K7 SECURITY

TECHNOLOGY OVERVIEW

Business Challenges Posed by Today's Threat Landscape

Every single day organisations face a deluge of malicious probes and attempts to breach their cyber defences. The automation and simplification of complex attack tools used for system and network reconnaissance and infiltration have considerably lowered the skill-set required for any bad actor to successfully compromise business systems and gain a foothold within the enterprise. The incentives for hackers to steal both Personally Identifiable Information (PII) and proprietary company information are many. Significant amounts of money can be made on the Dark Web from the illicit trade of stolen data for financial fraud, strategic business benefit, or nation-state advantage.

The architects of black market malware tools and the hackers that use them have created a trillion-dollar industry based on fraud, with strong ties to organised crime. While malware developers have targeted business-centric computing platforms for some time, they have also been developing tools that are capable of exploiting other platforms - including Android and iOS – to gain access deep within the enterprise. These personal devices usually forgo the necessary IT security checks required by other IT assets, allowing them to circumvent perimeter security controls and assist in the exploitation of business ecosystems.

Malware-centric threats to corporate networks include;

- **Viruses and Spyware** – surreptitious application modification and spread, data theft, deteriorating system performance, unauthorised software installation (PUPs) and redirecting browser activity
- **Phishing Trojans** – emails containing attachments (e.g. documents, PDFs, images) or embedded code to drop malware
- **Ransomware** – forced encryption of critical user files with ransom unlock demands
- **Backdoor Trojans and Keyloggers** – unauthorised remote system monitoring and access, leading to data theft
- **SpamBots and DDoS Botnets** - compromised systems used to send spam emails and to perform Distributed Denial of Service (DDoS) attacks
- **Remote Access Trojan (RAT)** - responsible for creating a backdoor in the target system to transfer complete system control to a remote attacker

Malware infection vectors are many, including:

- Sharing infected USB storage devices between multiple users and systems
- Executing malicious attachments in spam emails
- Malicious documents bundled with malware payloads
- Drive-by downloads that exploit a browser, application, or system vulnerabilities
- Vendor-hosted "App Stores" serving plugins, extensions, or applications that install malicious embedded code
- Self-replicating worms using the Internet to propagate malware and infect systems
- Sophisticated malware called Advanced Persistent Threats (APTs) that exploit a browser, application, or system vulnerabilities, and are much more difficult to detect and remediate
- Weak Bring Your Own Device (BYOD) policy helping perpetrators to deliver malicious payloads including malware

K7's Multi-Layered Security Technology

Malware is the number one threat to enterprise networks and has become the top concern for IT Administrators and CIOs alike. Malware is by far the most time and resource intensive threat for an organisation to mitigate due to its diversity, complexity, and persistence. Malicious attackers and threat actors continuously evolve their Tactics, Techniques, and Procedures (TTPs) to bypass perimeter security controls and system defences by using malware to gain a foothold within the network.

Closing the Window of Vulnerability

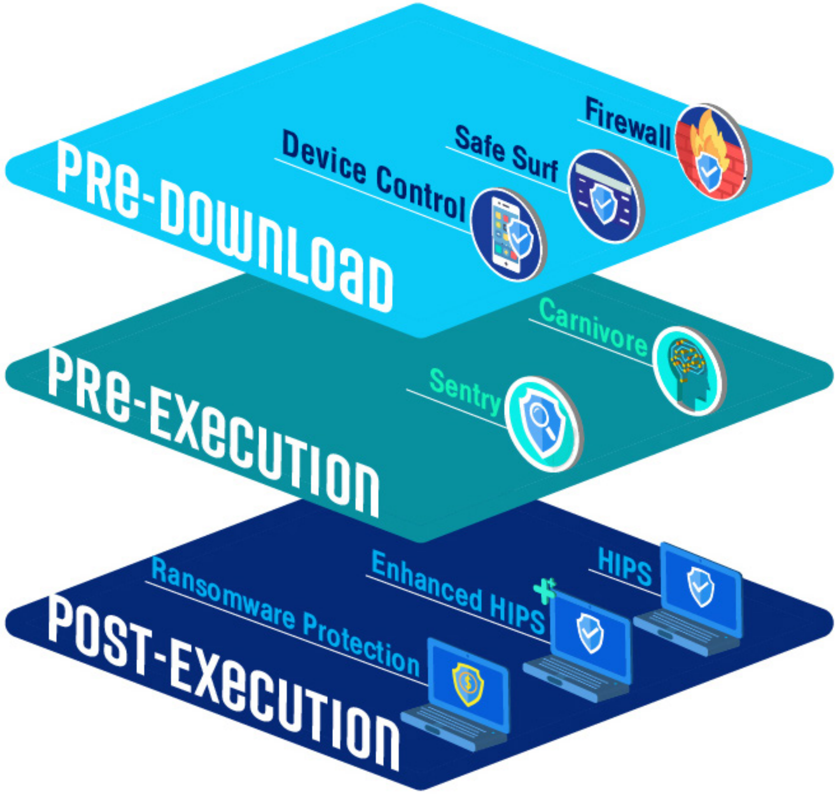
New threats and malware variants are created continuously and released into the wild to take advantage of the system and human weaknesses, making it difficult for companies to maintain a proactive security posture.

