CyberMDX

DATASHEET

CyberMDX Control Center

Define rules to put asset management, policy validation, compliance alignment, and asset tracking on autopilot.

CyberMDX Control Center is a flexible framework within the CyberMDX Healthcare Security Suite for asset tracking and management, policy validation and incident response. What's more, it's constantly updated with additional filtering and triggering capabilities, enabling almost unlimited creativity when defining custom policies and workflows.

Full-Featured Policy Engine

The CyberMDX Control Center is how smart healthcare organizations make the most of available technologies. Save labor and increase the accuracy and ability to update by converting daily user routines into automated rules. Powered by our flexible, rule-based policy engine, the CyberMDX Control Center enables you to fine-tune and customize the system behavior by defining granular rules and policies. Easily review, validate, and enforce the policies underpinning digital governance across your entire organization.

Command Control for Your Security and Policy

Let CyberMDX Control Center work for you – define rules/policies to put asset management, policy validation, compliance alignment, and asset tracking on autopilot.

Create custom rules or choose from pre-defined best practices. Rules can be based on various asset or network attributes (such as asset type, location, risk level, detected vulnerabilities, and much more) or behavior (such as communication with a high-risk country).

Simplify Compliance Alignment

- More than 100 cyber security framework (NIST, CIS, HITRUST) best practices out of the box.

Auto-Pilot Policy Validation

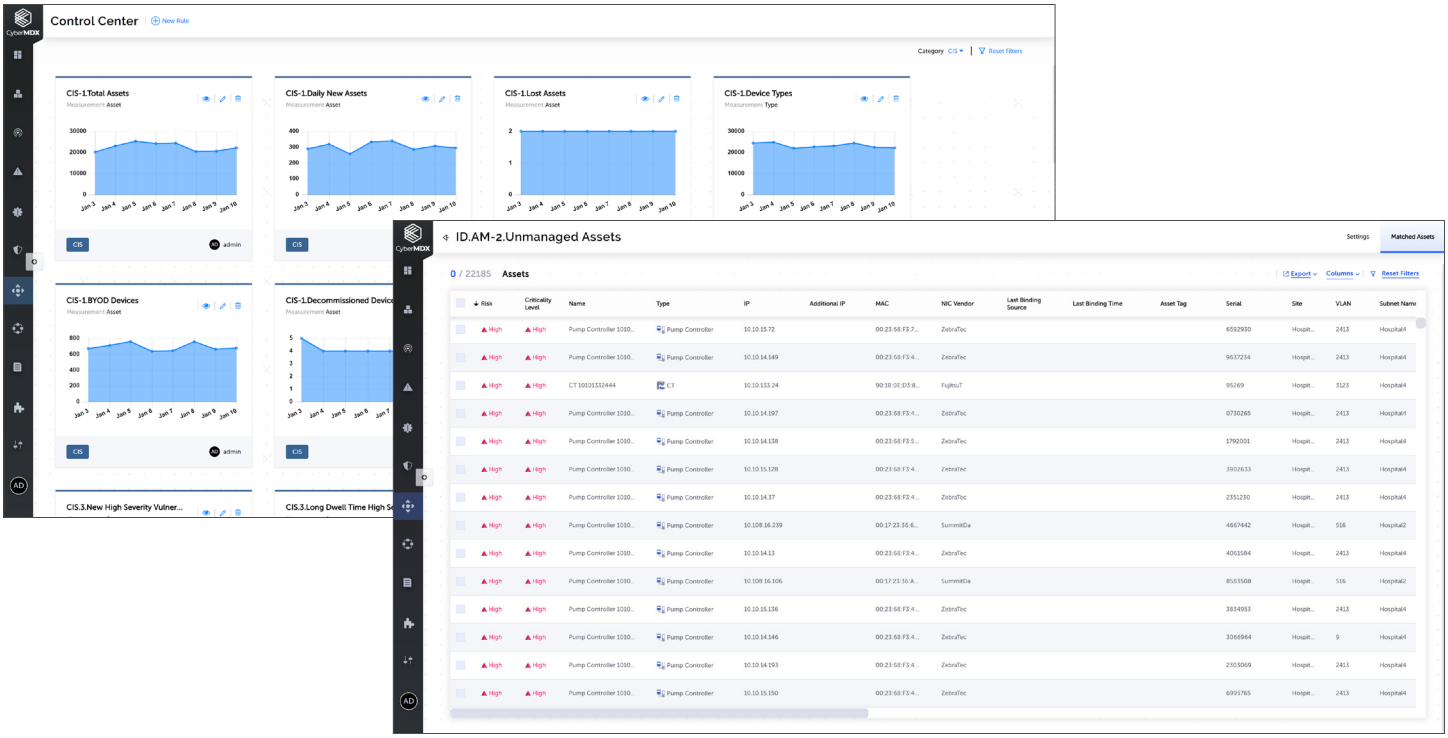
- Automate tracking of policy violations and incident response.

Flexible User Experience

- Customize the experience per your preferences, including dashboard, custom attributes, and custom tags.

Track all matching assets in real time. Zoom in on a specific set of results for more in-depth investigation.

Decide whether you want only a visualization of matching results, or additional actions that will be triggered by them. For example, creating tickets, sending email notifications, modifying asset attributes, implementing a smart security policy, and more.



Through the Control Center, CyberMDX users can easily review, validate and enforce the policies behind the digital governance across your entire organization, including:

- Limiting unsecured protocols between IoT and medical devices to strengthen segmentation
- Assuring firewall enforcement to block unencrypted traffic to and from forbidden IP locations
- Quarantining devices with malicious activity
- Tracking imaging device utilization by location and/or department