there are extensions available for both Google Chrome and Mozilla Firefox as well. Application Guard also helps securing Microsoft Office by isolating unsecure files in word, excel and powerpoint. Whether or not an application or browser session is protected by Microsoft Defender Application Guard is indicated with a shield in the corner of the application or sessions icon as shown in the image below.

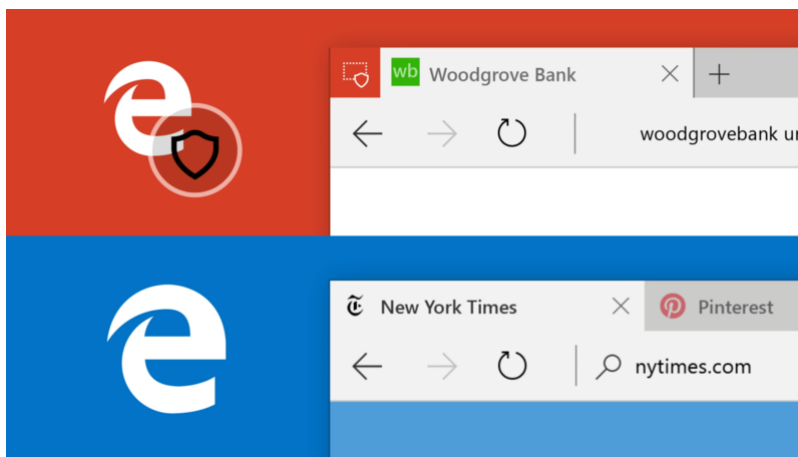


Figure 5: *Difference between explorer interface with Microsoft Defender Application Guard compared to explorer interface without. Retrieved 09.05.2022 from https://commons.wikimedia.org/wiki/File:ApplicationGuard_for_MicrosoftEdge.png*

Part 2: Testing, user experience evaluation and conclusion

Description:

This part of the thesis is dedicated to testing different security features and evaluating the user experience/friendliness of these features. These results will then be taken into account and used to discuss and arrive at a final conclusion.

10 Testing & user experience evaluation

10.1 Introduction

At NTNU employees use their computers for a wide spectre of different tasks. Some employees might need their computer for nothing more than writing and saving documents, while others might use their devices to perform more CPU-demanding tasks such as running virtual machines or heavy programs.

In this part of the report we will be testing some of the Windows 10 and 11 security functions that have been previously described, and look at the user experience. The tests will be done by using the remote desktop tool to connect to the SkyHiGh servers. This will influence the user experience a tiny bit, since using remote desktop is generally slower than using the computer physically. This should not be too much of an issue. We can still analyse the user experience from this.

10.2 Limitations

For the testing of the different security functions we had limited resources available. We did not have a computer with TPM 2.0 at our disposal after inquiring with NTNU, nor does SkyHiGh have TPM 2.0 capabilities. As previously explained TPM 2.0 is an integral part of Windows 11 security and many of it's features which made it difficult to test security features with TPM 2.0 requirements.

For this reason we decided to use SkyHiGh to test the most important functionalities that do not require TPM. Especially security that is based on virtualization technology like Hyper-visor.

To enable and configure the security features we were able to test in SkyHiGh used group policy editor since we were only configuring one single client. However and organization like NTNU would most likely use a mobile device manage (MDM) such as Microsoft Intune.

We will not be able to test out features like secure boot and trusted boot, since these features are a part of the system itself and cannot be measured in an easy way - neither on user experience nor performance.

10.3 Software and test-setup

10.3.1 SkyHiGh

SkyHiGh is the system that will be used for testing. This is a part of NTNU's server system, which we have gained access to for the purpose of testing. We have one instance running on SkyHiGh, since this is all we need to test basic security features.

10.3.2 Windows Remote Desktop

Windows Remote Desktop is the software we will use to connect to the Windows 10 client we will use for testing out security functions. This is built in software in Windows 10 and 11, which lets us connect to our SkyHiGh server.

10.4 Testing of Microsoft Defender Application Guard

We used our SkyHiGh server to test out the user experience in Windows Defender Application Guard, as well as taking a look at the performance aspect of it. Neither of us had the correct hardware to install the application guard on our own laptops, which lead us to using the virtual machine in SkyHiGh and receiving some less accurate results than we would otherwise. This is because the virtual machine interface has some latency, resulting in us not receiving the optimal user experience or representational CPU performance data that we otherwise would have received doing the testing.

10.4.1 Microsoft Defender Application Guard for Microsoft Edge - Testing

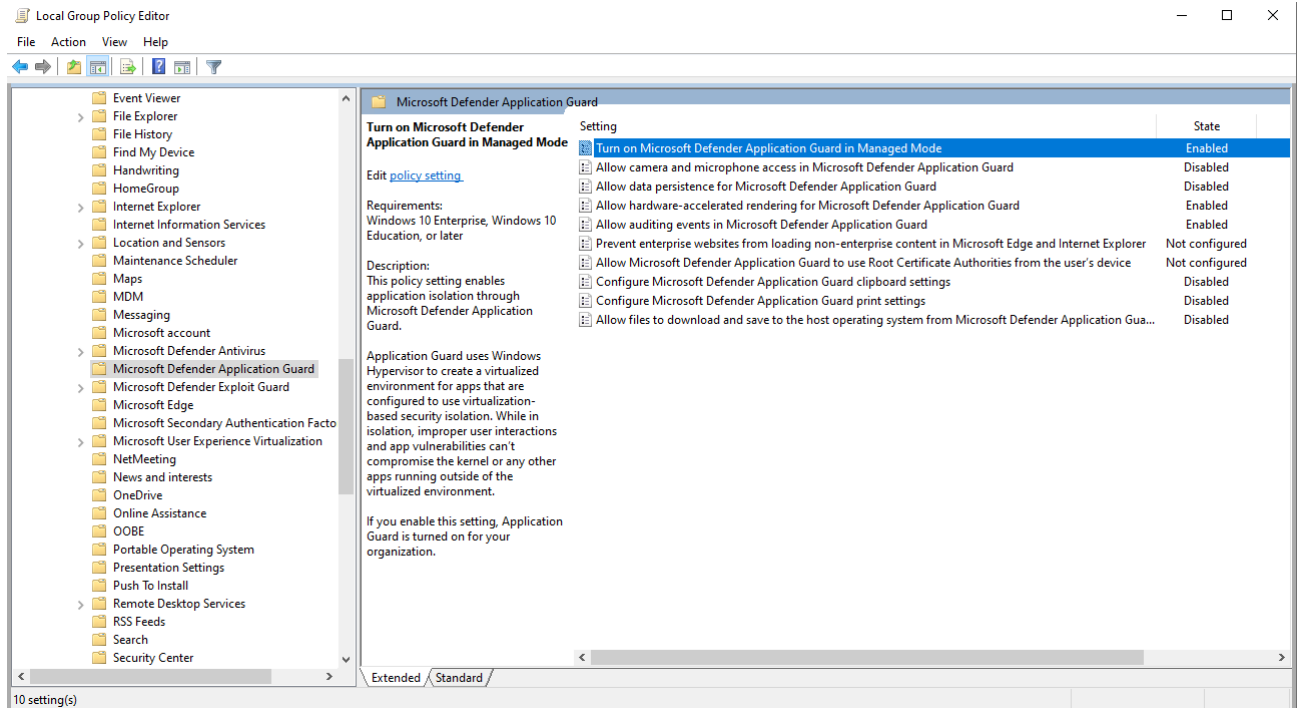


Figure 6: *Windows Defender Application Guard interface in the group policy editor. Screenshot taken 02.05.2022*

The first thing we did was enabling the application guard through the group policy editor. This is shown above. The settings we enabled were:

- Turn on Microsoft Defender Application Guard in Managed Mode.
- Allow hardware-accelerated rendering for Microsoft Defender Application Guard.
- Allow auditing events in Microsoft Defender Application Guard.

The rest were set to disabled and not configured. See figure 6.

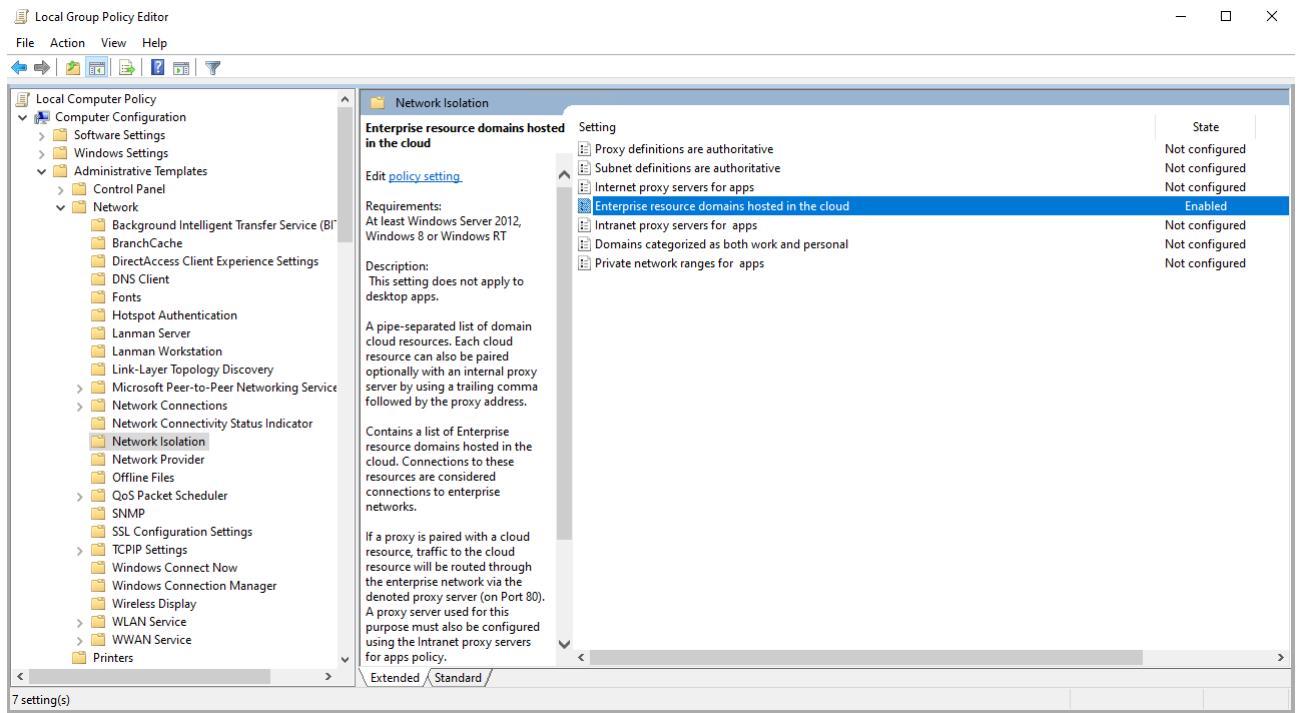


Figure 7: Network Isolation interface in the group policy editor. Screenshot taken 02.05.2022

We now had to configure allowed addresses that would not prompt the application guard. This was done by changing the Network Isolation settings in the group policy editor. The only setting we touched here were "Enterprise resource domains hosted in the cloud", which we set to enabled. See figure 7.

The "Enterprise resource domains hosted in the cloud"-setting were set to allow only `https://www.google.com/` in this test, meaning that the only web-page that would not prompt the application guard here were. See figure 8.

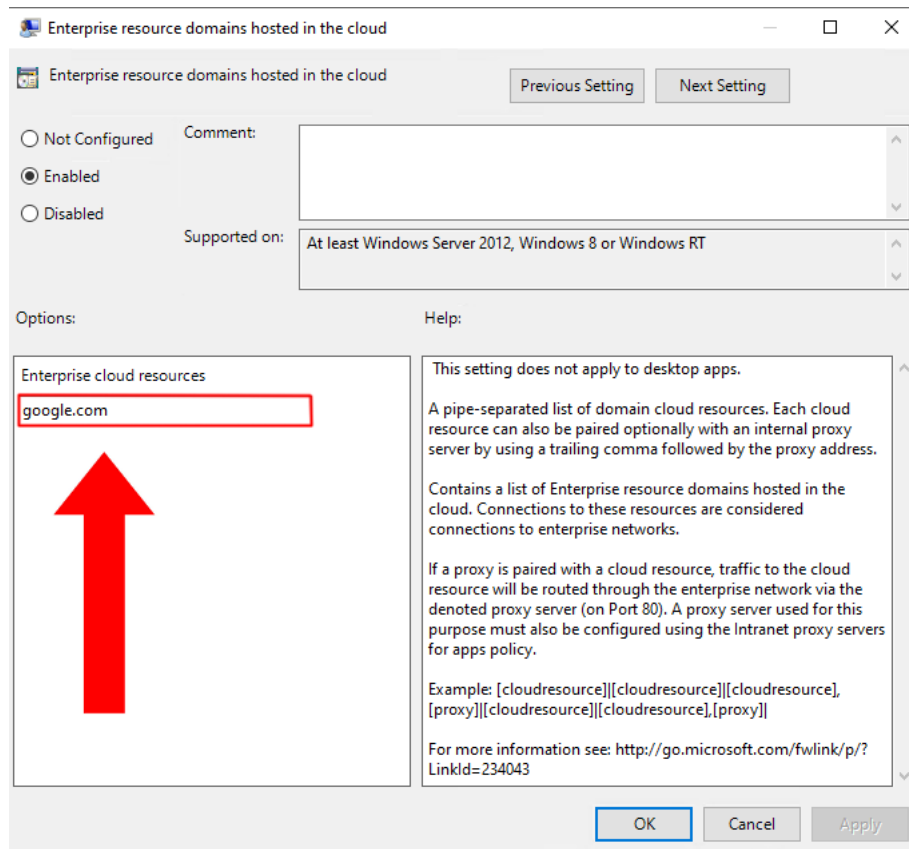


Figure 8: The interface for the enterprise resource domains in the group policy editor. Notice that google.com is set as allowed domain. Screenshot taken 02.05.2022

This worked, which meant that application isolation was enabled. When we tried to enter <https://www.vg.no/> in the Microsoft Edge web-browser, a new windows of Edge popped up, but this time it was the Application Guard variant of the browser. Notice the pop-up in the bottom tab that shows a shield. See figure 9.

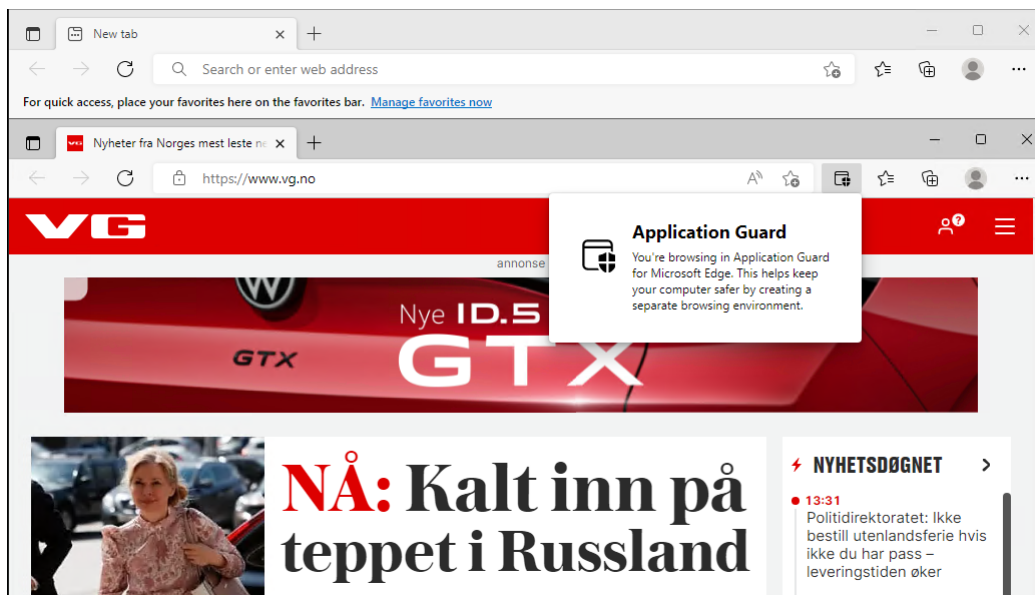


Figure 9: The upper window is the normal Microsoft Edge browser, while the one at the bottom is Microsoft Edge with Application Guard which opened automatically. Screenshot taken 02.05.2022

10.4.2 Microsoft Defender Application Guard for Microsoft Office 365 - Testing

As mentioned in chapter 9.3, Microsoft Defender Application Guard also works with Microsoft Products like Microsoft Office. This isolates files that are downloaded from emails and other websites from the rest of the computer using virtualization. We tested this part of the application guard with Microsoft Word.

The first task here was to enable the setting in the group policy editor. This part of the test-case focused on just the Microsoft Office 365 part of the application guard, and not the Microsoft Edge part. Because of this we chose setting 2, which was "Enable Microsoft Defender Application Guard for isolated Windows environments ONLY". Had we chosen setting 3, we would have had the functionality of the application guard in Microsoft Edge as well. See figure 10.

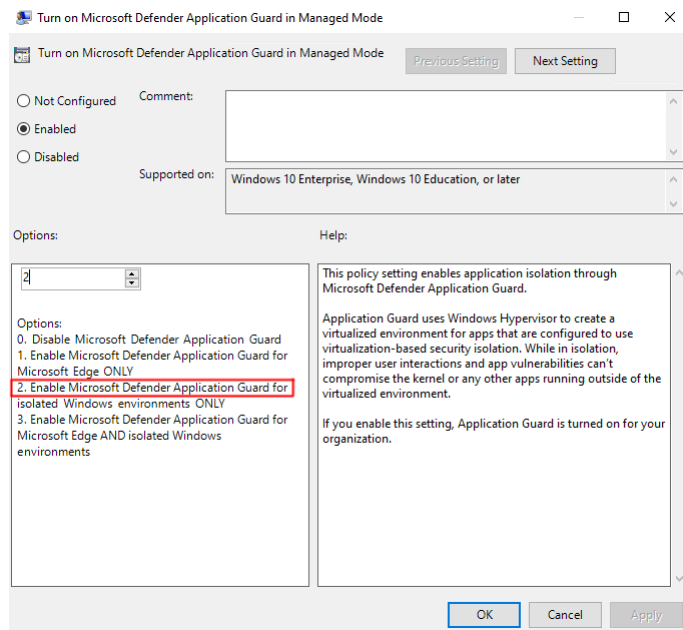


Figure 10: *The interface for the Microsoft Defender Application Guard in Managed Mode, showing option "2" being applied. Screenshot taken 02.05.2022*

After this, we constructed a Microsoft Office Word file for our test case. We attached this file to an email, which we opened and downloaded. This worked as expected - meaning that the Application Guard isolated this file from the rest of our system. We could still edit the file and save it, but it was isolated by the application guard. You can see two compared files in figure 11, one where application guard is active and one opened locally on the computer. Notice the shield icon in the top right, together with the pop-up.

