



# Syxsense Product Presentation

January 2024



# Understanding the challenge



Threat actors now use advanced tools and automation to attack businesses at scale. With remote and hybrid work patterns persisting, IT Operations and Security Teams must meet this challenge with equivalent technology to protect critical assets that may be distributed geographically.



Increased cyber threats  
More cyber incidents  
More types of attack  
Speed of attacks is accelerating



Expanding footprint  
Remote working  
More partners & suppliers  
Increasing number of devices



Pressure on resources  
Budgets constraints  
Skills shortages  
Pressure to deliver from CEO





# Live, Accurate IT Device and Security Management delivered real-time from the cloud

## LIVE

Live data from thousands of devices in under 10 seconds. Instantly respond to security events  
*No more stale data*

## ACCURATE

True cloud solution, manage your entire environment for 100% visibility  
*No more blind spots*



**SYXSENSE®**

## SECURE

Complete IT Visibility  
A single, comprehensive solution for IT and Security Management  
*No juggling multiple consoles*

## ACTIONABLE

Syxsense Cortex, the visual drag and drop solution to automate complex IT and Security tasks  
*No steep learning curve*



# Real-time visibility and control over endpoint devices, networks, and cloud infrastructure, helping organizations to protect against cyber threats, improve IT operations, and reduce risk.



Security, in and out of the network, in the cloud and at every endpoint



Detecting and remediating vulnerabilities with intelligent automation





# Syxsense Platform

Unified Endpoint Management (UEM) platform that centralizes the three key elements of endpoint security management: security and patch vulnerability management, remediation, and compliance controlled by a powerful drag-and-drop workflow automation technology called Syxsense Cortex™.

## Manage

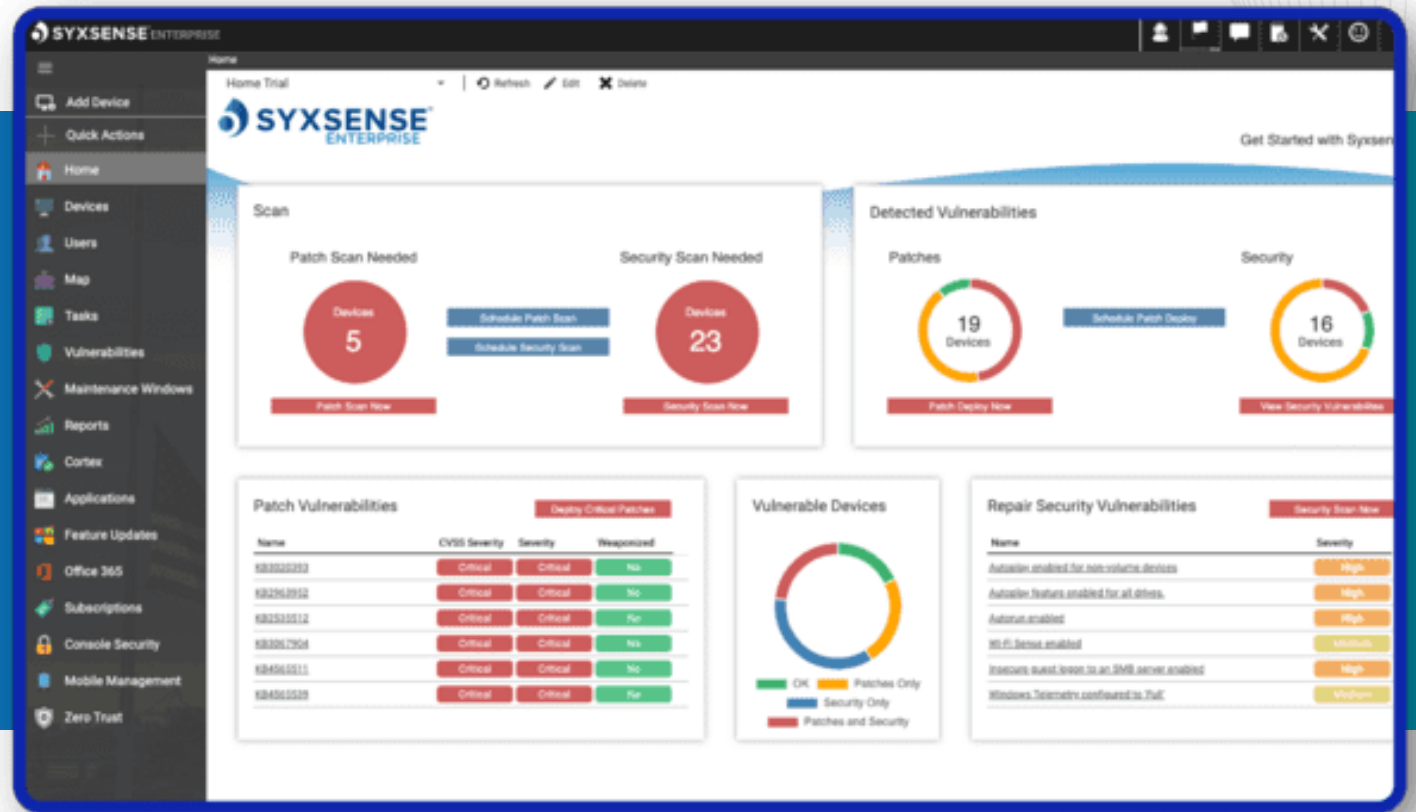
Gives control and visibility of desktops, laptops, and servers whether at home, on the network, or in the cloud.

