

Ivanti Neurons for App Control

Ivanti Neurons for App Control introduces new methods to secure your environment while enabling your users to work freely across the enterprise.

Utilizing over 20 years of enterprise experience in Application Control and Privilege Management, Ivanti is bringing these mature, scalable capabilities to the cloud for the first time with Ivanti Neurons.

Control what applications are introduced and launched in your environment without having to maintain cumbersome approve/deny lists. Reduce costs by allowing users to install and update trusted applications. Secure your environment by removing local admin rights for your users while still allowing them to launch applications that require elevated rights.





Ivanti Neurons for App Control strikes a balance between the high expectations and sophistication of end users and the high demands and limited resources of IT to manage and secure the enterprise environment.

Protect against unknown executables

Managing which applications can run in your environment can be cumbersome and time-consuming. The age-old method of creating and maintaining unwieldy lists of allowed or denied applications is an antiquated approach that is no longer fit for purpose. The immeasurable number of applications available to all of us through many more delivery methods requires a different approach.

Ivanti Neurons for App Control provides this different approach.

Instead of just considering the name of the application when deciding whether it is authorized to launch, Ivanti Neurons for App Control looks at who introduced the file into the environment. This procedure is called Trusted Ownership checking.

Every file in a Windows environment has an owner. This is set when a file is created or

copied and cannot be changed once set. Ivanti Neurons for App Control keeps a list of trusted owners. This list contains Admin, System and Trusted Installer accounts.

When any application tries to launch, App Control will cross reference the file with the Trusted Owners list and decide whether it is authorized to launch.

This means standard users cannot launch executables into the environment – on purpose or by accident. We do not need to know the name of the file in advance or have a signature or meta data for it. We simply need to know who introduced the file to decide whether it is safe to launch or not.

The Trusted Ownership approach ensures you have complete control over what is executed in your environment, greatly reducing the likelihood of nefarious software being introduced.

Granular exceptions to meet expectations

Trusted Ownership by itself is a powerful tool to manage risk in your environment. But by itself it does not offer the flexibility that modern enterprises need – or your end users expect.

There will be situations in which you need or want your end users to have limited access to manage their environments and applications. With App Control, you can specify exceptions to the Trusted Ownership rules and let users install or update applications they need to remain productive.

If IT maintains a list of trusted applications alongside the trusted owners list, employees can continue working without disruption.

Consider a scenario in which an employee is invited to a meeting with a third party, but the meeting is being held online on a platform the employee does not normally use. Instead of asking IT to install the software, the employee can install the application if the installer for the software has been approved and added to an exception list.

Conversely, there might be certain tools that will naturally have a trusted owner that you might wish to block, such as the command prompt or registry editor. App Control also allows exceptions to block or allow applications.

Resolve a huge security flaw by removing admin accounts

A scourge of IT administrators across all industries is the prevalence of local administrator accounts within the enterprise.

These accounts let users have high levels of access and privileges on their desktops, enabling them to install software, change system settings and run scripts. Users can be duped into introducing viruses, ransomware or other unsafe applications into your environment.



So why are end users often given local administrator rights?

Unfortunately, many applications require the user to have these rights for the application to run correctly. The reasons for this may include:

- **System modifications:** Applications that modify system settings, install or remove device drivers or update core system files often need admin rights. This includes applications for partitioning drives, formatting disks or managing user accounts.
- **Deep system access:** Software that needs to access or modify heavily protected system resources like the registry or kernel files typically requires admin privileges. These applications might be system monitoring tools, security software with deep system integration or system optimization utilities.
- **Hardware access:** Certain applications that need direct control over hardware components, like video capture software or network configuration tools, might require admin rights to function properly.

Because there is a legitimate need for these applications to require elevated rights to run, the only solution has been to add the user to the local administrator group, giving elevated rights to the entire desktop – not just the applications that require it.

Ivanti Neurons for App Control solves this problem by allowing specific applications to run with admin rights, without giving the user elevated rights elsewhere.

When the application launches, it will run as if the user is a local administrator and will have access to everything it needs to run correctly. All IT must do is specify a list of any applications that require administrator rights and that they know and trust, then add them to the Ivanti Neurons for App Control configuration.

Besides applications, IT can also specify system tools such as add/remove certificates or change date/time to elevate the users' rights to run, too.

Why is it important to remove local admin rights for standard users?

- **Enhanced security:** Standard users with local admin rights pose a significant security risk. Malicious software or accidental actions can have devastating consequences if a user has full administrative control. By removing these rights, you significantly reduce the potential damage a compromised account can cause.
- **Reduced risk of malware and viruses:** Many malware programs and viruses specifically target administrator accounts to gain full system access. Without local admin rights, standard users cannot install unauthorized software or make system


changes that could introduce vulnerabilities.

- **Improved patch management:** Applying security patches promptly is crucial for maintaining a secure system. When users have local admin rights, they can delay or block critical updates, leaving the system vulnerable. Removing these rights ensures updates can be deployed centrally and efficiently.
- **Stronger application control:** Local admin rights often allow users to install unauthorized applications. This can lead to software compatibility issues, licensing problems and potential security risks. By removing local admin rights, IT can control which applications are allowed on company devices.
- **Reduced help desk tickets:** Many user issues stem from accidental configuration changes or attempts to install unauthorized software. Removing local admin rights can significantly reduce the number of help desk tickets related to these issues.
- **Compliance with regulations:** Many industries have data security regulations that mandate specific security practices. Removing local admin rights is a common security best practice that can help organizations comply.

Overall, removing local admin rights for standard users strengthens the security posture of your enterprise environment. It reduces the attack surface, minimizes potential damage from human error or malware and allows for centralized IT control over systems and configurations.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The logo for Ivanti Neurons, featuring the word "ivanti" in a bold, lowercase, sans-serif font with a red dot above the 'i', followed by the word "neurons" in a lighter, lowercase, sans-serif font.A vertical red bar with a slight gradient, positioned to the left of the text.

For more information, or to contact Ivanti, please visit [ivanti.com](https://www.ivanti.com).