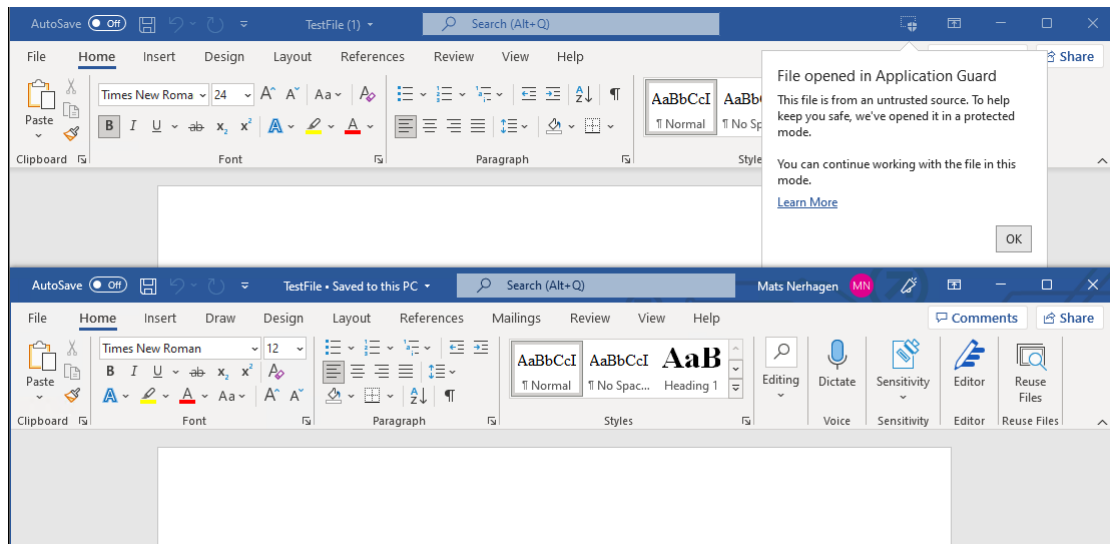


Figure 11: *Two different Microsoft Word files opened. The top one has been opened in Application Guard. Screenshot taken 02.05.2022*

10.4.3 Microsoft Defender Application Guard - User experience evaluation

Doing a substantial amount of work or performing many actions contained in a virtual machine might naturally feel a little slower than it normally would in a regular web-browser. This is something that could affect user experience without a properly detailed configuration of network isolation interface in the group policy editor. With a good configuration of what websites are considered safe/unsafe, NTNU's employees shouldn't be operating in application guard on a regular basis. Application guard on office files on the other hand is something users will run into a lot more on the regular when downloading and sharing office files. From our experience with application guard on SkyHiGh this seemed a little more time consuming and something that might occur more regularly. Currently users are used to opening office files in read-only mode which can be changed to activate editing with one click. Turning off application guard in office files on the other hand requires a few more steps from the user.

For example; to remove application guard protection on a word file the user must go into file info and click on "Remove protection". A pop-up will then appear asking the user to confirm that they want to remove protection as shown in figure 13. When the user confirms the removal, windows defender will scan the file for any malware before allowing it into the rest of the file-system. This process is an element of application guard that can prove to be time consuming for users.

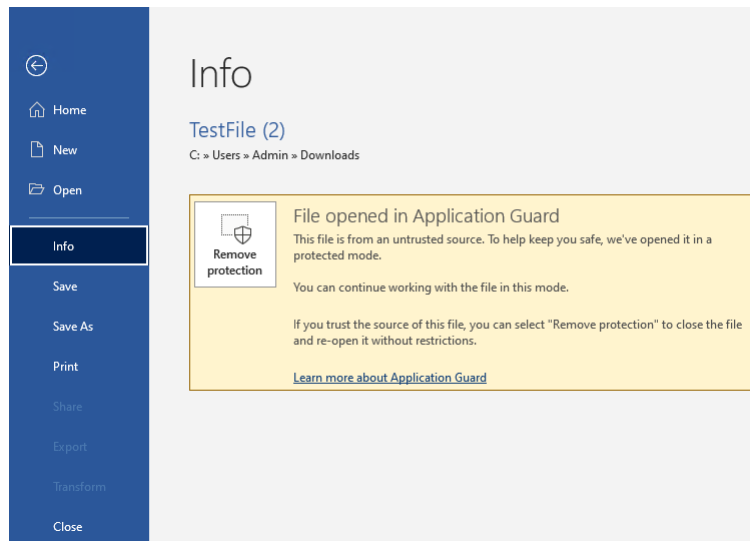


Figure 12: Process for removing application guard in word file. Screenshot taken 02.05.2022

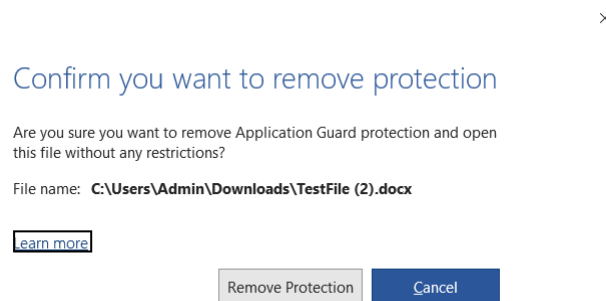


Figure 13: Process for removing application guard in word file. Screenshot taken 02.05.2022

10.5 Windows Hello - User experience evaluation

Windows Hello was hard for us to test due to the requirements of TPM. The main characteristics of Windows Hello is that it is bound to the device - meaning that even if someone steals your PIN code, it cannot be used. This requires TPM due to the PIN being stored there using encryption. We cannot test the biometric part of Windows Hello either, since we do not have access to the hardware components of the SkyHiGh servers and therefore cannot test the login functions using finger scan or face scan.

Due to reasons mentioned, we could not setup a specific test case here, but both of us have previous experience with Windows Hello through other ways. Some of the user experience here will therefore be based on our previous experience with the login method.

10.5.1 PIN

Using PIN with Windows Hello has a major upside when it comes to user experience: you only need to remember a PIN code, and this can be as short and simple as four numbers. This is for many people much easier than remembering a long and complex password. This results in a more pleasant user experience, and makes logging into the system much faster. In a big organization like NTNU, the likelihood of someone forgetting their password is bigger than someone forgetting their PIN. It would be more resource friendly for system administrators. There are very few negative sides with Windows Hello PIN, since it is considered safer and also easier than passwords.

10.5.2 Biometrics

Windows Hello with biometrics has a few client sided issues which can lead to bad user experiences. An example here is the face recognition login using the machines webcam. This can lead to a bad experience for the client if the webcam does not work properly, or are of bad quality. The webcam can also have issues if the lighting is poor - this means that the hardware on the machine itself influences the users experience with Windows Hello, even if this means through finger scans or face recognition. In a big system like NTNU, this greatly increases the hardware requirements if Windows Hello will be used as a standard.

10.6 Windows Event Viewer - User experience evaluation

As discussed in the main chapter, Windows Event Viewer does not provide any security directly. It is still an important tool for detection and backtracking to scout for attacks, breaches, system failures or other errors.

Event Viewer can be tricky to get into, both for administrators but also for normal users of the system. The fact that almost every Windows process and other programs gets logged here results in a big system of logs, which can be hard to navigate through if you are not familiar with the different ID's or the filtering that is being used. These logs do not only consist of error messages and critical failures, but also normal information such as when a restart or update is scheduled. This can make finding what you are looking for hard, especially for newer users.

Even though it can be hard to learn, Windows Event Viewer has a good user interface which is easy to understand but hard to master. The different categories and directories are in most cases structured well, which results in a good user experience IF the user knows what they is looking for. In other words: Event Viewer can be a very good tool for logging and analysing if you know what you are looking for, because of a good user interface.

10.7 Windows Defender - User experience evaluation

Windows Defender is the biggest and broadest security component on the Windows platform. However, many of the user based issues with this software are the same. Popups and notifications are the main point of irritation when it comes to the user's experience. The first thing that shows up when googling "Windows Defender pop up ..." is "... how to disable", "... blocker", "... disabler" and "... won't go away". This indicates an irritation among users when it comes to the warnings given by defender. These warnings can have different sources from the different parts of Windows Defender, based on the operation the user are doing. It is therefore hard to disable each one of these manually, and all alerts from Windows Defender must in that case be disabled. This however raises a new problem: you will not receive alerts notifications or alerts at all, meaning that the client can miss out on important security warnings regarding the system, or even worse, malicious files.

