SOLUTION BRIEF

oomnitza

Ensuring Compliance with CIS Critical Security Controls

Maintain accurate inventory controls for hardware, software and cloud assets to enforce CIS compliance

In the realm of cybersecurity, adhering to the Center for Internet Security (CIS) Controls is a best practice for IT organizations. The first two CIS controls stress the importance of inventory and control of hardware and software assets, which play a fundamental role in safeguarding an organization's digital infrastructure.

These controls mandate that you must maintain an accurate and up-to-date record of all technology assets that are connected to your environment, capable of storing or processing data, or involved in data transmission. These requirements are essential for identifying potential vulnerabilities, managing security patches, and preventing unauthorized access.

CONTROL 01

Actively manage (inventory, track, and correct) all **Hardware** assets (including unauthorized and unmanaged), connected physically, virtually, remotely, and within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.

CONTROL 02

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.

Failure to maintain proper inventory controls can lead to severe consequences, including security exposures, operational disruptions, financial penalties and reputational damage. Unfortunately, modern enterprise environments, characterized by hybrid and remote work, cloud services, and mobile technologies, have added layers of complexity to maintaining accurate inventory controls and good technology data hygiene.

Traditional IT Asset Management (ITAM) and CMDB-based solutions usually fall short in addressing this evolving technology landscape. Often, IT teams resort to manually pulling information from multiple sources, aggregating it painstakingly via spreadsheets, and contacting users to reconcile duplicate entries or populate gaps.

Challenges

- Keeping up with the fast pace of adoption of diverse devices, SaaS apps and cloud services
- Tracking and managing assets across remote workforce and growing number of locations
- Resource and cost overruns in obtaining and compiling technology inventory data
- Friction between IT and GRC teams due to poor inventory management and inaccurate compliance reporting

Benefits

- Single system for tracking all technology assets across hardware, software and cloud services
- Confidence in CIS inventory controls and compliance policies being met
- Better audit accuracy, efficiency and timeliness with automated workflows to streamline audit preparation tasks
- Cost savings by reducing manual effort, human error and the need for resource intensive IT projects
- Reduced risk of audit fines and failures
- Improved alignment and collaboration between IT and GRC teams

Ensure CIS compliance through rigorous inventory controls

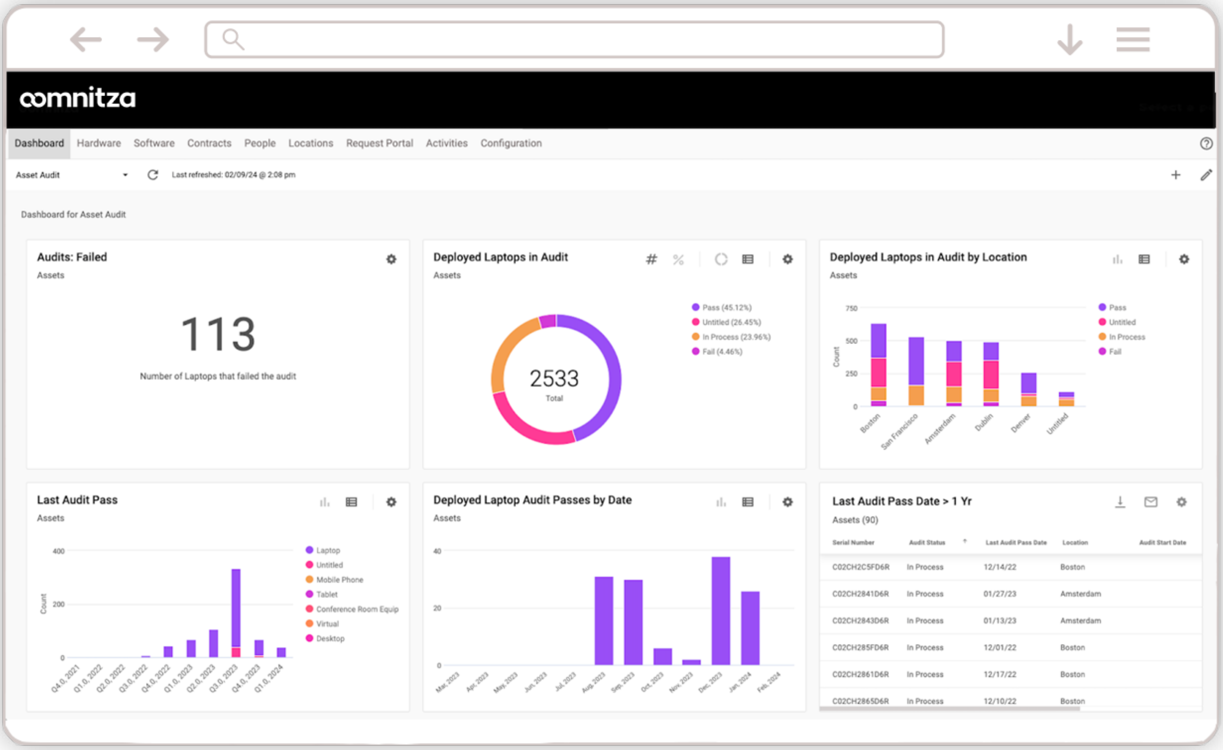
To enhance the accuracy, efficiency and timeliness of compliance with CIS inventory controls you need to embrace improvements in tools, processes and automation.

Enterprise Technology Management (ETM) solutions provide an integrated platform to manage and monitor your complete technology landscape. This proactive approach ensures compliance with CIS inventory controls as well as other industry standards/frameworks, while also improving your overall security posture.

ETM solutions address the needs of today's dynamic technology environments, overcoming the limitations of traditional ITAM and CMDB solutions by providing:

- Centralized inventory of all technology assets by leveraging existing tools and installed agents for comprehensive coverage, ensuring no asset goes untracked.
- Low-code/no-code workflows and pre-packaged workflow applications that are easily configured for your needs, to assess compliance, remediate issues and automate audit preparation tasks.
- Connector integrations with 160+ IT, security and business systems to discover, aggregate, normalize and enrich technology data for single-source audit data.

> "Oomnitza has empowered us to maintain continuous IT compliance with SOC 2 and CIS frameworks, while automating complex IT processes like technology refresh cycles and employee offboarding — all courtesy of its powerful and intuitive workflow engine. Additionally, Oomnitza's comprehensive aggregation of technology asset data has bolstered our position as a trusted partner to key stakeholders, including our security team, enhancing collaboration and reinforcing our commitment to operational excellence."
>
> **Alexander Jasanovsky**
> **Manager, Productivity Tools**
> ***priceline.com***



Serial Number	Audit Status	Last Audit Pass Date	Location	Audit Start Date
C02CH2C5FD6R	In Process	12/14/22	Boston	
C02CH2841D6R	In Process	01/27/23	Amsterdam	
C02CH2843D6R	In Process	01/13/23	Amsterdam	
C02CH285FD6R	In Process	12/01/22	Boston	
C02CH2861D6R	In Process	12/17/22	Boston	
C02CH2865D6R	In Process	12/10/22	Boston	

oomnitza

Learn more at
www.oomnitza.com

© 2024 Oomnitza, Inc. All rights reserved.
All trademarks are the property of their respective owner(s). 02/24