ivanti neurons

The Critical Role of Application Control and Privilege Management

Introduction

The enterprise application landscape is transforming dramatically, with cloud-based solutions introducing clear benefits – but also new security challenges. In this dynamic environment, organizations need a robust and layered approach to application security.

Cloud-based solutions are proliferating, driven by their affordability, scalability and ease of access. Traditional network perimeters are dissolving – and the attack surface is expanding.

Emerging threats, such as sophisticated malware, zero-day attacks and social engineering tactics target vulnerabilities not just in the software, but also in endpoint security configurations. Application sprawl, both sanctioned and unauthorized (shadow IT), creates a breeding ground for potential security breaches.

This paper explores the critical roles of application control and privilege management in mitigating these emerging risks. We'll delve into the capabilities of Ivanti Neurons for App Control, a comprehensive solution that empowers organizations to gain complete visibility across their entire IT infrastructure to enforce granular control and streamline application management.

Refocusing application management

The way we manage applications in the enterprise has undergone a significant shift. Traditionally, IT departments shouldered the burden of deploying, maintaining and securing a vast array of desktop software applications. This involved complex processes for software acquisition, licensing, distribution and patching.

The rise of cloud-based, browser-based applications has undoubtedly simplified aspects of application management. Gone are the days of managing individual software installations on every machine. Cloud solutions offer centralized deployment, automatic updates and simplified access for users. For IT departments, this translates to reduced administrative overhead and improved efficiency.

However, this shift toward browser-based applications is a double-edged sword: While it streamlines IT processes, it also creates a new set of challenges.

Control what runs in your environment

A fundamental priority for IT is managing what applications are allowed to run in an enterprise environment.

In some ways, the issue has become easier to manage over the past five years, as many core applications are now browser-based. This means there are fewer applications to manage, with less chance of nefarious executables sneaking in – and therefore less security risk.

Yet there are still many opportunities for unknown, unsafe applications to infiltrate your environment:

Shadow IT

- **Risk:** Employees install unauthorized applications (shadow IT) to improve productivity or address a perceived lack of functionality in approved applications. These applications often lack proper security controls and patching, making them vulnerable to malware or exploits.
- **Exploitation:** Malicious actors can develop malware that specifically targets these unsanctioned applications, knowing they might have weaker defenses. Once a user installs a compromised application, the malware can gain access to the system and steal data, install additional malware or disrupt operations.

Endpoint vulnerabilities

- **Risk:** Even with browser-based applications, vulnerabilities can exist on the user's device (endpoint). Outdated software, unpatched operating systems or weak browser configurations can create openings for attackers.
- **Exploitation:** Malicious actors can use these vulnerabilities to gain a foothold on the device. This could involve drive-by download attacks in which simply visiting a compromised website infects the system, or phishing emails tricking users into downloading malware disguised as legitimate software updates. Once a foothold is established, attackers can move laterally within the network or launch ransomware attacks.

Data-loss prevention

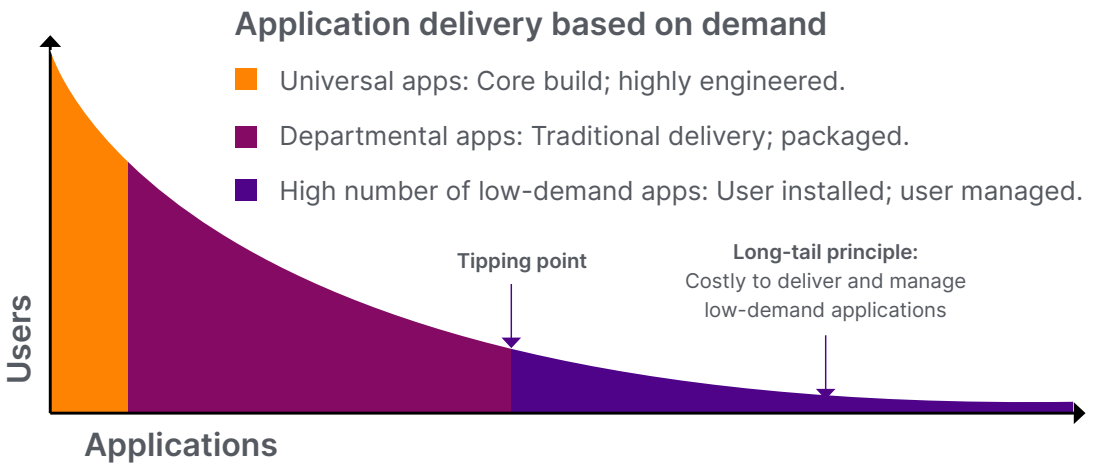
- **Risk:** Unauthorized applications can be designed to steal sensitive data such as customer records, financial information or intellectual property. These applications might exploit weak security measures or user permissions to gain access to this data and transmit it to an attacker's server.
- **Exploitation:** Data breaches are a common way attackers exploit this risk. Social engineering tactics can trick users into installing malicious applications or granting them excessive permissions. Once installed, the application can function as a backdoor, continuously exfiltrating data in the background without the user's knowledge.

Uncontrolled installations

- **Risk:** Uncontrolled software installations can strain system resources, leading to slow performance, crashes or freezes. This can disrupt workflows and decrease employee productivity.
- **Exploitation**: While not as critical as data theft, attackers can leverage this risk in denial-of-service attacks. They might manipulate users into installing resource-hogging applications, overwhelming systems and making them unusable for legitimate purposes. This can disrupt operations and cause financial losses.

Third-party risk

- **Risk:** Many cloud-based applications rely on third-party services and integrations to provide additional features or functions. Vulnerabilities in these third-party components can expose the entire application – and the user's data – to security risks.
- **Exploitation:** Attackers can target vulnerabilities in third-party components to gain access to the main application. This is known as a supply-chain attack. Once they have a foothold, they can steal data, inject malware into the application or launch attacks against the users of the application.



The long-tail principle of application usage.

Traditional ways to block unauthorized applications

In the ongoing battle against unauthorized applications, several methods have commonly been employed. Understand the advantages and limitations of these techniques to implement them in a comprehensive defense.

Denied and allowed lists

Denied lists: This method involves creating and maintaining a list of known malicious or unauthorized applications that are explicitly blocked from execution. Security teams compile these lists by referencing threat intelligence feeds, industry blacklists and internal security data.

Pros:

- Targeted defense: Blocks known threats effectively.
- Relatively simple to implement: Straightforward concept for IT teams to understand.

Cons:

- Maintenance burden: Keeping denied lists up to date is time consuming, requiring constant monitoring for new threats. Large organizations might spend weeks or months updating their denied lists.
- Zero-day ineffectiveness: New or unknown malware variants can bypass denied lists.
- False positives: Occasionally, legitimate applications might be mistakenly denied, causing disruptions.

Allowed list: This approach flips the script: Only pre-approved applications on an allowed list can run, while all others are blocked. IT administrators create and maintain the allowed list, ensuring only authorized software has access to system resources.

Pros:

- Stronger security: Provides superior protection against unknown threats and malware.
- Streamlined application control: Simplifies management of authorized applications.

Cons:

- Initial setup time: Creating a comprehensive allowed list for a large organization can be a complex and lengthy process. It can take months to create an initial whitelist for a large organization with thousands of applications.
- Maintenance challenges: Adding new applications requires ongoing updates to the allowed list, which can be cumbersome for IT teams.
- User productivity impact: Unapproved applications, even if legitimate business tools, get blocked, potentially hindering workflows until allowed.

Signature-based detection

Signature-based detection is a cornerstone of traditional antivirus software. This method relies on identifying malware based on predetermined patterns, or "signatures," within the application's code. When a scanned file matches a known malware signature, it's flagged and quarantined.

