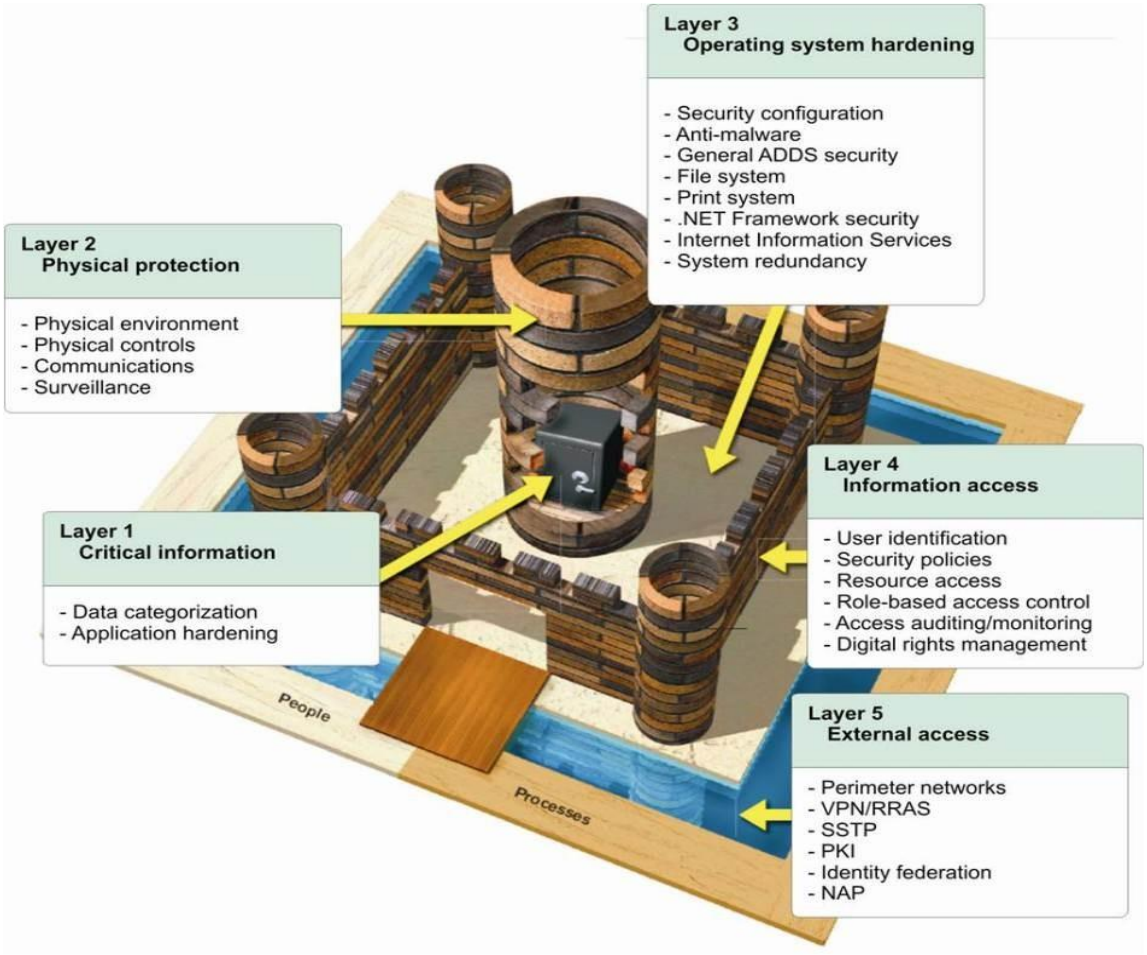
Reg. NIST / Data science 8V's / CIS 18 controls, MITRE ATT&CK / Kill-Chain & Zafepass Prevent & Protect.

Cyber-frameworks come in many variations – the main ones are NIST CSF, CIS, ISO, COBIT (ISACA), PCI, FedRAMP, CMMC – each with their own twist. Frameworks are extensive, often complex and require 'cyber-security expert and/or consultancy' guidance. Frameworks are used as A) control- and steering-tool and B) by the security-industry for evaluating Cyber-security exposure (risk, likelihood, impact (mainly financial) and to suggest mitigation actions.

