MAX SECURE™
Total Security. Total Peace of Mind.

AI powered Cloud Anti-Virus

for End Point protection

Windows Total Security
OS X/mac OS Total Security
Linux Security
Android Security

Deliver layered security services to multiple offices, networks, and devices with a single Cloud-based Platform offered as a service or On-premises

https://www.maxsecurecloud.com

Layered Anti-Malware Security Software as a Service

Manage your company Network Security without need to buy or install any hardware infrastructure, reducing the total cost of ownership and giving you time to focus on core business tasks, while we take care of security. Get started right away in few minutes and access your network from anywhere, anytime using a web-based console with full visibility. Also capability to deploy On Premises.

Max Cloud AV runs a small agent on the Client PC or VM

Deliver a range of IT security services with scans on the agent as well as on the Cloud that provide complete, in-depth protection against all forms of malware – whether they originate from inside or outside the network via email, websites, or the Internet. Connect securely to any device. Powered by several Artificial Intelligence models, diligently created Yara rules and Dynamic emulator leave no room for any Malware to creep in.

Deploy on Android Mobile devices, Mac and Linux if you require or just choose as per your installation requirements. Manage all distribution from one place.

Create Managed Network End Point protection & monitor from an Intuitive web console.

Centralized management portal allows you to apply policies, configuration settings, application control, schedule updates, alerts, remote software installation, reports, share documents and files, send/receive text message. Content search, vulnerability scanner and Inventory management. Cloud-assisted management Dashboard shows the most recent network security status, incident timelines, detections on computers, alerts on the top 10 infected computers and top 10 prevalent Malware in the network, Ransomware, installed and uninstalled devices etc.

Updates & Upgrades

Create update policies and schedule updates on client agents from management portal. For your On premises deployment, update tool is available for centralized updates form one location within the intranet.

Secure Internet & Email Security

Stop spam and secure incoming and outgoing emails and suspicious attachments from infecting your device. Web (URL) filtering blocks access to malicious websites, downloads, and locations to prevent attacks from harming your network or stealing any data.

Two-way Firewall with Application control

Enable Network monitor with intrusion detection prevention based on protocol/ip address, White list applications, block complete browsing or selectively add black and white list of web urls, restrict usage of web sites based on categories. Monitor internet and computer usage time. Only allow white listed application to run or have internet access and ban others.

USB Manager

Scan any external attached devices. White list external devices to only allow those devices to connect to protect data transfer or malware infections. Access control and Monitoring using DLP module.

Data Security with Backup & Restore

Protect your data in case any Ransomware encrypts with online and on premise back up and recovery options.

Threat protection

Artificial intelligence based next generation End Point Security for detection and remediation of Viruses, Malware and Ransomware. Automated Malware and Threat detection / removal, behavior analytics, enhanced remediation capabilities, process memory protection, active monitoring, signature-based protection.

Global threat intelligence and Sandbox for APT detection and heuristic detection.

No need to install any separate servers for Virtual device protection.

Groups, Configurations and Policy Management

Comes with pre-defined policies to best protect devices from all types of malware threats. Policies can be assigned to individual devices or users in Groups. Override policies in in one click immediately Highly configurable options make it versatile with many features. Groups could be created based on functions or locations.

Full Disk, Removable Media Encryption

One of the most effective ways of minimizing data exposure is to automatically encrypt the hard drives on desktops, laptops and servers. Simply disable from Portal if you do not require.

Encrypts the contents on removable devices such as Pen Drives, USB Drives and makes it accessible to the authorized users. Protects corporate data residing on endpoints with strong encryption algorithms such as AES, RC6, SERPENT and TWOFISH. Full disk encryption supports Microsoft Windows Desktops and Laptops. Only accessible to password owner.

Content Search

Audit the documents content for compliance on client devices by scanning for certain keywords in file name or content on wild card searches. Replace the keywords remotely on client agent files with another word from dashboard.

DLP: Data loss prevention

Prevent personal information theft such as driver license, credit card by copying on USB drive, Network drive or Email.
Also, add keywords and phrases which you want to monitor and document containing those be prevented from copying on USB drive, Network drive or Email.

Optional feature, if you Admin does not want to use it then can Disable by a simple click.