Windows Defender runs by default in most systems, unless it is forced to stay closed. This means that most users will not notice anything regarding the CPU speed of the computer, since they are likely already used to Windows Defender running in the background. Windows Defender does not take much CPU power, even when doing scans of the whole system [42]. Windows Defender does therefore not change the user experience performance wise by running in the background and slowing other processes down. The fact that Windows Defender supports mainly Microsoft Edge might lead to a somewhat worse user experience, since most people are running other options here. Dissatisfaction might arise due to the user being forced to user Microsoft Edge for complete protection.

10.7.1 Windows Firewall - User experience evaluation

The Windows Firewall has a very basic Graphical User Interface (GUI) in Windows 10 and 11, as seen in figure 3 in the chapter about security functions. The advanced GUI looks much like Event Viewer as seen in figure 14. The fact that you can choose to either use the simple GUI or the advanced one results in a good user experience, where users can begin with the simple and move over to the advanced if they need these features. Windows Firewall is also lightweight, which means that having it run in the background has no effect on other software running. This leads to a good user experience.

The custom filtering of packets in Windows Firewall can lead to a bad user experience if the organization or administrator has configured the firewall poorly. This can lead to blocking of safe web pages, that should be accessible, resulting in an annoyance for the end user.

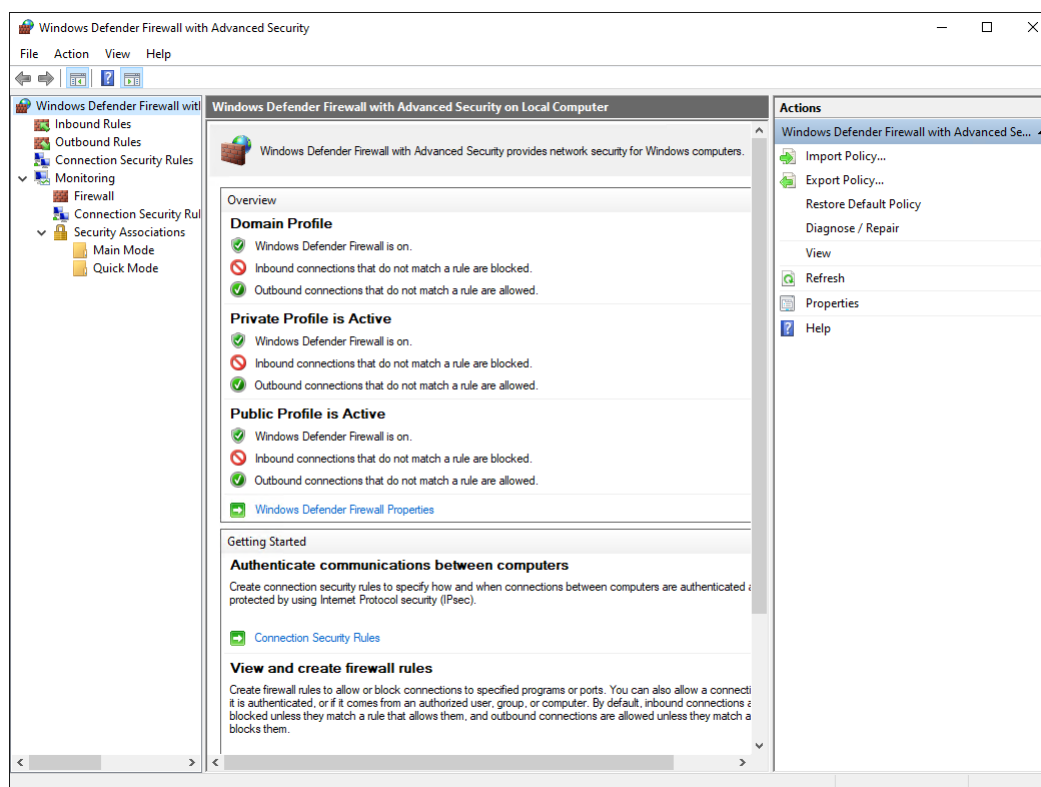


Figure 14: *Two different Microsoft Word files opened. The top one has been opened in Application Guard. Screenshot taken 02.05.2022*

10.7.2 Microsoft SmartScreen - User experience evaluation

Microsoft SmartScreen can impact the user experience negatively if it blocks web pages in Microsoft Edge falsely. This can become an annoyance if done it happens repeatedly, and falsely blocks users from web pages that are actually safe. The same goes for the email filter SmartScreen provides here. If SmartScreen marks an email as a false positive, which means that an email marked as dangerous is actually positive. This can make users feel unsure if they can trust a source or not.

According to Microsoft's FAQ section for Microsoft SmartScreen, it does not happen frequently that a web page or email results in a false positive. This should therefore not be an issue according to Microsoft [43].

Another downside of Microsoft SmartScreen is that it is only available in Microsoft Edge. This means that the user cannot choose their web browser freely, resulting in a bad user experience.

10.8 User Account Control (UAC) - User experience evaluation

User Account Control does not have many downsides when it comes to user experience, other than mild moments of annoyance. This is for example when an administrator has to run an executive program, and still gets prompted with the security warning. If you do not have administrator rights, a password prompt will appear here. If you are already logged in as administrator, a checkbox you have to accept is the only thing that shows. This can lead to a slightly worse experience for the user.

10.9 BitLocker

The only real affects Bitlocker might have on user experience is that it might cause latency when reading/writing to memory. The longer the encryption key is the higher the latency. However this varies greatly depending on the hardware specs of the device. If the computer has an HDD it will have a high negative impact on performance. On the other hand the latency on reading/writing to and SSD will be minimal and imperceptible to the user when performing regular tasks.

The pre-startup system integrity verification that Bitlocker provides might feel tedious from a users point of view. With two-step authentication this will require the user to provide three different authentication credentials before gaining access to the device. However the pre-startup verification from Bitlocker can be a four digit PIN which should be relatively fast to type in.

11 Conclusion & Recommendations

Now that the most important security functions have been explained in detail and evaluated from a user experience standpoint, we can finally discuss the results and conclude with an educated recommendation for what features NTNU should integrate into their system. Just like in part one this will be done categorically from hardware to application with a short summary at the end.

11.1 Hardware

For hardware there is less need for discussion. All NTNU devices would at the bare minimum require the necessary hardware components needed to run Windows 11 and it's various security features. TPM 2.0 is the main hardware requirement that is unique to Windows 11 when compared to earlier versions of windows. TPM 2.0 as previously explained, is essential for many of the Windows 11 security functions to work. It is one of the most important factors to ensure the concept of zero-trust is enforced, and subsequently Windows 11's security strategy as a whole.

This brings us to the next hardware requirement. To be able to tackle the security vulnerabilities that passwords bring with them, we think NTNU should strive to adopt a passwordless approach to authentication. For this reason we believe it is necessary for NTNU devices to support the necessary biometric hardware requirements for Windows Hello. This would include cameras or fingerprint scanners that comply with the Microsoft Windows Hello biometric requirements, or both.

11.2 Operating systems

In the operating system requirements several of the security features that has been elaborated on previously on this report are enabled by default. These are not necessarily features that affects the user experience in any way. But rather features that comes with Windows 11 and are important cogs in the operating system to make it work as it should. Secure boot, certificates and device health attestation all fall under this category. They are enabled by default and should stay that way to ensure proper maintenance of the zero-trust concept as they are strong metrics to prove identity and device health.

Following the NSM ground principles point 2.7[10] we believe it is important for any organization to have encryption for sensitive data, either if it's just a few chosen volumes or the entire OS drive. Especially for a university like NTNU where student and employees alike need to gather research and sensitive data which should be stored on an encrypted device. For this reason we have concluded that Bitlocker is a good solution and will provide needed encryption and security for data in both storage and transit. All though Bitlocker has shown it can reduce read/write performance depending on what specs the device has, we think that performance reduction is negligible with modern computer hardware. Considering the fact that NTNU would already need to make substantial updates to their hardware requirements to follow our recommended configuration, we assume that their clients will have modern enough hardware that this will not become an issue.

11.3 Software & Application

Many of the software features discussed in chapter 6 is already activated in both Windows 10 and Windows 11. Windows Defender will for most users be a standard security function that is already on the system, and this should not be tampered with by NTNU. NTNU should keep using Windows Defender due to it's broad aspect of built in security functions.

Making users use the Microsoft Edge browser can prove to be a hard task. On one side, Microsoft Edge has a broader selection of built in security tools both from Windows Defender, but also from applications like Microsoft SmartScreen. This means that the safest option for NTNU would be to force users to use Microsoft Edge because of added security. But is this really worth the negative

experience this can inflict on the client? Our recommendation here would be to give the users the freedom of using whatever web browser they would like, and instead use Microsoft Defender Application Guard fully since it has some of the same features. This way, the user can choose whatever web browser he likes and instead install the required extension in the browser provided for Application Guard. Application Guard can be a bit slower and more time consuming than focusing fully on SmartScreen, but this is a relatively small pay-off for more security. If NTNU has to choose between either Application Guard or SmartScreen seen relative to user experience, Microsoft Application Guard would be the best option.

Microsoft Defender Application Guard has its own feature for Microsoft Office 365. The negative side here is that it can sometimes feel jagged and a bit slow, resulting in a bad user experience. We will recommend NTNU using this feature due to the security it provides from for example Word files downloaded from the internet, however it can lead to some bad experiences.