Organisations try mitigate uncertainty, and these frameworks have grown, developed and adapted to IT-risk over 30-40 years. The last 5-10 years they have been challenged. Not only because they've grown in complexity, but also because the numbers of cyber-threats are exploding and now facing approx. 1,000 different KNOWN attack vectors, and according to the FBI and industry surveys, Cyber-criminals can 'break in' in less than 20 minutes – the slowest take less than 4 hours.

That's the reality.

The reactive approach to security is obsolete and is actually leaving organisations more exposed. IT is 'Defending the Castle' the best they can, but castles are expensive to build, maintain and defend – and therefore organisations are forced to prioritize the allocation of budget. Having a large IT/Sec.-team and unlimited budgets won't change things. All organisations are already or will be compromised within a 12-month cycle (PwC study).



Let's dive into the issues. If 'detect and response' e.g., Defending the Castle, and the use of control frameworks plus the many certifications and solutions – if that actually worked, would Cyber-crime be the third largest global economy (in revenue) and be able to destroy digital assets worth 8 trillion dollars on a global scale, here in 2023?

For a start, let's look at how the 8 V's in data science can be used to describe the challenges and characteristics of data, when applied to the field of cybersecurity? These V's can help explain the unique problems and considerations that arise in ensuring the security of data, users and systems:

1. **Volume**: In cybersecurity, the volume of data generated from various sources, such as logs, network traffic, and user activities, is massive. So are the Cyber-attacks. The challenge lies in efficiently storing, processing, and analysing vast amount of data to identify potential IoC's (indicator of compromise), threats and breaches without overwhelming security teams.
2. **Velocity**: Cyber threats and attacks occur at high speeds, requiring security systems to process and respond to incidents in real-time. The velocity of data generated by threat-detection, as well as the speed at which security solutions need to operate, play a significant challenge in a 99% reactive based detect and response model.
3. **Variety**: Data in cybersecurity comes in various forms, including structured logs, network traffic, unstructured text and more. This diversity makes it complex to integrate and analyse data effectively, requiring sophisticated techniques to identify patterns and anomalies across different data types.
4. **Veracity**: Data quality and accuracy are crucial in cybersecurity. Ensuring that the data used for threat detection and analysis is trustworthy and free from manipulation or corruption is a challenge. Attackers may attempt to insert fake or misleading data into systems to deceive security measures.
5. **Validity**: Validity refers to the reliability of data sources and the accuracy of collected information. In cybersecurity, the challenge is to ensure that the data being used to detect and mitigate threats is not compromised or tampered with, which could lead to false negatives or positives in threat detection.
6. **Volatility**: The threat landscape in cybersecurity is highly dynamic, with new attack techniques and vectors constantly emerging. Security systems need to adapt quickly to changing circumstances and be able to identify and respond to novel threats effectively.
7. **Vulnerability**: Data in cybersecurity often reveals vulnerabilities and weaknesses in systems, applications, and especially networks. Identifying and addressing these vulnerabilities asap is critical to preventing potential breaches and attacks.
8. **Value**: Can mean two things – the value of the breach (negative financial impact) – or the extraction of meaningful insights and actionable intelligence from cybersecurity data. This is challenging due to the complexity and often inaccurate interpretations. Ensuring that these insights are translated into effective security measures is an ongoing concern.

Zafepass Prevent & Protect leverage the 8 V's in the context of cybersecurity, turning them into an advantage for organizations to better understand the intricacies of managing and protecting their data and systems from evolving threats. The built-in methods for prevent, deter, obfuscate, deceive, mislead Cyber-attackers is creating an effective cybersecurity strategy that address these challenges and ensure data integrity, privacy and malicious activities to be successfully carried out.

