ACCELERATED CYBERSECURITY

Why K7 Security Prioritises Speed In Enterprise Cyber Protection

K7 SECURITY

Contents

Introduction

K7 Endpoint Security (K7 EPS) is well known for its speed – not just speed in scanning, but also speed in deployment and delivery of updates. It is quick in other, less obvious ways as well such as the speed at which the IT team can configure the solution to suit the requirements of their organisation, with little to no training required.

This is not by accident. K7 Security has speed in its DNA and makes it a priority in design and development. This focus on speed has been established based on our extensive 30-year experience in the cybersecurity industry, and is meant to achieve specific cybersecurity and business goals:

Cybersecurity Factor	Goal
Performance	• No impact on productivity • No increase in capital expenditure
Deployment	• Rapidly secure the entire organisation
Configuration	• Avoid overlooking weak spots • Avoid increasing IT headcount
Discovery	• Quick malware identification
Updates	• Quick lab-to-endpoint update journey • Protection under constrained bandwidth • No increase in operating expenses
Management	• Quick response supported by critical notifications
Support	• Quick return to normal operations

We will explore each of these priorities in detail and understand how the pursuit of speed in each of these areas helps organisations gain better cybersecurity, but we will first discuss why speed is important in cybersecurity.

Cybersecurity's Need for Speed

Facts to consider

350,000
new malware and Potentially Unwanted Applications (PUAs) are created every day

Ransomware attacks a business

EVERY 11 SECONDS

It takes

JUST 1 UNSECURED DEVICE

to cripple a large organisation

The takeaways from these statistics are simple:

- Every second counts in cybersecurity
- Every device counts in cybersecurity

Therefore, an organisation that seeks to be cybersafe should ensure that

- Every endpoint in the organisation is protected quickly
- The cybersecurity provider is able to discover malware quickly
- Every endpoint receives malware definition updates from the cybersecurity provider quickly
- The endpoint is able to scan for and identify malware quickly before it can deploy its payload
- The IT team can respond quickly to cybersecurity incidents and rapidly restore normal operating capability

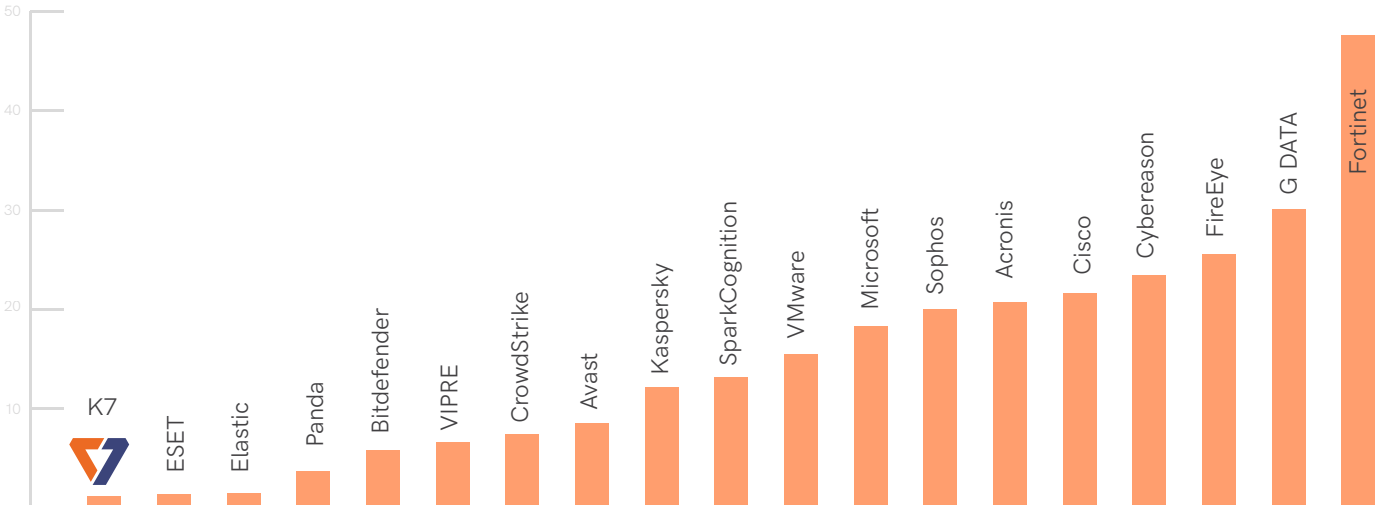
Speed is the common factor across these parameters, which is why K7 Security bakes speed into every one of our products and solutions. Being slow and steady does not win the cybersecurity race; being quick and nimble keeps you ahead of threat actors.

Optimising Cybersecurity Factors for Speed

Now that we have understood the importance of speed in cybersecurity, we can examine the cybersecurity factors that K7 optimises for speed.

Performance

K7 Security's cybersecurity solutions are world renowned for their low impact protection. AV Comparatives of Austria, an independent organisation that tests cybersecurity solutions, discovered that K7 Endpoint Security (K7 EPS) has the least impact on the performance of a device in their test that compared leading international cybersecurity brands.



Source: AV-Comparatives

Benefits from the low impact on device performance include:

- **Unimpaired Productivity –** Users do not even notice that the endpoint is being scanned for malware. Work is not held up by malware scans, and productivity is not lost
- **Quick Malware Identification –** The low consumption of resources results in K7 EPS scanning the endpoint very quickly for malware even if the device has modest hardware. This results in malware being found and blocked quickly
    - A critical enabler of K7 Security's quick scanning is our indigenously developed scan engine. We are not dependent on 3rd party code and we can optimise code with no restrictions on what we can tweak
- **No Hardware Upgrade –** The low CPU and RAM utilisation allows older devices to be used longer, deferring hardware upgrade investment

Deployment

We have already discussed the importance of securing every endpoint. The organisation's safety depends on how quickly the enterprise cybersecurity solution can be deployed across all endpoints. K7 EPS ensures a quick rollout of enterprise-wide cybersecurity through:

- **Small Installer Size –** The small size of the client installer allows quick download onto the endpoint even if bandwidth is constrained

- **Automatic Uninstallation –** The endpoint installer will automatically remove previous cybersecurity solutions before installing K7 EPS, avoiding the need for manual uninstallation by IT

- **Single 32/64 bit Installer –** K7 EPS simplifies installation by having a single installer for both 32 bit and 64 bit operating systems, avoiding the need to switch between installers in organisations that utilise endpoints with both types of operating systems

- **On-premises Deployment**

    - **Push Installation -** K7 EPS allows client installation to be pushed from the EPS server to the endpoint through Active Directory, Workgroups, and IP range based installation, avoiding the need for IT to travel to the endpoint or for the endpoint to come to IT for manual installation

    - **Combined Server/Console Installation –** K7 EPS features a single console and web server installation which avoids the need to troubleshoot integration issues

    - **Console On Any Machine –** The K7 EPS console can be installed on any machine in the network, whether endpoint or server. This avoids the time and expense of provisioning hardware with middleware like Apache or IIS

    - **In-place Upgrade –** Console can be upgraded with new features without requiring reinstallation

- **Cloud Deployment –** The cloud deployment model removes the need for the IT team, K7 staff, or end users to visit headquarters or branch offices, avoiding delays caused by travelling

Configuration

Cybersecurity solutions that are difficult to configure are a security and productivity issue:

- **Security –** A solution that makes configuration a challenge increases the risk of inappropriate settings and inadequate safeguards, allowing a threat actor to discover a weakness and enter the organisation

- **Productivity –** Time consumed in configuring the solution affects the IT team's productivity and may even result in increasing the IT headcount. User productivity may also be affected if incorrectly configured cybersecurity provisions require them to repeatedly call for IT help

These two factors may even combine, with the need to maintain productivity resulting in the implementation of lenient cybersecurity settings that lead to devastating cyberattacks. K7 Security recognises that complex configuration is a cyber hazard and mitigates this risk through:

- **Optimised Out-of-the-box Settings –** K7 EPS is pre-configured with cybersecurity settings that are appropriate for most organisations. This provides robust out-of-the-box configuration that requires minimal tweaking, significantly saving IT effort

- **Intuitive Interface –** K7 EPS is designed with a highly intuitive interface that does not require advanced cybersecurity knowledge for effective configuration where custom configuration is required; basic computer/network knowledge is sufficient and admins can configure K7 EPS quickly with little to no training. The ease of use ensures that no security feature is overlooked or set to an inappropriate level

- **Customisable Client Installation –** The client installation package can be customised with group and policy configuration, ensuring that endpoints will be protected with appropriate security policies immediately after installation without waiting for suitable groups and policies to be assigned to them

Discovery

The sooner malware is identified, the sooner a definition update can be released that will detect and block the malware in the user's device. Stopping cyberthreats is a race against time and K7 Security ensures that it leads the pack in cyberthreat detection through:

- **K7 Threat Labs –** The K7 Threat Labs was established in 1998 to conduct advanced malware and threat research. It analyses hundreds of thousands of malware samples every day and has been the first discoverer of several malware and is the first winner of the Real Time Threat List (RTTL) Contributor of the Year Award from the Anti-Malware Testing Standards Organisation (AMTSO) for contributing thousands of unique malware samples per week

- **Industry Affiliations –** K7 Security is the first and only Indian member of the prestigious Cyber Threat Alliance of cybersecurity leaders and the only Indian programme partner for the Microsoft Azure Sphere Security Research Challenge for IoT vulnerabilities, which enable it to develop insight into cyberthreats that are beyond the horizon

Cutting-edge research and industry affiliations position K7 Security at the forefront of threat discovery and ensure its customers receive malware definition updates before threat actors can compromise their operations.

Updates

We have already mentioned the very large number of malware that are created every day. Any cybersecurity solution is only as good as its last update, and the malware definition updates released by the cybersecurity vendor can boost the endpoint's cyber defence only if/when they are downloaded by the endpoint. K7 Security accelerates endpoint update through:

- **Frequent Updates –** K7 Security shortens the time between malware discovery and endpoint update by releasing multiple malware definition updates a day, every day. This ensures that updates are provided very soon after malware is discovered and the organisation's window of vulnerability is closed

- **Lean Updates –** K7 Security's updates are designed to be small to avoid bandwidth hogging. Lean updates also ensure that available bandwidth need not be upgraded to accommodate the cybersecurity solution, avoiding an increase in operating expenses

- **Local Update Server (On-premises) –** Updates are downloaded only once to the local EPS server and then distributed to endpoints using the local network to avoid bandwidth congestion. Endpoints pull updates from the local EPS sever to avoid choking the local network. Add-on servers avoid choking of a single local EPS server if a large number of endpoints need to receive updates

A state-wide co-operative bank with hundreds of remote rural branches trusts K7 to cybersecure the entire organisation as K7 Security was the only cybersecurity provider that could protect remote branches that only had 24 kbps connectivity. Our case study provides more information on our innovative solution.

It should be noted that cybersecurity solutions that provide bandwidth-intensive updates hamper end users, especially employees working from home, from meeting their KRAs by creating internet bottlenecks. End users are tempted to avoid downloading such updates, exposing them to cyberthreats. The K7 approach ensures that bandwidth is not constrained by updates and end users are always protected against the latest cyberthreats.

Management

Speed of response to cybersecurity incidents and rapid configuration changes based on updates to the organisation's cybersecurity policy ensure that organisational cybersecurity insight quickly translates into action. K7 Security achieves this through:

- **Critical Notifications –** Relevant notifications can be sent directly to admins who don't need to monitor the console to be aware of cybersecurity incidents or concerns
- **Global Search –** The K7 EPS console includes global quick search that supports searching for cybersecurity information such as endpoint details, applications, and threats from a single search box for quick identification of concern areas
- **Global Override –** Admins can implement revised cybersecurity measures for all endpoints without editing individual policies

Support

Unusual hardware configurations or unusual business requirements may require the active involvement of the cybersecurity vendor's support team to troubleshoot issues or optimise configuration. The speed of resolution is critical, in such cases, to maximise organisational cybersecurity in the minimum of time. K7 Security shortens response times through:

- **Complete In-house Development –** The lack of any 3rd party code ensures that K7 Support have the expertise and authority to fine tune any part of the cybersecurity solution and are not dependent on technology partners to troubleshoot their code contribution to the solution
- **Proximity to Engineering –** The support team is located in close proximity to the engineering team, enabling greater collaboration and quick issue resolution, avoiding delays in processing detection-related and feature-related customer requests

K7 Security's Enterprise Cybersecurity Solutions

K7 Security combines over 30 years' expertise in cybersecurity with a state-of-the-art threat research lab to deliver rapidly updated enterprise cybersecurity solutions that protect critical data and devices in SMEs and large enterprises across the world.

Endpoint Security

Our Endpoint Security utilises multi-layered protection, heuristic malware detection, ransomware protection, and a dedicated firewall to help defend the growing number of connected devices within organisations against cyberattacks

Network Security

Our Unified Threat Management, VPN Concentrator, and Connect 500 devices provide enhanced network security and secure connectivity between branch offices, headquarters, and the cloud

Our solutions are recognised across the world for 24x7 enterprise cyber protection. K7 Endpoint Security emerged as the winner against major international cybersecurity brands in the Performance Test conducted by AV-Comparatives (Austria).

K7 SECURITY

www.k7computing.com

MAY 2021