Avecto Infographic

Admin privileges: a hidden threat?

Remove admin rights and you immediately improve your security posture.

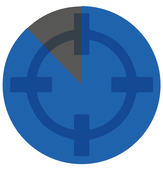
Combining **privilege management** and **application control** with **sandboxing** to create proactive defense in depth is crucial to overcoming unknown threats.

72% of temporary workers admit to being given admin privileges on their employers' IT systems.

Only half of temporary workers were informed of any restrictions during their induction period.

Over **30%** of companies have no policy in place for managing admin access.

88% of insider attacks are caused by privilege abuse.



89% of CIOs say digital is bringing new types and levels of risk.

By 2017, 1/3 of large enterprises engaging in digital business will have a Digital Risk Officer.

Recent breach examples

Home Depot breach

Hacker acquires third-party admin privileges.

Uses admin privileges to access network and install malware.

Steals data related to **70m** Home Depot customers.

Regin malware

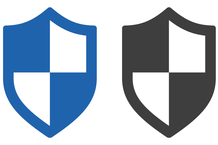
Malware program uses admin privileges to install loader on to target

Loader uses admin privileges to embed malicious code within the OS and evade detection.

Hacker able to to spy on emails, internet traffic and server activity.

Be proactive, not reactive

Antivirus systems are only effective **half of the time**...



...while **100%** of vulnerabilities affecting IE in 2013 could have been mitigated by removing admin rights...

...and **96%** of critical vulnerabilities affecting Windows OS could have been mitigated by removing admin rights.

Advice from the experts

Christian Byrnes - Gartner

"Security teams need to be the facilitators of a balance between the need to protect the organisation and the need to run the business."

Gartner Symposium ITxpo Nov 2014, Barcelona

Chris Sherman - Forrester

"Antivirus' reign as the king of endpoint protection is nearing an end."

Prepare For the Post-AV Era Part 1, June 2014

Creating a Defense in Depth (DiD) strategy

defendpoint

privilege management

Regain control over admin rights. Our flexible privilege management module assigns privileges to apps, not users, to protect the operating system.

application control

Protect your software environment. Use our app control module to easily block unauthorized applications, defending against targeted attacks.

sandboxing

Safeguard your corporate data. Our sandboxing module isolates untrusted web activity and places it into a secure container, capturing web borne threats.

UK
Hobart House
Cheadle Royal Business Park
Cheadle, Cheshire, SK8 3SR

Phone +44 (0)845 519 0114
Fax +44 (0)845 519 0115

Americas
125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone 978 703 4169
Fax 978 910 0448

Australia
Level 8
350 Collins Street, Melbourne,
Victoria 3000, Australia

Phone +613 8605 4822
Fax +613 8601 1180

Avecto
@avecto
Avecto

avecto.com
info@avecto.com

http://www.verizonenterprise.com/DBIR/2014/
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf
http://www.forbes.com/sites/gilpress/2014/10/09/gartner-predicts-top-trends-for-technology-it-organizations-and-consumers-for-2015-and-beyond/2/
http://www.smu.edu/~/media/Site/Lyle/Deason%20Institute/new%20healthcare%20vulnerability-deason%20institute.ahx
http://www.businessnewsdaily.com/4614-managing-administrator-access-security.html
https://blog.avecto.com/2014/02/the-simple-way-to-mitigate-over-90-critical-microsoft-vulnerabilities/
http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance
http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html
Taking Risk in Digital Business: A CIO Guide to Your New Relationship With Risk, Gartner Symposium ITxpo 2014, Barcelona
Prepare For The Post-AV Era Part 1: Five Alternatives to Endpoint Antivirus, June 2014