Pros:

- Effective against known threats: Can accurately detect and block common malware strains.
- Relatively low resource consumption: Doesn't require significant system resources to function.

Cons:

- Limited scope: Only detects malware with existing signatures; ineffective against zero-day attacks or novel malware variants.
- Signature updates required: Antivirus software needs frequent updates to include the latest threat signatures, potentially creating a window of vulnerability between updates

Application sandboxing

This technique creates a virtual environment in which unknown executables are run in isolation. If the application exhibits malicious behavior within the sandbox, it's prevented from accessing the main system.

Pros:

- Zero-day protection: Offers a layer of defense against unknown threats and zero-day attacks.
- Reduced risk: Even if malware executes within the sandbox, it cannot harm the main system.

Cons:

- Performance overhead: Running applications in a sandbox can consume system resources and potentially impact performance.
- False positives: Some legitimate applications might be flagged as suspicious in the sandbox, requiring manual investigation.

User education and awareness

Training employees to identify suspicious emails, attachments and websites can be a valuable first line of defense. Educating users about the risks of installing unauthorized software can help prevent them from inadvertently introducing unknown executables.

Pros:

- Human firewall: Empowered users can become a vital part of the security posture by recognizing and reporting suspicious activity.
- Cost-effective: Training programs are generally less expensive compared to deploying advanced security tools.

Cons:

- Human error: Social engineering tactics can still bypass user awareness, especially with sophisticated attacks.
- Ongoing training: Security awareness training should be continuous to keep users informed about evolving threats.

A layered approach

Traditional methods can be combined to create a more robust defense. For instance:

- Denied lists can be the first line of defense, blocking known threats.
- Allowed listing can be implemented alongside it for additional control.
- Signature-based detection can further enhance security by identifying malware that hasn't yet been blacklisted.
- Application sandboxing can provide an additional layer of protection against unknown threats.
- User education and awareness can empower users to become a vital part of the security posture.

However, it's crucial to acknowledge the limitations of these traditional approaches. The ever-evolving threat landscape, with new malware variants emerging daily, makes it challenging to maintain effective denied lists and signature databases. Additionally, the resource-intensive nature of maintaining allowed lists and the limitations of user awareness training can create challenges for IT teams.

While traditional approaches provide a baseline level of protection, they are no longer sufficient. Modern solutions that leverage advanced techniques like application behavior monitoring, machine learning and sandboxing are becoming increasingly important to comprehensively protect against unknown executables and sophisticated cyber threats.

> "We estimate that, across all UK businesses, there were approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud as a result of cyber crime in the last 12 months."
>
> **UK Government Statistics - 2024**

Ivanti Neurons for App Control: a modern approach

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

Leveraging 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.

Ivanti Neurons for App Control strikes a balance between the high expectations and sophistication of end users and the growing demands on IT to manage and secure the enterprise environment with limited resources. Now, IT administrators can:

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

Trusted Ownership checking

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 no longer fit for purpose. The immeasurable number of applications available to all of us through a growing number of delivery methods demands 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 by default, but more can be added if needed.

When any application tries to launch, App Control will cross reference the file with the trusted owners list and decide whether or not it is authorized to launch.

This means standard users cannot launch executables into the environment – either 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 that IT administrators have complete control over what is executed in their environment, greatly reducing the likelihood of nefarious software being introduced.

Exceptions to Trusted Ownership

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

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

If IT maintains a list of trusted applications alongside the trusted owners list, then employees can continue with what they need to do without disruption

For instance, an employee might be invited to a meeting with a third party, but the meeting is being held online with a platform the employee does not

normally use. Instead of asking IT to install the software for the employee, the employee can install the application if the installer for the software has already been approved and added to an exception list.

Conversely, there may be certain tools that will naturally have a trusted owner that you may wish to block for certain users, such as an HR application or SAP. App Control allows exceptions to block applications as well as allow them.

Remove local admin accounts

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

These accounts grant users high levels of access and privileges on their desktops, enabling them to install software, change system settings and run scripts. This, of course, can lead to security issues as users can be duped into introducing viruses, ransomware or other unsafe applications into your environment.

