Application allow lists

CANADIAN CENTRE FOR CYBER SECURITY

April 2024 | ITSAP.10.095

One of our top 10 recommended IT security actions is to implement application allow lists on your organization's systems. An allow list selects and approves specific applications and application components (executable programs, software libraries, configuration files) to run on organizational systems.

Why use allow lists

By using allow lists you can control which applications are installed and run on your systems. Allow lists prevents users from downloading malicious applications that could infect your server. Only applications that have been reviewed, tested, and approved are allowed to run. Allow lists are one of the most effective techniques available to combat ransomware.

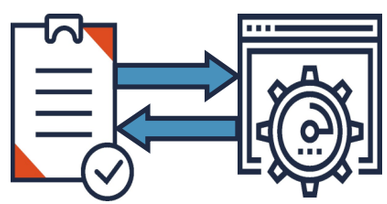
Your organization can also use application allow lists for purposes beyond controlling application access. Some examples include the following:

- **Software inventory:** Keep an inventory of applications and application versions installed on each host so that your organization can identify unauthorized applications.
- **File integrity monitoring:** Monitor and report attempted changes to application files.
- **Incident response:** Use the application allow list technologies to check other hosts for malicious files.
- **Endpoint protection:** Run the hash and compare against files on your system.

How allow lists work

Your organization creates a list of applications that are authorized for use in the workplace or that are known to be from a trustworthy vendor. When an application is launched, it is compared against the allow list. The application is only permitted if it is on that list. You can define your allow list by using file and folder attributes such as:

- file path, name, and size
- digital signature
- publisher
- hash value



We recommend using multiple attributes to define your allow lists.

For optimal security, remember to update your allow list when you patch or install an update for an application. Some allow list applications will automatically update to reflect these changes.

We recommend using observation mode when you start using an allow list tool. Observation mode allows you to see everything running on your network and exposes any unusual activity, to reduce the risk of a compromised server.

You should define and deploy policies on allow lists across your organization.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/10-095-2024E-PDF ISBN 978-0-660-69992-9

Application allow lists

CANADIAN CENTRE FOR CYBER SECURITY

April 2024 | ITSAP.10.095

Service provider allow lists

If your organization is working with a cloud service provider or managed service provider, consider the sensitivity of your data when defining and controlling data access.

Creating an effective allow list

To create an allow list that is effective in your organization, consider the following tips:

- Evaluate your business needs and security requirements to select applications that support your business objectives
- Review your organization's networks and systems so that a compatible solution is implemented
- Identify the resources that are required to successfully implement and manage the allow list, like administrator, and support staff
- Determine whether your hosts, such as desktops, laptops, and servers, have operating systems with built-in application allow lists and whether these technologies are suitable for your environment
- Update your allow list each time the applications are updated and patched, or when you start or stop using software
- Configure your application allow lists to allow only signed and trusted scripts where scripts are required

Selecting a trustworthy application vendor

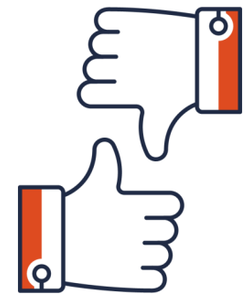
Use applications from vendors who have implemented security controls to ensure that their products are safe.

If you choose to use a commercial off-the-shelf allow list technology, make sure the vendor is reputable. Ensure you are configuring the product to meet the needs of your organization.

Testing your allow list

Test the allow list in observation mode for effectiveness before implementing it. Testing should include the following:

- Basic functionality
  - Can allow list applications run?
  - Are denied applications blocked?
- Administrator management capabilities: Can an administrator update or patch applications?
- Logging and alerts: Are changes logged?
- Performance: How is performance during normal and peak use?
- Security: Does the solution have any vulnerabilities that could be exploited?



Once you're comfortable with the allow list observation mode, you can transition to execution mode to start controlling which applications can run on your network.

Learn More

Implementing an application allow list is just one aspect of improving cyber security in your organization.

For more information about application allow lists, read our Top 10 IT security actions: No.10 Implement application allow lists (ITSM.10.095).

To best protect your organization against cyber threats, review and implement all the actions recommended in Top 10 IT Security actions to protect Internet-connected networks and information (ITSM.10.089).

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/10-095-2024E-PDF ISBN 978-0-660-69992-9