Unfortunately, there is often a gap between the time a new threat is identified and the availability of a signature to detect it. This gap represents a window of vulnerability leaving devices unprotected and vulnerable to attack and, ultimately, to compromise.

Detecting and removing malware once it has become embedded within a system is a non-trivial task that may take hours or days to achieve, so it is critically important to mitigate any threat before execution. Therefore the best defence is a proactive, multi-layered security approach to block threats throughout the different stages of the malware attack lifecycle.

K7 Endpoint Security for Enterprise

Endpoint security solutions today must provide accurate and up-to-date protection to ensure the survivability of the host, and, in turn, protect the enterprise environment from further exploitation. K7 Security develops and builds anti-malware solutions that utilise award-winning proactive detection and prevention technologies, along with enterprise-class manageability, to help keep critical business systems secure, and ready to meet and defeat new and existing cyber threats as they arise.



Business Protection against Multi-Platform Threats

Organisations today are challenged with the implementation of cost-effective security solutions that can keep pace with the continually changing threat landscape, while at the same time providing the capabilities required to maintain business continuity. Explicitly developed with SMB budgets and network environments in mind, K7's Business Solutions can help maintain operational efficiency and reduce the resources and costs associated with Internet-related and other threats.

K7's Business Solutions allow companies to:

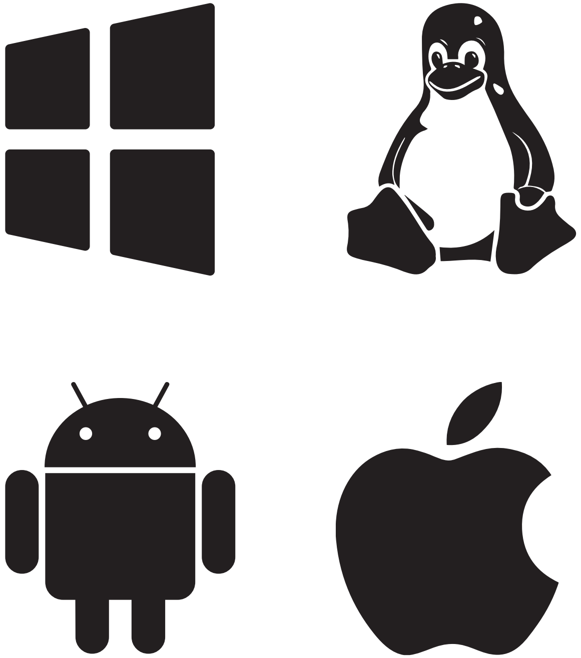
- Provide IT administrators with network-wide visibility into all malware-related incidents
- Implement a unified platform for remote installation, configuration and reporting of all K7 clients throughout the network
- Remotely configure and manage K7 client system settings
- Report on malware-related incidents to identify infection rates and trends
- Measure the effectiveness of the K7 anti-malware security program

Today's business security solutions need to go beyond essential malware detection and prevention to provide a solution capable of implementing controls and managing policy for a large number of endpoints and servers, all with minimum effort.

K7 Security supports the following platforms:

- Microsoft Windows
- Linux
- Mac OS
- Android
- iOS

Small and medium-sized businesses can quickly implement a defence-in-depth blacklisting policy via K7's Business Solutions to better protect their network against diverse threats.



K7 - Threat Mitigation Technologies

K7 Security Solutions uses many different detection and mitigation techniques and technologies to provide multi-layer protection against malware threats.

K7 Sentry – On Access / On-Demand Scanning

K7's on-access and on-demand scanning technology identify and block both known and unknown malware objects before they can execute or when invoked by using a combination of automated and custom signatures in addition to heuristic analysis. Generic signatures are designed to detect all variants of a specific malware family by identifying common traits, whereas heuristic analysis identifies suspicious or malicious characteristics of malware.

