



9 out of 10

cyberattacks start with a simple phishing email.

Only 38%

of global organizations claim they are prepared to handle a sophisticated cyber attack.

54%

of companies experienced **one or more** successful attacks that compromised data or IT infrastructure.

Features of superior anti-virus software



Real-time Scanning—Consistently checks the data coming into your computer and blocks any attempts to download malware.



On-Access Scanning—Scans files for any threats as they are opened or saved.



On-Demand Scanning—Provides an option for the user to manually scan anything, from a file to the whole computer, at any given time.



Heuristic-Scanning—Proactive scanning that is capable of learning from experience to detect new viruses before it has even been defined by the anti-virus software.



Compressed File Scanning—Works to detect and block compressed files or folders, such as ZIP, containing virus or malware.



Scheduled Scanning—Scans that occur on a regular schedule, typically during low usage times.



Automatic Updates—Updates the scanning definition of virus files regularly to keep computers current and secure from the latest threats.



WHY IS THIS IMPORTANT?

Anti-virus software (AV) is an important tool to help prevent cyber attacks and it's one of the last lines of defense to protect against the spread of a threat throughout a company's network. AV is pivotal in safeguarding against viruses and numerous types of malware, such as ransomware. If an individual has received a phishing email with a malicious attachment, AV can often block and delete the malicious attachment before it has a chance to infect the computer, or spread to other computers and devices on the network. By doing this, AV adds an extra layer of security and can prevent a hacker or virus from being successful in an attack.

END POINTS

