PRIVACY DATA PROTECTION

BY **AntiHACK**.me

Achive greater control of your data privacy

SUITABLE FOR ANY NETWORK SIZE AND INDUSTRY
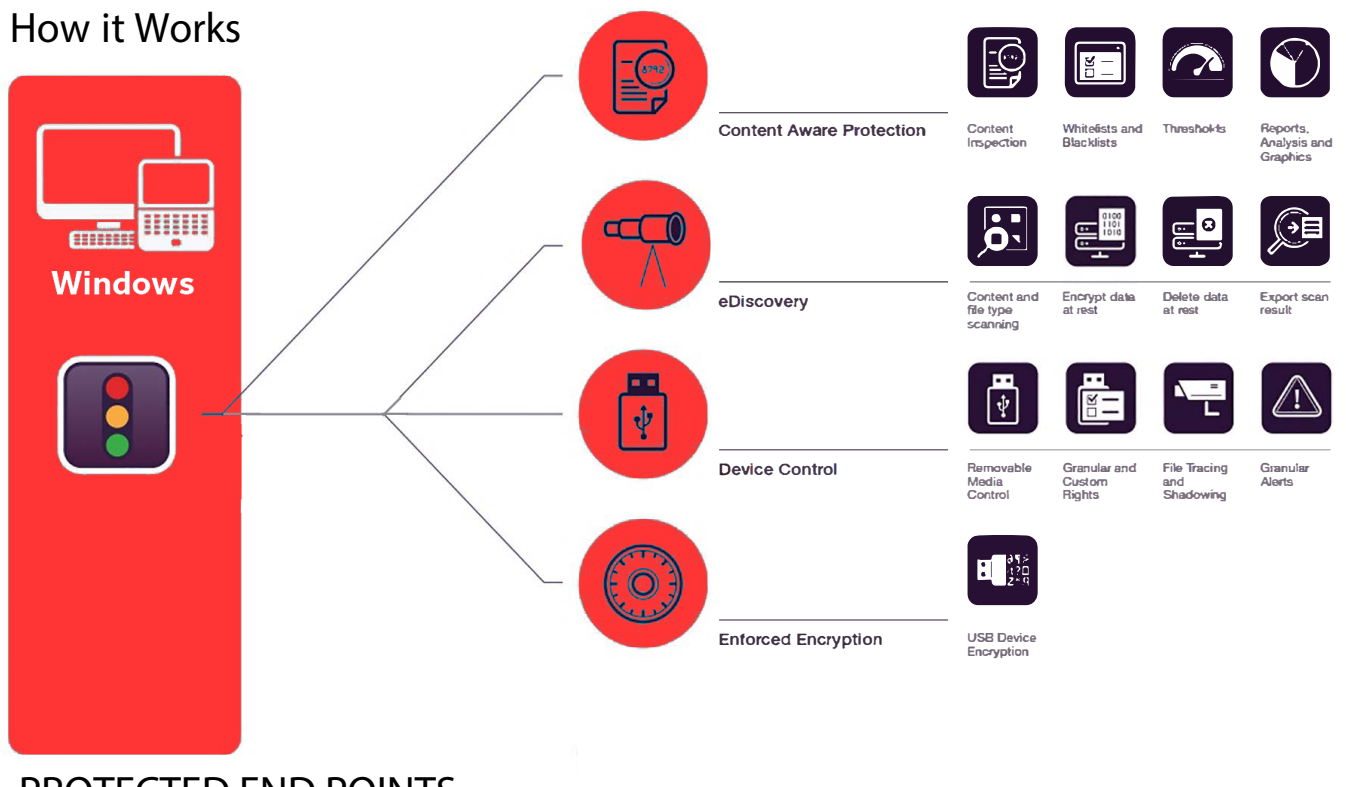
PROTECTING THE ENTIRE NETWORK

Out-of-the-Box Solution to secure sensitive data from threats posed by portable storage device, cloud services and mobile devices

In a world where portable, lifestyle devices, and the cloud are transforming the way we work and live, Privacy Data Protection is designed to protect confidential data against insider threats, while maintaining productivity and making work more convenient, secure and enjoyable.

The blacklist and whitelist-based approach grants flexibility in policy building. Organizations have the option to prohibit the use of specific removable devices and data transfers to file cloud sharing applications and other online services, to scan for certain PIIs, but to allow transfers to specific URLs and domain names for certain computers/users/groups, avoiding task interruption.

With Privacy Data Protection being offered as hardware or virtual appliance, it can be setup in minutes. Moreover, the responsive management interface allows managing policies and checking reports from any device, from desktop to tablet.

Privacy Data Protection dramatically reduces the risks posed by internal threats that could lead to data being leaked, stolen, or otherwise compromised. In addition to these, compliance with various rules and regulations is also met.

How it Works

Windows

Content Aware Protection

| Content Inspection | Whitelists and Blacklists | Thresholds | Reports, Analysis and Graphics |

eDiscovery

| Content and file type scanning | Encrypt data at rest | Delete data at rest | Export scan result |

Device Control

| Removable Media Control | Granular and Custom Rights | File Tracing and Shadowing | Granular Alerts |

Enforced Encryption

| USB Device Encryption |

PROTECTED END POINTS

Content Aware Protection
for Windows

Monitor and Control data in motion, deciding what confidential files can or cannot leave the company via various exit points. Filters can be set per File Type, Application, Predefined and Custom Content, Regex and more.

eDiscovery
for Windows

Scan data at rest on network's endpoints and apply remediation actions such as encrypt or delete in case confidential data is identified on unauthorized computers.

Device Control
for Windows

Monitor and Control USB and peripheral ports. Set Rights per Device, User, Computer, Group or Globally.

Enforced Encryption
for Windows

Automatically secure data copied on USB storage devices with an AES 256bit encryption. Cross-platform, password-based, easy to use and very efficient.

Content Aware Protection
for Windows

Email Clients: Outlook / Thunderbird / Lotus Notes • Web Browsers. Internet Explorer / Firefox / Chrome / Safari • Instant Messaging: Skype / Microsoft Communicator / Yahoo Messenger • Cloud Services & File Sharing: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Other Applications. i Tunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • OTHERS

Predefined Content Filters
Filters can be created based on predefined content such as Credit Card Numbers, Social Security Numbers and many more.

Custom Content Filters
Filters can also be created based on custom content such as keywords and expressions. Various Blacklist Dictionaries can be created.

Regular Expressions Filters
Advanced custom filters can be created to find a certain recurrence in data transferred across the protected network.

File Type Filters
File Type Filters can be used to block specific documents based on their extension, even if these are manually modified by users.

File Whitelisting
While all other attempted file transfers are blocked, whitelists can be created to avoid redundancy and increase productivity.

Domain & URL Whitelisting
Enforce company policy but allow employees the flexibility they need to do their work. Whitelist company portals or email addresses.

Reports and Analysis
Monitor activity related to file transfers with a powerful reporting and analysis tool. Logs and reports can also be exported to SIEM solutions.

Dashboard and Graphics
For a quick visual overview on the most important events and statistics, graphics and charts are available.

Active Directory
Take advantage of AD or similar tools, making larger deployment simpler. Import and sync all groups and entities.

Global and Regular Threshold for Filters
Define up to which number of violations a file transfer is allowed. It applies to each type of content or to the sum of all violations.

File Tracing
Record all file transfers or attempts to various online applications and cloud services, providing a clear view on users' actions.

File Shadowing
Save a copy of files that were transferred to controlled devices or through emails, cloud storage or other applications.

Create E-mail Alerts
Predefined and Custom e-mail alerts can be set up to provide information on the most important events related to confidential file transfers.

HIPAA Content Aware Policies
Allows for an in depth scanning of documents before the transfer is made for PHI info, FDA approved drugs, ICD-9 codes, etc.

eDiscovery
for Windows

File type: Graphic Files / Office Files / Archive Files / Programming Files / Media Files, etc. • Predefined content: Credit Cards / Personally Identifiable Information / Address / SSN / ID / Passport / Phone Number / Tax ID / Health Insurance Number / etc. • Custom Content / File Name / Regular Expression / HIPAA

Content and File Fype Scanning
Create custom eDiscovery policies defining what content is sensitive for your organization depending on file type, predefined content, custom content, file name, Regex or HIPAA protected content. Start scanning for sensitive data according to selected content.

Encrypt Data at Rest
Once confidential data is found, the option to encrypt it with AES 256 strong encryption solution is available in order to prevent unauthorized employees' access and to stop the possibility of leaking data.

Delete Data at Rest
Secure data and ensure compliance with industry regulations by deleting sensitive information immediately it is identified if it violates the company policy.

Export scan results
Scan results are available for export in Excel, PDF or CSV files and can be used as reports for the management or as audit documents. The scan results provide the details about on what computers sensitive data was found, what sensitive data, the path, time of discovery, if it was encrypted, deleted or reported, and other valuable information.

File Type Blacklist
File Type Blacklist can be used to detect specific documents stored on network's endpoints: graphic files, Office files, archive files, programming files and many others.

Predefined Content Blacklist
Add on the Predefined Content Blacklist information such as Credit Card Numbers, Social Security Numbers, Personally Identifiable Information and other data and discover if where it is stored and if it violates the company policy. This blacklist can help ensure compliance with regulations like PCI DSS, HIPAA and others.

Custom Content Blacklist
Create a blacklist based on custom content such as keywords and expressions. Various Blacklist Dictionaries can be created through Copy/Paste, Type or Import.

File Name Blacklist
Search for specific files based on their name and track their location. Results are displayed in the eDiscovery scan results with the list of found files and actions like delete, encrypt or decrypt can be performed.

Regular Expressions Blacklist
Advanced custom blacklists can be created to find a certain recurrence in data stored across the protected network.

HIPAA Protected Data
Allows for an in depth scanning of endpoints for PHI info, FDA approved drugs, ICD-10 and ICD-9 codes, etc. Meet compliance with HIPAA detecting where confidential healthcare information resides and applying remediation actions if necessary.

Thresholds
Avoid redundant scanning using the Threshold options. You can specify when inspection must stop according to a specific number of violations or what files must be scanned according to a minimum file size.

MIME Type Whitelist
Exclude MIME types from scanning, adding them in whitelists to avoid redundancy and increase productivity. Efficiently manage eDiscovery policies.

Allowed File Whitelist
Upload files in whitelists as exceptions from the scanning policies you defined in eDiscovery. Regardless if the policy is based in file type, predefined content, custom content, etc., the whitelisted files will be excluded from scanning.

AntiHACK.me

Device Control
for Windows

USB Drives / Printers / Bluetooth Devices / MP3 Players / External HDDs / Teensy Board / Digital Cameras / Webcams / Thunderbolt / PDAs / Network Share / FireWire /ZIP Drives / Serial Port / PCMCIA Storage Devices / Biometric Devices / OTHERS

Set Rights Globally
By default, device rights apply globally through the network. However, the module is extremely granular.

Set Rights per Group
Device rights can be granularly configured based on groups, allowing different access right for various departments.

Set Rights per Computer
Device rights can be configured per computer. Helpful when computers serve a unique role in the organization.

Set Rights per User
Based on their roles and tasks, each user can receive different device access rights according to the company policies.

Set Rights per Device
The granularity of the rights can be drilled down to the device level, based on Vendor ID, Product ID and Serial Number.

Custom Classes
Rights can be created based on classes of devices making management easier for products from the same vendor.

Trusted Device
For encrypted devices, different access rights can be configured based on the level of encryption (software, hardware, etc.).

File Tracing
Record all file transfers or attempts to various USB storage devices, providing a clear view on users' actions.

File Shadowing
Save a copy of files that were transferred to controlled devices that can later be used for audit purposes.

Offline Temporary Password
Temporarily allow device access to computers disconnected from the network. Ensure security and productivity.

Create E-mail Alerts
Predefined and Custom e-mail alerts can be set up to provide information on the most important events related to device use.
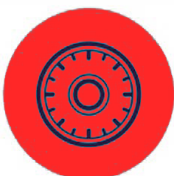
Dashboard and Graphics
For a quick visual overview on the most important events and statistics, graphics and charts are available.

Reports and Analysis
Monitor all activity related to device use with a powerful reporting and analysis tool. Logs and reports can also be exported.

Enforced Encryption
for Windows

USB Enforced Encryption
Authorize only encrypted USB devices and ensure all data copied on removable storage devices is automatically secured.

Strong Security Mechanisms
Government approved 256bit AES encryption, password protection and anti-tampering techniques to ensure application integrity.

Master Password
Creating a master password will provide continuity in various circumstances like resetting the user's password.

100% Deployment Flexibility

Suitable for any type of network, our products can be used by enterprise customers, small and medium business and even home users. With a client-server architecture, they are easy to deploy and centrally manage from the web-based interface. Besides the Hardware and Virtual Appliance, Amazon Web Services Instance and Cloud version, a Stand-alone version is also available for those looking for basic features.

My **Endpoint Protector**

Content Aware Protection, Device Control and Encryption are available for computers running on Windows.

Hardware Appliance   Virtual Appliance   Amazon Instance   Cloud Solution

Modules

Protected Endpoints

Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●