As many organisations use CIS 18 (CIS Controls v8), this document provide insight about how the Zafepass Prevent & Protect platform help mitigate IT, OT and/or IoT challenges many organisations suffer from. Decentralizing strategies, new devices and resources in the network, cloud services,

access from anywhere, any device, via insecure networks – leaves IT-teams with little or no control, and you've probably heard IT-teams use the phrase – ***'don't fix it, if it ain't broken'***. It referred originally to the production and manufacturing environments – where the 'factory' is the heart of the business and 'operational disruption' is a NO-GO. All businesses are digital today. IT-disruption, often has massive financial impact. Zafepass Prevent & Protect has been designed to avoid exactly that – non-interruptive, non-invasive and non-intrusive implementation, and have made the "don't fix what's not broken" argument obsolete.

What is 'The Kill-Chain'

In order to bring it all together, we also have to talk about the Lockheed Martin defined Cyber Kill-Chain. The first one is 'Recon' and 'Weaponization' which together with 'Delivery' is pre-attack methods. It's in this section the Zafepass Prevent & Protect platform is delivering most of its magic. The MITRE ATT&CK framework is using the same "layout" and builds upon real attack-information collected from thousands of attacks. The majority of security solutions are designed to 'early detect and identification' – but as these warning systems are reactive, they are often too late – because its signature based – e.g., based on known threats and MITREs define the attack-methods as TTPs – Tactics, Techniques and Procedures. The threat-intel is gathered in global "warning-systems" and offered by subscription by the large Cyber-security companies. This is not optimal, but eventually Zero-day exploits are detected (can take months or years) – and they are still based on known-knowns. The unknown-knowns and unknown-unknowns are simply not possible to detect.

Zafepass Prevent & Protect is designed in a different way. Every MITRE ATT&CK TTP – all +350, has been thoroughly analysed and made more or less immune. We'll happily deep dive into these elements in workshops. As mentioned, there are more than +350 TTPs. Cyber-criminals collect as much information as they can before they start build their attack-tactic. This process can take months – but in the end – their objective is to make money (it's an industry), or destroy, gain knowledge, place misinformation etc.

Depending on who the Cyber-criminals are, they are probably under some kind of KPI. They gain information about the IT-setup and the more information about vulnerabilities the more effective and efficient their attack can be. The right tools are being used – and it could be there are only +350

TTPs – but CISA (the Cybersecurity and Infrastructure Security Agency, USA) has released reports with close to thousand known vulnerabilities that can be exploited. Hate to break it – but Microsoft is 'owning' +30% of them. The average time, Russian State-Sponsored Attackers need to breach a network is 18 minutes – from initial attack to laterally moving around the network. 'Cyber-criminals' come in many forms and shapes – some a very target-oriented and with specific tasks, others are politically motivated and then there's others who want to see the world 'burn'.

CIS-18 Control-Framework

CIS has been 'adopted' under NIST (Nat. Inst. of Standards and Technology, USA). CIS is a good and relatively simple tool, which can be used by any organisation. NIST made in 2022 a 'mapping' of the CIS Controls and Zero-Trust – which is inserted below. In the early 00's, 'Deperimeterisation security' was defined by The Jericho Forum in the UK – which later became 'The Open Forum' and ended up in CSA (Cloud Security alliance). In 2010, Forrester Research defined Zero-Trust – modelling the de-perimeterisation manifest. Both assume everything IS compromised and access should only be on a 'need-to-know' basis and a constant validation of 'privileges'.

More information can be obtained in the NIST/CIS/Zero-Trust framework called 'SP800-207' – and the 7 areas the CIS Controls and Zero-Trust is touching upon is:

