# Attack Surface

## What Is an Attack Surface?

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.

Organizations must constantly monitor their attack surface to identify and block potential threats as quickly as possible. They also must try and minimize the attack surface area to reduce the risk of cyberattacks succeeding. However, doing so becomes difficult as they expand their digital footprint and embrace new technologies.

The attack surface is split into two categories: the digital and physical.

## Digital Attack Surface

The digital attack surface area encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers, and websites, as well as shadow IT, which sees users bypass IT to use unauthorized applications or devices.

## Physical Attack Surface

The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, and Universal Serial Bus (USB) drives. The physical attack threat surface includes carelessly discarded hardware that contains user data and login credentials, users writing passwords on paper, and physical break-ins.



Organizations can protect the physical attack surfac eil around their physical locations. They also must implement and test disaster recovery procedures

and policies.

### How Are Attack Vectors and Attack Surfaces Related?

The attack surface and attack vector are different but related. An attack vector is the method a cyber criminal uses to gain unauthorized access or breach a user's accounts or an organization's systems. The attack surface is the space that the cyber criminal attacks or breaches.

## Common Attack Vectors

Common attack vector types include:

1. Phishing: This attack vector involves cyber criminals sending a communication from what appears to be a trusted sender to convince the victim into giving up valuable information. Phishing messages typically contain a malicious link or attachment that leads to the attacker stealing users' passwords or data.
2. Malware: Malware refers to malicious software, such as ransomware, Trojans, and viruses. It enables hackers to take control of a device, gain unauthorized access to networks and resources, or cause damage to data and systems. The risk of malware is multiplied as the attack surface expands.
3. Compromised passwords: One of the most common attack vectors is compromised passwords, which comes as a result of people using weak or reused passwords on their online accounts. Passwords can also be compromised if users become the victim of a phishing attack.
4. Encryption issues: Encryption is designed to hide the meaning of a message and prevent unauthorized entities from viewing it by converting it into code. However, deploying poor or weak encryption can result in sensitive data being sent in plaintext, which enables anyone that intercepts it to read the original message.
5. Unpatched software: Cyber criminals actively search for potential vulnerabilities in operating systems, servers, and software that have yet to be discovered or patched by organizations. This gives them an open door into organizations' networks and resources.

## Common Attack Surface Vulnerabilities

Common vulnerabilities include any weak point in a network that can result in a data breach. This includes devices, such as computers, mobile phones, and hard drives, as well as users themselves leaking data to hackers.

Other vulnerabilities include the use of weak pas[illegible] po[illegible] a failure to patch software, which offers an open back[illegible] and organizations. Another common attack surface [illegible] exploited by hackers to steal data through man-in-the-middle (MITM) attacks.

## How To Define Your Attack Surface Area

Visualization begins with defining and mapping the attack surface. This involves identifying potential weaknesses, assessing vulnerabilities, and determining user roles and privilege levels. Organizations can assess potential vulnerabilities by identifying the physical and virtual devices that comprise their attack surface, which can include corporate firewalls and switches, network file servers, computers and laptops, mobile devices, and printers.

They then must categorize all the possible storage locations of their corporate data and divide them into cloud, devices, and on-premises systems. Organizations can then assess which users have access to data and resources and the level of access they possess. This helps them understand the particular behaviors of users and departments and classify attack vectors into categories like function and risk to make the list more manageable.

## What Is Attack Surface Management and Why Is It Important?

When an attack surface has been mapped, it is important to test for vulnerabilities and continuously monitor its performance. Attack surface management is crucial to identifying current and future risks, as well as reaping the following benefits:

1. Identify high-risk areas that need to be tested for vulnerabilities
2. Identify changes and any new attack vectors that have been created in the process
3. Determine which types of users can access each part of a system
4. Mitigate against targeted cyberattacks

## Government's Role in Attack Surface Management

The U.S. government plays a key role in attack surface management. For example, the Department of Justice (DOJ), Department of Homeland Security (DHS), and other federal partners have launched the StopRansomware.gov website. The aim is to provide a comprehensive resource for individuals and businesses so they are armed with information that will help them prevent ransomware attacks and mitigate the effects of ransomware, in case they fall victim to one.

The DOJ is also committed to fighting wider cyber crime, including partnering with international agencies to bring down the largest illegal Darknet marketplace and the REvil ransomware group. The agency is also fighting ransomware and cryptocurrency crime with new bodies like the Ransomware and Digital Extortion Task Force, the N… …n U… the Virtual Asset Exploitation Unit.



## Attack Surface Reduction in 5 Steps

Infrastructures are growing in complexity and cyber criminals are deploying more sophisticated methods to target user and organizational weaknesses. These five steps will help organizations limit those opportunities.

## 1. Implement Zero-trust Policies

The zero-trust security model ensures only the right people have the right level of access to the right resources at the right time. This strengthens organizations' entire infrastructure and reduces the number of entry points by guaranteeing only authorized individuals can access networks.

## 2. Eliminate Complexity

Unnecessary complexity can result in poor management and policy mistakes that enable cyber criminals to gain unauthorized access to corporate data. Organizations must disable unnecessary or unused software and devices and reduce the number of endpoints being used to simplify their network.

For example, complex systems can lead to users having access to resources they do not use, which widens the attack surface available to a hacker.

## 3. Scan for Vulnerabilities

Regular network scans and analysis enable organizations to quickly spot potential issues. It is therefore vital to have full attack surface visibility to prevent issues with cloud and on-premises networks, as well as ensure only approved devices can access them. A complete scan must not only identify vulnerabilities but also show how endpoints can be exploited.

## 4. Segment Network

Network segmentation allows organizations to minimize the size of their attack surface by adding barriers that block attackers. These include tools like firewalls and strategies like microsegmentation, which divides the network into smaller units.

## 5. Train Employees

Employees are the first line of defense against cyberattacks. Providing them with regular cybersecurity awareness training will help them understand best practices, spot the telltale signs of an attack through phishing emails and social engineering.

### How Fortinet Can Help?

Fortinet network security solutions are layered to protect organizations' entire attack surface. The FortiGate next-generation firewalls (NGFWs) not[illegible] the latest malware strains from entering a network. [illegible] access provides organizations with full visibility into [illegible] networks and authentication tools that ensure only approved users have access.

# 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.

## 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.







**Also of Interest**

Fortinet Security Fabric

FortiGuard IoT Service

What is an Attack Vector?