MAX SECURE™
Total Security. Total Peace of Mind.

AI powered Next-Gen Cloud / On-Premises Anti-Virus for End Point Protection

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

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

TABLE OF CONTENTS

AI powered Cloud / On Premise Anti-Virus

for End Point protection - Windows/ Mac/ Linux & Android

RUNS SMALL CLIENT AGENT

Delivers a range of IT security services with scans on the agent based on the Cloud platform, no server to set up and professionally managed. Provides complete, in-depth protection against all forms of malware – whether they originate from inside or outside the network via email, websites, Fileless Malware or the Internet. Connect securely to any device. Powered by Artificial Intelligence models, diligently created Yara rules, Dynamic emulator, Threat Intelligence and Sandbox for APT leave no room for any Malware to creep in

SOFTWARE AS A SERVICE

Layered Anti-Malware Security can 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.

SUBSCRIPTION MODEL

Register for 1 year, 3 year or 5 year as per your requirements. On our server or on your Premises installation options available.

MOBILE ENDPOINTS SECURITY

Manage protection from all types of Malware on Android, Linux and Mac Devices. Remotely scan, fetch Reports, Updates, View status of devices, Inventory, and Reports

GLOBAL THREAT INTELLIGENCE SUPPORT

Global threat intelligence, with access to Cloud Sandbox for APT detection and analytical reports. Our Threat intelligence feed enables us to search for new and unknown Malware. Sandbox allows organizations to significantly increase the level of protection of their workstations and servers against previously unknown malware, new viruses and ransomware, zero-day exploits, and others – without the need for highly specialized information security analysts. Only available for Online / Cloud installations. Admin can use this feature on demand.

SANDBOX FOR APT

On-demand, On-premise sandboxing services let you set up virtual environment that lets you define one/ multiple sandboxes, which integrate with Max Cloud Security product thin clients. An open web service API allows thin clients to submit samples and suspicious samples and receive full detailed analysis. Examines a wide range of Windows Executable, Microsoft Office, PDF, web content, and compressed file types.

ADVANCE PROTECTION FOR VIRTUAL ENVIRONMENT

Client agent does not take much resource, installed on any PC, Server or virtual environment, and connects immediately to the centralized Dashboard. No specific Virtual image required

SIGNATURE BASED PROTECTION

Scanning for Malware is based on multi-layered scanner. Scan includes signatures (Hash) based detection and specific code for Virus for repair, AI/Ml based scan for Generic Malware and Yara rules detection for Adware and Trojans.

Behavior based strong Anti-Ransomware protection catches all of them before they can spread and encrypt any data.

DATA PROTECTION: FULL DISK, FILE/EXTERNAL MEDIA ENCRYPTION

One of the most effective ways of minimizing data exposure is to automatically encrypt the hard drives on desktops, laptops and servers.

Encrypts the contents on removable devices such as external hard 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.

Admin using Dashboard has full control over which algorithm to apply on which device and password management for the encrypted devices as well.

DLP: DATA LOSS PREVENTION

Prevent personal information theft such as Driver license, PAN card, Aadhaar Card, Credit card etc. from being copied on USB drive, Network drive or transferred by Email.

Also, Content or Context or file extensions search which you want to monitor, are prevented from copying on USB drive, Network drive or Email with the Option to Block or Report

STORAGE SECURITY

Admin can remotely enable folder vault on any folder on Client agent PCs to protect Data, protected with a password. No malware or even Ransomware can infect this folder/folders.

DATA SECURITY WITH BACKUP & RESTORE

Protect your data in case any Ransomware encrypts, with online and on Premise backup and recovery options on same PC or Network Drive or Google Drive. Schedule backups for File extensions that you provide can be managed from Dashboard.

CLOUD-ASSISTED SECURITY NETWORK

For Servers and Client agents, which are online, our cloud hosted Malware database is used for scanning. Suspicious files are sent to Threat Intelligence and Live Sandbox waiting to do the dynamic analysis of files. For On-Premises / Off-line installations this module is not applicable.

ANTI-VIRUS FEATURE

Protects from all types of file infecting, polymorphic, metamorphic, boot sector, resident, scripting, Macros, browser hijacker and multi-partite virus, repairs the infected files

ANTI-MALWARE FEATURE

Prevents from all types of Malware such as Trojans, Worms, RATs, Spyware, Adware, Fileless Malware, Tracking cookies and unwanted applications

ANTI-RANSOMWARE FEATURE

Prevents from all types of Ransomware using signatures and behaviors. Terminates the suspect process and alerts the Admin on the dashboard

PERSONAL FIREWALL

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.

NETWORK ATTACK BLOCKER

Enable Network monitor with intrusion detection/ prevention based on protocol/ip address. Prevent malware spreading through network and block the ip address of the infected PC from spreading infection further

WEB CONTROL /URL FILTERING

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.

HOST BASED INTRUSION DETECTION/PREVENTION

We follow MITRE (ATT&CK) Techniques and Tactics Driven Detections knowledge base of adversary tactics and techniques closely to block host based intrusion

HOST INTEGRITY

Continuous monitoring of Client Agents for any Ransomware, DLP Policy violations, USB connect and Malware found, Offline/Online, Inventory change management is sent to Admin as email alerts and alerts on the Dashboard main menu

APPLICATION CONTROL

White list applications and : only allow white listed application to run or have internet access and ban others.

DEVICE CONTROL

Manage USB, Camera, Mobile, WI-Fi, Bluetooth, External CD/Hard Disk

USB DEVICE CONTROL / MANAGER

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

VULNERABILITY SCANNER AND PATCH MANAGER

Remotely scan client agents and determine the missing updates and security patches. Update all the available patches from a central location. For offline network, Downloader tool and Web based Patch manager allows updates from any device in the network and automatically installs on the clients

DECEPTION TECHNOLOGY

We keep decoy files to lure Ransomware and Malware into infecting them. It’s about increasing attack surfaces, creating more fake attacks, the moment they hit one of our traps, it’s over for them. We sit back and watch them fail

BROWSER PROTECTION

Protect yourself against online threats, like phishing and malicious websites. Use Firewall web protection to block known and unknown websites, websites falling under known categories such as social sites, gaming sites or block any particular website by domain name or keywords in the domain name.

ANTI-THEFT PROTECTION

In case any device is lost or stolen, mark from the Admin Dashboard as stolen and start getting the pictures and location details. Lock/Wipe device in case you still are unable to get it for data protection

ENDPOINT FORENSIC

The forensics functionality enables remote investigation securely over any network. Endpoint forensics works by monitoring all the processes running on endpoints at a given time. By doing this, it's possible to pinpoint processes often used in multi-stage malware and identify specific processes that deviate from normal behavior. Having access to telemetry on single Dashboard, organizations can investigate and analyze from endpoint forensic data capture

FILE SERVER PROTECTION

It will not noticeably slow your system down or interfere with business operations, even under heavy network load conditions. Expect ultra-reliable performance and stability

MEMORY PROTECTION

Process scanner and Active monitor is always keeping an eye any malware activity in the running processes, coming from network or any ransomware activity

ADVANCE MACHINE LEARNING

Artificial intelligence with machine learning module provides next generation zero-day detection and remediation of Viruses, Malware and Ransomware. Automated Malware and Threat detection / removal, behavior analytics, enhanced remediation capabilities

AUTO SAND BOXING

Using Web APIs analyzes suspected files on our server Sandbox automatically to detect unknown malware quickly. Only applicable for Cloud / online installations

DEVICE AUTHENTICATION CAPABILITY

There are several methods of installation such as Active Directory, Group Policy or Dynamic installer is used to authenticate the user while enrolling the device

FREE UPGRADATION TO HIGHER VERSIONS

Yes, daily definition updates and frequent upgrades available for On-line and Off-line installations

UPDATE DATA ROLLBACK

In case there is an issue with the new updates or upgrades, Admin can do selective rollback from Dashboard

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 change 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.

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.

