

# HOME PROTECTION GUIDE

Keeping our homes safe





# Endpoint Protection



The first step in keeping our homes safe is keeping our devices safe, and the most common tool that helps us achieve that is endpoint protection software or more commonly known as -antivirus.

There are numerous free and paid options available.

For most home users operating on Windows 11, it is recommended to utilize Microsoft Defender, the built-in protection system from Microsoft, which offers robust security features.

Consider implementing the following endpoint protection tools:



## Malwarebytes

This tool provides advanced malware detection and removal, complementing traditional antivirus solutions by targeting threats that may slip through the cracks.



## Norton 360

A comprehensive security suite that includes antivirus, firewall, VPN, and identity theft protection, making it suitable for users who need extensive protection.



## Bitdefender

Known for its strong malware protection and minimal impact on system performance, Bitdefender offers features like anti-phishing and anti-fraud protection.





## Additional tools



For users of Windows 11 Pro, it is advisable to utilize BitLocker, a full disk encryption feature that secures your data by encrypting the entire drive.

This is particularly important for protecting sensitive information from unauthorized access, especially if your device is lost or stolen.



# My WiFi - My Castle



A compromised network can expose sensitive personal and financial information to cybercriminals. Implementing robust security measures is essential to safeguard your data.

Implementing measures such as changing default passwords, enabling WPA3 encryption, and regularly updating your router's firmware can significantly reduce vulnerabilities.

Additionally, pre-approving devices that can connect to your network ensures that only trusted devices gain access, further enhancing security.

By taking these proactive steps, you significantly reduce the risk of falling victim to cyberattacks and enjoy peace of mind knowing your network is protected.





## Additional tools



Maintaining up-to-date software is crucial for home protection. Regular updates help patch vulnerabilities that cybercriminals may exploit. While this topic is covered in another guidebook, it's essential to prioritize updates as part of your security strategy.

Lastly, the importance of backups cannot be overstated. Regularly backing up your data ensures that you can recover important files in the event of a cyber incident or hardware failure. This topic will also be explored further in another guidebook, but for now, remember that a solid backup strategy is a key component of your overall home security plan.

By implementing these measures, you can significantly enhance your home's cybersecurity posture, ensuring that your personal and sensitive information remains protected in an increasingly digital world.





---

# AUTOMATED INCIDENT RESPONSE WITH AI

AI can automate and accelerate the incident response process, enabling faster identification, containment, and recovery from cyberattacks.

## 01

---

### THREAT DETECTION

AI algorithms monitor systems and networks for suspicious activity, triggering alerts and initiating automated responses.

## 02

---

### INCIDENT CONTAINMENT

AI-powered systems can automatically isolate affected systems, prevent the spread of malware, and mitigate the impact of attacks.

## 03

---

### RECOVERY AND REMEDIATION

AI can help restore compromised systems, identify and remove malware, and implement corrective measures to prevent future attacks.