VIPRE®

DATASHEET | ENDPOINT SECURITY SERVER EDITION

VIPRE ENDPOINT SECURITY

Server Edition

PROVEN, INDUSTRY LEADING ENDPOINT SECURITY FOR BUSINESS

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.

VIPRE Endpoint Security protects at the file, application and network layer, combining multiple layers of security with network- and application-agnostic DNS protection at no additional charge.

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 against ransomware, zero-day attacks, phishing, exploit kits, mobile threats and other malware that easily evade traditional signature-based antivirus. VIPRE Endpoint Security provides:

$4.62 MILLION

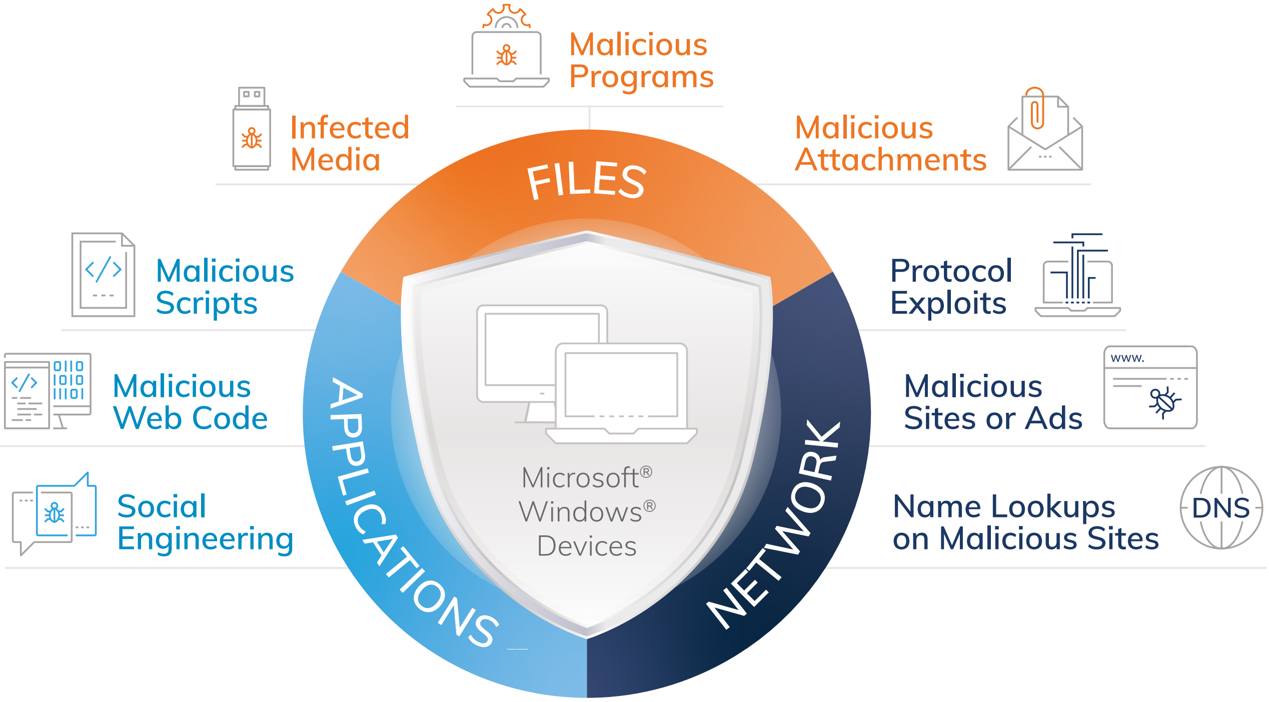
The Ponemon Institue reported that the average total cost of a ransomware breach in 2021, not including the cost of the ransom was *$4.62M (USD).*[1]

$11 MILLION

In 2021, Brazil-based food processor JBS S.A. paid a record *$11M (USD)* ransom after losing almost two *weeks of productivity* from a ransomware attack.[2]

- **Advanced Ransomware Prevention** - VIPRE's Advanced Active Protection uses real-time behavior monitoring, AI and one of the world's largest threat intelligence clouds 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.
- **Cloud-Based Roaming Services** - Secure and centrally manage remote PCs that leave the network via a cloud-based service using secure HTTPS protocols
- **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

MULTI-LAYER ENDPOINT SECURITY PROTECTION



FILE LAYER	
Managed Scans	Automatic and easy manual deep scanning for malicious files, with granular administrative control and delegation
Active File Protection	Interactive protection of every file touched on the system
Signature-based Detection	Definition database containing millions of known malware signatures updated several times a day
Emulation	Unwinds and interprets malware code in a virtual environment to quickly detect threats and catch advanced malware
Exclusions	Easily identify allowed files and business applications

APPLICATION LAYER	
Host Intrusion Prevention System (HIPS)	Rule-based system that prevents malicious processes from executing malicious activity
Active Process Protection	Leverages machine learning to interactively analyze process behavior and detect potentially malicious activity

NETWORK LAYER	
Intrusion Detection System (IDS)	Looks for suspicious data in the IP frame portion of the packet leveraging more than 8,000 rules, as well as within the application data itself
DNS Protection	Prevent users from accidentally visiting malicious sites by intercepting DNS queries for those known-malicious domains and replacing the normal IP address response with a redirect to our DNS sinkhole
Malicious URL Blocking	Prevents access to specific URLs by checking against a global threat intelligence network kept up-to-the-minute with the latest list of known-bad URLs
Web Exploit Prevention	Looks for suspicious data in the IP frame portion of the packet leveraging more than 8,000 rules, as well as within the application data itself
Browser Extensions	Protects encrypted web content by performing analysis within the browser itself, via browser extensions for Firefox and Chrome
Exclusions	Easily identify allowed files and business applications

WHY CHOOSE VIPRE?

VIPRE puts more than twenty years of advanced security intelligence, cutting-edge machine learning, real-time behavioral analysis, and a comprehensive threat intelligence network to work defending against today's attacks and even tomorrow's zero-day

- **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 pre-configured 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 Support** – VIPRE always has the customer's back with free, highly-rated, award-winning tech support.

> "Anyone familiar with that type of virus understands the potentioal damage it can cause to an organization. When our employee double-clicked on the cryptolocker file, VIPRE vaporized it instantly."
>
> **Matt Bauer**, *McKernan Packaging Clearing House*

VIPRE Endpoint Security Server Features

- ✓ Endpoint Protection and Anti-malware
- ✓ DNS Protection
- ✓ Active File Protection
- ✓ Machine Learning
- ✓ Active Process Protection
- ✓ Intrusion Detection System
- ✓ Host Intrusion Prevention System
- ✓ Malicious URL Blocker
- ✓ Email Protection
- ✓ Anti-phishing
- ✓ Firewall
- ✓ Low CPU and Memory Usage
- ✓ Competitive Agent Removal Tool
- ✓ Browser Extensions
- ✓ Third Party Patch Management
- ✓ Device Control and Encryption

[1] https://www.ibm.com/security/data-breach
[2] https://www.nytimes.com/2021/06/02/business/jbs-beef-cyberattack.html

Count on **VIPRE Endpoint Security Server** to stay ahead of the changing threat landscape.

LEARN MORE ABOUT SECURITY SERVICES FROM VIPRE

ENDPOINT

EMAIL

TRAINING

NETWORK