## Secure

Adds Software and security configuration, vulnerability detection and RMM

## Remediate

Automated, intelligent, real-time response to vulnerabilities





# Syxsense Features

## Endpoint management

- Discovery Agent
- nMap
- Device Management
- IoT Discovery
- Device Timeline
- Device Location Maps
- Configuration Management (Policies)
- MDM
- Network Map with Device Health

## Operations management

- Remote Control
- Reboot Management
- Maintenance Windows & Blackout Hours
- Wake-on-LAN
- 24/7 Intelligent Automation
- Real-Time Views & Actions
- Supercedence by Default
- Remote Console

## Application Provisioning

- Software Distribution
- Office 365 App Provisioning
- Windows Feature Update Management
- Prebuilt software library

## Compliance

- Policies
- Proof of Compliance (HIPAA, PCI, SOX)
- Zero Trust
- CIS Level 1 and 2 enforcement

## Patch Management

- Patch Scan
- Patch Management (OS & Third-Party)
- Dynamic Patch Tuesday Windows
- Schedule Localization
- Maintenance Windows

## Vulnerability management

- Security Vulnerability Scan
- Threat Alerts
- Security Vulnerability & Content Management
- Syxscore Risk Assessment
- Security Remediation
- Quarantine

## Remote monitoring and management (RMM)

- Prebuilt Device Monitoring Templates
- Alerting
- Customizable Dashboards
- Incident Response
- Ticketing Integration

## Syxsense Cortex™ Workflow Design

- Cortex Drag & Drop Workflow Builder
- Automated workflow intelligence
- Cortex Workflow Script Library
- Ansible Workflows

## Reporting and Analytics

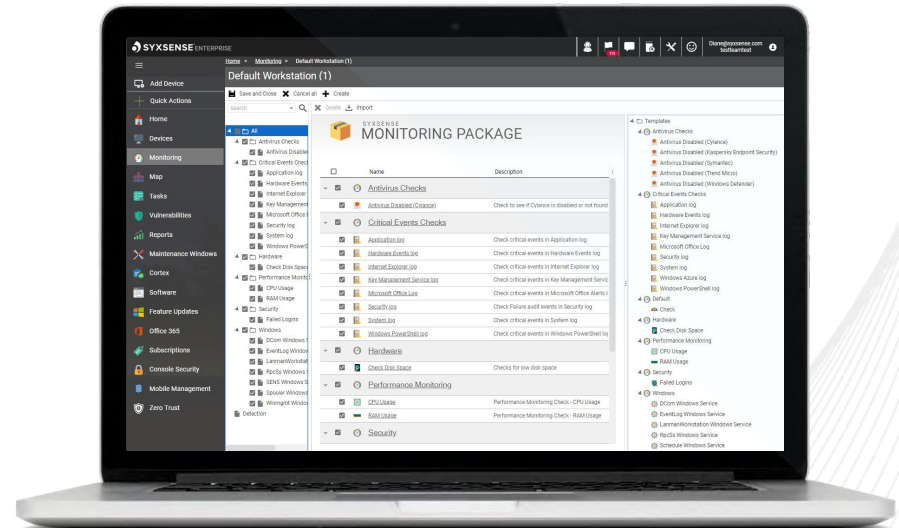
- Reporting
- Inventory History & Audit Logs
- Customizable Dashboards

## Architecture and integration

- Cloud-Based Architecture
- Open API
- Active Directory Integration
- Data export for SIEM

