WithSecure Elements Infinite
and CIS Controls Cybersecurity Compliance Framework

With Elements Infinite, our customers can achieve compliance quickly and meet industry standards. One of these compliance frameworks is the Center for Internet Security (CIS) framework. WithSecure Elements Infinite service helps fulfil CIS safeguards in overall seven different CIS control domains. This table contains information on these CIS control domains and descriptions of the different asset types and security functions and how Elements platform and Elements Infinite service steps in.

CIS Controls™ Version 8.1

CIS Domain	Asset Type	Security Function	CIS Framework Description	WithSecure Elements Infinite
01	Devices	IDENTIFY **1.1 Establish and Maintain Detailed Enterprise Asset Inventory**	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	**WithSecure Elements Infinite** provides means to regularly scan and inventory both external and internal assets on the networks.
		DETECT **1.3 Utilize an Active Discovery Tool**	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	
02	Software	IDENTIFY **2.2 Ensure Authorized Software is Currently Supported**	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Using device profiles, one can fulfil the technical capability to restrict what software is allowed to be installed and executed for a device group. Profiles can also be used to give certain devices documented exceptions to organisations allow lists. One can also restrict both what libraries and scripts are allowed on a device using device profiles. Restrictions can be based on digital signatures, versions, naming and more.
		RESPOND **2.3 Address Unauthorized Software**	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	
		PROTECT **2.5 Allowlist Authorized Software**	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	
		PROTECT **2.6 Allowlist Authorized Libraries**	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	
		PROTECT **2.7 Allowlist Authorized Scripts**	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	
04	Devices	PROTECT **4.4 Implement and Manage a Firewall on Servers**	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	**WithSecure Elements** template enable the use of firewall profiles that make special firewall rules for different device classes possible and automated. For a certain device profile, one may configure both port and service-based rules.
		PROTECT **4.5 Implement and Manage a Firewall on End-User Devices**	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	
		PROTECT **4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software**	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	
07	Software	PROTECT **7.3 Perform Automated Operating System Patch Management**	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	**WithSecure Elements Infinite** automatically identifies OS and application vulnerabilities together with recommended patches. In addition, it will also give prioritized recommendations based on business criticality, severity and if asset is present in critical attack paths in the environment. Both internal and externally exposed assets may be scanned. Patching and general software update for both OS and 3rd party applications can be automated or partially automated depending on business need.
		PROTECT **7.4 Perform Automated Application Patch Management**	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	
		IDENTIFY **7.6 Perform Automated Vulnerability Scans of Internal Enterprise Assets**	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.	
		IDENTIFY **7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets**	Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.	
		RESPOND **7.7 Remediate Detected Vulnerabilities**	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	
09	Software	PROTECT **9.1 Ensure Use of Only Fully Supported Browsers and Email Clients**	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	**WithSecure Elements** application control can restrict the use of webbrowsers and email clients that can be run on local device. Further more, multiple levels of URL restrictions may be put in place depending on organizational need.
	Network	PROTECT **9.3 Maintain and Enforce Network-Based URL Filters**	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	
10	Devices	DETECT **10.1 Deploy and Maintain Anti-Malware Software**	Deploy and maintain anti-malware software on all enterprise assets.	This domain is covered in full by the **WithSecure Elements Infinite** service. Anti malware software is an integral part of the domain and is continuously updated. **WithSecure Elements** supports extensive control and scanning of USB or alternatively attached storage, including automatic file execution. All aspects of **WithSecure Elements** is centrally managed through Elements Security Center. For anti-exploitation **WithSecure Elements** provides features, including behaviour-based, such as DeepGuard, DataGuard, Rollback, XFence (macOS) where data can be safeguarded from encryption, and it can even spot zero-day malware.
		PROTECT **10.2 Configure Automatic Anti-Malware Signature Updates**	Configure automatic updates for anti-malware signature files on all enterprise assets.	
		PROTECT **10.3 Disable Autorun and Autoplay for Removable Media**	Disable autorun and autoplay auto-execute functionality for removable media.	
		DETECT **10.4 Configure Automatic Anti-Malware Scanning of Removable Media**	Configure anti-malware software to automatically scan removable media.	
		PROTECT **10.5 Enable Anti-Exploitation Features**	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	
		PROTECT **10.6 Centrally Manage Anti-Malware Software**	Centrally manage anti-malware software.	
		DETECT **10.7 Use Behavior-Based Anti-Malware Software**	Use behavior-based anti-malware software.	
13	Devices	DETECT **13.2 Deploy a Host-Based Intrusion Detection Solution**	Deploy a host-based intrusion detection solution+F29 on enterprise assets, where appropriate and/or supported.	**WithSecure Elements Infinite** delivers an MDR service based on the EDR product. This EDR will both detect and enable response actions to be taken by WithSecure Detection & Response team. In addition, three important functions, WithSecure Threat Intelligence, Incident Response Team and the Detection & Response Team are collaborating to tune and evolve the EDR alerting to match the current and future threats.
		PROTECT **13.7 Deploy a Host-Based Intrusion Prevention Solution**	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	
	Network	DETECT **13.11 Tune Security Event Alerting Thresholds**	Tune security event alerting thresholds monthly, or more frequently.	