(1) all data-sources and digital services are considered 'resources',

(2) all communication shall be secure/secured regardless of location,

(3) access to resources shall be granted on an individual per session basis,

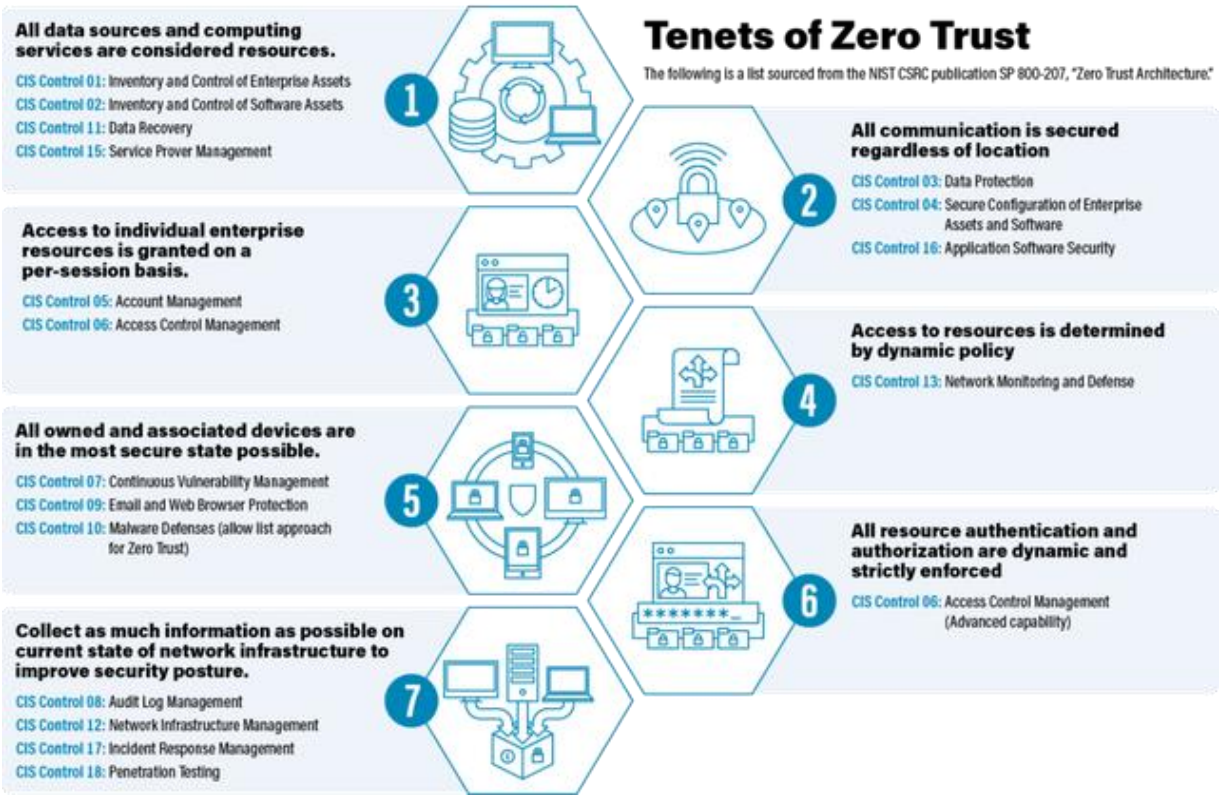
(4) access to resources should be determined by individual dynamic security policies,

(5) all devices should be in the most secure state as possible,

(6) all resource authentication and authorization are dynamically and automatically enforced– and

(7) collecting information from the environment to improve security posture.

Some of these relate well to the Zafepass Prevent & Protect platform – but as many of the Zero-Trust elements are tied to the network (which is what is most compromised) Zafepass brings a different dimension into these models. Remember why these controls are made – to make up for the flaws protecting the network (the Castle).



So how does Zafepass Prevent & Protect work with these Control-frameworks. Zero-Trust is per say not a framework – more a range of guidelines. Dealing with what Zafepass is, we have to introduce a range of other industry buzz-words.

SASE – Secure Access Service Edge. SSE – Secure Service Edge. SDP – Software Defined Perimeter. ZTNA – Zero-Trust Network Access. Zafepass Prevent and Protect is all of them, in one platform, and then added a range of other features and functions mot matched by anyone else.

