K7 SECURITY

DATA SHEET

K7 Endpoint Security

ADVANCED EDITION

Every day, organizations are challenged with defending their networks against malicious attempts to breach their cyber defenses. Cybersecurity is one of the most important IT buying decisions an organization makes to ensure successful and continuous business operations. The effects of a targeted malware attack can quickly bring a business to its knees, negatively affecting an organization's efficiency and incurring lost productivity from the workforce.

Protecting a company's intellectual property and securing customer data are good business practices, however, the cost of deploying, managing, and maintaining commercial IT management and security controls can be cost prohibitive for any up and coming business. The best endpoint and server anti-malware solutions deployed within the enterprise must strike balance between proactive threat detection, manageability, performance, and operational cost.

Business-Class Anti-Malware

K7 Security develops endpoint and server anti-malware solutions for small, medium-sized, and enterprise-class businesses, offering a broad range of features and capabilities to counter today's most destructive threats. Available in both Standard and Advanced editions, K7's Endpoint Security can support multiple centralized management (on premises or on cloud) modes to simplify deployment, streamline IT operations, and meet both internal and external compliance requirements.

Performance Optimized Endpoint Security

K7 leads the industry in performance optimization and a significantly small memory footprint, helping organizations to reduce the impact of resource intensive malware protection on existing systems. Performance and memory optimization can also defer future costs associated with low-end system replacement or hardware upgrades to a later date.

Integration with Centralized Management Platforms

K7 Security's Centralized Management platform gives IT Administrators organization-wide visibility into threats to proactively protect endpoints vulnerable to malware and malicious attacks. Managed via the cloud or deployed on-premises, centralized administration allows for remote installation, configuration, and reporting of K7 endpoint solutions deployed throughout the enterprise.

Hourly Updates Minimize Exposure and Risk

With hourly updates, K7 Security helps businesses protect against the latest malware threats around the clock - 24/7/365 days a year. Hourly updates reduce an organization's window of vulnerability by minimizing the risk and business impact of fast moving malware or outbreaks that quickly lead to system or network compromise.

Multi-Threat Protection

K7 Security develops proactive, multi-platform anti-malware solutions that detect and stop Trojans, viruses, spyware, adware, ransomware, and other malware threats that can compromise the integrity of endpoints and ultimately, the corporate network.

Offline Updates

The offline update facility enables high-security isolated intranets to receive program enhancements and malware definitions using data storage devices, gaining updated cyberthreat protection while avoiding the risks associated with internet connectivity.

Key Features

- Low cost, high performance endpoint protection and cyberthreat prevention for small and medium-sized businesses
- Detect and mitigate real-world threats such as viruses, spyware, ransomware, and phishing attacks
- Granular Firewall with integrated HIDS to block targeted system level attacks
- Device access protection against USB propagated malware threats
- Optimized performance and small memory footprint extends the useful life of older systems
- Flexible on-premises or cloud-based centralized management
- Create and enforce consistent endpoint security policy across desktops and servers
- Web Filtering allows centralized control and granular enforcement of website access based on pre-defined categories, including gambling, adult-related content, hacking tools, and more
- Centralized application control policies block unwanted or harmful applications
- Complex reports on applications, devices and threats for your unique business needs can be generated and extracted in Excel and PDF formats
- Enterprise Asset Management tracks all endpoint hardware asset on the network, generates reports, and sends notification on changes
- K7 Enterprise Security supports an effortless migration process. Ensuring a hassle free transition, K7 will uninstall any existing product and install itself automatically

K7 Sentry – On-access/On-demand Scans - On-access and on-demand scanning technology identifies and blocks both known and unknown malware objects before they impact systems.

Heuristic Malware Detection Technology – Complementing traditional signature-based detection, heuristic detection uses behavioral analysis to proactively identify and block unknown malware in addition to zero-day exploits.

Ransomware Protection - Ransomware protection monitors the behavior of potentially- suspicious processes, especially any process that writes to certain target file types and blocks attempts to change them.

K7 Firewall (HIDS/HIPS) – Proactively Block Threats - Host-based firewall with an integrated Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS) protect against direct application- and system-level attacks.

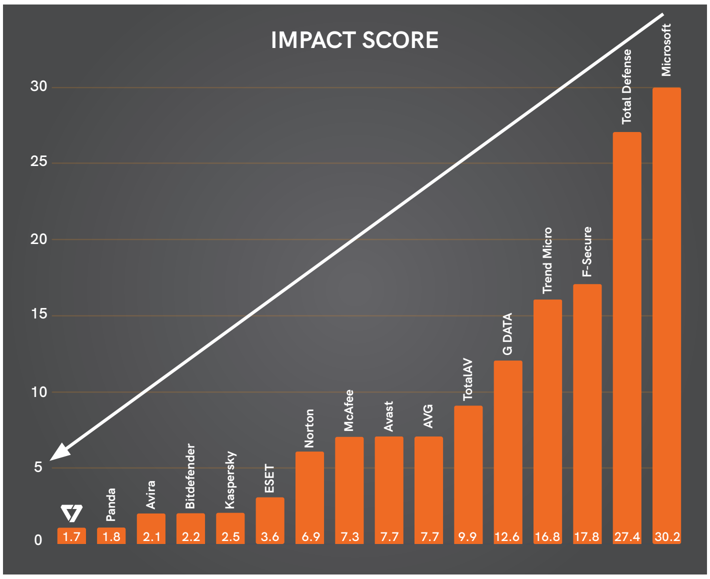
K7 SafeSurf – Secure Online Browsing - Protect endpoints from internet-based malware infections and drive-by-download attacks by using heuristic URL analysis and cloud-based website reputation services to block threats before malicious payloads can be deployed.

K7 Device Control – Eliminate USB and Storage Media Infection - Block access to unknown and unauthorized USB storage devices which may contain a malware payload.

K7 Application Control – Block Unauthorized Applications – Implement a centralized policy to control unwanted applications installed on endpoint systems. Instant messengers, Bit-torrent clients, or other bandwidth intensive applications can be blocked from running, accessing the network, or accessing the internet.

K7 Web Filtering – Block Unauthorized Content – Centralized policy definition and enforcement of endpoint website access to unauthorized or inappropriate content. Web filtering covers thousands of predefined websites grouped by category and blocked continuously or at scheduled times.

LOWEST IMPACT ON DEVICE PERFORMANCE



AV-Comparatives Performance Test – April 2023

K7 Security Platform Support:

Endpoint
Both 32- & 64-bit architecture*, except XP

- Microsoft Windows XP (SP2 or later)[32bit], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 (SP1 or later), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019
- Linux and Mac support is available

Server Console
Both 32- & 64-bit architecture*

- Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019

* ARM architecture is not supported

Features Comparison	Standard	Advanced
Detect Viruses, Spyware, and Phishing Attacks	✓	✓
Rootkit and Ransomware Detection	✓	✓
Safe Surf (URL Scanning)	✓	✓
Email Protection	✓	✓
Smart Firewall with Integrated HIDS/HIPS	✓	✓
Centralised Application Control and Enforcement	×	✓
USB Device Access Protection/USB Vaccination	×	✓
Web Filtering (Website Blocking/Filtering by Category)	×	✓
Centralised Management	✓	✓
Multiple Daily Updates	✓	✓
Security Information and Event Management (SIEM) Integration	✓	✓

About K7 Security

K7 Security develops endpoint and server anti-malware solutions for small, medium-sized, and enterprise-class businesses, offering a broad range of features and capabilities to counter today's most destructive digital threats. Available in both Standard and Advanced editions, K7's Endpoint Security can support multiple centralised management modes to simplify deployment, streamline IT operations, and meet both internal and external compliance requirements.

K7 Enterprise Security Private Limited
India | Singapore | UAE | USA

www.k7enterprisesecurity.com