Avecto

5 good reasons why you can't risk giving admin rights to your server administrators

This article covers the five top reasons why running server administrators with full admin rights no longer represents an acceptable level of risk, and explains why the principle of least privilege allows you to free sysadmins without security risk.

The world of desktop security has experienced a revolution. Respected consultants such as Gartner have become increasingly vocal in their firm recommendation that organizations should minimize the use of administrative rights.

Migration away from Windows XP has acted as a catalyst for the standard user revolution as global organizations adopt the principle of least privilege, delivering what's commonly referred to as the 'least risk' environment.

But server administrators (sysadmins) are surely a different kettle of fish: these are trusted, tech-savvy individuals who need to have the 'keys to the kingdom' in order to complete their job roles efficiently and effectively, right?

Wrong. Our message is clear – it's just as important, and possible, to protect servers as it is desktops.

Here are five good business reasons why allocating admin rights to server administrators is neither acceptable or necessary in a secure and operationally sound enterprise environment:

01 > Your server admins are just like everyone else: they're not perfect

The reality is that the business impact of taking down a single server or, at worst, taking down your entire data center is far greater than the impact of the same scenario on a desktop computer. What are the chances that a sysadmin within your organization could make an accidental misconfiguration when logging on to a server to complete a routine task? How severe could the impact be?

Implementing least privilege for sysadmins means that they are empowered to perform only the task at hand. If you could deliver the same level of usability and productivity for your admins whilst limiting the potential for mistakes, wouldn't you take this approach?

> "According to statistics reported by Gartner, 90% of security threats can be removed by running users as standard. Would your administrators welcome the opportunity to perform their roles in a more secure way?"
>
> Andrew Avanessian

Avecto

02 > Your server admins deserve to be protected against malware

Your administrators are highly skilled individuals, but those who write malware are some of the most sophisticated developers in the world. Targeted malware could take hold of an admin's machine without them even realising it, and detection is incredibly difficult. How great is the risk to your business? For example, a kernel mode root kit could be installed on a server, cloaking itself from detection and lying dormant.

User Account Control (UAC) helps to catch many security threats but due to its inflexibility, it hinders the ability of your admins to complete their roles efficiently. It is therefore common practice that this is turned off whilst work is ongoing: leaving your data center environment with virtually no protection against malware during configuration time. Where users run as admins, permissions mean nothing; malware can circumvent these and proliferate across your network.

03 > You need to deliver compliant servers

In line with overwhelming evidence from real-world attack data such as the Top 35 Mitigation Strategies from the Australian Department of Defense, the implementation of least privilege for all users within an organization is becoming mandatory under an ever-increasing number of internal and external compliance frameworks.

If you are subject to the requirements of PCI DSS, Sarbanes-Oxley (SOX), MAS, USGCB, PCN, HIPAA or similar internal mandates, the implementation of a least privilege environment in the data center will provide you with an adaptable security strategy to hit the constantly moving target of compliance in the long term.

04 > Your server admins are dedicated, hardworking, tech-savvy individuals

Your sysadmins are concerned with getting the job done as quickly and efficiently as possible, particularly in break-fix scenarios. As many organizations move towards removal of admin rights on servers without a least privilege approach, long-winded processes for the 'check-out' of admin passwords have often been implemented.

Once you have granted access to a temporary admin account, users often find a way around the approval process to find a quicker and easier path. They're techsavvy, so they know that they can create a separate, permanent admin account to access in a future break-fix scenario.

Implement least privilege in your data center environment and your administrators are empowered with the privileges they need to respond to urgent break-fix scenarios, without the need for you to allocate admin accounts.

05 > Your organization needs visibility of privileged activity in the datacenter

The growing significance of cloud computing, BYOD (bring your own device) and social media means that data is everywhere. As a result, it's critical that privileged access to such data can be audited and reported upon.

Comprehensive knowledge of who, what, when and why is the order of the day. With this approach, malicious activity, whether carried out by malware or an employee, can easily be identified and blocked. Utilizing admin rights to perform a particular task within the data center isn't an issue in itself, but performance of this task outside of usual hours or patterns of work must be automatically identified and blocked.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.

Andrew Avanessian

Andrew initially established Avecto's consultancy service, developing it into a world-class offering. Now responsible for the strategic direction of the consultancy, IT and customer support divisions, he regularly provides security and technology advice to large global enterprises. His background in IT infrastructure ensures he can clearly translate complex requirements, finding technical solutions to commercial challenges. With a keen interest in cyber security and the end user experience, Andrew is a regular contributor to press articles and security events.

You can contact Andrew at andrew.avanessian@avecto.com