Both Event Viewer (+ Sysmon) and Group Policies should absolutely be used by NTNU. Event Viewer is an important tool to log almost everything, and the extra functionality Sysmon provides makes it even better. As long as someone who knows how to use the software uses it, no bad user experience will show. Group Policies let's the system administrator decide for example what files, settings and applications your normal user has access to, which is extremely important for access control. Users can often find loopholes if Group Policies are not configured correctly. These two tools are important for NTNU to use in the future, and should be set up correctly by an administrator who knows how to use them to prevent negative user experiences. This goes for Windows Firewall as well, even though this can be configured using group policies.

User Account Control is likely already in the system, and NTNU should therefore continue to use this. It does not provide much negative user experiences other than a few moments of annoyance.

Due to this, leaving as many of these already enabled features on is convenient and will maintain NTNU's security. NTNU will not save much CPU or machine power from shutting off these features, and this will do more damage than good in the long run.

11.4 Passwordless authentication

With the expansion of hybrid workplaces the threat of phishing, brute force and weak passwords is a huge threat to cyber security. We believe as previously stated in this chapter that transitioning to passwordless two-factor authentication is the best way forward in addressing this threat.

Using Windows Defender Credential Guard is something we would recommend as this way of storing credential data in containers separate from the rest of the OS is one of the most effective ways of keeping credentials safe from possible attackers. This helps mitigate blast radius of attacks and keep credential data secure even after breach into the system. Credential guard has on the other hand been known to have a few issues with certain third party applications. All though these issues have gotten patched it does not exclude the possibility of third party applications being blocked by Credential Guard in the future. This might have an impact on user experience, but the frequency of these types of issues are not high and do not outweigh the benefits that Credential Guard provides in our opinion.

Windows Hello For Business is a feature that we would strongly recommend that NTNU implements. It addresses all the major security issues that comes with passwords and combats phishing. There are no real downsides to user experience at it only makes two-factor authentication with PIN and biometrics more convenient than long and complicated passwords. Implementing both Credential Guard and Windows Hello builds upon NSM principle 2.6 [14] providing a better system for authentication.

FIDO2 Security-key is a good feature seen from a security stand-point, but might not as viable from a user experience perspective. It does not provide that much more security than other alternatives like PIN and biometrics and it might be a big ask for NTNU employees to keep track of and bring a physical key with them to be able to access their devices. NTNU could possibly offer the possibility to use a FIDO2 Security-key, but this is not something that should be a security requirement in

our opinion.

11.5 Summary

These are our recommendations for what security features NTNU should implement if they look to transition over to a Windows 11 based IT-system. Through our research these are the features that we consider to give the most protection on all surfaces and give the most complete protection from both cyber-security threats that are prevalent today and that we see are emerging as new trends.

This recommendation tackles the issue of phishing and the threat it poses in todays hybrid work environment. With Windows Hello, Windows Defender Credential guard and Microsoft Defender Application Guard the threat of phishing is greatly reduced. And with several security mechanics enforcing the three principles of zero-trust; verify explicitly, least privileged access, and assume breach, the blast radius of any malware that might inadvertently make it's way into the system is contained much more easily.

By implementing these features the NTNU SOC will have an IT system with upgraded hardware that is more compatible to support the new widely adopted security concepts such as Zero-trust and it's three principles. Many of the new up and coming security features and technologies revolves around utilization of the TPM and virtualization based security. For this reason having TPM 2.0 integrated in their IT systems, NTNU will enable their systems to more quickly adopt new and effective security mechanisms in the future.

	Do not recommend	Recommended	Strongly recommended
TPM 2.0			X
Secure boot			X
Trusted boot			X
Device health attestation			X
Certificates			X
BitLocker			X
Windows Defender			X
Microsoft SmartScreen		X	
Microsoft Defender Application Guard (Browser)			X
Microsoft Defender Application Guard (Office)		X	
Windows Event Viewer			X
Windows Firewall			X
User Account Control			X
Windows Hello			X
FIDO2 Security Key	X		
Windows Defender Credential Guard			X

Part 3: Thesis conclusion and self evaluation

Description:

In part three we will be discussing the thesis as a whole. Here we will evaluate our work as a group, decisions we've made and possibilities for further work that can build on this report.

12 Thesis conclusion

12.1 Results compared to goals

When evaluating how the results of the thesis compared to our goals we can go through both the task requirements explained in chapter one as well as our result goals that we have described in our project plan.

12.1.1 Task requirements

Requirement 1 - "To map out the built in security mechanics in Windows 10 and 11"

This was perhaps the most time consuming part of the project. After we were done mapping out the different security mechanics in windows 10 and 11 we were all in all quite content with what we had. We made sure to follow the checklist in 1.3 "Framework" of aspects we thought was important to mention about each security feature. We also thought it was fairly well structured by categorizing the security mechanics into hardware, OS, software, application and authentication.

Requirement 2 - "To map out the built in security mechanics in Microsoft Office and explain how these can complement the ones already in Windows"

This requirement is one we feel we did not fully meet. Other than Microsoft Defender Application Guard we did not explore any other security mechanics in Microsoft Office. We hit a few speed bumps early on in the project with the split of the group and having to redefine the scope of our thesis. Because of this we made the decision to direct our focus at Windows 10/11 towards the end of the project as we realized that starting research on Microsoft office would be too late and would affect the report negatively.

Requirement 3 - "To analyze the different threats the built in security mechanics protects against, and how these can detect attacks"

Just as explained under requirement 1 we feel we were able to describe what type of threats each security mechanic protects against. We made sure to explain how each type of attack works and how the security mechanism detects and deals with the threat.

Requirement 4 - "To come up with a professional assessment of what features NTNU should use in their systems now and in the future for best possible security"

We have concluded the report with a recommendation of what security features NTNU should implement if they should make a transition to Windows 11. We have explained in detail why we recommended the security features that we did, as well as why we wouldn't recommend some of the other security mechanisms.

On the other hand we did not have the necessary resources available to perform more practical testing on more of the security features. For this reason we felt like we did not have as much concrete data to point to when substantiating our recommendation as we would have liked.

As we explained briefly in 10.1 "Introduction" we initially wanted to perform practical performance tests on as many of the security features that we could and give each security feature a score between 1-5 on both performance and user experience. Our plan was to use these scores to put into a matrix to create a risk/benefit analysis. But due to the limited technical resources available to us we were unable perform these tests on as many features as we would have wanted. Therefore we decided not to this as it wouldn't be a consistent metric between all the security features.

Requirement 5 - "To investigate if these security features can have a negative impact on the user experience in the NTNU systems"

In both chapter 10 and 11 we describe possible negative aspects of the different security mechanisms and how they might affect user experience. As previously mentioned we couldn't perform testing as comprehensive as we might have initially wanted but still think we have provided good reasoning

for how user experience might be affected by the different security mechanisms.

12.2 Limitations

Overall we found the project interesting and instructive. It was inspiring to be involved in a project on this scale, and we believe it is an important experience to work with a client such as NTNU SOC. However, we also encountered some challenges in this project that limited our work and the final results.

The main limitation of this project is the lack of hardware needed to test out many of the new features Windows 11 provides. For example, TPM 2.0 was missing, and NTNU had no way of providing us with this. We were not provided with access to a physical laptop with neither Windows 11 nor the correct hardware for us to use in test cases. The SkyHiGh servers did not have an image for Windows 11 due to the missing TPM 2.0 hardware. Because of this, we were not able to actually try out the built in functions in Windows 11. To remedy this we chose to focus all practical testing on the security functions that were already available in Windows 10 without a requirement of TPM 2.0.

The original project was more comprehensive. Due to a group split in mid-February, the original project was divided into two parts where we were given the responsibility of the Windows 10 and 11 versions of Windows, while the other part of the group got Windows Server 2019 and 2021. This generally felt like a limitation since the scope of the thesis was smaller now.

Ideally in a project commissioned by a client, it is important to have regular meetings to provide an update of the progress of the project and to ensure that it progresses in accordance with the client's expectations. We generally did not have as much communication with our contact person from the NTNU SOC as we would have preferred. This was due to the fact that it was hard to schedule meetings with him. This was partially because the response time to meeting inquiries we sent over mail would be long, and partially because of his packed schedule. We had in total two meetings with our contact person from the NTNU SOC. One before the split and one after. Because of this we needed to make more independent decisions of what direction we thought we should take the report and how to best interpret the task description.

12.3 Further work

This report lays a foundation for further work within testing a more detailed configuration of these security features on a device with the proper hardware requirements. The natural next step would be to optimize and then standardize that configuration so that it can be configured on a network level system using an mobile device manage (MDM) such as Microsoft Intune.

A suggestion for a possible further thesis here is one that examines and analyses TPM 2.0 as a whole and its functions.

12.4 Evaluation of our work

In this part we will evaluate our work and account for the process around writing this thesis.

After the group split the 16th of February, the task seemed overwhelming for two students. There was a small moment of uncertainty here about the road ahead. However, this did not stop us, and we continued to work towards the task requirements as best as we could with great help from our advisor Erik. We had an adjustment period right after the split, since the scope of the thesis was changed. This led to some wasted time. Much of the report itself was written after Easter break, since larger portions of our time prior to this went to research and some testing. Large parts of the testing were more complicated and time consuming than we thought, and we had to abandoned big parts of the planned testing due to missing hardware requirements (such as TPM 2.0).

