HEAT AntiVirus
Prevent Malware from Stealing Data and Disrupting Operations

New malware continues to be created at an exponential rate – at the start of 2015, AV-Test Institute was registering over 390,000 new malicious programs every day. Much of today’s malware is fueled by financially-motivated cyber criminals trying to gain access to valuable corporate, consumer and/or personal data.

With the enormous variety of malware in the wild today, organizations need an antivirus solution that provides fast and accurate identification of the vast amount of known malware. And with the sophistication of malware continuing to increase daily, organizations need an antivirus solution that employs multiple detection techniques to identify and block unknown malware (e.g. zero-day threats).

Use in Combination with Application Whitelisting to Ensure Defense-in-Depth Endpoint Protection
To prevent these threats from disrupting operations and potentially stealing data, organizations need strong and comprehensive endpoint protection using complementary solutions on different endpoints depending on their security requirements. HEAT AntiVirus provides advanced protection via traditional signature-matching and partial signature matching capabilities – as well as embedded malware detection, heuristic and sandboxing techniques to provide proactive protection against zero-day threats. HEAT AntiVirus is available as an integrated module in the HEAT Endpoint Management and Security Suite.

HEAT AntiVirus provides:
- Proven technology that incorporates a pioneering and industry-leading proactive anti-malware engine to block malware such as viruses, Trojans, worms, spyware and more from wreaking havoc on endpoints.
- Removal of identified malware to ensure that any detected malware is not allowed to remain on network assets.
- A complementary offering to other HEAT endpoint security modules that when combined delivers effective defense-in-depth security against targeted and blended attacks.

Key Features
- Full Signature Matching Capabilities
- Variant and Exploit Detection
- Behavioral Analysis Detection
- Real-time, Scheduled and On-Demand Scanning
- Granular AV Policy with CPU Throttling
- Comprehensive Malware Removal
- Automatic Signature Updates
- Integration with HEAT Endpoint Management and Security Suite

Key Benefits
- Complements application whitelisting technology for an effective defense-in-depth approach
- Combines traditional signature-based protection with unique behavioral analysis
- Prevents known and unknown malicious threats (zero-day exploits) from gaining unauthorized access to systems and data
- Provides the ability to create and schedule multiple AV scans per endpoint with different scan settings and resource utilization at different times
- Ensures comprehensive clean-up, including rootkit removal
- Fully automated detection of endpoints and signature updates
Key Features

**Full Signature Matching Capabilities:**
Recognizes, blocks, and removes viruses, worms, Trojans and other types of malware such as keyloggers, hijackers and rootkits. Anti-malware capabilities protect your network, endpoints and organization from malicious code which compromises security, privacy and/or performance.

**Variant and Exploit Detection:**
Protects against new and unknown malware (zero-day exploits) via partial signature matching that detects components of malware that have been re-used from previous attacks and via embedded malware detection, which detects and stops hidden malware that has been injected into otherwise benign file types such as PDFs.

**Unique Behavioral Analysis:**
Delivers another layer of protection via behavioral analysis which runs suspect executables in a safe emulation to look for malicious behavior and identify sophisticated zero-day malware.

**Real-time Scanning:**
Ensures protection against common malware entryways by enabling malware scanning of files as they are being opened for reading, writing or execution.

**Scheduled Scanning:**
Provides in-depth protection against malware by scanning entire endpoints on a predetermined schedule.

**On-demand Scanning:**
Delivers targeted in-depth assessment and protection by scanning malware on specific endpoints as needed.

**Targeted Scanning:**
Allows endusers to manually initiate on-demand AV scans pointed at specific drives, folder and files.

**Comprehensive Malware Removal:**
Ensures that any detected malware is removed or quarantined and not allowed to remain on network assets.

**Granular AV Policy Management with CPU Throttling:**
Provides finer-grained protection vs. performance control to better match organisation’s risk tolerance, thus ensuring endpoint performance and user productivity is not impacted by AV scans.

**Automatic Signature Updates:**
Allows for schedulable, automated and attendant-free operation, reducing administrative overhead and improving TCO while maintaining control.

**Integration with HEAT Endpoint Management and Security Suite:**
Integrates with other HEAT product modules to streamline and improve IT operations and security, reduce agent bloat and improve endpoint visibility.

**System Requirements**
Visit HEATSoftware.com for the latest product details and information.