9 Ways Privileged Users Create Security Risks

Beware of end-users who aren't trained as IT system administrators, but who hold full admin rights to your systems. Here's how they can increase your security risk and manageability costs and make it difficult to achieve compliance—plus what you can do about it.

1 Installing unauthorized apps that introduce malware

Stop admins from turning off User Account Control and prevent unauthorized apps or inadvertent system-setting changes.

2 Deactivating critical services such as Antivirus

Microsoft Management Console (MMC) allows users to load snap-ins that can control services. Make MMC inaccessible to end-users with admin privileges.

3 Overriding GUI-based restrictions

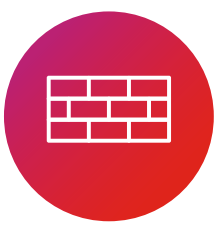
Restrict execution of commands or scripts to operating systems.

4 Uninstalling agents and protection software

Prevent privileged users from uninstalling third-party protection software.

5 Circumnavigating central management protection policies

Exclude privileged access to the Windows registry; stop users from changing configuration settings.



6 Disabling or changing endpoint Firewall setting

Defend against malicious software spreading through a network by preventing deactivation.

7 Changing application behavior through incorrect date or time

Block date-and-time changes to protect application integrity and timestamps for auditing or troubleshooting.

8 Killing protection software

Add process termination control to reduce security risk.

9 Elevating applications that could introduce malware

Restrict certain apps to run only with standard privileges.

With application-control capabilities in Ivanti® Security Controls, you can set simple restrictions immediately to reduce your risk, increase corporate compliance, and stop the raising of unnecessary IT tickets by someone who changes an administrative setting inadvertently.

DOWNLOAD WHITEPAPER

Copyright 2019, Ivanti. All rights reserved. IVI-2311 09/19 MK/BB/SL/DH