SYXSENSE®

Feature sheet

REMEDIATION MANAGEMENT

Automated Security Policy Validation and Enforcement

The first step in preventing a breach is identifying the devices in your network that are at risk, but a successful cybersecurity strategy also includes eliminating those vulnerabilities. By detecting and containing vulnerabilities before they spread within your network, you can prevent breaches that could harm your business.

Syxsense identifies and remediates vulnerabilities with a single agent. Using Syxsense's solution-driven platform, you can identify your target devices and decide what to do with them, when and how often.

Queries

Syxsense Queries are a powerful method to filter both inventory and available patches based on conditions you set. As items or values change status, queries are dynamically updated to give you greater control over organizing, prioritizing and grouping your inventory and applying patches.

Queries eliminate the need to apply filters or manually select items. You can safely deploy knowing that the queried results meet your deployment conditions. Device Queries can filter based on inventory attributes and values, such as:

- Operating system (OS)
- Connected devices
- Installed software
- Device Health
- Devices requiring critical updates
- And more

Tasks

Tasks in Syxsense provide real-time data on the status of every device in your environment during scans and deployments.

The Task Status is updated every few seconds with a progress bar and a complete overview of the devices that successfully completed the task, are waiting or partially completed the task, or that failed to complete the task.

Tasks drive actions in Syxsense to give you comprehensive control over your environment monitoring and security. Task options are entirely customizable and flexible enough to target a single device or a group of devices within a specific timeframe set by you, with extensive end user delay and reboot options.

Syxsense also enables software installation or rollback actions through application deployment or custom script files. You can initiate standalone tasks, recurring tasks, or complex task sequences with Syxsense's Cortex automation engine.

Policies

Policies transform tasks into protocols to create truly intelligent endpoints. Policies run continuously on the client based on conditions you set and send the information back to your Syxsense console. Once deployed, the policy is triggered locally even if the device is offline at the time it occurs, and the results are communicated and updated in Syxsense immediately as the device comes back online.

With Syxsense Policies, you create self-aware and self-managing devices that run tasks independently based on the triggered conditions you set. Automated policies reduce the time it takes to scan the health of a device and initiate remediation tasks to secure the device from found threats.

For remote IT teams, this provides the control of on-premise device management and eliminates wasted time between health scans and threat remediation as devices on your network come online.

Device quarantine

Quarantining devices is integral to maintaining your environment's security. Syxsense detects unknown devices entering your network as well as non-compliant devices returning to the network. Device communication is cut off until the device is back in compliance. This safeguards access to company data and resources.

Syxsense also quarantines devices when it detects suspicious processes running on them. Immediately segregating the device and cutting off communication prevents the malignant process from spreading through other devices on your network.

Security remediation

The time between identification and containment of a vulnerability can have a significant impact on the amount of damage a threat can do to your environment. The longer it takes to contain, the more harm it can do to your business, both in financial cost and reputational damage.

Syxsense provides real-time data on the status of your whole environment, as well as each device in your network. It identifies and alerts you to any attack vectors present in your network and ensures you can resolve them, from a single console with a single agent.

Get your endpoint management under control and mitigate cybersecurity risks.

Schedule a demo.

www.syxsense.com info@syxsense.com +1 949 270 1903

SYXSENSE®