MAX SECURE™

Total Security. Total Peace of Mind.

AI Powered SaaS based End Point Security For Business

Support Windows, Mac OS , Linux and Android Security

Delivers layered Anti-Virus protection to multiple offices, networks, and devices with a single Cloud-based console offered as a service or On-prem installation

https://www.maxpcsecure.com/cloudav.htm

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

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

Create, Protect & 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.

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.

Updates & Upgrades

Create update policies and schedule updates on client agents from management portal. For On premises deployment, update tool is available for centralized updates form one location for On-Premise installation

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.

Firewall

Enable Network monitor based on protocol/*IP* address, applications filter, 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. Email Scan Setting, Enable Intrusion detection.

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 and Complete control over USB devices, Copy/Write/ Execute and Monitoring.

Data Security with Backup & Restore

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

File Integrity and Monitor

Validates the integrity of an application software files or any directory/file using a verification method between the current file state with a known, good baseline. This comparison method involves validation of the file's original baseline and comparing with the current state of the directory/file such as Hash, Name, content change or any other metadata. Other file attributes can also be used to monitor integrity.

FIM is a cloud solution for detecting and identifying critical changes, incidents, and risks resulting from normal and malicious events.

Zero Trust

Zero Trust is the highest priority policy. Zero Trust means no application or web site or USB drive or Wi-Fi should be inherently. With one click add Applications, Websites, USB devices and Wi-Fi that you want to white list, rest will be blocked. Or choose Block All option.

Other Software Updates

Download and Install missing patches for non-Microsoft applications. ex: Adobe Reader, Adobe Acrobat, Adobe Flash Player, VLC, Java, Putty, Notepad++, 7-Zip, Mozilla Firefox and Thunderbird. Secure your devices from vulnerability in any of these and remain updated for best performance from one console. For Online as well as On Prem installation

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.

Hardware & Software 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

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 4 other phone numbers, drop an email or chat 24x7.

