SYXSENSE®

CASE STUDY

How EECO Addresses Vulnerabilities With Syxsense

Background

EECO, an electrical distributor with more than 300 employees across a dozen locations, specializes in Industrial Automation and power solutions, delivering high-quality products to manufacturing plants, machine builders, and construction teams.

Challenge

After years of inconsistent service with other services and solutions, while facing increasingly urgent security threats, EECO sought a single endpoint management and security solution that would enable them to improve support to their distributed employees across several states and face the challenge of remediating critical vulnerabilities such as Follina.

Solution

EECO used Syxsense to manage hundreds of endpoints: delivering patches and Feature Updates without having to rely on end users. After faing multiple critical vulnerabilities from PrintNightmare to Follina, EECO turned to Syxsense to improve their endpoint security. EECO upgraded to Syxsense Enterprise to leverage its unique Cortex automation and pre-built vulnerability scripts to push configuration changes to devices over the cloud. They now use Syxsense as part of a unified management and security approach, utilizing tools such as the vulnerability scanner to verify results and findings, automated Feature Updates, and real-time device reporting to ensure the security of their endpoints.

How to Manage and Secure Corporate Devices Across Multiple States

The six-person IT Operations team at EECO supports the enterprise infrastructure of 12 locations across the southeastern US staffed with 300 employees. Up until 2021, the company outsourced management of its networking, server maintenance, and endpoint management to managed service providers (MSPs). However, with consolidation across the MSP market, EECO ultimately chose to bring this management in-house to improve visibility and business operations.

With Syxsense Enterprise, EECO:

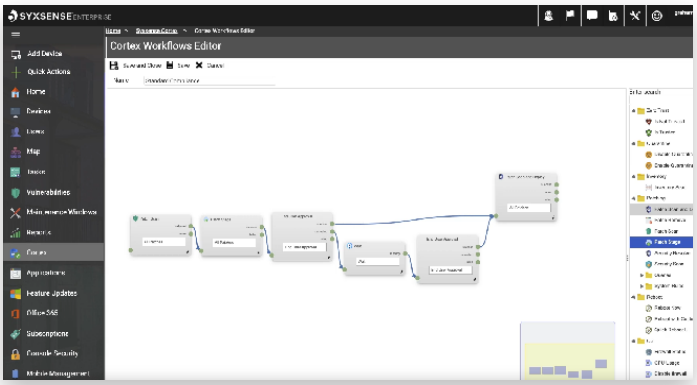
- Saves critical time by reducing mean-time-to-respond (MTTR) with pre-built vulnerability scanning and remediation scripts that automate the assessment of affected devices and the application of fixes and configuration changes.
- Accurately monitors for, detects, and remediates vulnerabilities in near real-time and provides detailed reporting for executive assurance.
- Saves hours of driving to physical locations and reliance on end users to monitor server performance and deploy updates.
- Can keep every endpoint up to date easily and efficiently with scheduling and reporting of patches and Windows Feature Updates.

Dive deeper into EECO's story on the following page.

Reducing the Burden with Unified Security and Endpoint Management

During the COVID-19 pandemic, EECO's transition from in-office work at their 12 locations to a hybrid work model created significant burdens on the small IT operations staff. With offices spread across several southeastern states, technicians were spending hours trying to update endpoints: some drove hundreds of miles to physically update devices, while others had to rely on end users to manage updates. This left the IT Operations team without an efficient way to manage or monitor devices.

"It's definitely been a time saver being able to do things like Feature Update pushes through Syxsense that you can't do through other tools."



In particular, the team struggled to stay up to date with Windows Feature Updates on remote and roaming devices. Now, with Syxsense's automated workflow builder, Syxsense Cortex™, they can push the update out automatically, targeting devices as they come online and reporting on the success or failure of the install on each device. This gives the team a global view of the status of the environment, including identifying devices that are missing the Feature Update and resolving the issue before the network is exposed.

Eliminating Vulnerabilities and Reducing Risk with Syxsense Enterprise

EECO found itself in a tight spot when CVE 2022-30190, commonly known as "Follina," was made public.

With no patch forthcoming, EECO took advantage of the pre-built vulnerability scripts available with Syxsense Enterprise. Access to the pre-built vulnerability scripts gave EECO the ability to push out the workaround and configuration change Microsoft provided. Their Cortex automation delivered the configuration changes out to all EECO devices seamlessly.

This not only reduced the burden on the small IT operations team and end users, but drastically reduced the amount of time the company's endpoints were at risk and eliminated the attack vector, especially given that the vulnerability that was known to have been exploited in the wild.

"The pre-built vulnerability scripts are ridiculous because obviously things cost money. But if it's a dollar and cents kind of math, it's not even a conversation. The amount of time that something like that saves is just invaluable."

Furthermore, the IT operations team was able to quickly report to leadership on the status of EECO's devices with Syxsense's vulnerability reports. The reports provided real-time data on the health of the environment, giving EECO's executive team a clear view of their risk and exposure and the effectiveness of the vulnerability remediation process. At the end of the day, all parties were confident the company's infrastructure was secure.