COMODO
Creating Trust Online®

Comodo
Internet Security

Software Version 11.0

Quick Start Guide

Guide Version 11.0.113018

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013
United States

Comodo Internet Security - Quick Start Guide

This tutorial explains how to use Comodo Internet Security (CIS). Please use the following links to go straight to the section that you need help with:

Installation

If you haven't done so already, please download the CIS setup file from **https://www.comodo.com/home/internet-security/security-software.php**

Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. More specifically, remove any other products of the *same type* as those Comodo products you plan to install.

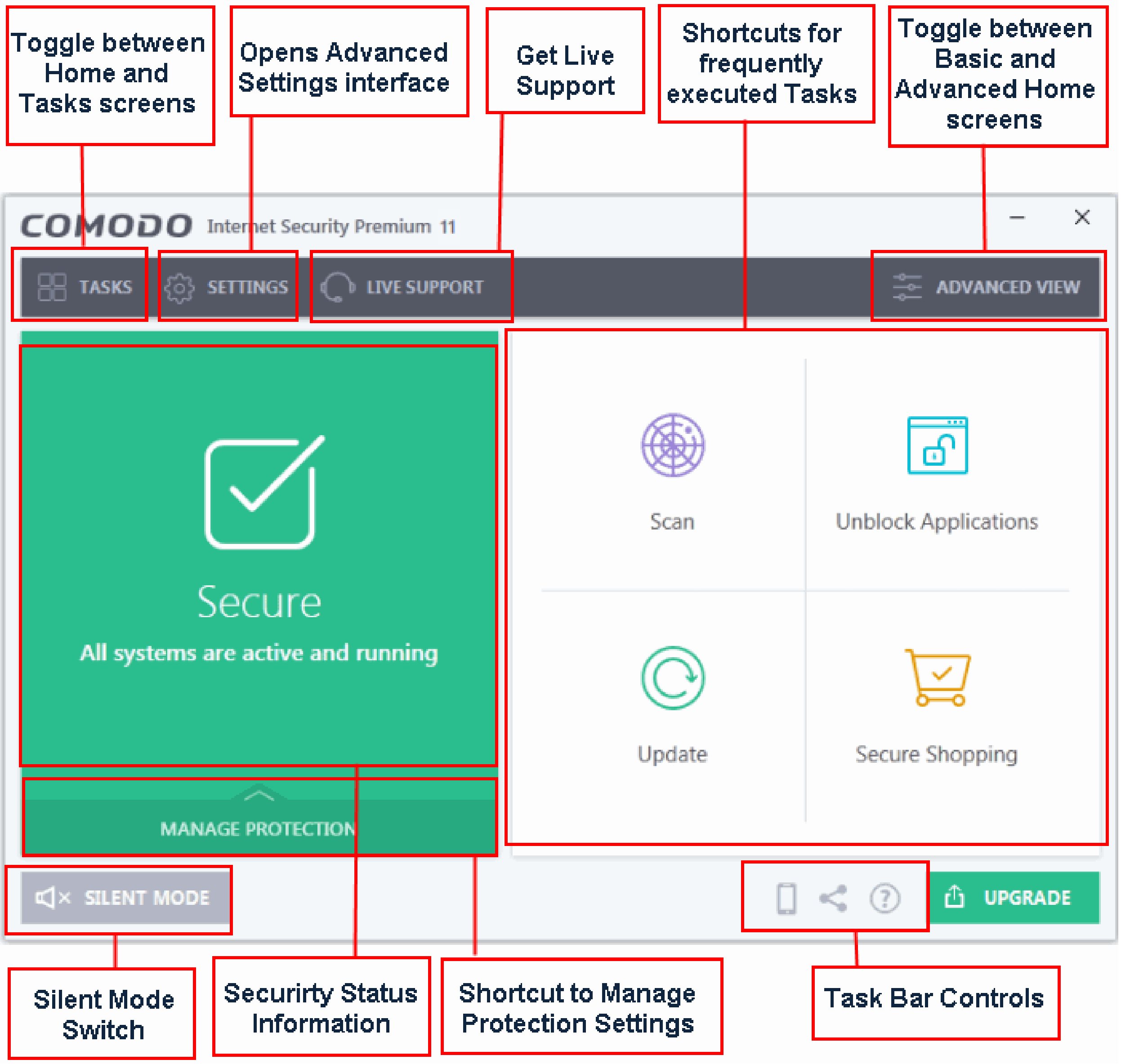
- Double click the CIS setup file to start the installation wizard.
- Click 'Customize Installation' if you wish to configure advanced options.
- After finishing the wizard, you need to reboot your computer to complete installation.
- After rebooting you will be asked to choose your type of internet connection
- On first load, the CIS interface will display a security status of 'At Risk', meaning you need to run your first antivirus scan.
- Click 'Fix It' to run the scan. The virus database will be updated automatically prior to the scan.
- After the scan has completed, click 'Fix It' again to deal with any discovered threats.