TRACK HARDWARE & SOFTWARE INVENTORY CHANGE MANAGEMENT

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

CONTROL MANAGER

For offline updates, we recommend using WSUS server on the Internet PC and Offline PC and synchronize. Our tech support team can help set it up properly as well.

However, we also offer our patch management solution. In case of multi – location installations, we have Control Manager. This receives all the reporting from the child servers and also can push updates centrally.

Manage reporting of all Child servers and their Clients.
Scheduled update of all reports to the (Parent) Control Manager once a day or as often
scheduled Dashboard with graphical charts with several parameters
Alerts for specific events
Alerts as sound notifications, email or view on dashboard

Patch Management: we have offline Patch Management tool which can download all the updates which can be copied to the Offline patch management server. Patch manager installed as a website in IIS can be installed to push updates on Client Pcs.

CUSTOMER SUPPORT

Max Secure provide 24x7 support. Customers can call, email, chat or request for remote support to resolve any registration or malware related issues.
Escalation can be raised to senior management in case any issues are pending.

CONTENT FILTER

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.

VALID LICENSE COPY TO BE PROVIDED

Yes

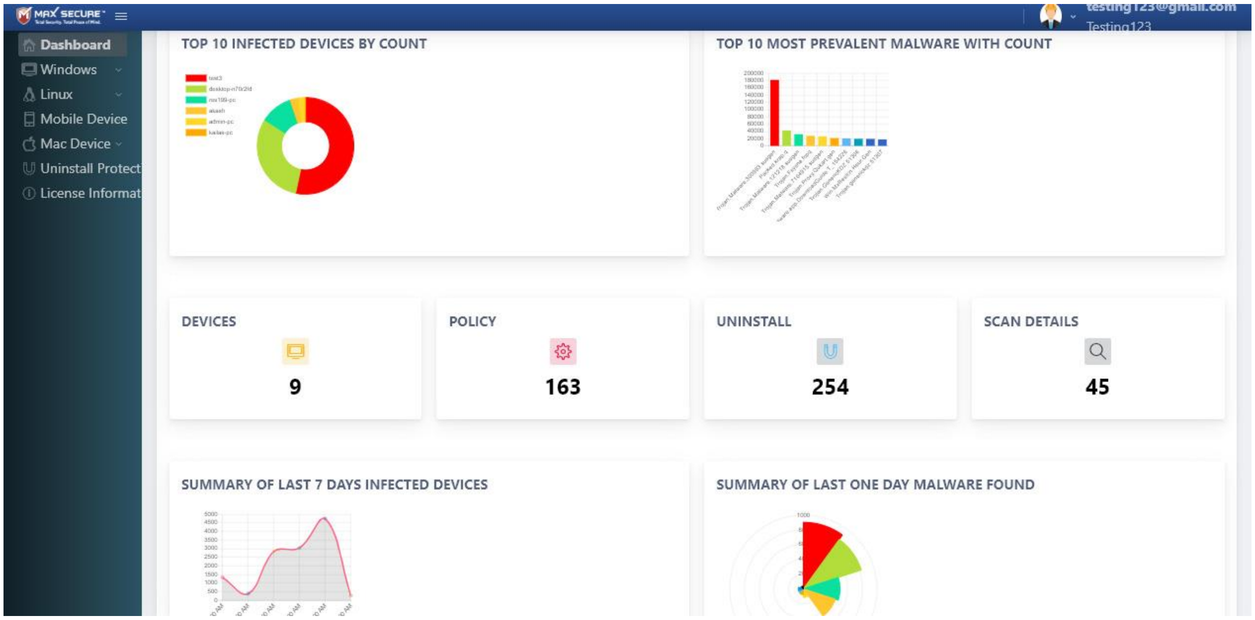
INSTALLATION AND DEMONSTRATION

yes

TRAINING ON-SITE/REMOTE

As per your requirements, we can support your device remotely and guide you to install or deploy a team to come and install on your Premises. This product enables remote support very easily.

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. Full disk encryption
14. Threat Intelligence
15. Network intrusion detection
16. Data Loss prevention through USB devices for credit cards and Driver license etc. personal information