

What is an Attack Vector?

Contact Us →

Attack Vector Definition

An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials. Such methods include sharing malware and viruses, malicious email attachments and web links, pop-up windows, and instant messages that involve the attacker duping an employee or individual user.

Many security vector attacks are financially motivated, with attackers stealing money from people and organizations or data and personally identifiable information (PII) to then hold the owner to ransom. The types of hackers that infiltrate a network are wide-ranging. They could be disgruntled former employees, politically motivated organized groups, [hacktivists](#), professional hacking groups, or state-sponsored groups.

The Difference Between an Attack Vector and an Attack Surface

Cybersecurity attacks are launched using an attack vector. This could be through [malware](#) or a [phishing](#) attack, which aims to steal user credentials and gain unauthorized access to corporate data or resources. [Social engineering](#) is another way to launch an attack.

The attack surface is the total network area an attacker can use to launch cyber attack vectors and extract data or gain access to an organization's systems. Devices and people are part of an organization's attack surface because their vulnerabilities, such as unpatched software, can be exploited by an attacker.

Hey there 🙋 Want to be in the know?

How Do Hackers Exploit Attack Vectors?

Hackers use multiple threat vectors to exploit vulnerable systems, attack devices and networks, and steal data from individuals. There are two main types of hacker vector attacks: passive attacks and active attacks.

Passive Attack

A passive attack occurs when an attacker monitors a system for open ports or vulnerabilities to gain or gather information about their target. Passive attacks can be difficult to detect because they do not involve altering data or system resources. Rather than cause damage to an organization's systems, the attacker threatens the confidentiality of their data.

Passive attack vectors include passive reconnaissance, which sees the attacker monitor an organization's systems for vulnerabilities without interacting with them through tools like session capture, and active reconnaissance, where the attacker uses methods like [port scans](#) to engage with target systems.

Active Attack

An active attack vector is one that sets out to disrupt or cause damage to an organization's system resources or affect their regular operations. This includes attackers launching attacks against system vulnerabilities, such as denial-of-service (DoS) attacks, targeting users' weak passwords, or through malware and phishing attacks.

A common example of an active attack is a masquerade attack, in which an intruder pretends to be a trusted user and steals login credentials to gain access privileges to system resources. Active attack methods are often used by cyber criminals to gain the information they need to launch a wider cyberattack against an organization.

Common Types of Attack Vectors

There are many types of attack vectors, with cyber criminals using many methods to target large or small organizations from any industry, as well as individuals from nearly every business level. Some of the most common threat vectors are listed below.

Compromised Credentials

Weak and compromised credentials are the most-used attack vector. Many users use weak passwords to protect their online accounts and do not change them often. When information like usernames or passwords are exposed to a third party such as mobile apps

Hey there 🙋 Want to be in the know?

and websites. This is frequently caused by victims of a phishing attempt revealing their login details to an attacker by entering them on a spoofed website. Lost and stolen credentials enable an intruder to access user accounts and corporate systems without detection, then escalate their access level within a network.

Employees must use strong passwords and consider using a password manager to limit the chances of an attacker stealing their credentials. To avoid the risk of compromised credentials, organizations must move away from relying on passwords alone and deploy multi-factor authentication (MFA) to verify users' identities. Employee education is also vital to ensuring users understand the security risks they face and the signs of a potential cyberattack.

Malware

[Malware](#) is a term that describes various strands of malicious software, which include ransomware, spyware, Trojans, and viruses. Cyber criminals use malware as a threat vector to help them gain access to corporate networks and devices, then steal data or damage systems.



Avoiding malware is reliant on understanding the signs of an attack, such as phishing schemes that urge users to share valuable information. Protecting against malware requires technology like sandboxing, firewalls, and antivirus and anti-malware software that detect and block potential attacks.

Phishing

[Phishing](#) is an email, Short Message Service (SMS), or telephone-based attack vector that sees the attacker pose as a trusted sender to dupe the target into giving up sensitive data, such as login credentials or banking details.

Organizations can protect their employees and customers from phishing attacks by using spam filters, deploying MFA, ensuring software is patched and updated, and blocking malicious websites. However, the best way to defend against phishing is to assume that every email is part of a phishing attack. This also comes down to employee education and relies on employees' awareness of common security risks, such as never clicking any link within an email.

Insider Threats

Some security attacks come from inside the organization, through employees exposing confidential information to attackers. While this can be accidental, malicious insiders expose corporate data or vulnerabilities to third parties.  e Hey there 🍌 Want to be in the know?  ed

It can be difficult for organizations to spot malicious insiders, largely because they are authorized users with legitimate access to corporate networks and systems. Therefore, businesses should monitor network access for unusual activity or users accessing files or systems they would not normally, which could be an indicator of insider risk.

Missing or Weak Encryption

[Encryption](#) is a technique that hides the true meaning of a message and protects digital data by converting it into a code or ciphertext. This ensures that the data within a message cannot be read by an unauthorized party, which helps prevent cyber criminals from stealing sensitive information.

Missing, poor, or weak encryption leads to the transmission of sensitive data in plaintext. This risks its exposure to unauthorized parties if intercepted or obtained through a brute-force attack. To avoid this, users should use strong encryption methods, including Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA) encryption, and always ensure sensitive information is encrypted while at rest, in processing, and in transit.

Unpatched Applications or Servers

Cyber criminals are always on the lookout for potential open doors or vulnerabilities in software and servers. When they find and exploit a vulnerability that no one is aware of until the breach occurs, this is known as a zero-day attack.

Organizations and users can avoid this type of attack by ensuring their software, operating systems, and servers are patched. This means applying a software update or fixing code to a program or server to remove the vulnerability. Regular patching by software developers is the best strategy for mitigating potential attacks. To assist with this and prevent any gaps that could present a vulnerability to an attacker, users should ensure automatic software updates are enabled.

Distributed Denial of Service (DDoS)

A [DDoS attack](#) occurs when an attacker overloads a server with internet traffic using multiple machines, also known as a botnet. This prevents users from accessing services and can force the organization's site to crash.

A DDoS attack can be mitigated through the use of firewalls to filter and prevent malicious traffic. Other defense tools include regular risk assessments to identify vulnerabilities, intrusion detection systems to prevent a targeted attack, and rate-limiting to restrict traffic.

How Fortinet Can Help?

Hey there 🙋 Want to be in the know?

raf...
ca...re.

Organizations can secure their network and [manage internal and external attack vectors with FortiGate](#). FortiGate is a next-generation firewall (NGFW) that blocks attack vectors, such as malware and phishing attacks, filters network traffic, and enables organizations to securely encrypt data to keep it out of the hands of cyber criminals, even if they manage to intercept it in transit. The FortiGate NGFWs evolve in pace with the threat landscape, which ensures that organizations' networks are always protected from new and emerging threat vectors.

[Contact us](#) to learn more about our solutions and the latest security technologies we can offer your team.

Quick Links



Free Product Demo

Explore key features and capabilities, and experience user interfaces.



Resource Center

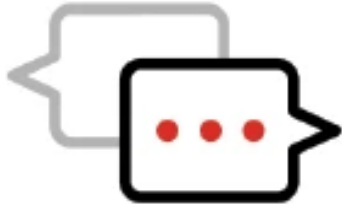
Download from a wide range of educational material and documents.



Free Trials

Test our products and solutions.

Hey there 🙋 Want to be in the know?



Contact Sales

Have a question? We're here to help.

PRODUCTS

PARTNERS

DISCOVER MORE

CONNECT WITH US

Enter Email Address

I want to receive news and product emails. Read our [privacy policy](#).

*@Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates, and is used herein with permission.
All Rights Reserved.*

Also of Interest

[Types of Cyber Attacks](#)

[Attack Surface](#)

[Watering Hole Attack](#)

Hey there 🙋 Want to be in the know?