Why are end users often given local administrator rights?

Unfortunately, many applications require the user to have these rights for the application to be able to run correctly. 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 in the past was to add users to the local administrator group, giving them elevated rights to the entire desktop – not just the applications that require it.

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

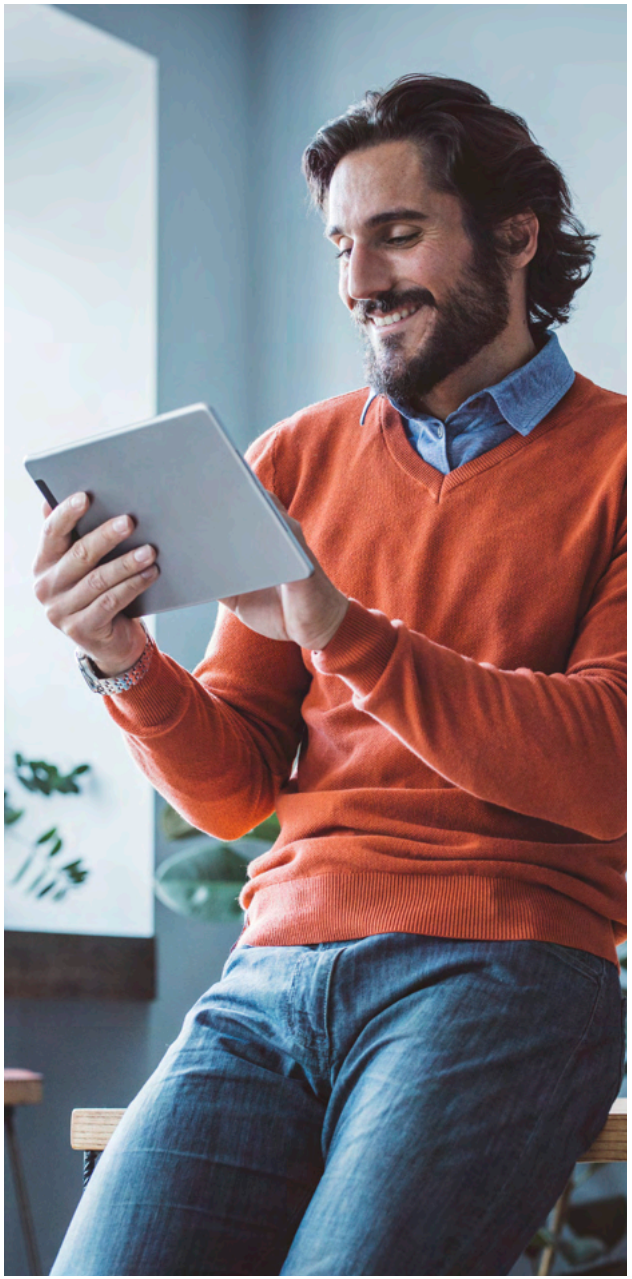
When the application launches, it will run as if the user is a local administrator and will have access to everything that it needs to run correctly.

All IT must do is specify a list of any applications that require administrator rights, and that they know and trust, and add them to the Ivanti Neurons for App Control configuration.

It's not just applications – IT can also specify system tools such as add/remove certificates or change date/time to elevate the users' rights to run, too.

Benefits of removing local admin rights

- **Enhanced security:** Standard users with local admin rights pose a significant security risk. Malicious software or even accidental actions can have devastating consequences when 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 even 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 with these regulations.

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

Ivanti Neurons for App Control is an essential part of securing your endpoints, making it easier to control what is introduced and launched in your environment. Coupled with privilege management to manage what rights an application has when running, Ivanti Neurons for App Control provides the essential tools we need to negate many of the common security issues we must consider when securing an enterprise environment.

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

ivanti neurons

For more information, or to contact Ivanti, please visit ivanti.com.