We spent the weeks after Easter writing on the report. A few parts of our report felt a bit too rushed, since we waited till last minute before we started on some tasks that we thought would be quick (but proved not to be...). This also gave us less time to focus on the Microsoft 365 part of the thesis (requirement 2). Because of this we made the choice to direct our focus on the Windows 10/11 aspect of the report, instead of introducing new features and not arriving at a thorough enough result on either. The last half week before submission were used mainly for rewriting chapters, corrective work and generally structuring the report.

During our work we have collaborated both physically on campus, but also from home with voice communication over Discord. Both of these work methods have been successful. After the group split, we did not find it necessary to log hours since we always worked at the same time either way. This worked out fine, and we finished the report. As a group we have worked well together. We both feel like we have done an equal amount of work, and we have divided the writing tasks between us along the way. For example: Mads did much of the writing under Windows Application Security, while Mats did large parts of the Software Security part. Project work over longer periods is something we both liked.

Looking back, the main impression we both have after looking at our work is that we have done a consistent and good job. The task itself was interesting, and we were happy that we got a theoretical task like this. We had the little obstacle in the beginning with the group split, and we waited too long before we got to work with some parts of the thesis that proved to be bigger than we thought. Some of the testing could also have been planned better, and we had some obstacles with missing hardware requirements for a few of the tests. We are all in all happy with our final report, even though some parts are not as polished as others.

References

- [1] Microsoft. Windows 11 security book: Powerful security from chip to cloud. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMyFE>, 2022.
- [2] Overleaf. How do i use overleaf? https://no.overleaf.com/learn/how-to/How_do_I_use_Overleaf%3F, 2019.
- [3] The LaTeX-Project. Latex – a document preparation system. <https://www.latex-project.org/>, 2015.
- [4] Nasjonal sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/hva-er-nsm-s-grunnprinsipper-for-ikt-sikkerhet/>, 2020.
- [5] Microsoft. Zero trust and windows device health. <https://docs.microsoft.com/en-us/windows/security/zero-trust-windows-device-health>, 2021.
- [6] Synopsys. Hardware root of trust: Designware ip. <https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html>, 2016.
- [7] Microsoft. Meet the microsoft pluton processor – the security chip designed for the future of windows pcs. <https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/>, 2021.
- [8] Microsoft. Tpm recommendations. 2021.
- [9] Justin D Osborn and David C Challener. Trusted platform module evolution. *Johns Hopkins APL Technical Digest (Applied Physics Laboratory)*, 32(2):536–543, 2013.
- [10] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.7. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/beskytt-data-i-ro-og-i-transitt/>, 2020.
- [11] Microsoft. Secure the windows boot process. <https://web.archive.org/web/20070521010313/http://www.microsoft.com/technet/technetmag/issues/2006/11/EventManager/>, 2022.
- [12] Microsoft. Secure boot and trusted boot. <https://docs.microsoft.com/en-us/windows/security/trusted-boot>, 2021.
- [13] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.2. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/etabler-en-sikker-ikt-arkitektur/>, 2020.
- [14] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.6. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/ha-kontroll-pa-identiteter-og-tilganger/>, 2020.
- [15] Microsoft. Bitlocker. <https://docs.microsoft.com/nb-no/windows/security/information-protection/bitlocker/bitlocker-overview>, 2021.
- [16] Microsoft. Bitlocker. <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>, 2021.
- [17] Microsoft. Bitlocker countermeasures. <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures>, 2021.
- [18] Robert Kingsley. Windows defender in windows 8 and windows 7 – what’s new different? <https://web.archive.org/web/20201219170833/https://www.digitalcitizen.life/windows-defender-windows-8-and-windows-7-what-s-new-and-different/>, 2020.
- [19] Windowscentral. What’s new in windows defender for windows 10 anniversary update. <https://www.windowscentral.com/whats-new-windows-defender-windows-10-anniversary-update>, 2016.

-
- [20] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.8. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/beskytt-e-post-og-nettleser/>, 2020.
- [21] Microsoft. Overview of windows firewall with advanced security. <https://technet.microsoft.com/library/6ff0e320-0369-496a-8f1f-0b7224c7f857.aspx>, 2009.
- [22] Privacy Hub. What is a backdoor attack? pro tips for detection protection. <https://www.cyberghostvpn.com/privacyhub/what-is-a-backdoor/>, 2022.
- [23] Cybersecurity Infrastructure Security Agency. Understanding firewalls for home and small office use. <https://www.cisa.gov/uscert/ncas/tips/ST04-004>, 2019.
- [24] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.5. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/kontroller-dataflyt/>, 2020.
- [25] Qomplx. Microsoft active directory golden ticket attacks explained: Qomplx knowledge. <https://www.qomplx.com/qomplx-knowledge-golden-ticket-attacks-explained>, 2020.
- [26] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 2.4. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-oppretholde/beskytt-virksomhetens-nettverk/>, 2020.
- [27] NSS Labs. Socially engineered malware protection comparative test results. 2009.
- [28] Microsoft. Microsoft defender smartscreen. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview>, 2021.
- [29] TechNet. New tools for event management in windows vista. <https://web.archive.org/web/20070521010313/http://www.microsoft.com/technet/technetmag/issues/2006/11/EventManager/>, 2006.
- [30] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 3.1. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/oppdage/oppdag-og-fjern-kjente-sarbarheter-og-trusler/>, 2020.
- [31] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 3.2. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/oppdage/etabler-sikkerhetsovervakning/>, 2020.
- [32] Nasjonal Sikkerhetsmyndighet. Grunnprinsipper for ikt-sikkerhet 2.0 - nsm 3.3. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/oppdage/analyser-data-fra-sikkerhetsovervakning/>, 2020.
- [33] Microsoft. Sysmon v13.34. <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>, 2022.
- [34] Microsoft. Group policy objects. <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects>, 2018.
- [35] Microsoft. How windows defender credential guard works. <https://docs.microsoft.com/nb-no/windows/security/identity-protection/credential-guard/credential-guard-how-it-works>, 2021.
- [36] Microsoft. Windows hello for business overview. <https://docs.microsoft.com/nb-no/windows/security/identity-protection/hello-for-business/hello-overview>, 2022.
- [37] Microsoft. Why a pin is better than an online password. <https://docs.microsoft.com/nb-no/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>, 2022.
- [38] Secret Doubled Octopus. Fido - fast identity online. <https://doubleoctopus.com/security-wiki/protocol/fast-identity-online/>, 2021.
-

-
- [39] Microsoft. Application control for windows. <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control>, 2021.
- [40] Microsoft. How user account control works. <https://docs.microsoft.com/nb-no/windows/security/identity-protection/user-account-control/how-user-account-control-works>, 2022.
- [41] Microsoft. Application guard for office for administratorer. <https://docs.microsoft.com/nb-no/microsoft-365/security/office-365-security/install-app-guard?view=o365-worldwide>, 2022.
- [42] Emsisoft. How to fix 'antimalware service executable' high cpu usage - emsisoft: Security blog. <https://blog.emsisoft.com/en/28620/antimalware-service-executable/>, 2021.
- [43] Microsoft. Vanlige spørsmål om windows defender smartscreen. <https://feedback.smartscreen.microsoft.com/smartscreenfaq.aspx>, 2021.

Appendixes

1 Introduction

1.1 Goals and framework

1.1.1 Background

The SOC (Security Operations Center) at NTNU (Norwegian University of Science and Technology) is part of the Digital Security department at NTNU. They have the function of detecting, analyzing and responding to digital security threats aimed at NTNU's systems. Our group has received this project from the NTNU SOC with Christoffer Vargtass Hallstensen as our contact person at the NTNU SOC.

Our task for this project is to examine the different security functions of the newer versions of Microsoft Windows and Microsoft Office, as well as identify the specific types of threats these security functions eliminates. This information will then be used to create a recommendation for a collection of security mechanisms that NTNU should implement to have a well-rounded and complete protection against most IT-security threats.

Project goals

Learning goals:

- Get a good understanding of the different security aspects in different versions of Windows and Microsoft Office.
- Learn to develop a best practice-plan in bigger systems based on gathered information.

Effect goals:

- Map out the various security features in Windows and Microsoft Office in depth.
- Map out the various threats in Windows and Microsoft Office.
- Use this overview and analysis to come up with a recommendation of what security mechanisms and controls NTNU should incorporate in their systems to provide well rounded security against the most relevant threats.

Result goals:

- Look at the differences in performance between the different versions of Windows when it comes to security features.

1.1.2 Framework

- The test environment will be in NTNU's internal cloud service SkyHigh.
- There will not be bought any licenses.
- There is no need to automate the setup of the test environment.
- The report will be written in English because it's a universal language that is commonly used to describe IT concepts and definitions.

