EXCALIBUR DATA SYSTEMS

VULNERABILITY SCANNING, PATCHING & EDR

# ALL IN ONE SOLUTION

## SYXSENSE SECURE | THE FUTURE OF THREAT PREVENTION

Syxsense Secure is world's first IT management and security solution that combines vulnerability scanning, patch management, and EDR capabilities in a single cloud console. With insight into the health of every endpoint across your network, you get the peace of mind that comes from predicting, preventing, and eliminating threats in real time. Make exposed risk and attack vectors a thing of the past.

## HIGHLIGHTS

- Advanced threat detection and real-time response capabilities
- Scan for software vulnerabilities, security compliance violations, and open threat vectors
- Deploy OS and third-party patches as well as Windows 10 Feature Updates
- Automated collaboration between IT and security teams
- Action tasks on devices to eliminate security risks identified by security scans
- Understand and prioritize exposed risk relative to your IT environment
- Scan for brute force attack vectors like password and user account violations
- Lock down insecure passwords along with ineffective user account policies

## STOP BREACHES WITH ONE SOLUTION

We revolutionize IT management and cyber security by centralizing live data on both OS vulnerabilities and the security weaknesses exposed by open ports, disabled firewalls, ineffective user account polices, and violations in security compliance standards. For the first time, these teams can collaborate in a single console to know and close attack vectors.

Experience real-time monitoring for malicious processes, automated device quarantine, and live data for insight into the health of every endpoint.

## 100% ENDPOINT VISIBILITY

Globally available from everywhere, and cloud hosted in Microsoft Azure, our solution consolidates desktops, laptops, servers, and IoT devices into a single console. With cross platform support for Windows, Mac, and Linux, discover all endpoints communicating over your network.

## ENDPOINT MANAGEMENT

Get full endpoint intelligence with OS, hardware, and software inventory details. Know if patches are missing or security standards are compromised. Critical devices are color coded in the datagrid, dashboards, and reports. Use sites, queries, and groups to target and view devices in logical subsets.

## SECURITY SCANNER

Prevent cyber attacks by scanning not just patches, but authorization issues, security implementation, and antivirus status. Receive actionable information on security profile weaknesses. Insights into OS misconfigurations and compliance violations reduce your attack surface.

## PATCH DEPLOYMENT

Scan and prioritize security and patching priorities relative to your exposed risk. Find out which patches have been released, their severity, and if vulnerabilities are being exploited. Automated Maintenance and Blackout Windows protect business productivity while deploying updates.

## DEVICE QUARANTINE

Instantly detect running .exes, malware, or viruses, and kill those processes before they spread. Device quarantine blocks communication from the infected device to the internet and isolates the endpoint. Through your console, you can access the device to understand and respond to the threat.

## ALERTING ACTIONS

Real-time data and device monitoring gives live, accurate information on disk space, RAM usage, CPU, registry information, process monitoring, software startup and more. Choose to be alerted, kill a malignant process, quarantine a device, or identify and remove blacklisted software.

## PROOF OF COMPLIANCE

Document your patching and security strategy success. Reports like Security Risk Assessment, Most Vulnerable Devices, and Task Summary can be scheduled for automatic receipt or exported to interactive reports. See detailed reporting to meet HIPAA, SOX, and PCI compliance.

## FEATURE UPDATES

Microsoft is ending support for older versions of Windows 10. Without the ability to install Feature Updates, your patches will be rolled back and devices remain vulnerable. Our dashboard shows an accurate count of all your Windows 10 versions, highlighting those in urgent need of upgrade.

## INTUITIVE TECHNOLOGY

Our architecture constantly innovates to combat security threats. Your data, devices, and users are safeguarded in Azure with encryption and secure transmission. The cloud native foundation uses a single, lightweight, responsive agent ready to be seamlessly deployed across your enterprise.

## ONBOARDING & SUPPORT

Industry-leading customer support is available to clients by phone, email, and chat. We provide quick resolutions to issues that block your path to results. With an easy-to-use interface, our intuitive platform allows you to get up and running in minutes using your own data.

## KEY FEATURES

- Threat Alerting & Quarantine
- Real-Time Security Management
- OS & Third-Party Patching
- Windows, Mac & Linux Support
- Live Device Location Maps
- Network and Site Maps
- Device Timeline
- IoT Support Device Discovery
- Unlimited Console User Accounts
- Device Discovery
- Hardware & Software Inventory
- Voice/AI Control
- Maintenance Windows
- Inventory History
- Custom Data Fields
- Remote Control
- Wake on LAN
- Audit Log
- Full Reports
- Patch Manager/Custom Patches
- Software Distribution
- Logical Air Gap Relay
- Agent-Based
- End User Access
- Priority Phone Support
- HIPAA, SOX, & PCI Reports

## ABOUT EXCALIBUR DATA SYSTEMS

At Excalibur Data Systems, our goal is to help customers improve, align, and automate their IT and business operations. Excalibur is one of the leading and most experienced partners of Cherwell with significant implementations in North America. We are a proud thought leader in the Cherwell Community while offering a breadth of other services.

START A FREE TRIAL OF SYXSENSE SECURE | syxsense.com/excalibur-syxsense-trial

✉ sales@excaliburdata.com

excaliburdata.com

☎ (724) 387-1331