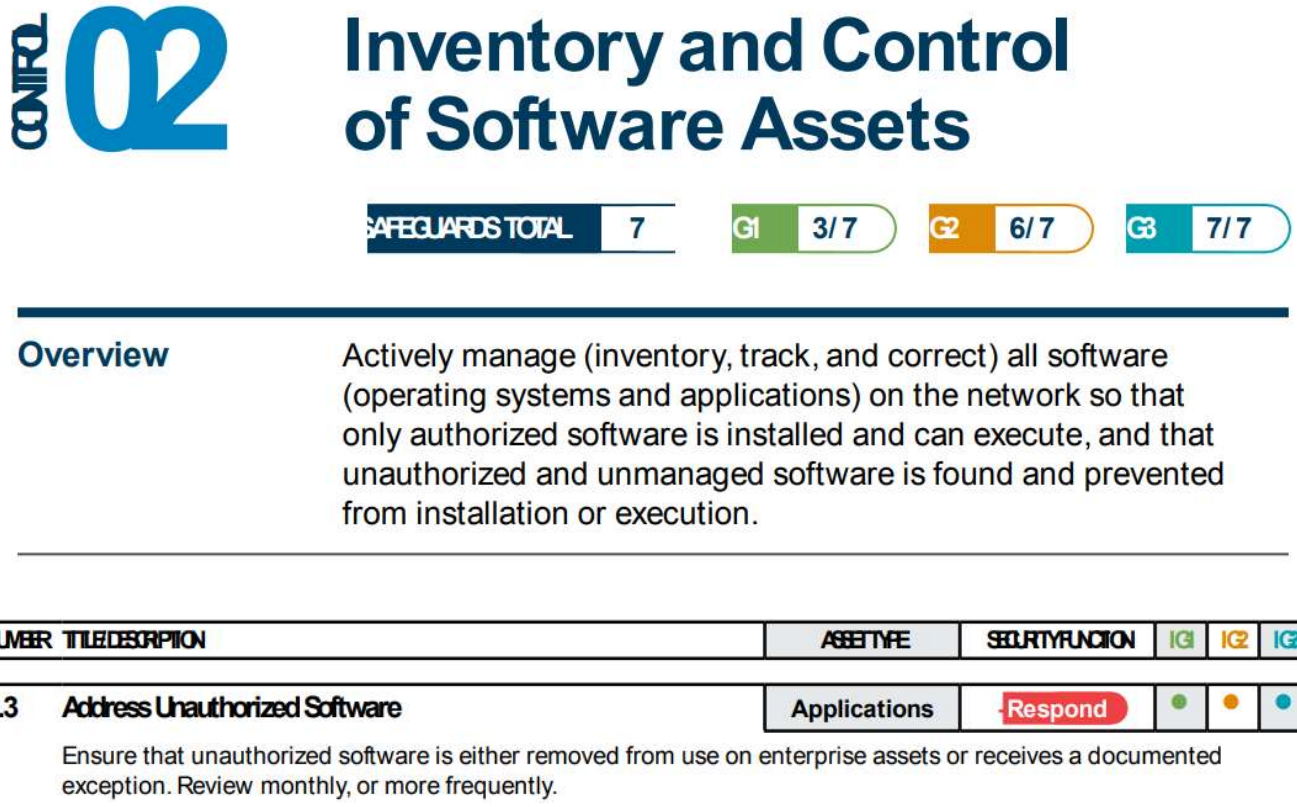
CHECK POINT
YOU DESERVE THE BEST SECURITY

CIS Controls & Avanan



CONTROL 02

Inventory and Control of Software Assets

SAFEGUARDS TOTAL	7	G1	3/7	G2	6/7	G3	7/7

Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.3	**Address Unauthorized Software**	Applications	Respond	●	●	●
	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.					

Avanan + 2.3 Address Unauthorized Software

Avanan monitors Shadow IT by looking for emails from 3rd party unapproved applications. When an end user uses an unauthorized 3rd party app, there is a trail in their email: welcome emails, password resets, notifications, ect. Avanan looks for these emails to alert the admin what 3rd party software is being used.

CHECK POINT
YOU DESERVE THE BEST SECURITY

CONTROL 03 Data Protection

SAFEGUARDS TOTAL	14	IG1	6/ 14	IG2	12/ 14	IG3	14/ 14

Overview Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.13	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●
3.14	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●

Avanan + 3.13 Deploy a Data Loss Prevention Solution

Avanan allows you to enforce a DLP policy within the email environment to alert and/or prevent sensitive data from entering or leaving the network.

Avanan + 3.14 Log Sensitive Data Access

Avanan stores logs of who is sending and receiving sensitive data. User Management roles control access to sensitive data and Audit logs show user interactions within the platform.

CHECK POINT
YOU DESERVE THE BEST SECURITY

CONTROL 09 Email and Web Browser Protections

SAFEGUARDS TOTAL	7	IG1	2/7	IG2	6/7	IG3	7/7

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.6	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●
9.7	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●

Avanan + 9.6 Block Unnecessary File Types

Avanan can block attachments by file type as defined in the Anti-malware block list rule.

Avanan + 9.7 Deploy and Maintain Email Server Anti-Malware Protections

Avanan uses over 300 AI indicators to protect against malware, including attachment scanning and sandboxing. It relies on ThreatCloud, the largest data lake of threat intelligence in the world to understand with extreme detail and nuance the ever-evolving threats hitting the inbox.

