

# K7 Endpoint Security

## Advanced+ Edition

Every day, organisations 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 organisation 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 organisation'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 a 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 Standard, Advanced, and Advanced+ editions, K7's Endpoint Security can support multiple centralised management (on premises or on cloud) modes to simplify deployment, streamline IT operations, and meet both internal and external compliance requirements.

### Performance Optimised Endpoint Security

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

### Integration with Centralised Management Platforms

K7 Security's Centralised Management platform gives IT Administrators organisation-wide visibility into threats to proactively protect endpoints vulnerable to malware and malicious attacks. Managed via the cloud or deployed on-premises, centralised administration allows for remote installation, configuration, and reporting from K7 Endpoint Security clients deployed throughout the enterprise.

### Hourly Updates Minimise 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 organisation's window of vulnerability by minimising the risk and business impact of fast-moving malware or outbreaks that quickly lead to device 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 cyberthreats 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, medium-sized, and enterprise-class businesses
- Detect and mitigate real-world threats such as viruses, spyware, ransomware, and phishing attacks
- Granular Firewall with integrated HIDS to block targeted device-level attacks
- Device access protection against USB propagated malware threats
- Optimised performance and small memory footprint extends the useful life of older devices
- Flexible on-premises or cloud-based centralised management
- Create and enforce consistent endpoint security policy across desktops and servers
- Web Filtering allows 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
- Complex reports on applications, devices, and threats relevant to your unique business needs 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 notifications on changes
- K7 Endpoint 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 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 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 unauthorised USB storage devices which may contain a malware payload.
-  **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 accessing the internet.
-  **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.

### K7 Security Platform Support

#### Endpoint

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

- Microsoft Windows XP (SP2 or later) [32 bit], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2003 (SP1 or later), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

- Linux and Mac support is available

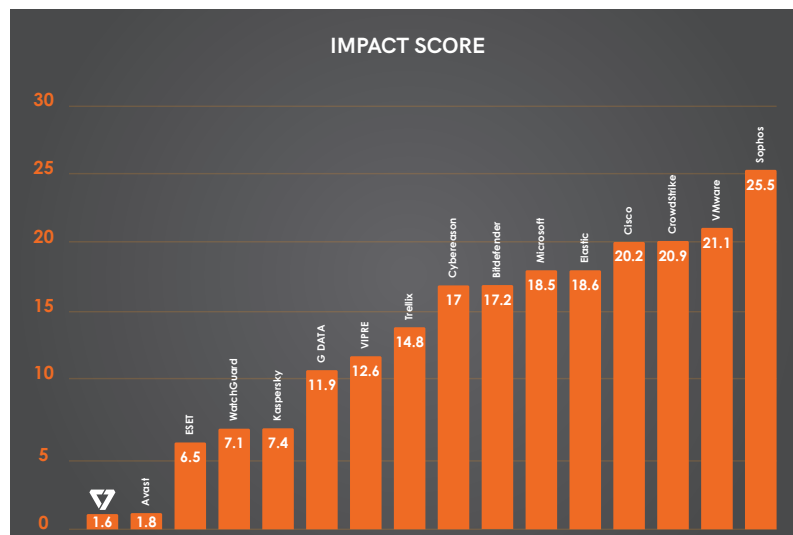
#### Server Console

Both 32- & 64-bit architecture\*

- Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, , Windows 11, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

\* ARM architecture is not supported

### LOWEST IMPACT ON DEVICE PERFORMANCE



AV-Comparatives Performance Test – November 2023

#### Additional Features

- |                              |                                  |
|------------------------------|----------------------------------|
| ✓ Cloud Sandbox              | ✓ Virtual Keyboard               |
| ✓ Backup and Restore         | ✓ PC Tuneup Tools                |
| ✓ Encrypted File Vault       | ✓ Automatic Bandwidth Management |
| ✓ Data Loss Prevention (DLP) | ✓ Global Threat Intelligence     |
| ✓ Full Disk Encryption       | ✓ Update Rollback                |
| ✓ Password Manager           | ✓ Endpoint Forensics             |
| ✓ Social Media Protection    | ✓ Patch Management               |
| ✓ Cloud Backup Space*        | ✓ 24-hour Support*               |

\* Pricing based on scope

### 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. 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](http://www.k7enterprisesecurity.com)