My most recent Windows update is Windows 11 version 24H2. One of the security issues it addresses is better protections around LAN Manager / NTLM / legacy authentication protocols, stronger Kerberos safeguards. Here an attacker could use the attack vector of misconfigurations. They could take advantage of improper permission settings, weak default credentials, or other security misconfigurations. The update tightens those permissions and credentials up.

Another security issue addressed is hardening of User Account Control (UAC) rules, improvements to Microsoft Defender Antivirus default settings and behaviors and other enterprise‑oriented security controls and configurations tighter by default. For these three vulnerabilities hackers could take advantage of the software vulnerabilities to be able to access or break defenders walls easier. Default settings and security configurations constantly need to be improved to protect against any attacks. If these issues were not addressed on my system hackers could have broken down my Microsoft Defender Antivirus due to poor default settings and installed malware or prompted me (the user) to install malware.

I found a case on fox news where hackers were able to disable Microsoft Defender Remotely. Specific details were hard to find but I am sure that improved settings will help prevent against a hacker being able to gain that level of access. The sad part is, you can never be fully protected, as fast as developers find fixes to bugs and security issues, hackers find a new or better way to access what they want to access. Your system or settings may not even be technically "vulnerable" but if the developers can find a way to make your system just that much safer from attacks, then they will do it.

The following screenshots are the security settings that my system had. My system had all of the recommended settings already configured, except for the smart screen setting which is now "smart app". Unfortunately in order to change the setting to evaluation or to on I would have to reinstall windows, which is not a process that I can afford to go through right now while I use my computer to do just about everything for my classes. I also looked into what smart app control is, and due to me being a Computer Science Major smart app would probably get in my way sooner or later and create more of a headache by blocking apps and programs that I am developing.

This is one of the reasons why programmers use windows instead of macs. Windows allows you to let yourself get in trouble, and as a Computer Science Major, I have to get myself in trouble sometimes. A mac has so many security precautions and settings like "smart app" that blocks any untrusted apps which is great for an everyday computer user but makes it difficult for someone to program or run a linux machine on their computer.

While finding that the settings that I should "have to change" are already implemented does make it difficult to complete the last part of the assignment I am relieved and proud of my system for already having the correct settings implemented. This laptop is only about 2 years old which tells me that over the past few years computers have come out of the box safer than they used to. The fact that the assignment expected at least 3 settings to not be implemented means that most computers did not or have not had the safest settings. To go into my windows security settings and see 5 little green checkmarks is a good feeling. In a world where a hacker could take over any second it is great to see how my Operating system protects itself with so many great tools and implementations so that someone who doesn't have the knowledge of a Cybersecurity professional can be safe in their everyday device usage. Now that I have the

knowledge of these settings, I will be visiting these settings often to make sure my device continues to be in a safe state.

Virus & threat protection

Protection for your device against threats.

⟳ Current threats

No current threats.
Last scan: 9/26/2025 3:41 AM (quick scan)
0 threat(s) found.
Scan lasted 1 minutes 33 seconds
38526 files scanned.

Quick scan

Scan options

Allowed threats

Protection history

⚙ Virus & threat protection settings

No action needed.

Manage settings

⟳ Virus & threat protection updates

Security intelligence is up to date.

Last update: 10/1/2025 6:43 PM

Protection updates

▣ Ransomware protection

No action needed.

Manage ransomware protection

⚙ Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

🔵 On

🏢 Domain network

Firewall is on.

🏠 Private network

Firewall is on.

☕ Public network (active)

Firewall is on.

Smart App Control

Enhanced protection from untrusted apps.

○ On

If Smart App Control spots a malicious or untrusted app it will block it to help protect your device.

○ Evaluation

While Smart App Control is in Evaluation mode, it will learn if it can help protect you without getting in your way too much. If so, it will automatically be turned on. Otherwise, it will automatically be turned off.

🔵 Off

If Smart App Control is off it can't be turned on without reinstalling Windows.

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

Learn more