Hardware Inventory

Displays data about hardware installed on endpoints. About CPU, RAM, monitors, disk drives, input devices and printers, including vendors, models, and serial numbers, it can serve as an overview of the company inventory

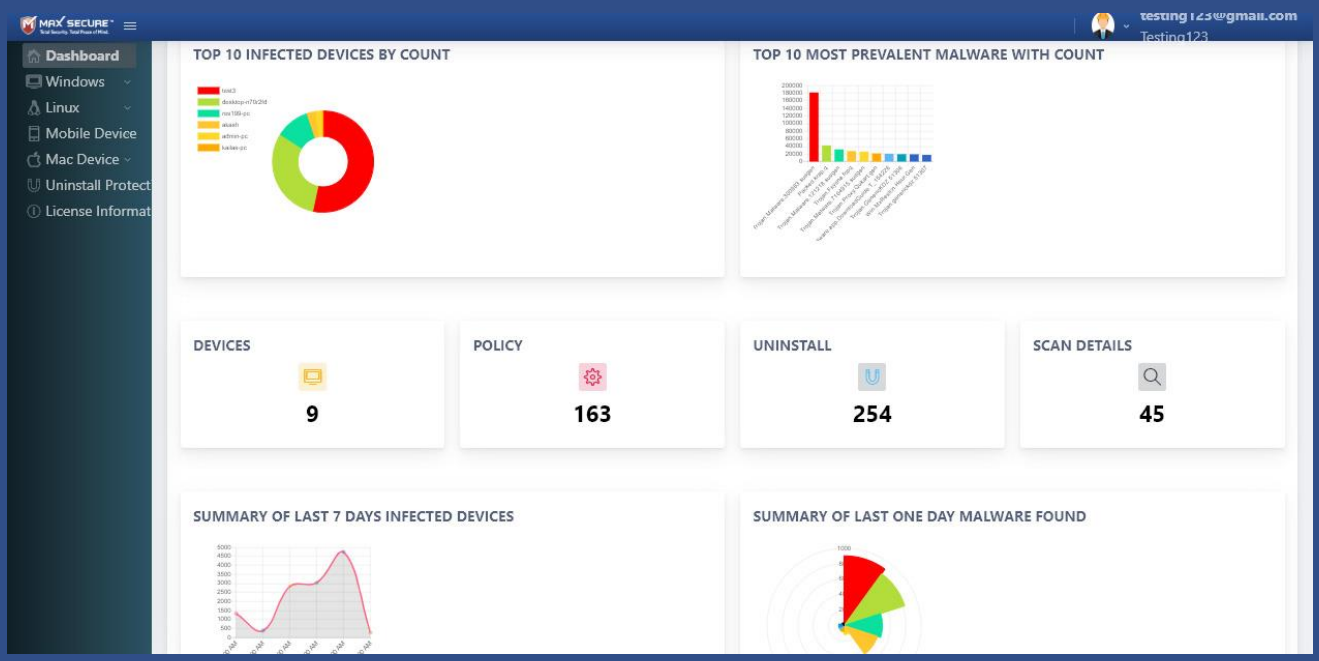
Comprehensive Reporting

Endpoints continuously report to Cloud Administrator whenever they connect to internet. Administrators can monitor the overall status in the main dashboard or drill down to more specific Device or complete Scan Details to oversee the status of computers, threats or quarantined items.

Customer Support

Max Secure Support provides 24x7 support. Client agents can request connection to support to resolve any registration, malware or functional issues using built in remote desktop support app, call on toll free and other phone numbers, drop an email or chat 24x7.

Intuitive Dashboard



Summary: Remote Functions

1. Deploy Dashboard On-Premises or on our cloud as SaaS
2. Schedule Live-updates and Scan
3. Delete quarantine folder if it reaches defined size
4. Remote Logout, Reboot, Shut-down, Disable network, Execute any program from command line
5. Install/Uninstall Firewall
6. Send and receive message to devices
7. Share Documents and Files between server and agents
8. Password protect and White list USB devices
9. Turn ON/Off Real time protection
10. Silent scan on end point devices or with user mode
11. Content search and replace objectionable items
12. Data back and Restore remotely
13. Select Scan options remotely on the agents
14. Full disk encryption
15. Threat Intelligence
16. Network intrusion detection
17. Data Loss prevention through USB devices for credit cards and Driver license etc. personal information

Visit https://www.maxpcsecure.com/CloudAV.htm , Support : info@maxpcsecure.com , Call: 18002091111 , 0 800 761 3111 0 898 338 3200, **0 860 510 0500 / 0844 629 9299**