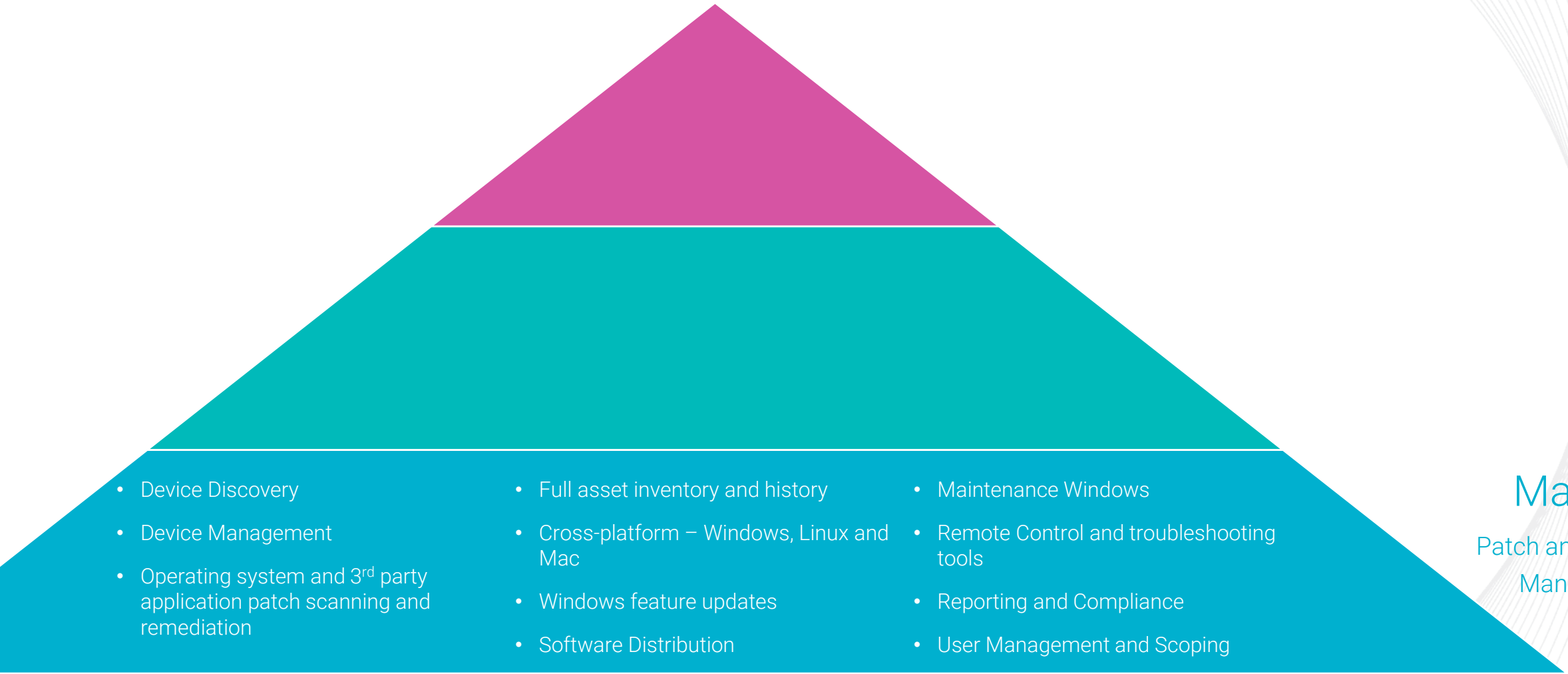
## Setup and configuration

- Easy deployment
- User Management & Scoping
- Custom Data Fields





# Syxsense Products



- Device Discovery
- Device Management
- Operating system and 3<sup>rd</sup> party application patch scanning and remediation
- Full asset inventory and history
- Cross-platform – Windows, Linux and Mac
- Windows feature updates
- Software Distribution
- Maintenance Windows
- Remote Control and troubleshooting tools
- Reporting and Compliance
- User Management and Scoping

Manage  
Patch and Device  
Management





# Syxsense Products

- Syxsense Cortex Automation Engine
- Policies and playbooks
- Security Configuration Vulnerability Scanning and Reporting
- Network Map
- Alerting
- Remote Monitoring and Management

- Device Discovery
- Device Management
- Operating system and 3<sup>rd</sup> party application patch scanning and remediation
- Full asset inventory and history
- Cross-platform – Windows, Linux and Mac
- Windows feature updates
- Software Distribution
- Maintenance Windows
- Remote Control and troubleshooting tools
- Reporting and Compliance
- User Management and Scoping

Secure  
Vulnerability Management  
and RMM  
+

Patch and Device  
Management







# Syxsense Products

- Open API
  - Zero Trust access
  - Security Vulnerability Remediation
  - Mobile Device Management – Android and iOS
- Syxsense Cortex Automation Engine
  - Policies and playbooks
  - Security Configuration Vulnerability Scanning and Reporting
  - Network Map
  - Alerting
  - Remote Monitoring and Management
- Device Discovery
  - Device Management
  - Operating system and 3<sup>rd</sup> party application patch scanning and remediation
  - Full asset inventory and history
  - Cross-platform – Windows, Linux and Mac
  - Windows feature updates
  - Software Distribution
  - Maintenance Windows
  - Remote Control and troubleshooting tools
  - Reporting and Compliance
  - User Management and Scoping

## Enterprise

Security Automation  
Compliance  
and MDM  
+

Vulnerability Management  
and RMM  
+

Patch and Device  
Management





# Syxsense Products

- Open API
  - Zero Trust access
  - Security Vulnerability Remediation
  - Mobile Device Management – Android and iOS
- Syxsense Cortex Automation Engine
  - Policies and playbooks
  - Security Configuration Vulnerability Scanning and Reporting
  - Network Map
  - Alerting
  - Remote Monitoring and Management
- Device Discovery
  - Device Management
  - Operating system and 3<sup>rd</sup> party application patch scanning and remediation
  - Full asset inventory and history
  - Cross-platform – Windows, Linux and Mac
  - Windows feature updates
  - Software Distribution
  - Maintenance Windows
  - Remote Control and troubleshooting tools
  - Reporting and Compliance
  - User Management and Scoping

## Enterprise

Security Automation  
Compliance  
and MDM  
+

## Secure

Vulnerability Management  
and RMM  
+

## Manage

Patch and Device  
Management





**SYXSENSE®**