# CAPACITY ENHANCEMENT GUIDE
## SOFTWARE REMOVAL GUIDE

## PURPOSE

Recent cyber incidents highlight the need for organizations to understand and manage the supply chain risk introduced by commercial and open-source software. In some cases, Federal Government agencies have identified specific concerns with the use of a particular vendor, product, or open-source component. An organization's ability to identify, isolate, and remove problematic software within the environment is critical to efficiently mitigating associated cyber risk. This guide includes information that organizations can use to leverage their software asset management capabilities to remove risky software from their environment.

## AUDIENCE & SCOPE

Capacity Enhancement Guides support efforts to reduce risk to the Nation's cyber and physical infrastructure by sharing high-priority recommendations, best practices, and operational insights in response to systemic threats, vulnerabilities, and risks. This guide is intended to provide organizations with high-level recommendations and guidance on how to identify and remove problematic software from their environments and monitor for any future reintroduction. It also discusses some considerations when evaluating exceptions to a removal policy.

The examples provided do not express any tooling preferences. They illustrate the steps common to most enterprises in dealing with the identification and removal of problematic software.

## RECOMMENDATIONS

Organizations should build and regularly update a complete software asset inventory for all devices within their environment. This inventory should capture detailed information on all software including (but not limited to) product name, version, vendor, and installation date. Organizations should strive to build this inventory to include all software (operating system, hardware, applications, common libraries, etc.) on all devices within the enterprise. Additionally, organizations should regularly scan and update this inventory, as an accurate and up-to-date inventory is critical in being able to rapidly identify and remove unwanted, restricted, or problematic software. Furthermore, organizations are encouraged to define a formal process for evaluating, authorizing, and reviewing exceptions to a removal policy.

### At-A-Glance Recommendations

- Use asset management capabilities to identify restricted or unwanted software
- Create policies to remove and/or block applications
- Routinely update software inventories to continually monitor for new occurrences
- Establish a process to deal with exceptions

## IDENTIFY

Organizations should consult their software asset inventory, sometimes included as part of a comprehensive Configuration Management Database (CMDB), to identify instances of unwanted or problematic software on their networks.

1. Identify key characteristics that describe the targeted software such as vendor name, product name, file name(s), version numbers, or file hash.

2. Query the software asset inventory and compile the list of potential matches.
3. Review and refine the list of results to eliminate components that are out of scope, paying particular attention to instances reported on devices no longer on the network.
4. Pull the unique set of devices with the unwanted software installed.

## REMOVE

Once identified, organizations should use their SWAM and EMM toolsets to orchestrate the removal of all instances on all devices within the enterprise.

1. Within the SWAM tool, start by creating a new software package or job.
2. Configure the job to look for the target software on the device and if found, proceed.
3. Supply the appropriate uninstall or removal commands for the target software and report success or failure.
4. Publish the job to all devices on the network.
5. Using the list of unique devices compiled in the "Identify" step above, review the results of the removal job to ensure all devices with unwanted software successfully complete the removal process.

## CONTINUALLY MONITOR

Software inventories change on a continuous basis, and thus the removal of a software component does not prevent its reintroduction later. Organizations should continually monitor their environments to ensure problematic software, if redetected, is promptly addressed.

1. Schedule regular updates to the organization's software asset inventory, ideally targeting no more than 72 hours for a full refresh.
2. Establish a regular cadence for reviewing the current software asset inventory to look for new instances of unwanted software, using the saved queries defined in the "Identify" step.
3. For any new occurrences, follow the organization's standard operating procedures as defined in the "Remove" step.

Additionally, many SWAM and EMM capabilities allow organizations to define polices that will preemptively block the installation of unwanted software. If available, organizations should define and publish such policies.

1. Within the SWAM/EMM tool, create a new restricted software policy.
2. Provide the relevant details (product name, executable file name, vendor, etc.) to identify the unwanted software.
3. Publish the policy to all devices within the organization.

.

## HOW TO DEAL WITH EXCEPTIONS

In some cases, an organization may determine a limited number of instances of restricted software is warranted and any associated risk is acceptable in meeting business objectives. In such a scenario, it is recommended that the organization establish a formal process to receive, evaluate, and authorize exceptions to the default restriction policy. Organizations are encouraged to document business justifications for any exception and regularly review these to reevaluate their applicability.

For more information or to seek additional help, contact us at central@cisa.dhs.gov.