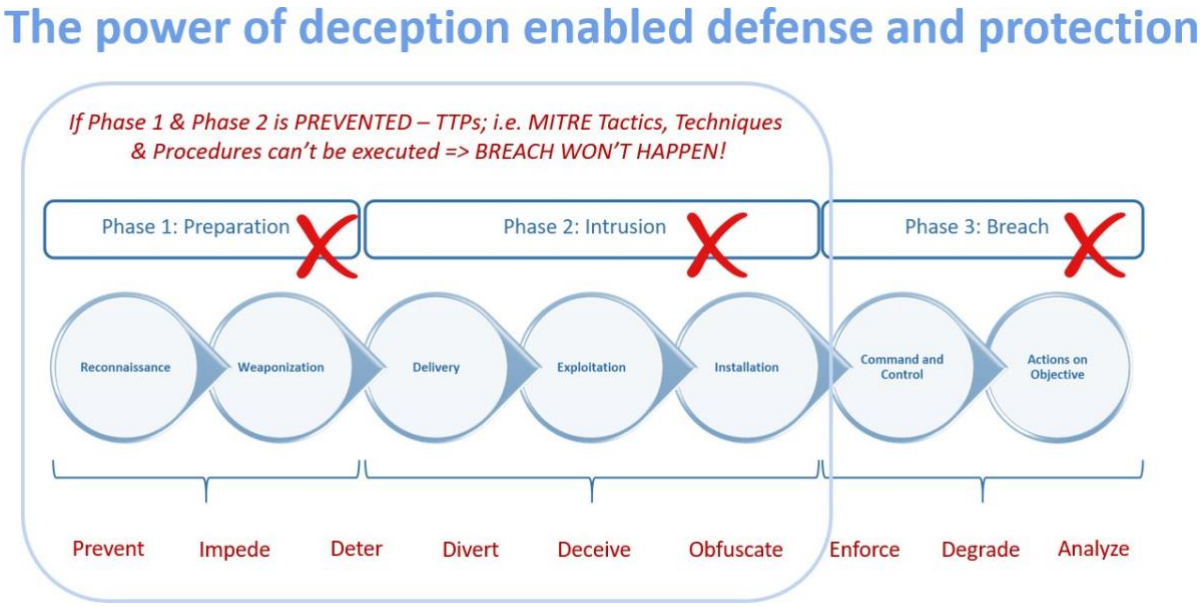
Zafepass Prevent & Protect is first and foremost an access solution with built-in guard-railed micro-perimeter-based security – a dynamic security policy engine that enforce the defined security policies around each session – automatically. Zafepass create the connectivity (Virtual Private Connectivity) between any given resource and any given (entitled) user. Zafepass 'isolate' the data, user, applications and services into "transport tunnel" leveraging the infrastructure and using the network as a simple "backbone". A resource is called a 'DAAS' element e.g., Data, Applications, Assets and Services. Every DAAS element has their own guard-railed micro-perimeter based security policy – which is not possible in 'detect & response' environments where Zero-Trust is implemented as an "add-on" in the security strategy.

Zafepass Prevent & Protect is rooted in the Deperimeterisation-manifest, and that results in many of the CIS Controls has no influence on the DAAS elements Zafepass manages. The 'kill-chain' issue is more or less eliminated as reconnaissance is not possible – implants are not possible either and malware can 'get in' -but has no effect because it can't communicate (spread) through Zafepass.

Therefore, more and more turn to Prevent & Protect based solutions and see them as much more efficient and effective – and these technologies should be phased in as soon as possible.

The strength in Zafepass Prevent & Protect

Zafepass Prevent & Protect eliminate every attempt (both inside and outside the existing perimeter) to collect information used for Cyber-attacks. Information from port- or network scans can't be retrieved. Code-injection, brute-force and lateral attacks cannot be performed and phishing attacks can only damage the user's device – not the data Zafepass handles, not the sessions and not the backend systems. The mal- or ransomware can be delivered – but cannot connect to the outside world through Zafepass. Thereby these attacks remain detained and related only to the user-device – but not the data Zafepass guards on the user-device. There are many other elements of security in modern Prevent & Protect solutions, and we're always open for a dialog about these.



Zafepass Prevent & Protect is designed to prevent, obstruct, deceive, deter, impede and obfuscate everything a Cyber-criminal need for planning a Cyber-attack. It's extremely hard if not impossible to successfully breach an organisation using this kind of technology. Therefore, it has a huge impact on the control-frameworks used- and below there is a high-level overhaul of every single CIS Control.

The marks Red, Yellow or Green indicates the impact Zafepass will have on the particular control when fully implemented.

