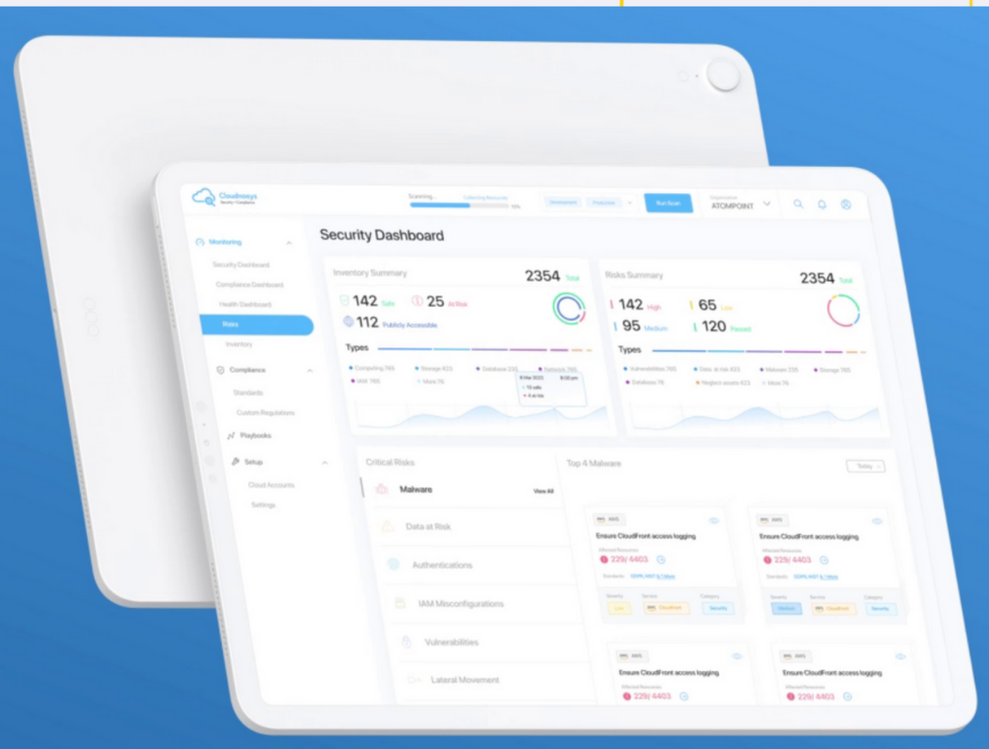
Cloudnosys
Security • Compliance

CIS Top 18

CIS Controls Cloudnosys Offers & How?

Description of CIS Top 18	Cloudnosys	How Cloudnosys Offers it?
• Control 1: Inventory and Control of Hardware Assets	Yes	• Solutions enable organizations to discover and identify devices as they connect to corporate assets, whether it is via the network, over email services, or through cloud applications.
• Control 2: Inventory and Control of Software Assets	Yes	• Solutions automatically scan systems and catalog the running applications to check them for known vulnerabilities, known malware, and other potential risks. Including OS, Files, and Software Packages used.
• Control 3: Data Protection	Yes	• Solutions identify password strengths, usage, and other sensitive data, monitor for exfiltration attempts, and identify the usage of non-standard file transfer protocols, encryption standards, and much more.
• Control 4: Secure Configuration of Enterprise Assets	Yes	• Our products scan existing systems and monitor activity across the modern environment to identify misconfigurations and toxic configurations, using Cloud well-architected frameworks and beyond basic CIS Standards.
• Control 5: Account Management	Yes	• Solutions monitor access controls (IAM) and baseline permitted access to systems in the critical environments to identify any of policy change in settings. For example, MFA is not turned on for MFA accounts, our solution can discover this in 20 seconds and then remediate dynamically if policy is set via playbooks.
• Control 6: Access Control Management	Yes	• Solutions monitor access controls (IAM) and baseline permitted access to systems in the critical environments to identify any of policy change in settings. For example, MFA is not turned on for MFA accounts, our solution can discover this in 20 seconds and then remediate dynamically if policy is set via playbooks.
• Control 7: Continuous Vulnerability Management	Yes	• Solutions enable continuous data collection from all systems through agentless scanning and simplify remediation workflows via the playbooks feature. It can tie into your change management workflow such as ServiceNow, Jira, etc. All CVEs, for OS, Files, and Libraries are checked.
• Control 8: Audit Log Management	Partial Yes	• The solution only tracks if Log files are configured for Encryption, version controlled, backups, and not open to the public. Currently, analysis of log file transactions is out of scope for Cloudnosys and we recommend having a log management tool in place to analyze events, like bit coin mining etc.

• Control 9: Email and Web Browser Protections	No	• This is out of scope. We recommend client invest in a email filtering tools.
• Control 10: Malware Defenses	Yes	• Solutions detect both known malware and unknown suspicious software. We check over 10 CVE databases for Vulnerabilities.
• Control 11: Data Recovery Capabilities	Partial Yes	• The solution today checks for back up best practices, and will flag as log files, and other data policies are not configured. However, the scope of this check is limited and does not provide full backup protection, we recommend client implement a solution. Our Services team can make recommendations for the backup and restorations process
• Control 12: Limitation and Control of Network Ports, Protocols, and Services	Yes	• All ports and protocol configurations are checked for best practices. For example, WAF is configured correctly or closing down RDP ports etc.
• Control 13: Network Monitoring and Defense	Yes	• Solutions audit system authentication controls, check for weak, old, and shared passwords, and alert on any potential authentication-based attacks or misuse of privileges. We help to ensure authentication control policies are followed appropriately.
• Control 14: Implement a Security Awareness and Training Program	No	• We request our clients to implement and assess the security skills of all employees through simulated phishing and social engineering campaigns and the identification of asset misuse and abuse.
• Control 15: Wireless Access Control	No	• Our Services team can recommend solutions in this area.
• Control 16: Application Software Security	Partial Yes	• Solutions scan custom applications, third-party software, and databases to identify vulnerabilities and produce clear remediation recommendations. Currently we don't check for OWASP top 10, however it is on our roadmap to deliver in the near future
• Control 17: Incident Response and Management	Partial Yes	• Solutions test existing incident response capabilities and ease the detection and response process, optionally through technology or a managed service.
• Control 18: Penetration Tests and Red Team Exercises	No	• This is out of scope. We recommend client invest in a pen testing tools.



Cloudnosys

Security • Compliance

Full Stack **Cloud Security Platform**

Visit us at **cloudnosys.com**