Protect your business with Cisco

Types of Network Security

Access control

Not every user should have access to your network.To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Application security

Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Antivirus and antimalware software

“Malware,” short for “malicious software,” includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Data loss prevention

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Behavioral analytics

To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

Email security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Firewalls

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be

hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.

Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

Web security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

Talos Threat Intelligence

Talos is Cisco's industry-leading threat research and intelligence team, and every Cisco security product is protected through Talos. Talos has more than 250 threat researchers working round the clock and across the globe, with a repository of 100 terabytes of threat intelligence.

We see a third of the world's email traffic daily and over 2 percent of the world's DNS requests. We encounter over 1.1 million unique malware samples each day through our Advanced Malware Protection (AMP) and threatGRID technology, which allows us to block 19.7 billion threats a day on our customers' networks.

That's right-19.7 billion threats blocked a day.