Cybersecurity INSIDERS RECOMMENDED

PRODUCT REVIEW: SYXSENSE ENTERPRISE

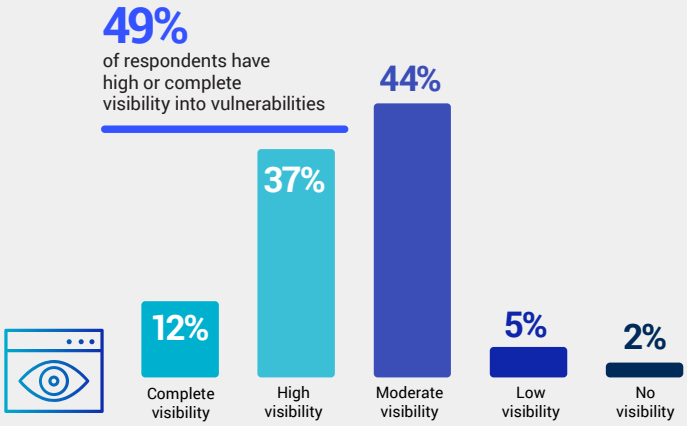
SYXSENSE®

Today's digital transformation is rapidly changing the IT and cybersecurity landscape: Remote work and the increased shift to the cloud has broadened the attack surface, introducing new vulnerabilities as employees connect from everywhere. This situation is compounded by the rise of sophisticated cyber threats, like ransomware and phishing, demanding proactive defensive security measures.

Addressing these challenges, Syxsense Enterprise offers a comprehensive solution engineered to reduce an organization's attack surface and risk profile.

Syxsense Enterprise is the world's first cloud-based IT management and cybersecurity solution that combines patch management for operating systems and third-party applications, security vulnerability scanning, and remediation with a powerful no-code automation engine. This combination delivers a complete, unified solution that supports patching, security, and compliance needs efficiently.

What level of visibility do you have into vulnerabilities across your IT environment?



About half of the respondents (49%) have high or complete visibility into vulnerabilities across their IT environment, while the other half (51%) have, at best, only a moderate level of visibility. This is concerning, as lack of visibility can lead to unaddressed vulnerabilities and subsequent breaches.

Source: 2023 State of Vulnerability Management Report produced by Cybersecurity Insiders

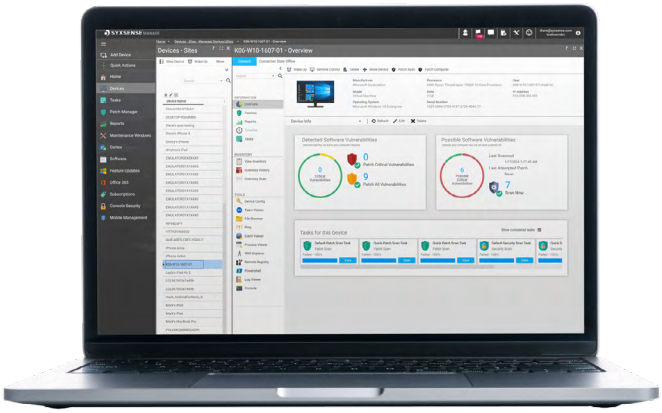
COMPLETE VISIBILITY AND MANAGEMENT OF IT ASSETS

According to a 2023 Cybersecurity Insiders vulnerability management survey, 49% of the respondents have high to complete visibility into vulnerabilities across their IT environment, while the other half (51%) have, at best, only a moderate level of visibility. Syxsense Enterprise addresses this challenge by providing complete visibility and management of IT assets regardless of their operating system (Windows, Mac, Linux, iOS and Android) or location (roaming, at home, on the network, or in the cloud). This is achieved through a live, two-way connection to devices, providing real-time data that enables not just automated remediation but also more accurate compliance reporting.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

ROBUST ENDPOINT MANAGEMENT

The platform's endpoint management capabilities deliver critical intelligence on operating systems, hardware, software inventory, and a complete endpoint timeline. This feature ensures that any missing patches, from the operating system to third-party applications like Adobe, Java, and Chrome, are immediately visible, presenting a clear picture of device changes over time. This allows security and IT operations teams to scan, track, prioritize, and customize security and patching actions, focusing on the most critical patches relative to exposed risk.