Heuristic Malware Detection Technology

In addition to traditional signature-based detection, heuristic detection uses behavioural analysis to identify and block unknown malware, along with zero-day exploits, proactively. Because heuristic scanners look for behavioural characteristics rather than relying on simple pattern-matching, they can detect and prevent new and emerging threats before a malware signature is released.

K7's heuristic scanner can detect and mitigate a wide range of threats including malicious code attempting to exploit browser vulnerabilities, malicious files, and ransomware execution.

K7 - Threat Mitigation Technologies

K7 SafeSurf – Secure Online Browsing

Without the right protections, the chances of picking up a malware infection from surfing the Internet are incredibly high, as the majority of malware are encountered online. In many cases malware is hosted unwittingly by legitimate websites that have been previously hacked, thus stealthily distributing malware to unsuspecting end-users. The compromised websites are used in drive-by-download attacks, automatically installing malware on vulnerable end-users who visit the webpage. To combat surfing threats, K7 proactively identifies malicious websites using heuristic URL analysis and cloud-based website reputation services, protecting against malicious website code long before a payload can be deployed.

K7 Firewall / HIPS – Proactively Block Threats

A host-based firewall is the cornerstone of adequate system security. K7's Firewall works in concert with the integrated Host Intrusion Prevention System (HIPS) that can stealth a system's ports and protect against direct application and system-level attacks. The Firewall's Intrusion Detection System (IDS) capability detects and blocks known malicious network-based exploits such as remote kernel exploits, SQL injection, and RDP attacks before the system can process them.

K7 Device Control – Eliminate USB and Storage Media Infection

One of the most successful malware propagation methods to infiltrate deep into an organisation happens when end users share files using USB storage devices. K7 Device Control can be configured to block access to unknown and unauthorised USB storage, and other media devices such as CD/DVD or floppy drives, which may contain a malware payload. To minimise the risk of USB infection, Administrators can set host-level policies to enforce device password access and file execution restrictions in addition to on-demand and automatic device-scanning configurations.

Ransomware Protection

Readily available on the Dark Web, ransomware toolkits can make a relatively mediocre hacker into a successful cybercriminal with lots of money-extorting potential. Being hit by ransomware is a scary proposition that can bring a company to its knees. Wannacry is just one infamous example of ransomware that crippled the U.K's National Health Service (NHS) by locking out 30+ hospitals from their computer systems. Wannacry ransomware manipulated the ETERNALBLUE exploit developed by the NSA (in the USA) with a self-replicating malware that rapidly spread to unpatched Microsoft Windows systems and encrypted their files.

Stopping Ransomware Cold

Ransomware is a particularly destructive type of malware that locks out a user from their computer until a financial ransom is paid to unlock it - usually in the form of untraceable Bitcoin or another cryptocurrency. Important personal or company sensitive files can be irreversibly-damaged by ransomware, so it is imperative to take several precautions to lessen the impact of ransomware and stop it in its tracks before significant damage takes place.

K7's ransomware protection monitors the behaviour of potentially-suspicious processes, especially any process that attempts to modify certain target file types and blocks these attempts fundamentally. Ransomware protection also examines any sudden large increases in the randomness of content (entropy) for unrecognised file types, such as free-flowing text files, to identify and block any malicious encryption behaviour.

K7 was the first security solution vendor to devise and share with the security community a near fool-proof protection mechanism in the fight against ransomware. Ransomware is so damaging that K7 researchers shared their knowledge of proactive ransomware blocking techniques at an international security conference, thus helping to protect users globally against this dangerous and destructive menace.

The K7 Security Scan Engine

A malware scan engine must be capable of identifying many different forms of malware across multiple platforms and device types. K7's award-winning scan engine has evolved over many years and has been recognised by leading certification bodies, including AV-Test, AV-Comparatives, ICSA Labs, Virus Bulletin, and West Coast Labs, for its unmatched proactive anti-malware protection, providing some of the quickest and most accurate malware detection in the industry. Today, the K7 engine supports in-depth analysis of thousands of different objects from various executable binary formats, to several static and dynamic archives, scripts, documents, etc., along with automated and bespoke generic and heuristic malware detection for them all. Signatures can either be in an interpreted byte-code format or crafted to execute natively, providing great flexibility with speed.

Multi-Step Scanning Increases Detection Accuracy

1. In order to provide maximum security, the K7 scan engine uses a four-step scanning process.
2. Each time a file is accessed, copied or downloaded via the Web, email or instant messenger, the file is intercepted and sent for scanning.
3. The file is checked against the K7 Signature Database that is updated very frequently (currently on an hourly basis).
4. If the file contents match a signature, the product automatically tries to disinfect the malware.
5. If this action fails, the file is moved to the quarantine folder. If no signature is matched, the file is passed to the Carnivore heuristics module for further analysis.

Secure Deconstruction

A file designated for scanning goes through a secure dissection process in a sandboxed environment where complex objects are broken down into their components, with each element scanned rigorously for malicious content. If an object contains layers of obfuscation, an "unpacking" process using specific combinations of decryption and decompression is used to unravel the underlying object, thus revealing the real functionality and true intent of the malware.

Signature Optimization Engine

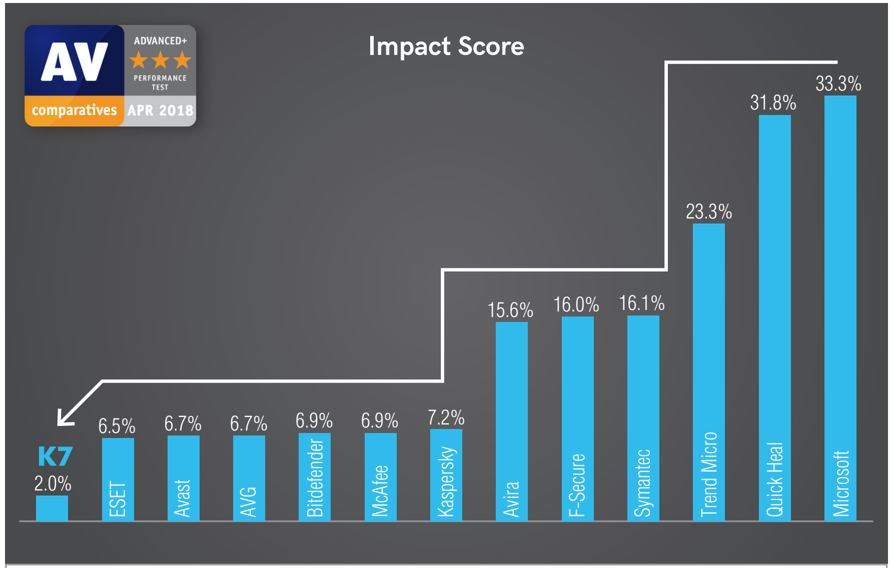
Optimal code execution and the minimal use of computing resources has been a key component of K7's engineering DNA.

The challenge for many AV vendors is achieving superior malware detection capability without impacting the performance of the endpoint or server it is installed upon. Anti-malware solutions are expected to detect thousands of different malware families and hundreds of thousands of malware variants to keep a system safe. It is therefore understandable that the size of the detection signature database would increase exponentially over time and that system resources would be required to bridge that performance shortfall.

Superior System Security without Performance Degradation

To minimise the system performance impact, K7 Security has developed a proprietary lean data-loading algorithm and ordering mechanism which minimizes the use of computing resources, both RAM and CPU, from the on-disk signature detection data. The K7 Signature Optimization Engine reduces the memory footprint to less than 25% of its actual value, ensuring that the K7 engine outperforms rival solutions on system resource usage while maintaining a robust malware detection capability.

LOWEST IMPACT



AV Comparatives Performance Test April

Advanced Threat Detection and Mitigation

Malware authors use advanced obfuscation (self-camouflage) techniques by employing multiple layers of polymorphic or metamorphic code patterns, forced exceptions, undocumented opcode commands, high-entropy encrypted or compressed data, and randomised strings to hamper reverse engineering attempts or detection efforts. While malware architects use obfuscation to make it harder to detect, it is not 100% infallible. The malware must "uncloak" before delivering a malicious payload, which provides an opportunity for security solutions to dynamically detect and block malware while it is resident in memory.

Contextual Blocking of Active Malware Threats

The K7 HIPS and Enhanced HIPS components allow complex, strategic and highly-contextual blocking of malware objects and APT's at runtime, whether a malware object is heavily obfuscated or not.

- HIPS (Host Intrusion Prevention System) – blocks specific malicious behaviour such as the creation of known malicious objects at the network level and in the file system or registry.
- Enhanced HIPS –by analysing the content and the runtime activity of files, K7's Enhanced HIPS technology can detect and block potentially malicious processes that create suspicious objects in non-standard locations, or initiate outbound connections to suspicious remote website URLs or external IP addresses.

K7 Enhanced HIPS can monitor fundamental runtime activity within the file system, registry, process, and network domains by analysing objects at execution time, and can assess an object's process memory use, which is no longer obfuscated, monitoring for malicious activity. K7 Enhanced HIPS also covers blocking of malicious code-injection attempts into known clean processes, and can even be extended to detect cases of "fileless" malware which typically reside within the registry and other repositories to be invoked directly into memory.

Web Categorization and Content Filtering

Malware infections often start as a website visit by an unsuspecting user. Therefore using a Web Categorization feature as part of an endpoint solution helps businesses define the types of websites and content their users can access while using company-owned devices. The organisation may choose to limit access to sites that they feel could impact productivity, such as social media websites during business hours, or block access to unwanted downloads found on hacking websites, gaming, chat services, or other potentially dangerous or inappropriate content.

Increase Organizational Security and Maintain Employee Productivity

The K7 Web Categorization Engine classifies websites based on content analysis using artificial intelligence. When an end-user connects to a website, K7 submits the website URL being visited to the K7 Web Categorization Cloud for assessment. K7 Web Categorization Cloud returns a categorisation status if one already exists, or queues the URL for further AI-based analysis. Once the content has been categorised and validated against the policy, the K7 client either blocks access to that URL or adds the URL to a local cache for future visits.

The classification categories include 65 pre-configured categories like Gambling, Pornography, Tobacco, Drugs, Abortion.

Administrators also have the flexibility to create different web filtering policies based on business or leisure hours and update those policies via the centralised management console.

Anti-Spam / Anti-Phishing Protection

Unsolicited emails are more than just an annoyance. Spam email consumes significant personal time if not appropriately managed. Much of spam email today include phishing attacks with links to nefarious websites to harvest personal data or malware distributed as attachments, which, if executed, could lead to internal network compromise. The immediate impact of a severe virus outbreak propagated by email is lost workforce and infrastructure productivity, and the cost of IT resources used to mitigate the infection. Other concerns are a loss of reputation and damage caused, for example, by an employee accidentally sending out an infected email to unsuspecting business partners or customers alike.

Prevent Unsolicited Spam Emails and Malicious Phishing Threats

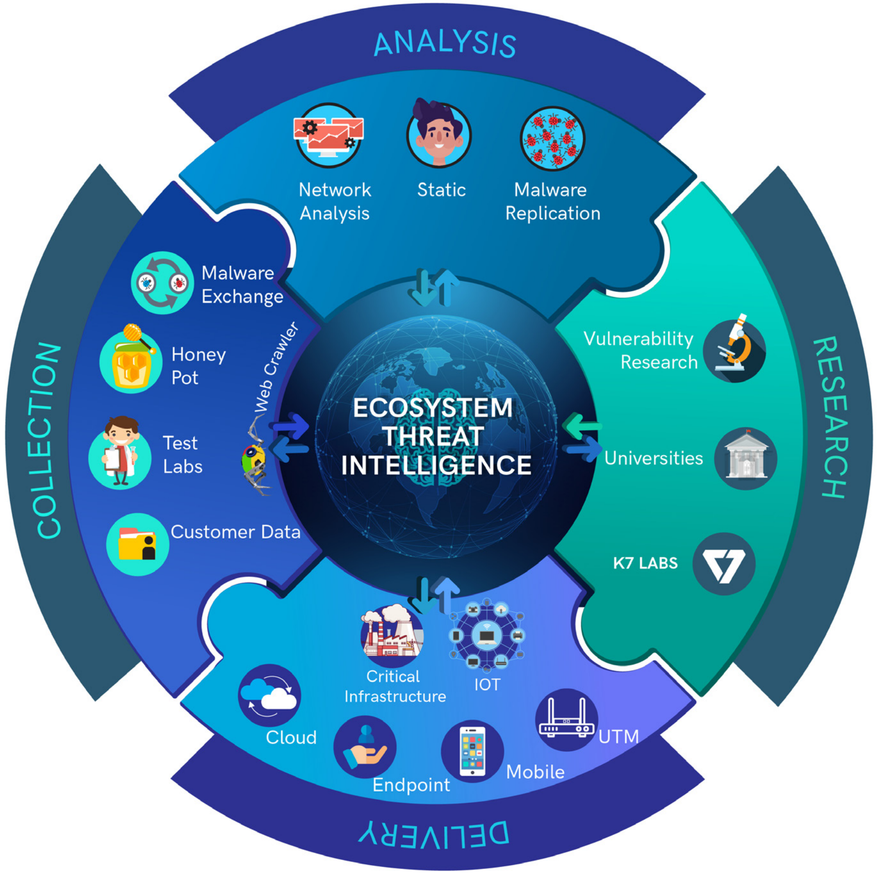
Spam email sent by servers or compromised zombie machines is checked against the K7 white and blacklists before being sent to the K7 scan engine to identify threats. URLs and attachments contained within the email are scanned and, if clean, delivered to the user's inbox. If any elements are deemed malicious, the objects can be quarantined or deleted based on a pre-configured policy, protecting the endpoint from phishing threats before they can be successfully executed.

