Avecto Whitepaper

Compliance series

Guide to the NIST Cybersecurity Framework

In this paper, Avecto looks at the role least privilege security and application control play in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a voluntary standard for public and private industry sectors supporting critical infrastructure, helping organizations improve security and comply with common regulatory standards.

The NIST Cybersecurity Framework was created on a White House directive in 2013, and according to Gartner, while intended as a voluntary code, has been adopted by 30% of public and private enterprises in the US. CSF differs from many other regulatory codes in that rather than providing a checklist of security controls, it is a risk-based approach where organizations must evaluate their risk position and implement controls as appropriate.

> “While intended as a voluntary code, [NIST] has been adopted by 30% of public and private enterprises in the US.”
>
> Gartner[1]

Framework overview

The CSF does not replace existing security programs or risk management processes but is intended to improve processes to allow organizations to describe their present security posture, target state, assess progress towards achieving a new state and communicate about cybersecurity risk to stakeholders.

The CSF consists of three parts: the **Framework Core**, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core contains a list of cybersecurity activities, anticipated results, and related references to industry standards and guidelines that can be used to achieve the desired results. Five functions are used to provide an overview of an organization’s cybersecurity risk profile: Identify, Protect, Detect, Respond, and Recover. These functions are then further subdivided into categories and subcategories that relate to Informative References giving further information about industry standards and best practice guidelines.

[1] Source: http://www.nist.gov/itl/acd/cybersecurity-rosetta-stone-celebrates-two-years-of-success.cfm

Framework Implementation Tiers, which range from Partial (Tier 1) to Adaptive (Tier 4), are used to categorize an organization's cybersecurity practices, with Tier 4 describing a cybersecurity posture where an agile and risk-informed approach to security has been adopted.

Framework Profiles define an overview of an organization's current or target cybersecurity position. Profiles are developed by reviewing all the categories and subcategories of Framework Core Functions, and can then be used to help move the current cybersecurity posture forwards to achieve a target state, as defined in a Target State Profile.

> "Access permissions are managed, incorporating the principles of least privilege and separation of duties."
>
> CSF section PR.AC-4

CSF and privilege management

While the CSF doesn't provide a list of checkbox security controls, the Framework Core includes technical requirements that can be best achieved using a Privilege Management solution. This paper focuses on the Framework Core access control requirements relating to privilege management and application control.

Access control

The use of principles of least privilege is directly referenced in the CSF's access control requirements (section PR.AC-4) as part of the Protect function. A key factor in achieving least privilege is the removal of administrative rights from users. It's always been possible to run without administrative privileges in Windows, but standard user accounts faced restrictions that often made it impractical to perform everyday tasks, such as installing software or changing system settings.

Because of the difficulties traditionally associated with servicing PCs where users run without administrative privileges, many organizations choose not to deploy standard user accounts. But with a privilege management solution and improvements in Windows, standard users can do more without requiring intervention from IT.

User Account Control

Windows Vista introduced User Account Control (UAC), a set of technologies that allows consumers to run with standard user rights most of the time but elevate to administrative privileges as required. As part of the work undertaken with UAC, common tasks, such as changing the time zone or installing devices with signed drivers, can be performed by standard users in Windows 7. However, unlike a third-party privilege management solution, UAC doesn't give organizations the ability to control which processes users are able to elevate, customize dialog message boxes, or prevent users from running unauthorized software with elevated privileges.

Privilege management

Privilege management products let IT define which processes users can elevate, ensuring systems are secure but still flexible to use. And unlike UAC, can assign the minimum number of privileges to processes and applications while leaving users with restricted access tokens.

Advanced features of privilege management products go further by allowing users to quickly and easily elevate processes, even when a policy hasn't been defined by IT, using a challenge/response system where IT provides the user with an authorization code. Such capabilities are important for supporting notebook users when they have no connection to the intranet.

Section PR.AT-2 states it should be the case that privileged users understand roles & responsibilities. A privilege management solution can be configured to allow users to elevate processes on request but also require that they justify their actions by providing a reason that's logged, increasing the likelihood that users take responsibility for activities performed using elevated privileges.

> "The Framework has established a meaningful way for Microsoft to discuss, assess, and refine our cybersecurity risk management maturity."
>
> J. Paul Nicholas, Microsoft Senior Director of Global Security Strategy and Diplomacy

Protective technology and data security

Application control (section PR.PT-3) is also an important layer in an organization's security defenses. While removing administrative privileges from users is a critical step, preventing users from executing code obtained from untrusted sources is also central in protecting system integrity and sensitive data.

Application control allows IT to determine which applications and processes users are allowed to run, using a whitelist to block anything that's not approved. Third-party Application control solutions improve on Windows Software Restriction Policies and AppLocker by integrating with other security products, making it easier to create and apply rules.

In addition to the requirements relating directly to least privilege security, there are others that indirectly rely on least privilege if they are to be implemented effectively. Protections against data leaks (section PR.DS-5) could involve using specialist data loss prevention (DLP) solutions designed to prevent company data from being intentionally stolen by employees or malicious actors. But restricting users' privileges significantly reduces the risk of a hacker being able to install software that could be used to steal credentials or sensitive data without the logged in user's knowledge.

Baseline configurations (section PR.IP-1) can be preserved for longer periods when administrative rights are removed from users because system-level settings can only be changed by an authorized member of IT staff, or by a user on request. Furthermore, security and configuration settings applied using Group Policy can be circumvented by administrative users. Application control also plays a role in maintaining baseline configurations by ensuring only the software approved for each build can be installed and run.

> "32% IT professionals are using application whitelisting techniques."
>
> Computing.co.uk, March 2016[1]

[1] Source: http://www.computing.co.uk/ctg/news/2452094/ninety-seven-per-cent-of-it-professionals-think-standard-antivirus-software-will-stop-zero-day-attacks

Sandboxing

In the knowledge that there is no such thing as 100% secure, isolating content in a sandbox allows organizations to protect data in cases where zero-day vulnerabilities may exist in installed products. While privilege management and application control can provide better protection than definition-based AV, sandboxing adds an additional layer of defense that isolates malicious code from other applications and user data.

When used together, least privilege, application whitelisting and content isolation solutions allow organizations to benefit from more secure and reliable systems where users and malicious actors aren't able to make unauthorized system-level changes, or run malicious code, that might lead to a compromise or instability. But, at the same time, users can work without relying on IT to perform tasks that require administrative privileges.

> "Less than 50% of respondents use standard tools such as patching and configuration to help prevent security breaches."

Cisco, 2015[2]

[1] Source: Cisco Annual Security Report 2015

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