thycotic

BEST PRACTICE GUIDE FOR RESTRICTING UNKNOWN APPLICATIONS

BEST PRACTICE GUIDE FOR RESTRICTING UNKNOWN APPLICATIONS

Application control allows least privilege policies to be successful because users can continue using applications they need with no downtime or loss of productivity.

Your security and IT operations teams must work together to create application control policies that match the needs of your organization. In an initial discovery phase, create a list of all applications in use and flag those that require privileged accounts. Once you have this list, you can create policies that cover all potential scenarios for trusted, untrusted, and unknown applications.

Create an allowlist of acceptable applications and processes

After you determine which applications are safe to run, you can add them to a trusted "allowlist" based on their name, signature, digital certificate or other file metadata criteria. Once you set up an initial allowlist policy, you can apply it to all protected endpoints. From that point forward, instead of managing each application request one-by-one in real time, most applications will simply be allowed to run.

Take care to prioritize applications requiring privileged access. While you're reviewing all applications that need to be included in your allowlist, pay special attention to the applications that require administrative, root, or elevated rights. Once your users are no longer local administrators on their own machines, they'll still expect to run apps that they require to do their job. You don't want to overload your IT operations or desktop support team by forcing these applications to be approved after the fact.

Block known “bad” files with a denylist

The most common security tactic to protect against malware is denylisting, whereby malicious code is flagged and subsequently denied from executing on any protected machine. An important additional layer of security with your application control solution utilizes integration with application reputation systems, such as VirusTotal, or your own virus protection software, such as Cylance, to provide the latest threat intelligence and block known threats from executing on endpoints.

What about the threats you don’t know? Account for the unknown with a restrictlist

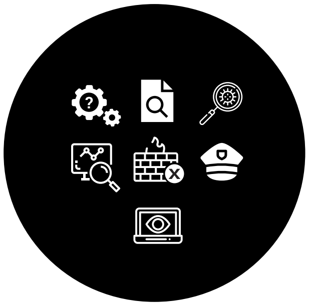
Allowlisting and denylisting are top-down strategies, often set by your IT leadership team. They work for a known set of applications. After you apply allowlisting and denylisting policies, you will still have a small subset of unknown applications to manage.

This subset is constantly changing as new applications come to your attention from the bottom up. Sophisticated hackers are adapting code to evade detection by threat intelligence systems. Also, your users are frequently downloading new software and accessing new SaaS tools. Development teams, for example, often search for solutions on Github or the open web and install applications or code. As developers are typically also privileged users, this behavior introduces a high level of risk.

As you approach application control, you need to have a plan for how you will handle these scenarios. In addition to allowlisting and denylisting, you should have a “catch-all” policy for applications you don’t know about yet. This “restricting” strategy is highly customizable to match your risk scenarios and your workplace culture.

ALLOWLISTING
APPROVES

Printers, drivers, conferencing, known and trusted business applications



DENYLISTING
DENIES

Untrusted applications, suspicious files identified by threat intelligence

RESTRICTLISTING
RESTRICTS

Require approval, request user justification, quarantine file, run in sandbox/restricted mode

Define a restrictlist policy that works for you

There is no single best practice for restrictlist management. It will be different for every company depending on how strict you want to be. Your restrictlist will require less maintenance if you continue to build up your allowlists and denylists.

- The least intrusive restrictlist policy would be to simply allow new applications without prompting an end user to provide details or reasoning for needing the app at all.
- A bit more controlled policy would require a justification first from the end user and then allow the app to execute immediately. An administrator could retroactively review all new applications and their justifications on a regular basis – perhaps every Friday – and add them to existing allowlisting or denylisting policies.
- The strictest approach would be to sandbox any unknown applications and deny access until you feel confident that they're safe to run. Sandboxing allows you to investigate applications and requires approval steps. Routing approval of an installation or application execution through an IT administrator, for example, adds an additional layer of security and works well for organizations with mature least privilege implementations. Requiring approvals would be the most intrusive approach for end users, however. It may not be scalable for an organization at the beginning phase of a least privilege implementation.

Get granular

Rather than make blanket decisions at the application level, you could choose to be more lenient for some functionality and more strict for others.

For example, you could decide to elevate an application in a limited way so users can do their jobs, but not allow them to touch any system folders or underlying OS configurations, isolating the system from malicious behavior. You could block commands or executable processes, or perhaps restrict access to an endpoint's desktop, display settings, registry, clipboard, and handles/hooks.

For web-based applications, you could decide to block components of a page – buttons, forms, etc. – rather than an entire URL. For example, you may choose to block users from accessing Facebook at work. But your social media team requires access to the corporate Facebook account to do their jobs. Therefore, you could allow only them to access to specific functionality and sections of the site.

You may want to allow processes to run only on certain types of endpoints, by certain organizational groups, in certain geographic regions, or during certain times of day. If you find that there are applications attempting to run outside of the accepted conditions, you'll be able to flag those applications and potential malware attempts.

State of Indiana set up a simple process for new application requests

> I've created a small form that lets me know what executable files users are going to be running in advance. I throw it straight into a policy, I turn it around, I throw it right back at them and say, 'Here you go, you can go ahead and install this stuff. You don't need my help.'
>
> – System Administrator, State of Indiana

WATCH THE FULL STORY

Advance planning saves time and decreases risk

With a well-defined application control strategy, the majority of applications are managed automatically, based on granular, contextual policies. As a result, most applications are either approved or denied without any extra work from IT, leaving only specialized or new applications for hands-on review and approval. Your support queue is smaller, and you have more time for other IT and security priorities.

Thycotic Privilege Manager automatically adds trusted applications to a allowlist, relies on the latest intelligence from threat databases to create denylists, and adds unknown applications to a restrictlist for further assessment. Thycotic Cloud Access Controller allows you to manage and control web applications at a granular level.

Talk with Thycotic experts about creating application control policies that match the needs of your organization.

Additional resources

eBook: Least Privilege Cybersecurity for Dummies
https://thycotic.com/resources/wileys-least-privilege-for-dummies/

Webinar: Insider's Guide to Successfully Implementing Least Privilege
https://thycotic.com/company/blog/event/insiders-guide-successfully-implementing-least-privilege/

Blog: How to remove admin rights without reducing productivity
https://thycotic.com/resources/top-10-keys-to-successful-least-privilege-adoption/

Report: Top 10 Keys to Successful Least Privilege Adoption via Application Control
https://thycotic.com/resources/top-10-keys-to-successful-least-privilege-adoption/