K7 Ecosystem Threat Intelligence

Threat Intelligence (TI) relates to strategic information about an adversary's capabilities and tactics which can be used to prevent, detect, and mitigate future cyber threats or attacks against IT assets deployed within enterprises, government, and other high target-value organisations.

The collection of K7 Ecosystem Threat Intelligence relies on:

- Collating threat-related metadata from a variety of globally-distributed sources, including live threat event telemetry via K7 Security Solutions, in addition to dedicated decoy systems and honeypot networks
- Distilling collected metadata to develop content for distribution to other platforms and security controls including SIEM systems, and to analyse the tactics and techniques of vile threat actors
- Packaging threat intelligence data into industry-standard formats such as STIX
- Distributing STIX packages via an industry-standard framework such as TAXII



K7 products gather actionable intelligence in the form of statistics and event data from hosts within a K7 enterprise deployment. Stored within a secure K7 cloud repository and analysed to aid in the mitigation of risk, the collected telemetry data is used to profile malware and mitigate actively-spreading outbreaks in the future.

- Outbreak intelligence can be used to identify fast-moving infections and aid security researchers in developing automated security responses.
- Proactively identify and remediate potential false positives, using intelligent automation to improve detection accuracy and minimise the misclassification of legitimate objects as malware.

Centralised On-premises or Cloud-based Management

Small and medium businesses (SMBs) are limited by strict budget requirements and often rely on freeware, shareware, or illegal software to meet their business objectives. Many SMBs do not have dedicated resources that can deploy and manage an effective endpoint anti-malware solution due to the lack of in-house expertise and the costs involved. Centralised management can help improve the IT department's reaction time to network-wide security incidents to near real-time, such as minimising the impact of a virus outbreak or reconfiguring software settings to mitigate risk.

Simple to Deploy and Easy to Manage

K7 Security helps companies effectively protect large numbers of client workstations and critical servers by using the Centralized Management Server's ability to consolidate multiple threats, implement endpoint security policies, and manage them effectively with fewer IT resources.

The centralised web-based management console can manage the installation of K7 software on multiple endpoints, allowing the creation of user groups, policy definition and enforcement, task scheduling, updates, with remote management of K7's core capabilities such as anti-virus, firewall, application control, and web content filtering.

About K7 Security

Many small and medium businesses require low-maintenance security solutions that are easy to deploy and manage due to the limited IT resources they have available. Without centralised management, the challenge of installing, configuring, managing, and reporting on a large number of endpoints becomes impossible with limited IT resources. The centralisation and automation of these policy implementation and endpoint management tasks allow a single IT resource to more effectively manage the security posture.

Solutions for Securing Business Operations

Over the last decade, endpoint anti-malware solutions have become bloated with features that significantly impact system performance, degrade the end-user experience, and are expensive to maintain. At K7 Security we create solutions that provide high efficacy and performance with low overhead, and the functionality required to ensure the integrity of endpoints deployed throughout the enterprise. Each core component of the K7 endpoint solution is developed to minimise the use of valuable system resources and maximise the sharing of contextual security intelligence. This allows for real-time threat analysis and rapid response to both known and unknown threats, without compromising the performance integrity of the host itself.

Independent Testing and Certification

K7 Security solutions are regularly tested and certified by the world's leading independent testing organisations including AV-Test, AV-Comparatives, Virus Bulletin (VB100) and ICSA Labs. K7's commitment to fighting malware has been recognised within the industry for its contributions to malware research and innovations in threat detection and prevention technology.

www.k7computing.com

K7 Computing Private Limited

4th Floor, Tower - B, Tek Meadows
No. 51, Rajiv Gandhi Salai, Sholinganallur
Chennai - 600 119, Tamil Nadu, India.

K7 SECURITY

Confidence in an insecure world