A more detailed description of the options available during installation can be found in the installation guide at **https://help.comodo.com/topic-72-1-772-9444-CIS-Premium-%E2%80%93-Installation.html**

The Main Interface

The CIS interface is designed to be as clean and informative as possible and lets you carry out tasks with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

Basic View


Toggle between Home and Tasks screens
Opens Advanced Settings interface
Get Live Support
Shortcuts for frequently executed Tasks
Toggle between Basic and Advanced Home screens
COMODO Internet Security Premium 11
TASKS
SETTINGS
LIVE SUPPORT
ADVANCED VIEW
Secure
All systems are active and running
Scan
Unblock Applications
Update
Secure Shopping
MANAGE PROTECTION
SILENT MODE
UPGRADE
Silent Mode Switch
Securirty Status Information
Shortcut to Manage Protection Settings
Task Bar Controls

- Overall security status is shown in the large box on the left. If problems are found, this box will show a large red 'X" and a 'Fix It!' button which will allow you to remediate the issue
- Click 'Home'/'Tasks' button at the upper left to switch between the home screen and the tasks interface
- The four smaller boxes on the right of the home screen show frequently executed tasks.
- To add or remove tasks in this area, click the 'Tasks' button at top-left then click the 'pin' icon 📌 next to your desired task
- Click 'Scan' to run an instant antivirus scan
- Scan individual files or folders by right-clicking on them and selecting 'Scan with Comodo antivirus'
- Flip between 'Advanced View' and 'Basic View' by clicking the toggle button ☰ at the upper-right
- Advanced view shows 'Antivirus', 'Containment' and 'Firewall' activities in greater detail. This includes the number of detected threats, last virus database update time, number of inbound and outbound connections and more. This view also allows you to quickly change security settings for each component.

- The 'Manage Protection' button in the 'security information' tile lets you to turn security components on or off.
- Switch on 'Silent Mode' to make sure nothing interrupts you while you play a full screen game
- The 'Upgrade' button allows Premium users to upgrade to CIS Pro or Complete
- The icons at the bottom-right corner of the home screen let you download Comodo mobile security apps, report problems or chat with Comodo security experts.

Scanning and Cleaning your Computer

Comodo Internet Security allows you to run on-demand virus scans at any time. If any threats are found then an alert screen will be displayed along with cleaning options.

- **Run a Quick Scan**
- **Run a Full Computer Scan**
- **Run a Rating Scan**
- **Run a Custom Scan**

Run a Quick Scan

The 'Quick Scan' profile will scan those critical areas of your computer which are most often targeted by viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files.

To run a Quick Scan

- Click the 'Tasks' button at top-left to open the 'Tasks' interface (if is not open already)
- Click 'General Tasks' > select 'Scan' > 'Quick Scan'
- The scanner will start and first check whether your virus signature database is up-to-date
- To pause, resume or stop the scan, click the appropriate button at the bottom of the interface
- If you want to run the scan in the background, click 'Send to Background'.
- On completion, the scan results screen will be displayed. The results screen shows the number of objects scanned and the list of identified threats (Viruses, Rootkits, Malware).
- Use the drop-down menu on the right to choose whether to clean, move to quarantine or ignore each threat.

Run a Full Computer Scan

A 'Full System Scan' scans every local drive, folder and file on your system. Connected devices such as USB drives, storage drives and digital cameras will also be scanned.

To run a Full Computer Scan

- Click the 'Tasks' button at top-left to open the 'Tasks' interface (if it is not open already)
- Click 'General Tasks' > select 'Scan' >' Full Scan'
- The scanner will check whether your virus signature database is up-to-date then start the scan
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'
- On completion, the scan results screen will be displayed. The results screen shows the number of objects scanned and the list of identified threats (Viruses, Rootkits, Malware).
- Use the drop-down menu on the right to choose whether to clean, move to quarantine or ignore each threat.

Run a Rating Scan

- The 'Rating Scan' feature is designed to evaluate the trust-level of all files and root certificates on your computer. Root certificates are used by your browser to verify the legitimacy of SSL certificates on websites that you visit.
- The scan will run a cloud-based assessment of your files and certificates and report back to you with a verdict on their rating.

Files are rated as follows:

- **Trusted** - The file or SSL certificate is safe
- **Unknown** - The trust-level of the file could not be determined. By default, unknown files will be automatically run in the CIS container. 'Unknown' files should be submitted to Comodo's Valkyrie system where they will undergo behavior analysis to identify whether they are safe or not.
- **Malicious** - The file is malware. You will be presented with disinfection and removal options for such files.
- **Untrusted** - Root certificates only. The root certificate is not safe.

To run a Rating scan

- Click the 'Tasks' button at top-left to open the 'Tasks' interface (if is not open already)
- Click 'General Tasks' > select 'Scan' > 'Rating Scan'

You can filter the results by rating using the 'Show' drop-down:

- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Auto-run**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately
- **Action:** Displays a drop-down with actions to be executed on Unrecognized and Malicious files identified.

Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis.
- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing to neither 'Clean' nor 'Trust', this file will be detected by the next ratings scan that you run.
- **Trust** - Files that you assign 'Trusted' status to will not be flagged in future scans. They will also be given a 'Trusted' rating in the 'File List' ('Settings' > 'File Rating' > 'File List').

You can apply an action to multiple files as follows:

- Select your preferred action from the drop-down menu at top-left
- Select all files to which you want to apply the action
- Click the 'Apply Selected Actions' button to implement your choice.

Run a Custom Scan

Comodo Antivirus allows you to create custom scan profiles to scan specific areas, drives, folders or files in your computer.

To run a custom scan

- Click the 'Tasks' button at top-left to open the 'Tasks' interface (if is not open already)
- Click 'General Tasks' > select 'Scan' >'Custom Scan'

The 'Custom Scan' panel will open with the following options:

Scan a folder - Scan the contents of folders and sub-folders. Choose the target folder in the 'Browse for Folder' window and click 'OK'.

Scan a file - Scan a specific file stored on your hard drives or external devices. Click 'File Scan' from the 'Custom Scan' pane to choose your target file.

More Scan options - Create a custom scan profile which lets you choose exactly which files and folders are scanned, when they are scanned and how they are scanned.

To create a custom scan profile

- In 'General Tasks', click 'Scan' > 'Custom Scan' > 'More Scan Options'
- In the 'Advanced Settings' interface, the 'Scans' pane opens with a list of pre-defined and user created scan profiles
- Click 'Add' from the options at the top create a new custom scan profile
- Type a name for the profile in the 'Scan Name' text box
- The buttons at the top allow you to add the items to be scanned in three ways:
  - **Add File** - Allows you to add individual files to the profile
  - **Add Folder** - Allows you to select entire folders to be included in the profile
  - **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory' and 'Trusted Root Certificate Store')
- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice
- Click 'Options' to further customize the scan
- Click 'Scan' beside the profile name to launch your scan

Run an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders, files and removable storage

To instantly scan an item

- Right click on a file, folder or drive and select 'Scan with COMODO antivirus' from the context sensitive menu

  OR
- Click the 'Advanced View' button (top-right)
- Drag and drop the item you wish to scan into the 'Drop Files to Scan' box

Set up the Firewall For Maximum Security and Usability

Note - the firewall is already configured to provide total security. This section is only for advanced users who wish to tweak the settings even further.

Stealth Ports Settings

Port Stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, sending no response to opportunistic port scans.

1. Open 'Firewall Tasks' from the Tasks interface
2. Open 'Stealth Ports' interface by clicking the 'Stealth Ports' icon from the' Firewall Tasks' panel
3. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

Network Zones Settings

The 'Network Zones' settings allows you to configure connections for a router/home network. (This is usually done **automatically** for you).

To view the configurations

1. Click 'Settings' > 'Advanced Settings' >'Firewall'>'Firewall Settings'
2. Click 'Network Zones' under 'Firewall' from the left hand side pane
3. Click 'Network Zones' tab from the 'Network Zones' interface
4. Inspect the Loopback zone and Local Area Network #1 by clicking the '+' button beside the zone name.
    - In most cases, the loopback zone IP address should be 127.0.01/255.0.0.0
    - In most cases, the IP address of the auto detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0
5. Click 'OK'.

Firewall Settings

The 'Firewall Settings' option allows you to configure the protection level for your internet connection and the frequency of alerts generated.

To open Firewall Settings panel

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'Firewall Settings' under 'Firewall' on the left.
3. Ensure that 'Enable Firewall' is selected and choose 'Safe mode' from the drop-down beside it.

Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the Advanced Settings interface:

- Deselect 'Do not show pop-up alerts'
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.

Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select **Filter loopback traffic**
- Ensure that the **Block fragmented IP traffic** is selected
    - **Block fragmented IP traffic -** When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack.

Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow your download time.

- Select the **Do Protocol Analysis** checkbox to detect fake packets used in denial of service attacks
- Select **Enable anti-ARP spoofing**

Click 'OK' for your settings to take effect.

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules on an application-specific and a global basis. You can also create and deploy predefined firewall rule-sets.

To view Application Rules

- Click 'Settings' to open the 'Advanced Settings' interface
- Click 'Firewall' > 'Application Rules'
- Use this interface to add, edit, enable/disable or remove internet connection rules for specific applications.

To view Global Rules

- Click 'Settings' to open the 'Advanced Settings' interface
- Click 'Firewall' > 'Global Rules'
- Use this interface to add, edit, enable/disable or remove global rules which apply to all traffic

To view Predefined Firewall rulesets

- Click 'Settings' to open the 'Advanced Settings' interface
- Click 'Firewall' > 'Rulesets'
- Use this interface to add, edit, enable/disable or remove rulesets

Set up HIPS for Maximum Security and Usability

The Host Intrusion Prevention System (HIPS) provides maximum security from malicious programs that try to execute on your system, protecting you from data theft, computer crashes and system damage. It prevents buffer overflow attacks, root-kits, inter-process memory injections, key-loggers and more.

To configure HIPS

- Click 'Settings' to open the 'Advanced Settings' interface
- Click 'HIPS' > 'HIPS Settings'
- Select 'Enable HIPS' and choose 'Safe Mode' from the drop-down.

Monitoring Settings

- Click 'Monitoring Settings' from the 'HIPS Settings' interface
- Make sure that all the check boxes are selected and click 'OK'

Advanced Settings

- Make the following settings under 'Advanced' in the HIPS Settings interface
    - Optional - Enable adaptive mode under low system resources. Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems.
    - Optional - Enable 'Block all unknown requests if the application is not running'. Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been

shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked.