Tools

Tool	Description
PowerShell	Scripting
SkuHigh/Openstack	Cloud infrastructure for developing test environment
Toggl	Time tracking and planning
Overleaf	Collaboration on the assignment
Discord	Communication
Microsoft Teams	Meetings, documents, file sharing, Kanban board
Teamgantt	Gantt chart

1.2 Scope

1.2.1 Restriction

The project will focus on the built-in security features of Windows 10, 11, Server 2019 and 2022. We will not look at other versions of Windows due to the task specifications. If we at some point must prioritize which version of the operating system to analyze, we will focus on Windows 11 and Windows server 2022 due to the future-oriented nature of the task. We will always focus on the newest version of Microsoft Office.

1.2.2 Situation

NTNU's systems have thousands of users every day together with much personal data. Due to this, upgrading to newer operating systems can prove to be a hard but necessary task to provide the best possible security. NTNU will need much testing and analyzing before they safely can upgrade to the new systems, since the newer operating systems might have bugs and new threats that need to be mitigated. Scalability and performance are also something that needs to be ensured to keep the up-time high.

Due to this, a part of our task is to analyze the possible threats and attack vectors, so NTNU can transfer gradually and safely to these newer operating systems.

1.2.3 Case

The task is to investigate different security features built into newer versions of Microsoft Windows (10, 11, Server 2019, Server 2022) and Microsoft Office. The task also includes mapping which threats, and attack vectors can provide effective risk-reducing measures. In addition to investigating how attacks can be detected. The Client also wants us to look at available safety controls for NTNU's management system for information security, and thus make an assessment and recommendation about which security controls NTNU should introduce to increase information security and the ability to detect digital threats on the Windows platform.

1.3 Project organizing

1.3.1 Organization chart

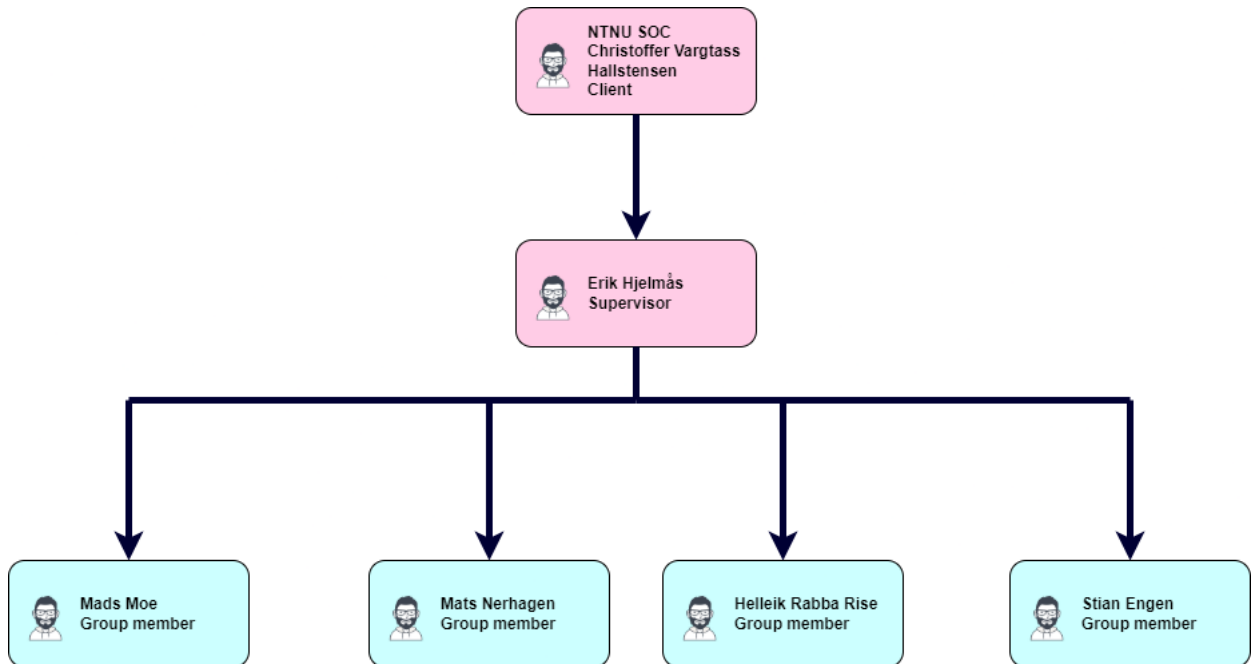


Figure 1: Organization chart

1.3.2 Responsibilities and roles

Roles:

Group leader – Mads Reneflot Moe

Secretary – Mats Nerhagen

Group member – Helleik Rabba Rise

Group member – Stian Engen

Responsibilities:

Book rooms – Helleik Rabba Rise

Overseeing Gantt-scheme compliance – Mats Nerhagen

Overseeing Overleaf structure – Mads Reneflot Moe

Overseeing Toggl Track – Stian Engen

Group rules

1. Work hours each week should be around 30 hours per person. You are allowed to work more than this if you have an upcoming absence that you know of.
2. Missed work hours must be compensated for in the two following weeks.
3. Work hours must be logged by Toggl Track by everyone each day.
4. Should a group member get sick they have to notify the rest of the group if this prevents them from attending meetings or completing tasks with a set deadline.
5. It is important that group members notify the group of any planned absence they might have so this will not affect the planning of any future meetings or deadlines.

-
6. If any group member breaks the rules, a meeting with the other members should take place to decide further actions. See next rule.
 7. If any group member makes commits serious infractions on the rules, a meeting with the advisor should take place to decide if the member will get dismissed from the group.

1.3.3 Routines

- Every group member must meet for group meetings over internet every Monday 10:00, unless something else is specified.
- Every group member must meet for status meetings over the internet every Friday at 10:00, unless something else is specified.
- Physical group meetings should take place every Wednesday both before and after the guidance meeting (09:30) when the situation allows it.
- Workdays are from Monday to Friday every week. Working hours are primarily between 09:00 and 16:00.
- We will use the built in Kanban board in Microsoft Teams (called “planner/tasks”). All tasks should be logged using that Kanban board.

1.4 Planning, follow up and reporting

1.4.1 Project structuring - Development model

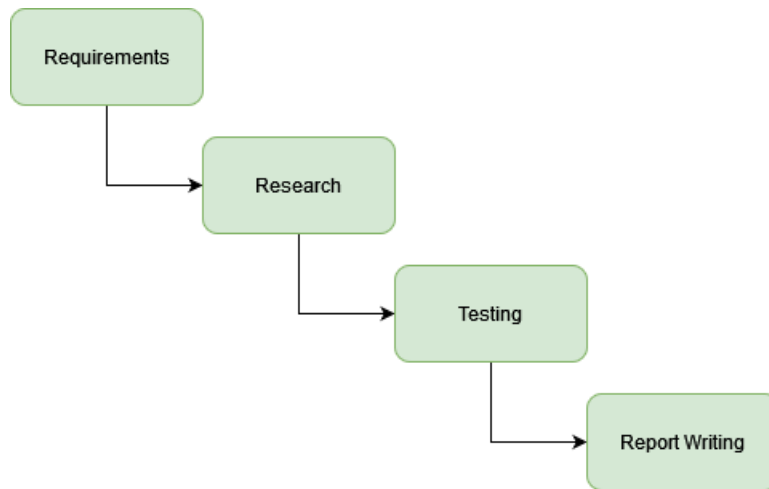


Figure 2: Waterfall model

1.4.2 Method and approach

We will use the app “Tasks delivered by Planner and To do” as a Kanban board in Teams to organize our work. The Kanban board is implemented to enable better collaboration, and to reduce the need for status meetings since the status information of each task will be available through the card information and position. The Kanban board will visualize the workflow from start to finish with the five different columns Backlog, In progress, Testing, Review and Completed.

All tasks the group decides on will be put under the Backlog column. When a group member starts to work on a task the task will be moved from Backlog to In progress. If there is something regarding the task that needs to be tested the task will be moved to Testing. When a group member is done with a task the task will be moved to Review where all the finished tasks will

be put. After another group member has gone through the task and approved it the task will be moved to Complete. Complete is where all the approved tasks will be put.

Each individual task will be assigned to different group members, and you will be able to set dates for deadlines, how urgent the task is and how much progress has been made. Using a Kanban board will therefore help us prioritize our work and get a good overview of all our tasks.

1.4.3 Plan for meetings

We plan to have status meetings with all group members every Monday and Friday at 10:00 where we talk about our progression on the different tasks. We will plan additional meetings if we feel the need to.

Meetings with Erik Hjelmås (advisor) will take place every Wednesday at 09:30 and will require physical attendance (when possible) after week 4. These meetings will have an associated report written.

Meetings with NTNU-SOC will take place when needed, primarily after a new milestone is reached to plan further work. These meetings will have an associated report written.

1.5 Organizing

1.5.1 Documentation, standards, and source code

The report will be written in a Latex document, where all the members will be able to edit and update the report simultaneously. Overleaf, an online editor, will be used for this.

We will use Microsoft Teams to share documents as a standard.

1.5.2 Risk assessment

In our risk assessment we have mapped out and identified different risks based on likelihood and consequence. We have also added countermeasures to reduce the likelihood and consequences of each risk.

Nr.	Risk	Description	Countermeasures
1	Difficulties with setup of test environment.	Too complex test environment.	Good research and planning.
2	Downtime OpenStack.	Server downtime for the test environment due to NTNU servers.	Planning according to scheduled downtime.
3	Accidental loss of documents.	Accidental loss of documents or files Due to human error.	Saving often and usage of backup often.
4	Malicious software.	Installation of malicious software onto the test environment due to human error.	Check the files hash values before and after downloading.

