

Highest-Rated Protection Thanks to a Layered Security Approach

Build a layered defense against today's most prevalent malware threats with VIPRE. Secure your endpoints, email servers, virtual environments and mobile devices from emerging threats like viruses, Trojans, rootkits, exploits, spyware, malicious websites, phishing attacks and more.

Mission #1 for your endpoint security solution is stopping malware and VIPRE Endpoint Security accomplishes this through next-generation scanning technology, always-on Advanced Active Protection, heuristics, signatures and other sophisticated detection methods.

Advanced Malware Defense

Powered by next-generation advanced machine learning, one of the world's largest threat intelligence clouds, and real-time behavior analysis, VIPRE Endpoint Security protects from ransomware, zero-day attacks, phishing, exploit kits, mobile threats and other malware that easily evade traditional signature-based antivirus. VIPRE Endpoint Security provides:

Advanced Ransomware Prevention - VIPRE's Advanced Active Protection uses real-time behavior monitoring, artificial intelligence and one of the world's largest threat intelligence clouds to help prevent ransomware.

Integrated Patch Management - Ensure installed third party applications are up to date and secure against exploit kits delivering ransomware and data-stealing payloads.

Intelligent Anti-Phishing and Email Security - Defend one of ransomware's top threat vectors by keeping employee inboxes safe from malicious attachments and phishing links.

Removable Device Control and Encryption - Limit the risk presented by introducing infected devices to the network and keep your data out of the wrong hands with encryption.

Mobile Device Management - Secure Android™ devices from mobile malware and locate, lock and wipe lost Android and iOS devices.

Cloud-Based Roaming Services - Secure and centrally manage remote PCs that leave the network via a cloud-based service using secure HTTPS protocols.

Malicious URL Blocking - Block users from visiting malicious websites or links serving malware and accidentally infecting their PCs and the network.

Unprotected Computer Identification - Alerts are sent when any machines accessing the network without antivirus protection, helping to stop infections before they spread.



Simply the Best.

VIPRE wins Top-Rated Security Product and consistently wins 100% block rates and zero false positives from AV-Comparatives.

Schedule a Demo

See how VIPRE's award-winning malware defense can bolster your security by scheduling a demo today!

Let's Talk

Contact us today to learn how we can bolster your defense against ransomware and other advanced threats evading traditional antivirus.

Leading the Industry

VIPRE receives top ratings from the industry's leading independent testing authorities.



Why VIPRE

The Best Protection at the Best Price – VIPRE consistently outperforms big name security vendors in the industry's most comprehensive independent testing.

Easiest to Use – VIPRE's intuitive management console and preconfigured settings makes it easy to secure your networks from ransomware and other threats.

Fastest to Deploy – Admins can deploy VIPRE in less than 10 minutes and have the option of automatically removing any old antivirus agents.

Small Footprint – VIPRE proves speed and security do go together by protecting you from malware without slowing down your PCs.

Free U.S.-Based Support – VIPRE always has the customer's back with free, highly- rated, award-winning, U.S.-based tech support.

Advanced Active Protection

Emerging and undiscovered threats like zero-day vulnerabilities mean businesses must stay on the cutting-edge or risk an attack. Malware creators have learned to change their behavior to evade systems, and that means protection should continually advance as well.

How It Works

VIPRE's Advanced Active Protection monitors the processes that run on endpoints and looks at new ones when they start. The actions taken are then measured against heuristic rule sets. The sophisticated algorithms detect malicious behaviors and stops the threat from acting. Any actions the malicious process took can then be reversed, where possible. What's more, the discovered behaviors are shared with integrated cloud services, enabling researchers to create even more proactive detections. All of this is accomplished without bogging down systems, keeping users happy and secure.