K7 SECURITY

DATA SHEET

K7 Cloud Endpoint Security

ADVANCED EDITION

Businesses are under constant cyberthreat as criminals resort to data theft, industrial espionage, sabotage, and ransom demands to monetise their cyberattacks. A mobile workforce and employees working from home increase the cybersecurity challenge as the business premises no longer define the IT perimeter. K7's Cloud Deployed Endpoint Security is the comprehensive, cost-effective, protection that isn't restricted by time or place which the modern enterprise can rely on.

Cloud Console

Unlike conventional cybersecurity products that require a dedicated on-premises server to run the admin console, Cloud Deployed Endpoint Security has its admin console in the cloud, avoiding the cost of additional hardware and hardware redundancy measures.

Remote Deployment

The cloud deployment enables 100% remote deployment, where neither employees nor K7 personnel need to visit the business's offices to install K7's cybersecurity. The quick and hassle-free deployment ensures rapid protection of the entire organisation.

Anytime, Anywhere Control

Cyberattacks are not restricted by working hours, time zones, or regions; cyber defences need to be similarly unrestricted to be effective. Using just a web browser, IT administrators can access the K7 cloud console at anytime, from anywhere, having instant, centralised, and complete control over the business's cybersecurity.

Enterprise-Class Malware Protection

Enhanced with artificial intelligence, K7 Security's protection for endpoints and servers helps small, medium, and large businesses secure data, protect devices, reassure clients, and comply with contractual and regulatory requirements.

High Performance, Low Resource Impact

K7's products are engineered to provide potent anti-malware defences without taxing system resources. Low memory footprint and blazingly fast scans on modest hardware allow businesses to save costs by deferring hardware upgrades without compromising cybersecurity.

Multiple Daily Updates

New cyberthreats are constantly emerging and cybersecurity needs to be frequently updated to counter them. K7 Labs analyses lakhs of malware samples every day and distributes multiple malware definition updates daily to ensure that businesses are always protected against the latest cyberthreats.

Comprehensive Threat Protection

K7 Security products provide comprehensive protection against viruses, malware, ransomware, Trojans, phishing, spyware, zero-day attacks, social engineering, and many other cyberthreats. Threat protection includes both signature-based detection and heuristic analysis, with secure deconstruction to identify and defeat obfuscation attempts.

Key Features

- Cloud control for anytime, anywhere administration through a web browser
- 100% remote installation
- No dedicated machine on premises
- Low cost, high performance endpoint protection
- Detect and mitigate real-world threats such as viruses, spyware, ransomware, hacker intrusions, and phishing attacks
- Granular Firewall with integrated HIDS to block targeted system-level attacks
- Device access protection against USB propagated malware threats
- Optimised performance and small memory footprint extends the useful life of older systems
- Create and enforce consistent endpoint security policy across desktops and servers
- Centralised control and granular enforcement of website access based on pre-defined categories, including gambling, adult-related content, hacking tools, and more
- Centralised application control policies block unwanted or harmful applications
- Detailed reports on applications, devices, and threats can be generated and extracted in Excel and PDF formats
- Enterprise Asset Management tracks all endpoint hardware assets on the network, generates reports, and sends notification on changes
- Effortless migration process. K7 will uninstall any existing product and install itself automatically

Multi-layered Protection

- **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 behavioural analysis to proactively identify and block unknown malware in addition to zero-day exploits
- **Ransomware Protection** – Ransomware protection monitors the behaviour 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) protects against direct application and system level attacks

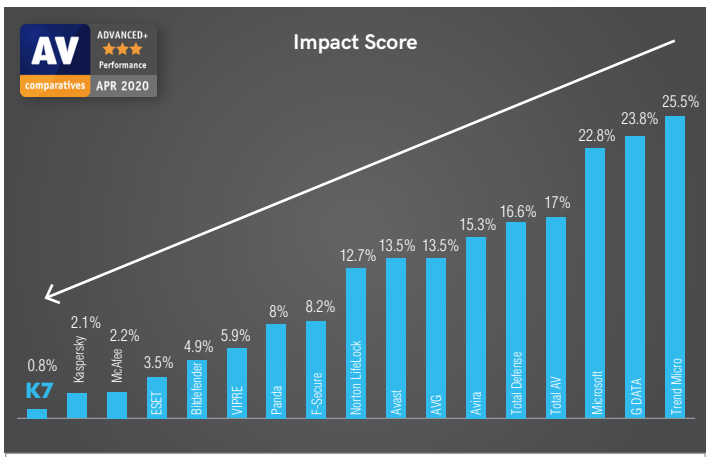
K7 Security Platform Support

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

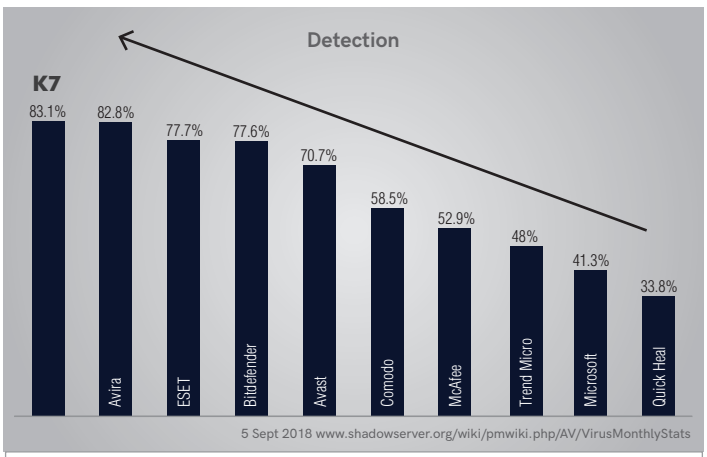
- **K7 Safe Surf – Secure Online Browsing** – Protects endpoints from internet-based malware infections and drive-by-download attacks by using heuristic URL analysis and cloud-based website reputation services
- **K7 Device Control – Eliminate USB and Storage Media Infections** – Block access to unknown and unauthorised USB storage devices which may contain a malware payload. Set host level policies to enforce device password access, file execution, and on-demand or automatic device scanning configurations
- **K7 Application Control – Block Unauthorised Applications** – Implement a centralised policy to control unwanted applications installed on endpoint systems. Instant messengers, BitTorrent clients, or other bandwidth intensive applications can be blocked from running, accessing the network, or completely denying internet access
- **K7 Web Filtering – Block Unauthorised Content** – Centralised policy definition and enforcement of restrictions on access to unauthorised or inappropriate content. Web filtering covers thousands of predefined websites grouped by category and blocked continuously or at scheduled times

LOWEST IMPACT



AV-Comparatives Performance Test April 2020

HIGHEST IN PROTECTION



Zero-Day Detection

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, and enterprise-class businesses that offer a broad range of features and capabilities to meet today's most ardent 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 Computing Private Limited 4th Floor, Tower – B, Tek Meadows, 51 Rajiv Gandhi Salai, Sholinganallur
Chennai – 600 119, Tamil Nadu, India. Toll free : 1800 4190077 | **www.k7computing.com**.

EPS CDS AD Feb 2021