Run Untrusted Programs in the Container

Comodo Internet Security allows you to run programs in the container on a one-off basis. This is helpful to test the behavior of new executables that you have downloaded and/or you are not sure that you trust. There are a couple of ways of doing this:

Run a program inside the container by right-clicking

1. Browse to the installation folder of the .exe file through Windows Explorer
2. Right-click on the program that you want to run inside the container
3. Choose 'Run in COMODO container' from the context sensitive menu

Run a program in the container from the 'Containment Tasks' interface

1. Click 'Containment Tasks' > 'Run Virtual' from the 'Containment Tasks' interface
2. To run an application inside the container, click 'Choose and Run' then browse to the application. The contained application will run with a green border around it. If you wish to run the application in the container in future, then select 'Create a virtual desktop shortcut'.
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Note. By default, all 'unknown' programs are automatically run in the container. You can disable this behavior and/or modify containment rules in the 'Auto-Containment' settings area. To access this interface, open CIS > 'Settings'

Browse the Internet and Run Untrusted Programs inside the Virtual Desktop

The Virtual Desktop allows you to browse the internet and run untrusted programs inside a 100% virtual environment. Programs running inside this virtual environment are isolated from the rest of your computer and so cannot infect it. For example, if you inadvertently download malware from the internet while browsing in the virtual desktop, then that malware will not be able to damage your computer or access your private data.

Start the Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

  Or

- Click 'Run Virtual Desktop' from the basic view of CIS home screen

Note: Please ensure Comodo Dragon and Microsoft Silverlight are installed to utilize the 'Virtual Desktop' to its full potential.

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left of the Virtual Desktop
2. Select the browser you want to run

Desktop Shortcuts

Files and shortcuts on your real desktop are available to you when you open the Virtual Desktop. Simply open the

Virtual Desktop, double-click on one of your desktops files or shortcut, and that item will open the virtual environment.

Shared Space

The Virtual Desktop creates a folder Shared Space in the location "C:\ProgramData\Shared Space". This space is shared by your host operating system and the Virtual Desktop and allows you to move items between the two environments. It also provides another way for you to open programs in the virtual environment.

The shared space folder can be accessed in the following ways:

- Click 'Open Shared Space' under 'Containment Tasks' in the 'Tasks' Interface

To open an application or file from your host system in the Virtual Desktop

1. Open 'Shared Space' as mentioned above
2. Copy/Move your application or file into the Shared Space
3. Start the Virtual Desktop
4. Open 'Shared Space' inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.
5. Double click on the application/file in the shared space to open it inside the 'Virtual Desktop.'

Renew or Upgrade Licenses

CIS will notify you when it is time to activate or renew your license:

Activate CIS

- Click 'Activate Now' beside 'Subscription' in the home screen to activate your License. You should have received your license key through email if you have purchased CIS Pro/Complete.

For CIS Complete / Pro activation:

    - Complete the registration form to activate your license.
        - If you already have a Comodo account, select 'I already have a COMODO Account. Enter your username and password and click 'Next'.
        - If you haven't yet created an account, select 'I do not have a COMODO account' and click 'Next'.

- Comodo servers will validate your purchase and activate your license.
- Click 'Continue' to exit the wizard. The main interface will show the number of days remaining on your license.

Renew / upgrade your license

To renew or upgrade your license,

- Click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left').
- The 'Product Activation' wizard will start.
- Click the 'Get License Key' link. You will be taken to **https://secure.comodo.com/home/purchase.php?afl=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDlDNDE4MzBDQjc1NDlENUIzRkY&lid=&** .
- Select your CIS Package.
- Select 'Existing Comodo User' in the 'Enter Customer Details' area. Type your username and password and complete the payment form.
- Your license key will be sent to you by email. Activate your license with the new key.

More Help

User Guide - **https://help.comodo.com/topic-72-1-623-7587-Introduction-to-Comodo-Internet-Security.html**

Community Forums - **https://forums.comodo.com/comodo-internet-security-cis-b125.0/**

Product Support (Pro and Complete customers only)

- General questions and advice - please use the Geek Buddy client to instantly chat with a Comodo technician
- Submit support tickets at **https://support.comodo.com/**

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: EnterpriseSolutions@Comodo.com