Table 1: Technical risk

Nr.	Risk	Description	Countermeasures
5	Requirements not met	The groups focus diverges too far away from the original task description, and therefore does not meet the requirements.	Reading the case and assignment again together with status meetings with advisor.
6	Loss of gathered information.	Not filling in the source list as it should, making it hard to find later.	Be consistent with good source notation.

Table 2: Business risk

Nr.	Risk	Description	Countermeasures
7	Sick group member.	A member of the group is unable to work due to sickness.	Explain what has been done to the group member, so he or she catches up.
8	Uncoordinated work.	Uncoordinated work due to bad workflow and communication.	Using Tasks to know what we should work on and when we should work on it. And regular meetings to coordinate.

Table 3: Project group risk

Consequence→ Likelihood↓	1-Low	2-Medium	3-High	4-Critical
4-Highly likely				
3-Likely	7			
2-Less likely		1	5, 8	
1-Unlikely	2	6	4	3

Table 4: Risk matrix before countermeasures

Consequence→ Likelihood↓	1-Low	2-Medium	3-High	4-Critical
4-Highly likely				
3-Likely	7			
2-Less likely		1		
1-Unlikely	2	3, 5, 6, 8	4	

Table 5: Risk matrix after countermeasures

1.6 Implementation plan

1.6.1 Milestones

26.01.2022 Project plan completed
 23.02.2022 Setup of test environment completed
 13.05.2022 Report completed
 16.05.2022 Presentation completed

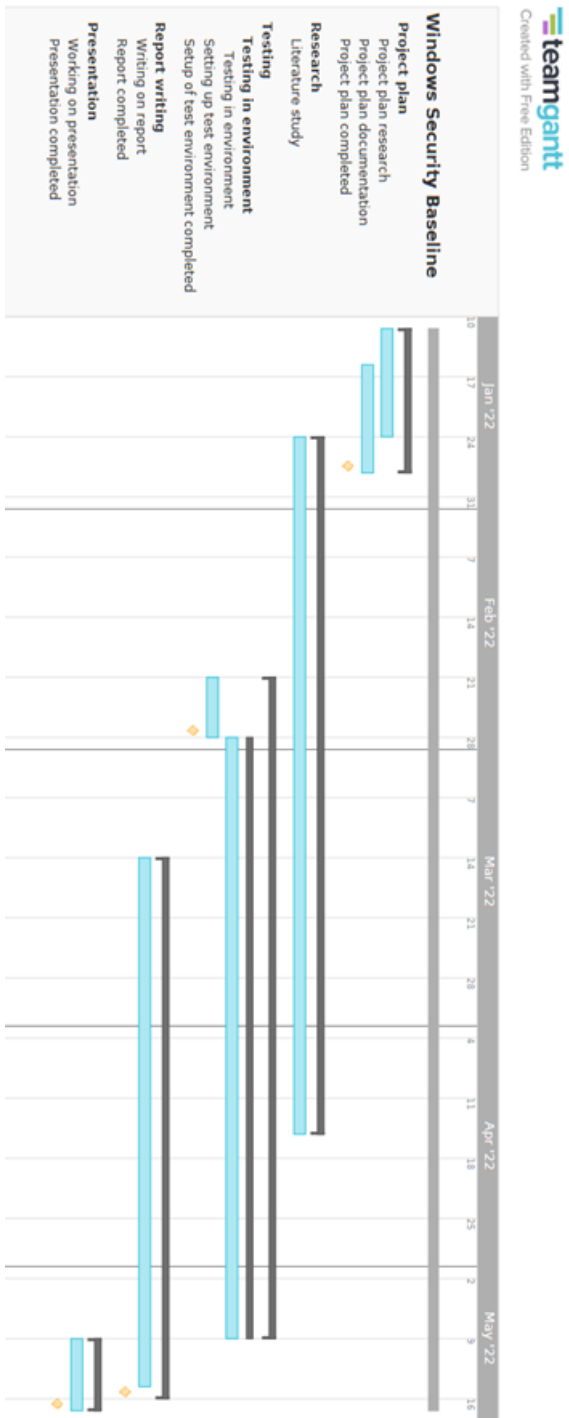


Figure 3: Gantt chart

1.6.2 Research

The research phase will last from 27.01 to 18.04. This research phase will focus on researching different threats that exist, together with the built-in security mechanisms in Windows and Microsoft Office. This research phase will go in parallel with writing the report and doing



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett

Er den rett som den som skaper et åndsverk har til å fremstille eksemplarer av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater

Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater

Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn

Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring

Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for Informasjonssikkerhet og Kommunikasjonsteknologi
Veileder ved NTNU: Erik Hjelmås e-post og tlf. erik.hjelmås@ntnu.no , 93034446
Seksjon for Digital sikkerhet, NTNU IT Christoffer Vargrass Hallstensen, Faggruppeleder SOC Epost: Christoffer.hallstensen@ntnu.no Tel: 61135145
Student: Stian Engen Fødselsdato: 18.10.1999
Student: Helleik Rabba Rise Fødselsdato: 19.05.1999
Student: Mads Reneflot Moe Fødselsdato: 16.09.1996
Student: Mats Nerhagen Fødselsdato: 15.02.1999

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 11.01.2022
Sluttdato: 20.05.2022

Oppgavens arbeidstittel er: NTNU Windows/Office Security baselines

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:
--

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven¹. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

¹ Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

<input type="checkbox"/>	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven
--------------------------	--

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

<input checked="" type="checkbox"/>	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt
-------------------------------------	---

Begrunnelse: Seksjon for Digital sikkerhet beholder eiendomsretten til resultatet for å sikre at ressurser betalt av offentlige midler skal gå til fellesskapets beste etter NTNUs strategi om «Kunnskap for en bedre verden». Seksjon for Digital sikkerhet forplikter seg til å lisensiere kode og rapport som åpen kildekode/creative commons slik at studentene kan ta med seg arbeidet nedlagt i prosjektet videre etter studier, men samtidig ivaretar at fremtidige studenter og andre kan bygge videre på arbeidet.

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig
---	------------------------------

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss

Sett dato

	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.


Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder

punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:	
Veileder ved NTNU: Dato:	
Seksjon for Digital sikkerhet, NTNU IT: Dato: 31.01.2022	
Student: Stian Engen Dato: 31.01.2022	<i>Stian Engen</i> NORGE TEKNISK-NATURVITENSKAPELIGE UNIVERSITET
Student: Helleik Rabba Rise Dato: 31.01.2022	<i>Helleik Rabba Rise</i>
Student: Mads Reneflot Moe Dato: 01.02.2022	<i>Mads R. Moe</i>
Student: Mats Nerhagen Dato: 01.02.2022	<i>Mats Nerhagen</i>



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDMAL ved avtale om konfidensialitet mellom student og ekstern virksomhet i forbindelse med studentens utførelse av oppgave (master-, bachelor- eller annen oppgave) i samarbeid med ekstern virksomhet, jf. punkt 9 i standardavtale om utføring av oppgave i samarbeid med ekstern virksomhet.

Student ved NTNU: Stian Engen Fødselsdato: 18.10.1999
Student ved NTNU: Helleik Rabba Rise Fødselsdato: 19.05.1999
Student ved NTNU: Mads Reneflot Moe Fødselsdato: 16.09.1996
Student ved NTNU: Mats Nerhagen Fødselsdato: 15.02.1999
Ekstern virksomhet: Seksjon for Digital sikkerhet, NTNU IT

1. Studenten skal utføre oppgave i samarbeid med ekstern virksomhet som ledd i sitt studium ved NTNU.
2. Studenten forplikter seg til å bevare taushet om det han/hun får vite om tekniske innretninger og fremgangsmåter samt drifts- og forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde for den eksterne virksomheten. Det er den eksterne sitt ansvar å sørge for å synliggjøre og tydeliggjøre hvilken informasjon dette omfatter.
3. Studenten er forpliktet til å bevare taushet om dette i 5 år regnet fra sluttdato.
4. Kravet om konfidensialitet gjelder ikke informasjon som:
 - a) var allment tilgjengelig da den ble mottatt
 - b) ble mottatt lovlig fra tredjeperson uten avtale om taushetsplikt
 - c) ble utviklet av studenten uavhengig av mottatt informasjon
 - d) partene er forpliktet til å gi opplysninger om i samsvar med lov eller forskrift eller etter pålegg fra offentlig myndighet.

Signaturer

Student: Stian Engen Dato: 31.01.2022 Stian Engen
Student: Helleik Rabba Rise Dato: 31.01.2022 Helleik R. Rise
Student: Mads Reneflot Moe Dato: 01.02.2022 Mads Reneflot Moe
Student: Mats Nerhagen Dato: 01.02.2022 Mats Nerhagen C. Nerhagen
Seksjon for Digital sikkerhet, NTNU IT: Dato: 31.1.22



NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET

Windows Security Baseline

Project plan

- Project plan research
- Project plan documentation
- Project plan completed

Research

- Literature study

Testing

Testing in environment

- Testing in environment
- Setting up test environment
- Setup of test environment completed

Report writing

- Writing on report
- Report completed

Presentation

- Working on presentation
- Presentation completed

