K7 SECURITY

K7 CLOUD ENDPOINT SECURITY

GRAPHENE EDITION

THE NEW STANDARD IN
ENTERPRISE RANSOMWARE PROTECTION

Businesses are under constant cyber threat as threat actors resort to data theft, industrial espionage, sabotage, and ransom demands to monetise their cyber attacks. Cyber security solutions help mitigate this risk but slow down hardware and networks, hampering operations and requiring IT infrastructure upgrades that drive up the cost of cyber security.

K7 Cloud Endpoint Security – Graphene incorporates K7's patent-pending technology to help enterprises protect their operations without impacting productivity and profits by delivering cost-effective, efficient, proactive EDR. Graphene is a supermaterial that is 200 times stronger than steel and 1,000 times lighter than paper, perfectly representing K7's robust protection that is light on hardware and network resources.

Cloud Console

Unlike conventional cyber security products that require a dedicated on-premises server to run the admin console, K7 Cloud Endpoint Security – Graphene has its admin console in the cloud, avoiding the cost of additional hardware and hardware redundancy measures.

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.

Patent-pending Deception Technology with Proactive EDR

K7 Endpoint Security – Graphene combines patent-pending Deception Technology, developed by K7, with K7's Proactive EDR to anticipate, identify, and block the next generation of ransomware before a malicious payload can be deployed.

Remote Ransomware Protection

Remote ransomware, which threat actors deploy on unprotected endpoints to attack files in shared folders on protected endpoints, cannot be detected by conventional endpoint security solutions. K7 Cloud Endpoint Security – Graphene has been specially developed by K7 to identify and stop remote ransomware and automatically block the unprotected infected endpoint to secure enterprise IT infrastructure.

Safe Mode Protection

K7 Cloud Endpoint Security – Graphene's antivirus and firewall protection is enabled in Safe Mode (Network Only, Minimal Only, Network and Minimal Only) ensuring that ransomware cannot infect an endpoint that is started in Safe Mode to run diagnostics.

Enhanced Malware Startup Entry Cleanup

The proactive protection framework in K7 Cloud Endpoint Security – Graphene prevents ransomware, and other malware, from initialising through Startup Entries, Scheduled Tasks, and Windows Management Infrastructure (WMI) Event Subscription.

Extended Anti-Ransomware Policy Configuration

Admins can force K7 user-mode services to start very early in the order of services with dynamic management of conceding resources to the operating system, ensuring K7 protects other services during device boot; save scanning time by reducing double scanning; and include/exclude specific processes and targets from ransomware monitoring.

Threat Intel Logs for SIEM Integration

K7 Cloud Endpoint Security – Graphene provides Threat Intel Logs that have been designed by K7 Threat Labs to integrate with Security Incident and Event Management (SIEM) solutions, enabling seamless data transfer for proactive security management by enterprise IT teams.

Key Features

- Cloud control for anytime, anywhere administration through a web browser
- 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 device-level attacks
- Device access protection against USB propagated malware threats
- Optimised performance and small memory footprint extends the useful life of older devices
- 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 notifications on changes
- Effortless migration process. 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

Best-in-Class Ransomware Protection – AI-enhanced ransomware protection that monitors the behaviour of potentially suspicious processes, with advanced protection against remote ransomware

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

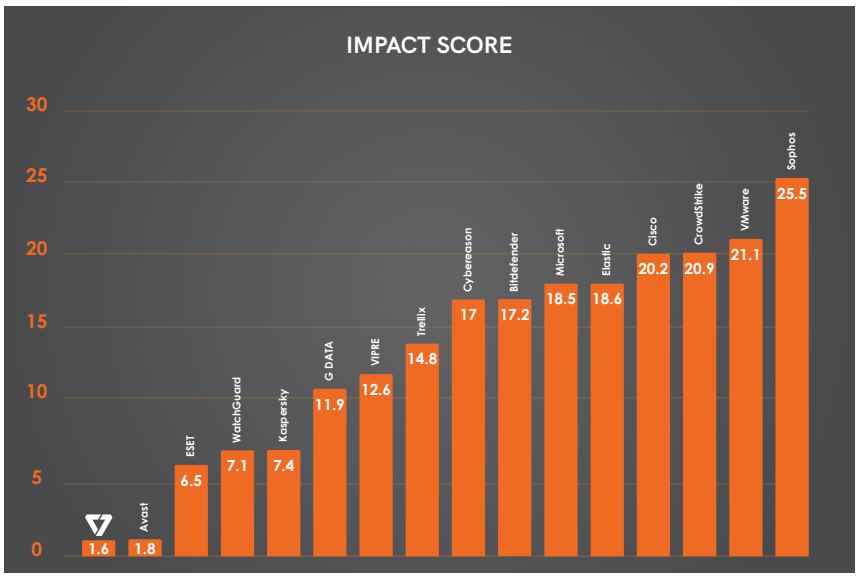
K7 SafeSurf – Secure Online Browsing - Protects endpoints from internet-based malware infections and drive-by-download attacks by using heuristic URL analysis and cloud-based website reputation services

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 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

LOWEST IMPACT ON DEVICE PERFORMANCE



AV-Comparatives Performance Test – November 2023

Features Comparison	Advanced	Graphene
Detect Viruses, Spyware, and Phishing Attacks	✓	✓
Ransomware Protection	✓	✓
Remote Ransomware Protection	×	✓
Safe Mode Protection	×	✓
Deception Technology	×	✓
Enhanced Malware Startup Entry Cleanup	×	✓
Safe Surf (URL Scanning)	✓	✓
Email Protection	✓	✓
Smart Firewall with Integrated HIDS/HIPS	✓	✓
Centralised Management	✓	✓
Threat Intel Logs for Security Information and Event Management (SIEM) Integration	×	✓

K7 Security Platform Support

Both 32- & 64-bit architecture*

- 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

* x86 only

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 SECURITY

The Global Cyber Security Pioneer

India | Singapore | UAE | USA

www.k7cybersecurity.ae

March 2024