SYXSENSE®

CORTEX AUTOMATION

Instant detection and response with intelligent automation.

Every year, cyber threats grow in number as well as sophistication, increasing the strain on IT budgets and resources. Administrators need to keep aware of emerging global threat intelligence while constantly monitoring and analyzing the attack vectors inside of their own network.

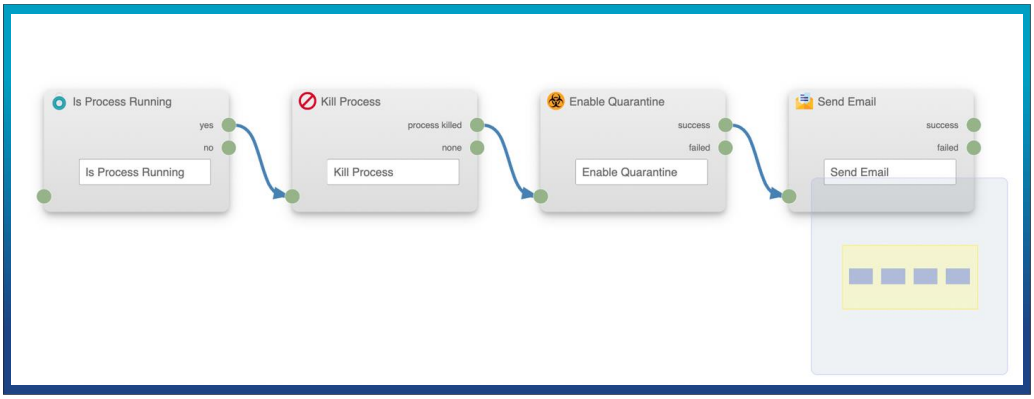
In addition, attack surfaces expand as people transition to remote or hybrid work and as more organizations allow employees to work on personal devices. This means more endpoints to manage outside the network and even more potential for a breach if a system is overlooked.

SYXSENSE CORTEX

Syxsense's Cortex task sequencing and automation engine reduces this burden more effectively and rapidly eliminates threats to your systems. It's a powerful, no-code interface for IT and security teams to easily perform complex, automated jobs with a drag-and-drop interface.

Cortex utilizes hyperresponsive receptors to gather data on behavioral and state changes on your endpoints and transmits that information to your Syxsense console in real-time. This data is then used to initiate complex workflows that respond to any detected changes, so you can protect your systems with faster detection, intervention, and elimination of security threats, without the need for large teams or specialists.

Data such as vulnerability state, network location, software installations, processes running, and more, trigger Cortex's Workflow Processor. The real-time, two-way communication between devices and the Syxsense console creates intelligent endpoints by predicting behaviors and executing protections faster. With Cortex, you can identify, detect, protect against, and respond to threats faster and more effectively.

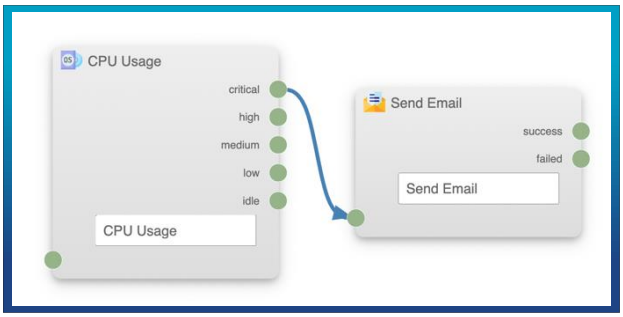


The countdown to a security breach begins the moment a threat enters your network. With Cortex, you can systematically collect accurate data on your endpoints in real-time and instantly respond when a change is detected.

Cortex allows you to monitor your endpoints and identify and remediate security threats without constant human intervention. You can automatically deploy complex workflows, without any scripting required.

With Cortex, you can:

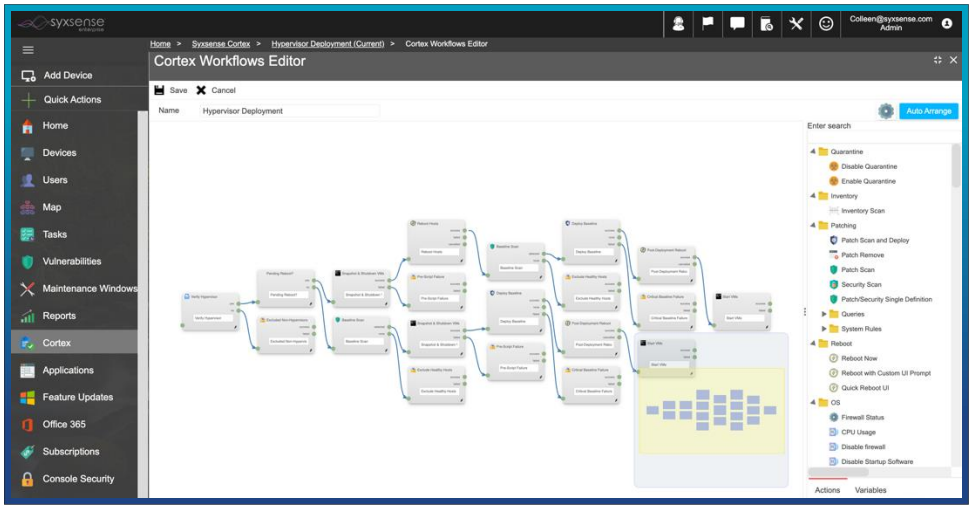
- Immediately detect devices as they enter your network, quarantine them, run Patch and Security scans, deploy patches, verify their health status, and return devices to full privilege.
- Monitor CPU, RAM, and disk usage space triggers that alert you to critical spikes.
- Run PowerShell scripts, send automated email approvals, scan, deploy, reboot, and run cleaning scripts.
- Silently check for installed software and upgrade or install new versions.



For more information on comprehensive vulnerability and remediation management with Syxsense, check out our guides to Patch Management, Security Management, and Remediation Management.

VISUAL WORKFLOW DESIGNER

Cortex simplifies complex IT processes with a drag and drop interface that requires no scripting to implement. You can deploy pre-built templates or design custom multi-step task sequences in the Cortex engine.



To use custom scripts, Cortex utilizes a visual user interface that allows you to upload scripted actions in Syxsense and add them to your Cortex workflows, without the need to script the entire sequence.

ESSENTIAL QUESTIONS

What triggers automations?

- Changes to a device state as defined in custom policies
- Time and date or opening of a Maintenance Window
- Network changes
- Security group changes

Can you require one or more approvals as part of an automation?

Can automations be logic-based?

- Does it have diskspace?
- Is the device a server?
- Is the device a Mac?

Does the solution provide or publish pre-built automations?

Is scripting knowledge required?

Can you see where endpoints are in the automation flow in real-time?