K7 SECURITY

DATA SHEET

K7 Cloud Endpoint Security

STANDARD EDITION

21st century business has to be just as connected and mobile as its customers to serve them effectively. This expands the attack surface as the number of devices connecting to the enterprise network increases, and devices used by remote workers or employees working from home connect to business networks without the protection of secured enterprise IT infrastructure. K7's Cloud Deployed Endpoint Security is the cybersecurity solution that modern businesses need to secure their operations against the increasing number of cyberthreats that target digitally enabled businesses.

Cloud Console

K7's Cloud Deployed Endpoint Security has its admin console in the cloud. No dedicated machine is required on-premises, which saves costs.

Remote Deployment

Some employees rarely, or even never, visit your office but their device still needs to be cybersafe. Cloud deployment enables 100% remote deployment where neither your staff nor ours need to visit your office to roll out K7 cybersecurity across your organisation.

Anytime, Anywhere Control

Use just a web browser to access the cloud console at anytime, from anywhere. Being able to immediately respond to cybersecurity requests or incidents gives you the confidence to rapidly add new devices, users, and locations to your business.

Enterprise-Class Malware Protection

Businesses need cybersecurity not only to protect their operations and users but also to comply with contractual terms and statutory requirements, and to avoid penalties for non-compliance. K7's cybersecurity products help small, medium and large businesses meet these requirements with robust protection for endpoints and servers.

High Performance, Low Resource Impact

Businesses shouldn't have to upgrade hardware just to run a cybersecurity product. K7 Security's renowned low memory footprint, low bandwidth consumption, and fast scans ensure that device performance and user productivity is not affected even on older devices with lower hardware specifications.

Multiple Daily Updates

We analyse lakhs of malware samples every day because cybercriminals are constantly creating new attacks, and we release multiple malware definition updates every day to ensure that devices and clients always enjoy protection against the latest threats.

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. New cyberthreats are constantly emerging and threat actors try to obfuscate their attacks to evade cybersecurity. K7 employs multiple technology approaches to detect and defeat malware, including artificial intelligence, signature-based detection, heuristic analysis, and secure deconstruction.

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
- Detects and mitigates real-world threats such as viruses, spyware, ransomware, hacker intrusions, and phishing attacks
- Granular Firewall with integrated HIDS to block targeted system-level attacks
- Optimised performance and small memory footprint extends the useful life of older systems
- Create and enforce consistent endpoint security policy across desktops and servers
- 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

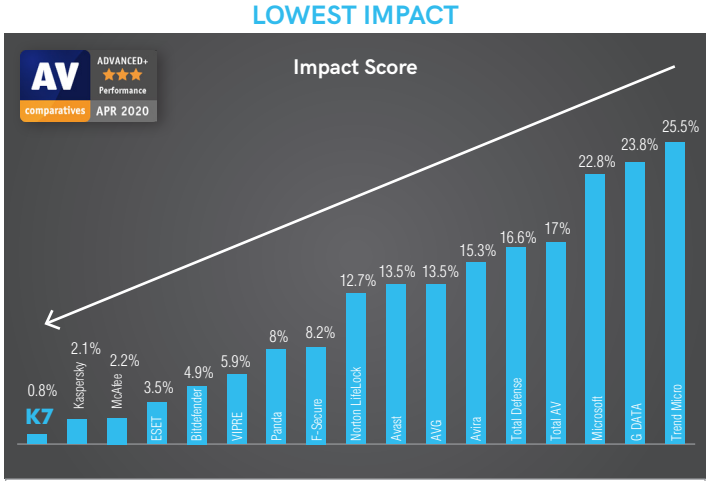
- **K7 Sentry – On Access/On Demand Scans** – On-access and on-demand scanning technology identifies and blocks both known and unknown malware objects before they impact systems
- **Heuristic Malware Detection Technology** – Complementing traditional signature-based detection, heuristic detection uses 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 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 Security Platform Support

Both 32 & 64 bit architecture, except XP

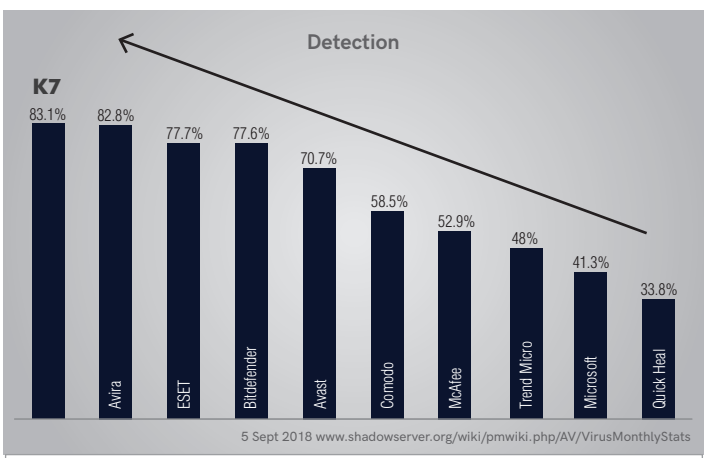
- Microsoft Windows XP (SP2 or later)[32bit], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 (SP1 or later), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019

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 SD Feb 2021