

REAL-TIME THREAT PROTECTION



WEBROOT
SecureAnywhere®



PREVENT MALWARE AND RANSOMWARE TAKING ROOT

Laptops, desktops, smartphones, tablets, servers, and virtual environments - just some of the things we all use in our day to day jobs and are vital to keeping your business running. So why wouldn't we protect them if they're so important?

Endpoint protection/security means cybersecurity services for network endpoints, like laptops, etc. These services include antivirus and antimalware, web filtering and more. Endpoint protection helps you keep critical systems, intellectual property, customer data, employees, and guests safe from ransomware, phishing, malware and other cyberattacks.

Webroot delivers real-time protection and prevents malware, viruses and ransomware infections from taking root, securing your device wherever you connect. Its DNS protection automatically blocks inbound threats for endpoints and networks, as well as cloud-based threat intelligence services - giving you 360° security, by covering you and your devices.

PROVEN SECURITY BY THE NUMBERS

Webroot protects you from:



6,000

New phishing attacks
every day



25,000

New dangerous websites
every day



101,000

New malicious files
every day

“Not only has it saved us from a widespread attack, but it continually finds malware when other products have failed. Webroot caught over 1900 viruses and malware that had infected our corporate network. The management, notifications, and ease of use have been stellar. We are extremely pleased with Webroot and you have a lifetime customer.”

TONY GRECO, SENIOR SYSTEMS ADMINISTRATOR, RUMBERGER, KIRK & CALDWELL

Webroot offers complete protection from viruses and identity theft for all your devices, without slowing you down.

And it's all down to the smarter cybersecurity layers consisting of 3 services:

- Endpoint Protection
- DNS Protection
- Security Awareness Training



ENDPOINT PROTECTION

Easily secure users across all stages of a cyberattack in real time.

Powered by the industry-leading cloud-based Webroot Threat Intelligence Platform, Webroot solutions combine the latest real-time intelligence with advanced behaviour and machine learning. Using up-to-date, cloud-based technology, Webroot can detect, analyse, categorise, score and highly accurately predict the threats each endpoint is experiencing in real time.

Why you need it

- 93% of all malware is polymorphic/unique
- 36% increase in phishing attacks in 2018
- Ransomware protection - a major threat



DNS PROTECTION

Stop up to 88% of malware at the domain layer across corporate and guest networks.

With DNS Protection, there's a straightforward and highly effective way to prevent everyday web usage from becoming a major security risk. The intuitive web-based DNS Protection console enables admins to finely tune web access policies by IP address or IP range, and limit access to any other websites that you may consider a risk to your network.

Why you need it

- Filters out 88% of inbound threats
- Secures against DNS attacks, redirection etc
- Covers all network traffic not just devices



SECURITY AWARENESS TRAINING

We can educate you and other members of staff with safer practices to help look after your business.

Webroot's Security Awareness Training offers comprehensive and affordable cybersecurity education for you and your business. Training consists of simple, easy to run courses and campaigns that minimise user-generated risks and help reduce infection rates, thereby driving down your remediation costs and reducing the overall risk to your business.

Why you need it

- Cyber-criminals target employees/end users
- Click rates fall-37% to 12%, in just 6 months
- Affordable, effective and high ROI

PRODUCT FEATURES AND BENEFITS, YOU CAN SEE WORKING FOR YOU



LIGHT ENDPOINT AGENT

Webroot's agent doesn't take up much space meaning it won't affect the performance of your machine.



WEB TRAFFIC THREAT REPORTING

Get detailed reports on demand on all threats the business would've been susceptible to without DNS Protection in place and get full visibility into risk and usage.



IDENTITY THEFT PROTECTION

Webroot protects your usernames, account numbers, and other personal information against keyloggers, spyware, and other online threats targeting valuable personal data.

SECURITY FEATURES AND BENEFITS, ALWAYS WORKING HARD IN THE BACKGROUND



FEATURES	BENEFITS
Web Threat Shield	Blocks known threats encountered on the internet and displays a warning.
Identity Shield	Providing safe internet browsing and data protection, blocking attempts to gain personal information without user consent. During online transactions, it watches for Trojans or phishing sites that try to steal personal data, including usernames, passwords, and account numbers.
Real-time Anti-Phishing	Verifies sites at the time of the request to ensure they are genuine and safe.
Outbound Firewall	Protects against outgoing traffic originating inside a network or on an endpoint.
Real Time Shield	Blocks known threats from running and monitors unknown programs to determine whether they contain threats.
USB Shield	Monitors installed USB flash drives for threats, and blocks and removes any threats that it finds.



FEATURES	BENEFITS
Offline shield	Protects your system from threats even on systems that are disconnected from the internet.
Behavior Shield	Analysing the applications running on managed endpoints. If it detects a suspicious file, it opens an alert and prompts the admin to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage or steals information.
Core System Shield	Monitors system structures of your devices and ensures that malware has not tampered with them. If the shield detects a suspicious file trying to make changes, it opens an alert and prompts the admin to block or allow the item.
Journaling & Rollback	Continuous infection monitoring. If a file or process can't be immediately classified as good or bad, then the agent begins monitoring all events. If a monitored process is categorised as malicious, any changes to local drives are automatically reversed.
Heuristic Control	Behavior-based interception capabilities analyse potential threats in real time, reducing the window between a threat emerging to it being detected.
Agent Commands	Within the console Webroot offers a range of over 40 agent commands, including the high degree of remote-control. Cutting down on physical visits and associated man-time costs and making it much easier for your IT provider to remotely manage multiple endpoints.

SECURE YOUR BUSINESS TODAY

Tel:

Email:

Web: