Application whitelisting

Application whitelisting is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

Whitelisting is the opposite of blacklisting. Instead of blocking specific addresses or devices, whitelisting allows only specific addresses or devices to access data or networks. This is usually done by keeping a list of trusted users or devices and only allowing traffic from those addresses. Whitelisting can be used to allow specific websites, email addresses, or even IP addresses to a specific network. This approach is trust-centric and blocks access as the default setting.

When it comes to email, whitelisting allows only specific email addresses or domain names to pass through your email server. This measure is helpful when you want to make sure that only emails from people you know and trust get through while keeping out spam and other unwanted messages.

**Benefits**

It's a very secure approach to data security. If you only allow trusted devices or users to access your data, it's much harder for someone to get in and cause damage.

It's very effective at blocking untrusted sources. If you have a list of addresses or devices that are known to be malicious, whitelisting them can be a very effective way to stop them from causing damage.

**Disadvantages**

It can be difficult to implement. It requires a lot of specific information about each organization and when new tools or applications are installed, the whitelist needs to be updated.

It's not very flexible. Users are restricted with what they can do on their systems.

It's not foolproof. Even with a whitelist, it's possible for malicious devices or users to get through if they manage to spoof a trusted address or device.

Greylisting

Greylisting is similar to blacklisting, but it's not as aggressive. Items on a greylist have not yet been confirmed as either safe or harmful. These items are temporarily blocked from your system until it is further analyzed. Once it has been determined safe or not, it moves to either the blacklist or the whitelist.

Most commonly greylisting is used in email security. Greylisting is used to combat spam by temporarily rejecting all email messages from sources that you don’t recognize. By temporarily rejecting all emails, greylisting effectively filters out most spam messages while allowing legitimate emails to get through.

Application Blacklisting

Application blacklisting, sometimes just referred to as blacklisting, is a network administration practice used to prevent the execution of undesirable programs.

Blacklisting is a method of controlling access to data or networks by identifying users or devices that are not allowed. This is usually done by keeping a list of known bad actors or dangerous IP addresses and blocking any traffic from those addresses. Blacklisting can be used to block specific websites, email addresses, or even entire countries. This approach is threat-centric and allows access as the default setting.

Email providers use blacklists to protect users from spam by blocking messages from known spam sources. If your emails are marked as spam consistently, you're likely on multiple blacklists.

**Benefits:**

It's a proactive approach to security. You're not just waiting for someone to try and access your network, you're actively preventing them from doing so.

It can be very effective at blocking known bad actors. If you have a list of addresses or devices that are known to be malicious, blacklisting them can be a very effective way to stop them from causing damage.

It's easy to implement. Blacklisting only requires a list of addresses or devices to be blocked. It doesn't require any extra hardware or software.

**Disadvantages:**It's not foolproof. Just because an address or device is on a blacklist doesn't mean it's definitely malicious. It's possible for legitimate addresses or devices to be blacklisted.

It can be time-consuming to maintain. If you want your blacklist to be effective, you need to keep it up-to-date with new threats. This can take a lot of time and effort.

It's not very flexible. Once an address or device is blacklisted, it can be difficult to unblock it if you need to.

It's useless against unknown threats. New attacks won't be stopped as they wouldn't be on your blacklist

Patch applications

Application patch management is the process of testing, acquiring, and installing patches (code changes) on computer systems. By repairing vulnerabilities in your system and identifying defective patches, this process helps your computer stay updated and secure.

Patch operating systems

Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.

Restrict administrative privileges

Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.