Avecto Datasheet

Avecto & SANS Critical Controls

The SANS 20 Critical Security Controls for Effective Cyber Defense prioritizes a list of measures that are effective in combating real-world threats. Derived from the most common attack patterns and vetted across government and industry bodies, the 20 Critical Controls focus on a small number of actionable controls with immediate benefits. This document focuses on the First Five Quick Wins identified by SANS, and how Avecto's Defendpoint technology can help you meet many of its recommendations.

Control	Requirement	How Avecto Maps to the Control	
CSC 2-1	**Application Whitelisting:** "Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system."	Defendpoint provides application whitelisting and blacklisting capabilities, with the broadest set of supported application types and criteria for identification, even for Windows 8 store apps. Apps that require admin rights can be targeted and standard UAC prompts can be replaced with custom messaging. Defendpoint's contextually aware application control allows you to easily apply much stricter whitelists to untrusted internet content through its sandboxing module.	First 5 Quick Win
CSC 2-2	**List of Authorized Software:** "Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses."	Avecto's enterprise reporting tools will provide a list of all executed software, including those that require admin rights to run.	
CSC 2-3	**Alerting of Unauthorized Binaries:** "Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives."	Defendpoint proactively prohibits unauthorized binaries.	
CSC 2-6	**Monitor Dangerous File Types**	Defendpoint provides the ability to track downloads and apply app control based on origin. Behavior of most powerful apps can be restricted.	
CSC 3-1	**Maintain Standard Configurations:** "Establish and ensure the use of standard secure configurations of your operating systems."	Defendpoint allows you to maintain your gold standard build by providing the most granular, flexible approach to policy build. This means configurations scale easily with a firewall-style engine for management and clear, logical process flows. Avecto leverages existing infrastructure and integrates tightly with Microsoft Group Policy or McAfee ePO. In addition, all users will be standard users and therefore not be able to manipulate the build.	First 5 Quick Win
CSC 3-3	**Removal of Admin Rights:** "Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system."	Defendpoint allows for all Windows users to operate as standard users across desktops and servers, with the admin rights applied directly to applications, tasks and scripts according to the needs of individuals and groups of users.	First 5 Quick Win

Avecto & SANS Critical Controls

Control	Requirement	How Avecto Maps to the Control	
CSC 3-10	**Deployment of Configuration Management:** "Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals."	Active Directory GPO can be overwritten with admin rights - Defendpoint prevents this.	
CSC 4-8	**Patching Vulnerabilities :** "Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization. Alternative countermeasures should be considered if patches are not available."	Defendpoint Sandboxing protects the user by isolating vulnerable or potentially vulnerable applications such as Java from the users data, this provides reassurance until patching is completed.	
CSC 4-9	**Continuous Vulnerability Assessment:** "Evaluate critical patches in a test environment before pushing them into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality."	Application Control can be used to temporarily block a vulnerable application from running, and force the user to update, where a patch or update is available, before they proceed.	
CSC 5-3	**Prohibit Auto Running of Apps from External Media:** "Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares."	Applications can be controlled and monitored with policies that allow, block or prompt apps based on granular rules, with fully customised messaging.	
CSC 11-1	**Ensure that only ports, protocols, and services with validated business needs are running on each system.**	Defendpoint allows you to control installing and starting services which are not a "validated business need". Removing admin rights also prevents users or applications from opening ports on the system.	
CSC 12-1	**Minimize Admin Privileges:** "Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior."	Defendpoint allows all Windows users to operate as standard users across desktops and servers, with the admin rights applied directly to applications, tasks and scripts according to the needs of individuals and groups of users.	First 5 Quick Win
CSC 12-2	**Audit all Admin Use:** "Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive."	Avecto's reporting software provides visibility of privileged user activity and admin rights use over time.	

CSC 12-7	**Ensure Real Admin Accounts Are Only Used for Sysadmins:** "Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients especially must be configured to never run as administrator."	Defendpoint can be deployed across desktops and servers with control for sysadmins provided by control for services & drivers, remote powershell control and on demand elevation. Sysadmins can run apps as different users without the need for admin access (with custom messages, granular control, auditable log of activity).	
CSC 12-8	**Audit Admin Group Modifications**	Defendpoint protects against admin group modification with privileged account protection to ensure that elevated processes cannot be used to attack the solution i.e. make any changes to policies or create privileged accounts.	
CSC 12-12	**Use Multifactor Authentication for Admin Access, including domain administrative access.**	Defendpoint provides a number of multifactor authentication options, including Smart Cards, Passwords, Dual Control (over the shoulder authentication).	
CSC 12-14	**Block Access to a Machine (either remotely or locally) for Administrator-Level Accounts.**	Built-in anti tamper prevents rogue admin accounts being created by standard users or sysadmins. All admin use can be fully controlled / restricted with reports and audits to aid visibility and compliance.	

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