CIS 01: Inventory & Control of Enterprise Assets. (Yellow)

Zafepass has indirect impact. All 'Enterprise Asset' can be configured to become a validation factor leveraging the guard-rail based security policy engine – "***Attribute based Access, Communication & Identity Control***". Zafepass has no influence on the inventory element – except they are listed in the access logs with the needed attributes automatically retrieved by Zafepass.

CIS 02: Inventory & Control of Software Assets (Green)

Zafepass has major impact on this control, as all 'Software Asset' can be managed (controlled) by, and fully protected using the guard-railed micro-perimeter based dynamically enforced security policy engine. When a Zafepass Gateway (reverse dual proxy) is installed in front of a resource (DAAS element) – this assed will only be accessible from the Zafepass access provided to an entitled user. A software asset can also be a validation factor using for instance the serial-number as an attribute in the "***Attribute based Access, Communication & Identity Control***" module. Zafepass has no influence on the 'inventory'.

CIS 03: Data Protection (Green)

Zafepass has major impact on this control. As DAAS elements is configured to 'operate' through the Zafepass environment – they become fully protected. No non-intended will be able to "gain" access to a DAAS element or the session being in use. Data can be "stolen" in transit, but as the Zafepass environment use a special method for encryption and there is no use of 3rd party certificates – the information will be useless and it will take some time to decrypt a 4,096bit key randomly generated.

CIS 04: Secure Configuration of Enterprise Assets and Software (Yellow)

Zafepass has both direct and indirect impact on this control. Zafepass itself is designed for "secure access to the provisioning console". Zafepass DAAS elements don't have to be 'securely configured' as the resource cannot be accessed by any non-entitled users. The access isn't vulnerable to Man-in-the-Middle attacks of alike.

CIS 05: Account Management (Green)

Zafepass has direct influence on this control. Users and Account management can be managed through MS Active Directory and synchronized with Zafepass. After synchronization the AD can actually go 'off-line' without any user is affected. It is possible (and recommended) that external 3rd party user access is configured directly in Zafepass. This means the organisation own employees are isolated from external stakeholders (they can, but don't have to be managed in the AD or other user management systems). As Zafepass don't work with privileges – users 'only' has configured and controlled access to resources (DAAS – element) og there are no possibility to elevate any rights.

CIS 06: Access Control Management (Green)

Zafepass has direct influence on this control with its extreme secure access to resources using the Zafepass VPC (Virtual Private Connectivity).

CIS 07: Continuous Vulnerability Management (Yellow)

Zafepass has both direct and indirect impact on this control and is designed to eliminate attack surfaces. The percentages are very high, but determined by the implementation of Zafepass and other vulnerabilities in the infrastructure. A Zafepass DAAS element doesn't have to be securely

configured – as the resource cannot be accessed from unentitled users. The way to compromise a Zafepass user, is to physically take over the keyboard. A copied Zafepass VPC client and even having the right login credentials will not provide access – and cannot be brute-force attacked either.

CIS 08: Audit Log Management (Yellow)

Zafepass has both direct and indirect impact on this control. Everything transaction in Zafepass is logged. In another context – an ISO re-certification has proven to been very fast for Zafepass clients, as access and security is detailed, specific and consistent.

CIS 09: Email and Web Browser Protection (Green)

Zafepass has both direct and indirect impact on this control. Depending on configuration, a Zafepass gateway can be installed in front of a resource 'handling' e-Mail. Some browser based applications allow for direct access – which makes it pointless to use Zafepass for "containerizing" the browsers individual windows. It is of course possible to operate for instance Salesforce (or other SaaS based services) through Zafepass, but it has to be evaluated what additional security it provide.

CIS 10: Malware Defences (Green)

Zafepass has direct influence on this control. Mal- and ransomware will NOT be able to communicate with the external "server" which it needs for actioning on the objectives. Non-Zafepass software WILL NOT be able to communicate with the Zafepass Gateway.

CIS 11: Data Recovery (Red)

Zafepass has basically no impact on this control. Potentially an indirect influence, as Zafepass has encrypted storage areas only accessible via Zafepass that cannot be accessed by any non-entitled user or any external software – also in the cloud (data at rest). Recovery refers to a different topic – and Zafepass is an access solution.

