Avecto Whitepaper

Compliance series

CPNI Critical Security Controls for effective cyber defense

The Critical Security Controls for Effective Cyber Defense are an internationally recognised baseline standard of information security best practices developed by the Centre for Internet Security with input from the UK Centre for the Protection of National Infrastructure (CPNI) and other government and industry bodies from around the world. In this paper, Avecto examines the controls that directly require the use of proactive endpoint security. Six of the controls directly pertain to privilege management and application control, but we will also outline how content isolation (sandboxing) can also be used as an additional line of defense to further protect systems.

The 20 controls presented in the Critical Security Controls (CSC) for Effective Cyber Defense document are intended to help prioritize the implementation of security best practices and select which out of the many technologies, standards, and benchmarks and recommendations available today are most effective at improving an organization's security posture.

Prevention is better than cure, but many organizations neglect fundamental security best practices, such as the use of standard user accounts, instead relying on antivirus and endpoint firewalls as a band aid. But definition-based AV is increasingly less effective at preventing compromises where in many cases, proactive endpoint security can stop even advanced and zero-day exploits.

What follows is an explanation of how proactive endpoint security, such as that provided by Avecto Defendpoint, is essential for achieving the goals set out in the document.

Critical Security Controls requiring proactive endpoint security:

1. **Controlled use of administrative privileges**
2. **Control access based on the need to know**
3. **Inventory of authorised and unauthorised software**
4. **Secure configurations for hardware and software on mobile devices, laptops, workstations and servers**
5. **Malware defenses**
6. **Application software security**

> "70% of IT pros do not have confidence in their organization's security technologies."
>
> Intel Security[1]

[1]Source: http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

Controlled use of administrative privileges and access based on the need to know

Do you know how many domain administrator accounts you have or what privileges IT staff have been given to sensitive systems? Many organizations have a poor understanding of when, where and to whom administrative privileges have been granted. Controlling administrative access is key to securing servers, and has long been understood and practiced in the Unix community.

End user systems also play a role in the overall security posture, and failure to follow security best practices can easily lead to a compromise that could be used by an attacker to move undetected from a low-risk notebook to a server hosting critical data or applications.

A privilege management solution controls how administrative rights are used on servers and end user systems, providing an audit trail of privileged credential use, granular control over the rights granted to individual processes as opposed to users, customizable messaging and challenge/response authorization for situations where users need to elevate privileges but no pre-defined rule allows them to do so.

> “Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”

Kevin Mitnick, former hacker

Inventory of authorised and unauthorised software

Not only should organizations perform a software inventory, track and remediate issues, but also actively prevent the installation and execution of unauthorized software. Best practices set out by Microsoft require that software should be installable without administrative privileges, but the majority of vendors fail to follow this advice, so the use of standard user accounts prevents the installation of software that might otherwise be outside the control of IT.

Portable software, i.e. software that doesn't modify protected parts of the registry and filesystem, is sometimes made available explicitly to allow users to install an application even when administrative privileges have been removed. Probably the most well-known example of this Google Chrome, which while by default requires administrative privileges to install, can be installed as a standard user.

If removal of administrative privileges protects system-level configuration, application control is required to protect the user space. The introduction of User Account Control (UAC) in Windows Vista, a collection of technologies that provides users an administrative access token only when required, has necessitated that malware writers change tactics so that lack of administrative privileges doesn't prevent code from executing, even if the level of access to the system is severely restricted.

Secure configurations for hardware and software on mobile devices, laptops, workstations and servers

The deployment of operating system 'builds' that use a known configuration has long been practiced in larger organizations that have the resources and knowledge to utilize technologies like Microsoft's System Center Configuration Manager (SCCM). Known configurations help keep costs down because they provide an environment where IT can be sure that line-of-business software works and the OS provides a reliable and secure platform on which to support the organization's activities.

> "In 60% of cases, attackers are able to compromise an organisation within minutes."

Verizon Data Breach Investigations Report 2015

But configuration creep can quickly destroy the value provided by pre-configured OS builds if users are granted administrative rights. System-level access gives users the ability to make unauthorized changes that are hard to control and monitor. Administrative users can even bypass technologies like Group Policy that are intended to enforce configuration settings. Privilege management and Application control add value by allowing IT to roll out builds but as stated in the CSC document: 'maintain a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings'.

> "The probability of a vulnerability being exploited hits 90% between 40-60 days after discovery."
>
> Kenna Non Targeted Attacks Report, 2015[2]

Malware defenses

Antimalware is still an important layer of defense, but definition-based antimalware software is becoming less effective as viruses mutate faster than ever before and attacks become more sophisticated. It's long been recognized that removing administrative privileges from users can mitigate a large number of critical security vulnerabilities in Windows, which malware writers use to gain system-level access to systems.

Application control also has an important role to play. Enforcing whitelists of approved software ensures that malicious applications, scripts and other executables that find their way onto systems cannot run. Sandboxing can also bolster security by isolating running programs from the OS, each other and user data, limiting the damage an infected document or web site can inflict.

Application software security

Not only does application control allow IT to block software that's not included on a whitelist, but out-of-date software can also be prevented from running. Application control policies allow IT to set a minimum level for the version of an executable to ensure applications that haven't been updated cannot run, preventing users from exposing systems to known vulnerabilities in unpatched software. In cases where a zero-day exploit might be present in a current software release, sandboxing can mitigate the threat.

[2] Source: https://www.kennasecurity.com/asset_pipeline/public/Kenna-NonTargetedAttacksReport.pdf

About Avecto

Avecto is an innovator in endpoint security. Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development