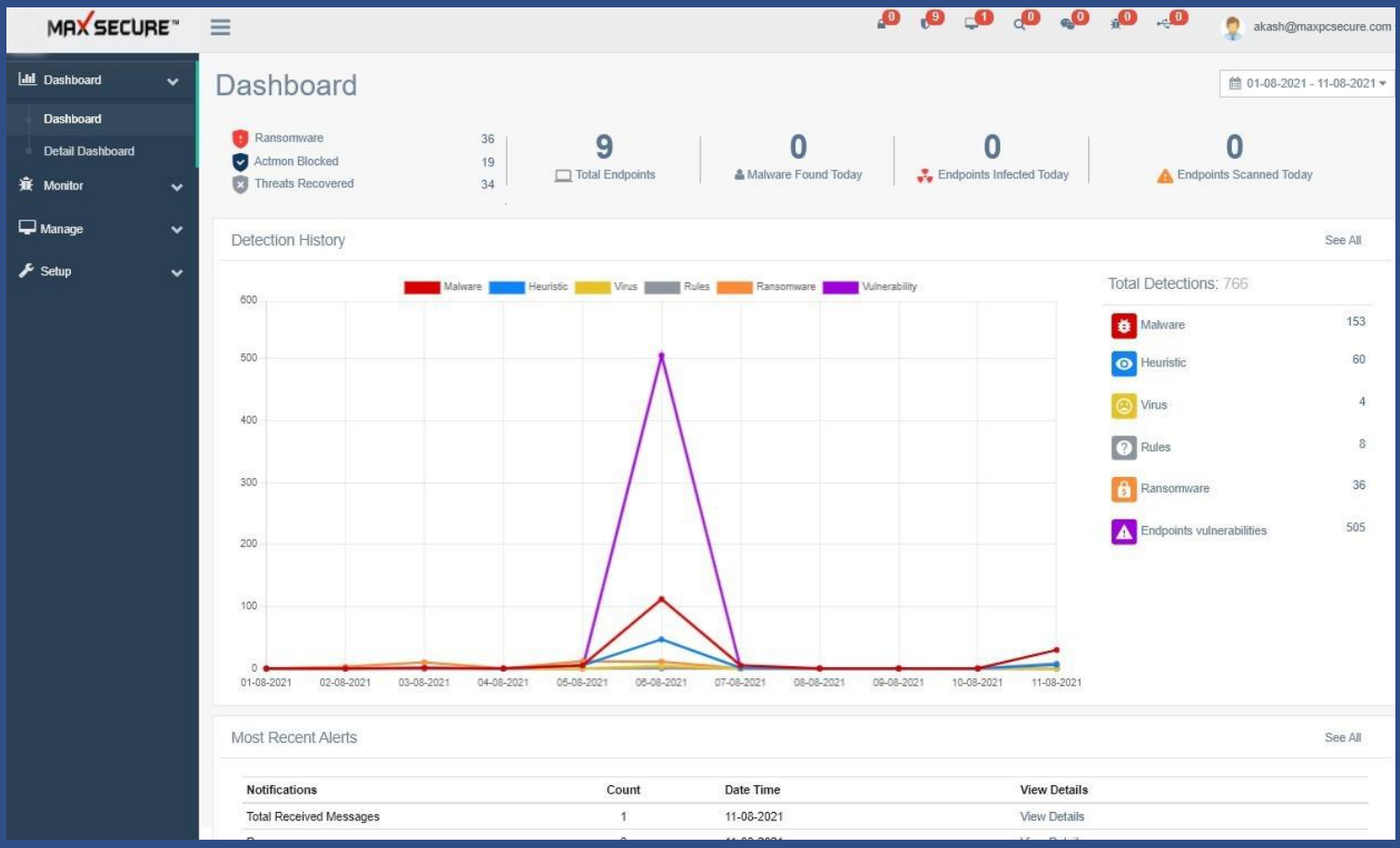
Content Search

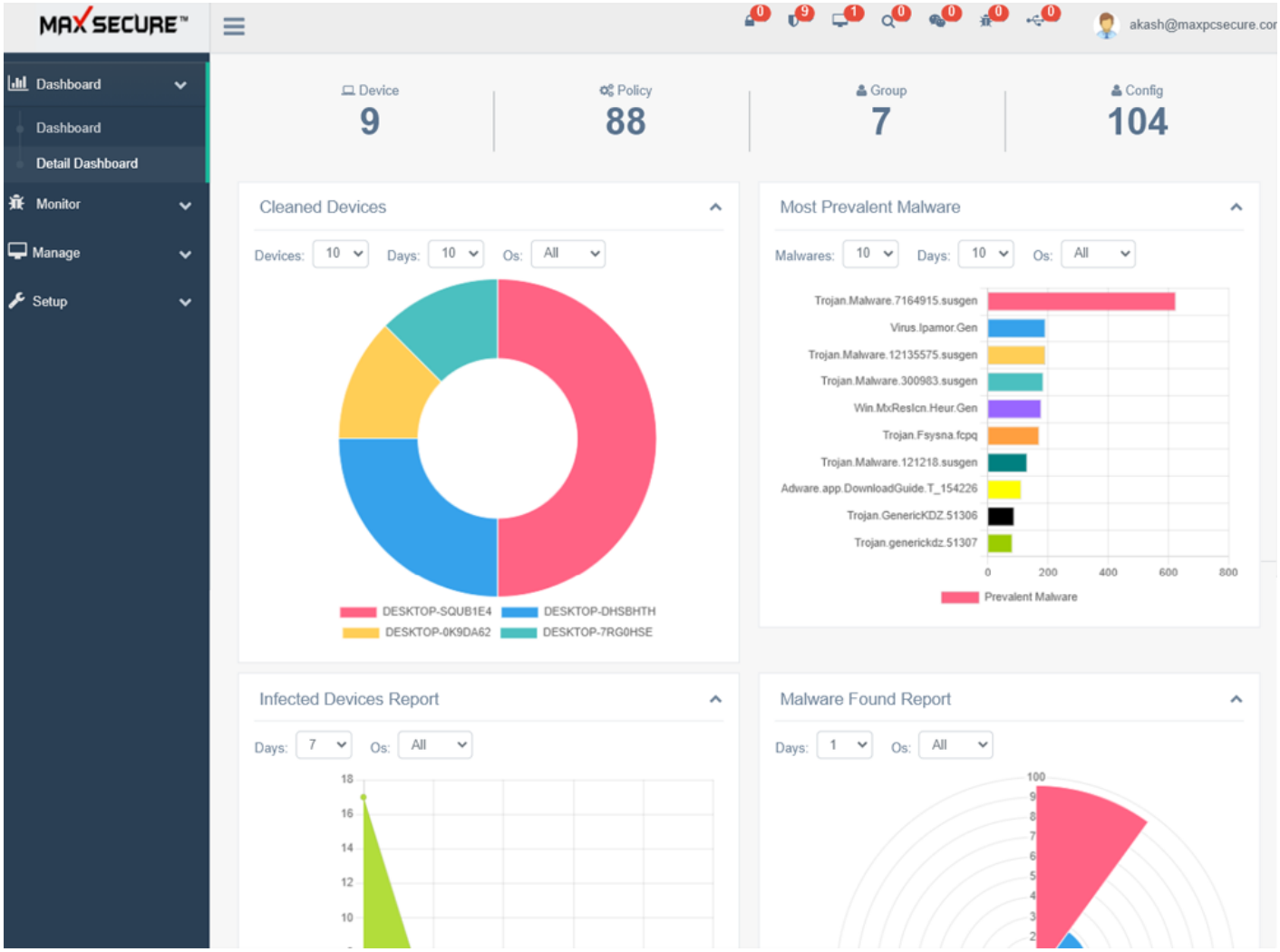
Audit the documents content for compliance on client devices by scanning for certain keywords in file name or content on wild card searches. Replace the keywords remotely on client agent files with another word from dashboard.

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.

Intuitive Dashboard





Minimum System Requirements

Server : Windows® 11,10 , 2012, 2016 and 2019 (All 32 and 64 bit editions)
Client: Windows® 11,10 , 8, 8.1, 7, 2012, 2016 and 2019
CPU: 1 GHz
RAM: 1 GB
Disk Space: 1 GB
Browser: IE 6.0 and higher
Available online as SaaS or On-Prem

Summary

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
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
18. File Integrity Monitoring to monitor Directory & Files. (FIM is a cloud solution for detecting and identifying critical changes, incidents, and risks resulting from normal and malicious events.)
19. Device Control can Block or Allow Bluetooth, Wi-Fi and Block Network
20. Configurations allows you to add several Settings and Tasks to selected devices or Groups Likes Application Whitelist, backup & Restore, Wi-Fi Whitelist, Exclude Folder, File Block, Ransomware, Scheduler, USB Whitelist,Folder Vault, Instant Remediation.
21. User management enables IT administrators to manage resources and provision users based on need and rolewhile keeping their digital assets secure. For end users, the action is Admin, Basic User and Sub Admin.
    - Admin user: Has all the rights
    - Sub-Admin: has all the rights except that he cannot create/delete users
    - Basic User: Can view things like policies etc. but not take actions/configuration etc.
22. Uninstallation password makes sure that users do not uninstall the security software from their devices.
23. Rollback to previous stable version.
24. USB Disable Protection disables protection temporarily.
25. User can give command from server to devices.
26. Vulnerability, Non Microsoft & Microsoft patch management.