CIS 12: Network Infrastructure Management (Yellow)

Zafepass has no or maximum indirect influence on this control. The reason for the YELLOW status is that Zafepass is NOT dependent on vulnerabilities in the infrastructure. However, it must be noted that infrastructure is the means of transport for the communication that takes place between users and resources. If the infrastructure is hit by an outage, Zafepass will halt communicating, and when the connection is re-established, communication will continue where it halted.

CIS 13: Network Monitoring and Defence (Green)

Zafepass has a direct influence on this control, since Zafepass removes a large number of attack surfaces, monitoring and the "Detect & Response" part will become far more effective and efficient. This corresponds to the haystack becoming 90 times smaller, thereby the needle can be located much faster and thereby have a major influence on "dwell time".

CIS 14: Security Awareness and Skills Training (Green)

Zafepass has direct influence on this control. Users cannot compromise Zafepass or the resources it controls. In order for a user to be compromised, an attacker must know an unknown number of individual attributes (not likely). Furthermore, each individual session leverage never-reused

'Zafepass certificates'. Awareness- and skills-training can therefore be limited, as users can only execute and use what is displayed in their “Zafepass launchpad”.

CIS 15: Service Provider Management (Green)

Zafepass has a direct influence on this control. There are three primary Zafepass application areas. The "Zafepass license owner" who has the provisioning console access - controls all resources (DAAS element), users and their access.

(1) An organization having the Zafepass "site license" can choose any Service / Cloud providers who will NOT be able to understand (in readable format) the data that is stored / handled in the Zafepass environment.

(2) An organization can choose to let a service provider handle the Zafepass "site license" as a kind of managed service / hosting.

(3) A service provider (ala MSP) that handles a Zafepass "site license" can offer "full managed service including "SECURITY-AS-A-SERVICE".

CIS 16: Application Software Security (Green)

Zafepass has a direct influence on this control. All resources handled by Zafepass will ONLY be made available to entitled users via guard-railed micro-perimeter-based security policy enforced access. It is highly unlikely that anyone un-entitled will be able to compromise a Zafepass protected resource.

CIS 17: Incident Response Management (Green)

Zafepass has a direct influence on this control. Since 90% of all incidents are likely to disappear this reduction results in less IoCs to be analysed. Those alerted should be faster analysed and the IT team can focus on faster mitigation.

CIS 18: Penetration Testing (Green)

Zafepass has a direct influence on this control. The following is recommended. Perform a pen-test and network-scan pre and post implementing Zafepass. If applicable, do the same for every resource element that Zafepass should handle. Not for Zafepass’ sake, but it will provide an audit document that can be used for the organisation’s stakeholders, regulators and compliance auditors.

See previous description of Zafepass under the point "the strength of Zafepass Prevent & Protect".

Zafepass works flawlessly in both IT, OT and IoT environments and can solve a number of GRC, GDPR and NIS related challenges "out-of-the-box".

These links provide additional information about the functionality and why the Zafepass Prevent & Protect platform has been designed as it has.

https://zafehouze.com/approach/the-why-what-and-how

https://zafehouze.com/about/guard-railed-cyber-security

https://youtu.be/zi5n1v88slM

Glossery / Appendix

NIST	- National Institute of Standards & Technology
CIS	- Centre for Internet Security
DAAS	- Data, Application, Asset and/or Service
MSP	- Managed Service Provider
SP	- Service Provider – cloud services, managed services, internet services etc.
Dwell-Time	- The time an attacker is active on a network without being detected/eradicated
ISO	- International Organization for Standardization
COBIT	- Control Objectives for Information Technologies (ISACA) (IT-Governance)
Gateway	- In Zafepass it means a “Reverse Dual Proxy” – an instrument handling client request to the appropriate backend resource (DAAS-element) providing an abstraction layer incl. control ensuring covert handling, scalability, performance, resilience and security.

If you need further information, feel free to contact the Zafehouze main-office;

Zafehouze ApS, Langebjerg 1, 4000 Roskilde.

https://zafehouze.com

Email: info@zafehouze.com