With additional features such as pre-built security vulnerability remediations, a policy-based, Zero Trust evaluation engine, and extensive integration capabilities with ITSM tools through its Open API, Syxsense Enterprise addresses the multifaceted challenges posed by current IT and cybersecurity trends. It not only ensures the security of systems but also supports robust audit and compliance initiatives, including compliance proof, ultimately enabling organizations to maintain operational efficiency and security.

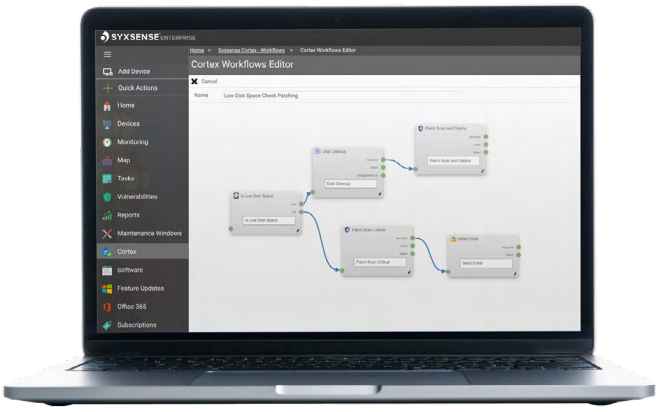
UNIFIED SECURITY VULNERABILITY MANAGEMENT

Syxsense Enterprise also offers a single console for vulnerability scanning, remediation, and advanced policy automation. Coupled with endpoint management, this unified approach enables teams to work from a singular information source that is fully aware of the environment's health and each endpoint's state. Such comprehensive visibility is critical for improving security, making smarter decisions to reduce risk, and maintaining compliance through actionable insights.

Furthermore, the integration of endpoint management and remediation workflows alongside a Zero Trust evaluation engine allows organizations to build trusted profiles for enterprise devices and verify each device is in a trusted state before granting access, ensuring a seamless blend of security and management capabilities.

ENHANCED PRODUCTIVITY WITH NO-CODE AUTOMATION AND ORCHESTRATION

At the core of Syxsense Enterprise is Syxsense Cortex™, a no-code workflow designer that enables operational staff to orchestrate complex IT and security processes without needing specialist scripting skills. Cortex is designed to streamline IT and security operations through automated endpoint and vulnerability management, enabling organizations to concentrate on their core business objectives rather than being bogged down by IT and cybersecurity risks.



Copyright © 2024 Cybersecurity Insiders. All Rights Reserved



KEY CAPABILITIES

Syxsense Enterprise distinguishes itself with an array of innovative features that empower organizations to streamline processes, enhance security, and ensure comprehensive endpoint management:

1. **Syxsense Cortex™ Workflow Builder:** An intuitive, no-code automation and orchestration builder that simplifies complex IT and security processes with a drag-and-drop interface. Syxsense Enterprise includes an extensive library of pre-built Cortex™ playbooks, ready to deploy at the push of a button for effective management and monitoring of devices.
2. **Security Policy Enforcement:** Easily implement a Zero Trust approach for continuous evaluation and authentication of both user and device, alongside automatic remediation of noncompliant endpoints to enforce compliance with security policies.
3. **Vulnerability Scanning and Remediation:** Automatically identifies and resolves vulnerabilities upon detection through policies triggered by predefined conditions.
4. **Vulnerability Database:** Features over 3,800 common configuration vulnerability fixes and more than 1,500 security remediation workflows. These are designed to conditionally respond to behavioral and state changes and are available as standalone tasks or as part of automated policies on local systems.
5. **Unified Secure Endpoint Management with Open API:** Cloud-native and OS-agnostic, Syxsense supports cross-platform management (Windows, Mac, Linux, iOS, and Android), enabling the administration of desktops, laptops, servers, virtual machines, and mobile devices (MDM) from a single console. Syxsense Enterprise includes software distribution, feature updates, configuration management, a network map, and troubleshooting tools like remote control.
6. **Patch Management and Deployment:** Detects OS and third-party patch updates and security configuration issues, prioritizing the management and deployment of updates to devices at critical risk. It keeps systems up to date on releases, prioritizes critical patches, and targets vulnerable devices with accurate detection and rapid deployment.
7. **Customizable Dashboards:** Allows customization and sharing of discoveries and actionable insights with key stakeholders through interactive visualizations of vital security metrics.
8. **Compliance Reporting:** Generates proof of compliance reports for audits by regulatory agencies, covering standards like HIPAA, PCI, and SOX.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

KEY BENEFITS

Exploring the benefits of Syxsense Enterprise, we highlight how it enhances security, improves operational efficiency, and drives cost savings for organizations:

- **Reduced Risk of Security Breaches:** The risk of data breaches and unauthorized access due to exploitation of unpatched vulnerabilities is markedly reduced with Syxsense Enterprise's comprehensive approach to vulnerability scanning and remediation. The capability to quickly identify and address vulnerabilities is crucial, especially when considering that 44% of organizations report systems with unintended open access and 24% have reported breaches caused by unaddressed vulnerabilities.
- **Improved Security Posture & Uninterrupted Productivity:** Syxsense Enterprise offers real-time visibility into all devices within an organization, identifying those in need of patches or harboring vulnerabilities. This enables IT teams to prioritize critical tasks effectively, ensuring that productivity remains uninterrupted, contributing to a remarkable 80% reduction in unplanned downtime.
- **Improved Productivity & Reporting:** With Syxsense, reporting on key IT infrastructure metrics becomes effortless, from patch status and time-to-patch to compliance with regulatory requirements. This streamlined reporting contributes to a 30% decrease in IT support cases related to maintenance. Moreover, the solution facilitates a more than 50% faster resolution of IT support cases, underlining its efficiency-boosting benefits.
- **Cost Savings Through Automation:** The solution offloads tedious tasks, allowing IT professionals to redirect their focus on more strategic initiatives. Specifically, Syxsense has been shown to reduce patch management resource needs by up to 90% by automating policy application and software installation, freeing up significant amounts of time for IT staff.

DEPLOYMENT

As a cloud-native software vendor, Syxsense delivers its solutions via Software as a Service (SaaS), ensuring a seamless integration into existing IT infrastructures without the need for additional hardware investments. This cloud-based delivery model not only facilitates rapid deployment and scalability but also offers the flexibility required to adapt to evolving security needs.

Speed of Deployment

One of the standout features of Syxsense Enterprise is its quick deployment time. Organizations can have the solution up, configured, and operational within 15 minutes, a stark contrast to the days or even weeks required for deploying traditional IT management solutions. This rapid deployment capability is especially beneficial in scenarios requiring swift action to mitigate existing vulnerabilities or to enhance IT management efficiency without significant downtime.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

Subscription Pricing

Syxsense operates on a subscription-based pricing model, which is dependent on the number of endpoints managed. This model allows for a scalable and flexible approach to pricing, ensuring that organizations can tailor their subscriptions according to their specific needs and growth trajectories. Additionally, for Managed Service Providers (MSPs), Syxsense offers specific packaging options, enabling MSPs to utilize the platform both for managing their endpoints and for offering vulnerability management services to their clients.

Free Trial

Prospective clients can explore the benefits of Syxsense through a free trial, available for up to 50 devices and 50 mobile devices for 14 days. This trial offers organizations the opportunity to evaluate the solution's effectiveness and ease of use in their environment before committing to a subscription.

CONCLUSION

In summary, Syxsense Enterprise stands out as a unified solution tailored for the modern digital enterprise, tackling the multifaceted challenges of endpoint and vulnerability management with a comprehensive, efficient, and scalable approach. By providing detailed visibility, control over endpoints, and a suite of automated vulnerability management and remediation tools, it enables organizations to safeguard their IT environments against the evolving threat landscape while ensuring compliance and operational efficiency. In essence, Syxsense offers a robust platform that not only fortifies an organization's cybersecurity framework but also streamlines its IT operations. Its comprehensive approach to managing security, efficiency, and compliance across a variety of use cases makes it an extremely valuable asset in the arsenal of modern IT and cybersecurity teams.

ABOUT SYXSENSE

Syxsense is the world's first software vendor providing cloud-based, automated endpoint and vulnerability management solutions that streamline IT and security operations. With our advanced platform, businesses gain complete visibility and control over their infrastructure, reducing IT risks and optimizing operational efficiency. Our real-time alerts, risk-based vulnerability prioritization, pre-built remediations, and intuitive automation and orchestration engine enable organizations to focus on their core business goals—confident in the knowledge that their enterprise is secure, compliant, and running smoothly.

US: +1 949 270 1903 | UK: +44 1256 806567 | info@syxsense.com | www.syxsense.com

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved