

SECURING WORK FROM HOME

Cybersafe Remote Working With
K7 Security



 **K7 SECURITY**

Contents

Executive Summary	3
Work From Home Cybersecurity Challenges And Risks	4
Is Personal Antivirus Enough?	6
Overcoming Work From Home Cybersecurity Challenges with K7 Security	6
Inadequate Device/User Protection.....	6
Lack of Centralised Cybersecurity Management	7
Difficulty in Remote Cybersecurity Deployment.....	7
Segmenting Web Access for Personal and Professional Use	8
Use of Unauthorised Hardware	8
Use of Unauthorised Applications and Services.....	9
Poor Communication Security.....	10
Limited Hardware Resources.....	11
Constrained Bandwidth.....	12
Complex Remote Access Requirements	13
Lack of In-Person IT Support.....	14
Limited Cybersecurity Awareness	15
K7 Enterprise Cybersecurity – Robust, Tested, Trusted	16



Executive Summary

The way we work witnessed a sea change in 2020 when COVID-19 shuttered offices and employees began working from home on an unprecedented scale. Organisations were quick to see the opportunity in the problem: operating costs reduced and productivity increased. Cyberattackers also saw opportunity: employees were accessing enterprise networks and data without enterprise protection, and the pandemic was soon accompanied by a 500% increase in cyberattacks.

COVID-19 has been with us for a year now and a 2021 global IT security survey revealed that more than 60% of respondents agree that their organisations suffer from data security issues due to pandemic-driven remote working. However, it is clear that working from home is here to stay and is likely to be the preferred choice of both employers and employees even after the pandemic is behind us, and threat actors will continue to target remote working employees to launch attacks on their employers.

K7 Security has spent the last year working with some of the most security sensitive organisations in India to secure their operations while their employees function from their residences. This whitepaper has been prepared based on our analysis and mitigation of the real-world cyberthreats encountered when remote working is implemented on a large scale. We discuss

- Work-from-home cybersecurity challenges and risks
- Endpoint and network security concerns
- Limitations in using personal antivirus to protect remote workers
- Protecting the distributed enterprise with K7 Security's enterprise cybersecurity solutions

We conclude this whitepaper by examining the knowledge gap that threat actors use to attack end users and the organisations that employ them, and how this gap can be closed.



Work From Home Cybersecurity Challenges And Risks

Working from home brings both rewards and risks to the organisation. The rewards are lower cost of operations and a happier workforce. The risks arise due to increased susceptibility to cyberthreats because employees are working outside their organisation's IT perimeter without the protection of enterprise cybersecurity.

The risk is compounded by employees using personal devices and networks which create a fragmented IT environment that is comprised of a variety of devices running on different platforms with different levels of security patches and also using any number of networking devices and ISPs to connect to head office resources and the cloud. The organisation's IT infrastructure is now distributed across a large number of small home workstations spread across the country (or even the world) and the number of variables has dramatically increased, making it difficult to secure. Threat actors who wish to gain a foothold within the organisation can aim their attacks against individual employees, who are relatively soft targets, instead of trying to breach hardened corporate defences.

The cybersecurity challenges and risks arising from employees working from home include:

Challenges	Risks
Inadequate Device/User Protection	• Cyberattacks against devices through malware and malicious websites • Cyberattacks against users through phishing
Lack of Centralised Cybersecurity Management	• Fragmentation of cybersecurity norms across the organisation • Organisation is only as secure as its least-secured device/user
Difficulty in Remote Cybersecurity Deployment	• Devices/users may function with poor, or without any, cybersecurity
Segmenting Web Access for Personal and Professional Use	• Removing all restrictions for personal web access may allow cyberattacks while working, or impair productivity
Use of Unauthorised Hardware	• Hardware mods/upgrades may lower cybersecurity standards and lead to cyberattacks or data loss



Challenges	Risks
Use of Unauthorised Applications and Services	- Shadow IT increases the attack surface for cyberattacks 3rd party providers' jeopardous terms & conditions - Data security and sovereignty concerns
Poor Communication Security	Interception of communication between remote workers and head office
Limited Hardware Resources	Cybersecurity CPU and RAM requirements may overwhelm modest hardware often found in personal devices
Constrained Bandwidth	Cybersecurity updates may choke personal networks if bandwidth is constrained
Complex Remote Access Requirements	Some applications (like Tally) require complicated and expensive remote desktop solutions for remote access
Lack of In-Person IT Support	Speed of response may be impaired due to lack of physical proximity
Limited Cybersecurity Awareness	- Remote workers may not practise adequate cyber hygiene - Remote workers may be misled into performing actions that benefit cyberattackers

We will examine how these challenges can be resolved with K7 Security's enterprise cybersecurity solutions but we will first discuss if organisations can rely on employees' use of personal antivirus to secure business operations.



Is Personal Antivirus Enough?

Personal antivirus may offer world-class protection at an individual level e.g., K7 Security's products for home users offer the same award-winning standard of protection as its enterprise cybersecurity solutions. But home cybersecurity products are designed to be configured and controlled by the home user, who can turn off or even uninstall the program if they so desire, which is not appropriate for enterprise protection. Personal antivirus products also do not create secure channels of communication between the user and the enterprise.

K7 Security's enterprise cybersecurity solutions offer additional features that are required by businesses for centralised management of enterprise-wide cybersecurity while aligning with business objectives. We also offer enterprise network security products that enable corporate VPN for secure communication. The benefits of enterprise cybersecurity solutions in a work-from-home context will be discussed in detail in the following section.

Overcoming Work From Home Cybersecurity Challenges with K7 Security

Inadequate Device/User Protection

Remote workers may be using their personal devices or employer-provided devices to work from home. It is not unusual to see personal devices with no cybersecurity and obsolete/unsupported software, or corporate devices with poor cybersecurity due to hasty provisioning of endpoints to enable remote work. This exposes the employee, and consequently the organisation, to many cyberthreats:

- Ransomware can cripple the device and spread via employee communication to impair operations across the entire organisation
- Keyloggers can be used to acquire employee credentials to attempt financial and data theft
- Remote Access Trojans (RATs) give the attacker access to the user's device and can be used for surveillance, data exfiltration, and for criminal activities against other victims which will be attributed to the user
- Zero-day Attacks permit the attacker to perform malicious activities without being detected by using unknown vulnerabilities

K7's Solution

K7 Cloud Endpoint Security

- Comprehensive, multi-layered antivirus, anti-malware, and anti-spyware defences
- Signature- and behaviour-based protection to stop both known and unknown threats
- K7 Labs analyses hundreds of thousands of malware samples a day and releases multiple updates every day to secure users and organisations against the latest threats
- Host Intrusion Detection System (HIDS)/Host Intrusion Protection System (HIPS) monitors suspicious behaviour and events
- Advanced ransomware protection identifies and blocks malicious encryption attempts while allowing legitimate encryption
- Email scanning stops malicious attachments and links
- Protection against phishing, spear phishing, and whaling
- Tamper protection prevents cyberthreats from affecting K7 EPS



Lack of Centralised Cybersecurity Management

Having a large number of remote workers spread across the country, or even the world, and running different cybersecurity protocols can quickly become a security nightmare as it takes [only one device with a cybersecurity weakness](#) to provide entry to an attacker who can then bring the entire organisation and its associated operations to a halt. Maintaining organisational cybersecurity across a widely dispersed workforce without physical access to endpoints for IT will be an impossible endeavour unless the cybersecurity solution supports centralised management.

K7's Solution

K7 Cloud Endpoint Security

- Complete centralised management through the cloud console with granular, endpoint-level control over applications, devices, and web access
- Centralised reports provide easy-to-understand organisation-wide cybersecurity information that aid rapid action against anomalies
- Centralised client removal simplifies license management

Difficulty in Remote Cybersecurity Deployment

Centralised management of endpoints is possible only if an organisation-wide rollout of endpoint cybersecurity has been implemented. Installing endpoint security on individual endpoints is easy to accomplish when the target device is within the organisation's office or in the possession of IT; similar deployment when the endpoints are not within the corporate network presents multiple obstacles:

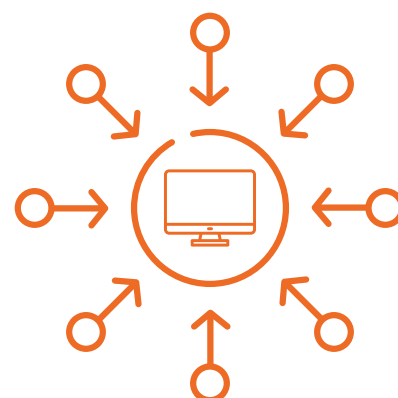
- Endpoint security installers need to be downloaded onto each endpoint
- Remote workers will need to install the software on the endpoint
- IT will then need to perform remote configuration of endpoint security

Remote deployment has become a critical factor for enterprise cybersecurity after the spread of COVID-19 as employees are recruited and onboarded without them ever visiting the organisation's office, making it impossible for IT to perform direct installation of endpoint security on the employee's device if employees use their own devices.

K7's Solution

K7 Cloud Endpoint Security

- Support for 100% remote deployment as the cloud deployment model does not require on-premises installation of the console. Organisation-wide deployment of K7 Cloud Endpoint Security is possible without the employees, IT, or K7 staff visiting the organisation's office
- Download link for the installer can be sent to the employee via email for a single-click download
- Small installer size permits quick download on residential internet
- Installer can be customised with the group information pertaining to the specific employee, avoiding the need for further configuration by IT





Segmenting Web Access for Personal and Professional Use

Many remote workers use their personal devices when working from home. As it is not reasonable to prevent personal web access (and the freedom associated with personal use) on a personal device, employers have to grapple with the extent of restrictions that should be applied to balance personal freedom with enterprise cybersecurity and productivity requirements. All too often, no restrictions are applied on a personal device which causes productivity losses while working.

K7's Solution

K7 Cloud Endpoint Security

- Category-based website filtering prevents access to websites that may affect productivity
- Time-based web access can be combined with category-based web access to segment access based on business hours and leisure hours

Use of Unauthorised Hardware

Organisations that issue computing devices to their employees for remote working choose hardware specifications that improve cybersecurity and productivity, both of which can be impacted if the employee alters the hardware e.g., the employee may replace a hardware component with a component that is known to have vulnerabilities in its firmware, opening the doors to a cyberattack or data breach.

Cybersecurity solutions cannot scan firmware because firmware functions outside the operating system of the endpoint. This makes compromised hardware difficult to detect and organisations will need to depend on the prevention of hardware component modification/upgrade to maintain organisational cybersecurity and data security.

K7's Solution

K7 Cloud Endpoint Security

- Device management enables allowing/blocking devices by Class ID and Device ID, preventing the use of unauthorised external devices like USB storage media and Wi-Fi dongles
- Hardware Asset Management monitors endpoints and notifies administrators of hardware changes, alerting them to hardware modifications





Use of Unauthorised Applications and Services

Employees who are working from home seek applications and services that reduce friction in communication, resource sharing, and team work. This leads to the use of unauthorised digital tools (called Shadow IT) that may suit the immediate needs of the employee but have a long-term cybersecurity impact on the organisation:

- Shadow IT increases the attack surface as unauthorised tools haven't been vetted by IT for vulnerabilities or the vendor's ability/inclination to provide security patches. Each team may use different tools to achieve the same ends, further increasing the attack surface of the organisation without increasing organisational capability
- Unvetted digital tools carry the risk of unknown terms and conditions, such as rights of the vendor to access or use client data e.g., messenger apps are [known for accessing files through shared links](#). This can have cybersecurity ramifications especially where Personally Identifiable Information (PII) or proprietary information is concerned
 - The data security practices of the vendor may also be questionable e.g., How is data encrypted? Is data encrypted only at rest or also in transit? How often is the data backed up? What is the procedure to restore backed up data and how long will the process take?
- Data sovereignty has emerged as a critical issue with nations requiring data pertaining to their citizens to be stored in data centres located within their borders. Shadow IT may violate these regulations as the IT team haven't verified where the data is stored or stipulated where the data should be stored when negotiating a contract with the vendor

K7's Solution

K7 Cloud Endpoint Security

- Advanced website filtering including category-based blocking prevents use of unauthorised web-based services
- Application control features allow blocking of unauthorised applications based on MD5 value/checksum
 - Applications can be allowed to run but internet/network access can be blocked if the application is deemed to be necessary but allowing it to communicate outside the device is considered unsafe





Poor Communication Security

Remote working necessarily requires the transmission of data from to and from headquarters by the remote worker from wherever they are located. This implies that the data will be transmitted through networks that are outside the organisation's control and can be intercepted by a cyberattacker who may misappropriate or modify the data. This risk is magnified when working from home is implemented at scale as the number of users and the number of networks cause a significant increase in the attack surface.

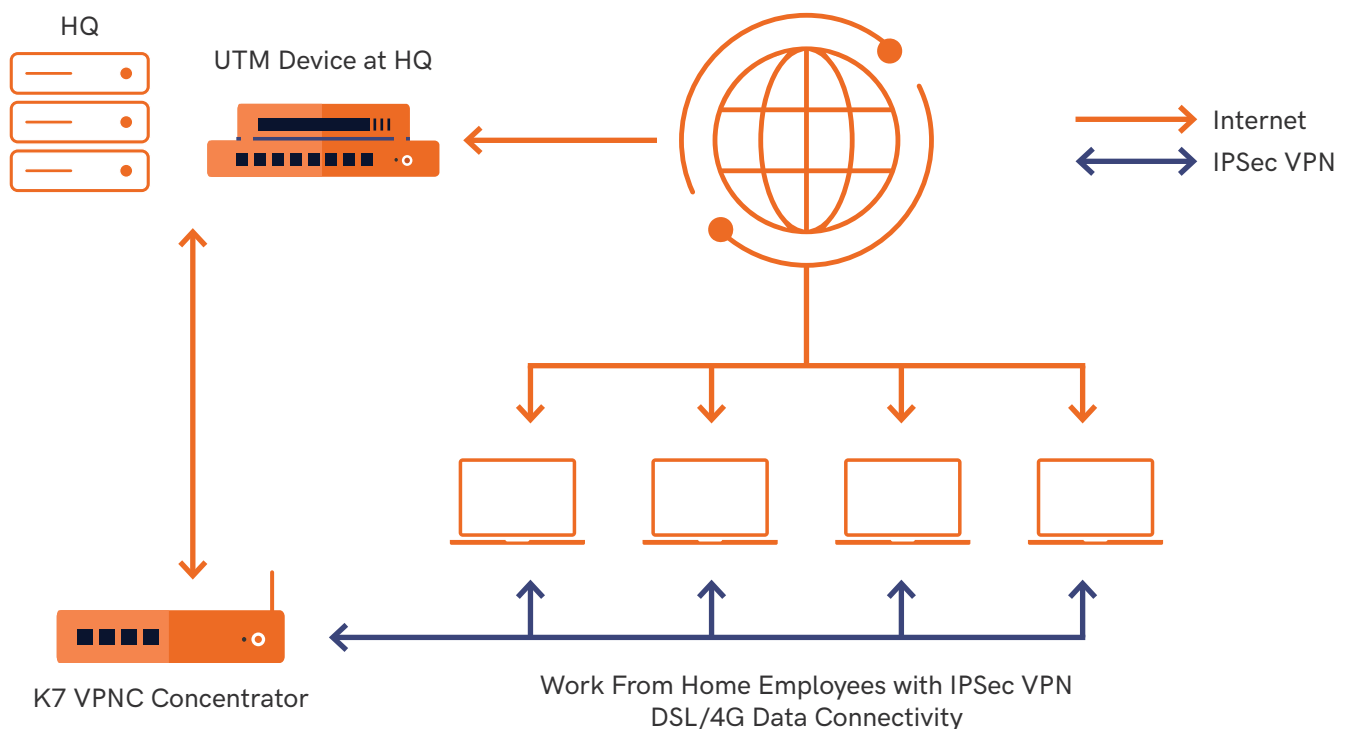
VPN solutions mitigate this risk by enabling encrypted communication between the remote worker and the head office, but conventional VPN solutions are expensive, support a limited number of users and locations, and have bandwidth requirements that make them an impractical choice for employees working from home.

K7's Solution

K7 VPN Concentrator

The K7 VPN Concentrator is a network security appliance that is installed at headquarters and creates multiple VPN tunnels to support hundreds of users

- Employees can use any ISP of their choice to communicate with headquarters
- Load balancing and automatic failover of VPN tunnels ensure high availability for reliable and secure remote access to CRM, ERP, and Intranet applications





Limited Hardware Resources

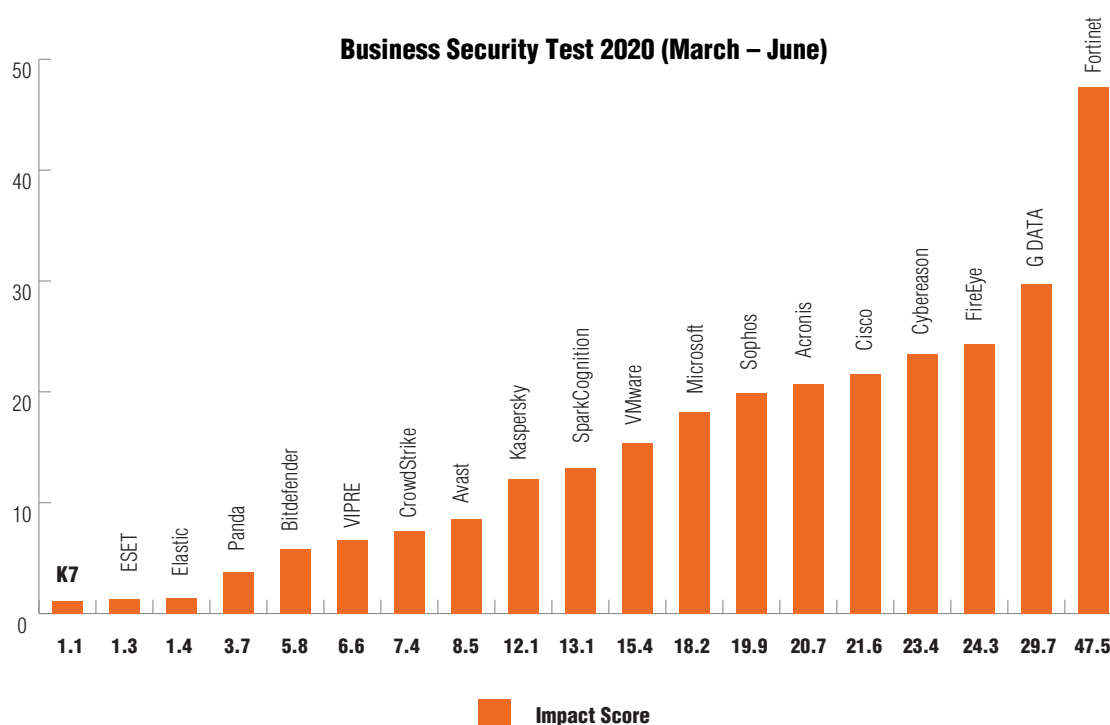
The rush to implement working from home following the pandemic lockdowns limited organisations' ability to procure powerful hardware. Many remote workers are also using their personal devices which often cannot match the specifications of enterprise hardware.

- Resource hogging cybersecurity solutions can become productivity bottlenecks as employees working from home grapple with slow device speed or are even unable to work while a scan is running
- Employees will be tempted to look for ways to turn off cybersecurity in order to meet their deadlines, exposing them and the organisation to cyberthreat risk

K7's Solution

K7 Cloud Endpoint Security

K7 Security's Endpoint Security solutions are world renowned for their minimal consumption of device resources thanks to the sophisticated engineering behind the K7 scan engine that ensures unobtrusive protection. AV-Comparatives of Austria, a leading independent cybersecurity testing organisation, found K7 Endpoint Security to have the [least impact on device performance](#).





Constrained Bandwidth

Employees working from home may struggle with inadequate internet connectivity for 2 reasons:

- Residential bandwidth, even in major cities, may not match the bandwidth available in offices. This is particularly true for employees who utilise mobile internet via a hotspot to work from home
- Employees may not remain in major cities to work from home, as they may have been using temporary accommodation in the city only to improve their employment prospects. Working from home allows employees to return to their hometowns which may be in remote locations that are underserved by ISPs

Cybersecurity solutions necessarily have to provide multiple malware definition updates a day and sync with the endpoint for product updates and policy changes as well. This consumes bandwidth which the employee requires to interact with their colleagues and carry out their responsibilities. Heavy data consumption by cybersecurity products affects employee productivity and tempts them to block updates, especially if they use metered internet, which leaves them exposed to cyberattacks.

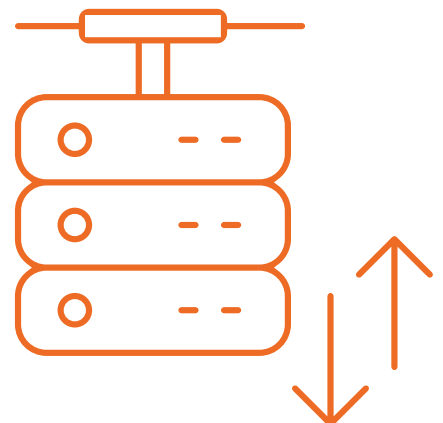
K7's Solution

K7 Cloud Endpoint Security

K7 Endpoint Security is designed to support lean updates that consume minimal internet bandwidth.

A state-wide co-operative bank with hundreds of remote rural branches needed to cybersecure the entire organisation but faced a significant challenge: some remote branches only had 24 kbps connectivity. K7 Security was the only cybersecurity provider that could protect their IT infrastructure under such connectivity constraints. [Our case study provides more information](#) on our innovative solution.

K7 Endpoint Security's ability to provide protection without choking available bandwidth ensures that employees' endpoints are protected irrespective of which ISP they use and how they obtain connectivity.





Complex Remote Access Requirements

Many organisations use applications like Tally which make working from home difficult due to the need for remote access for multiple users to the application server. Accessing Tally through conventional remote desktop solutions can be challenging as

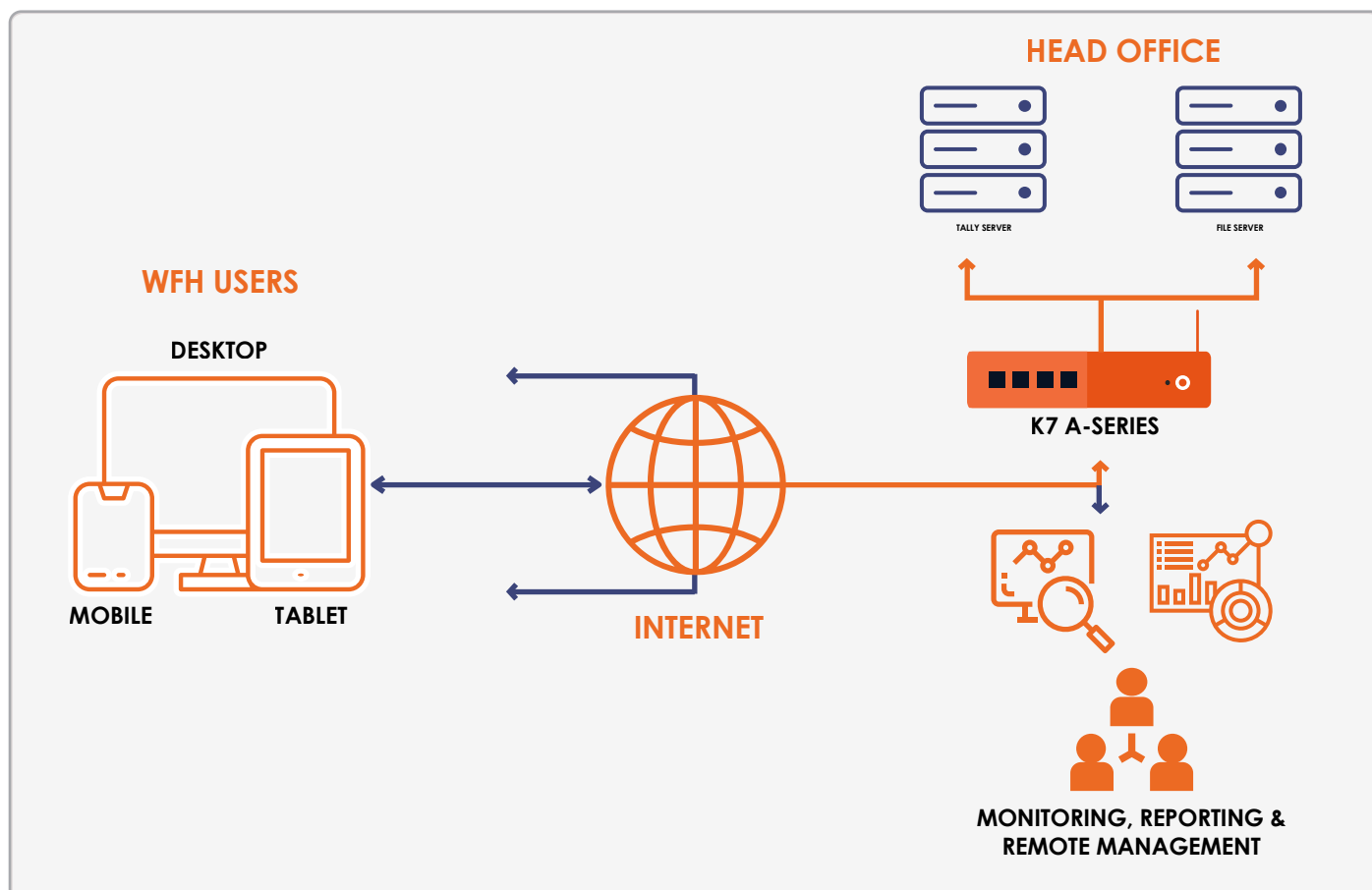
- They are complicated and expensive
- They introduce lag which impacts productivity

K7's Solution

K7 Tally on WAN

The K7 Tally on WAN appliance is installed in your head office and enables simple, secure, and cost-effective access to the Tally application server for remote workers.

- Does not require a Terminal Server, Remote Desktop Protocol, Virtual Desktop Interface, or Client Access Licenses
- Does not require changes to network or installation of plugins on the Tally server
- Prevents unauthorised users from accessing the Tally server
- Employees working from home can work on Tally using ADSL, broadband, mobile internet, or a hotspot from any ISP



The K7 Tally on WAN device can be repurposed as a Unified Threat Management device (payment required) if the work from home facility is withdrawn.



Lack of In-Person IT Support

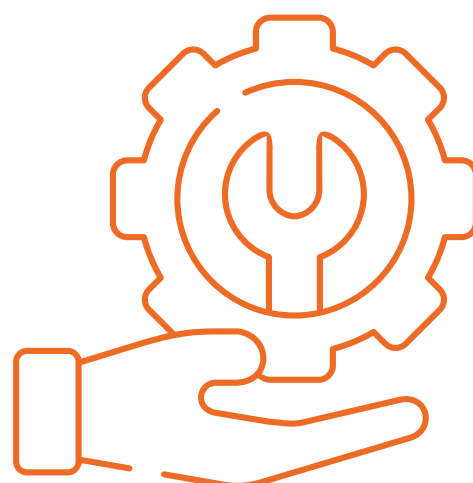
Enterprise IT support teams and users often depend on in-person IT support to resolve their technology-related issues. This extends to cybersecurity as well with installation, configuration, and subsequent troubleshooting involving direct access to the endpoint. Working from home prevents such direct access, making issue resolution difficult. IT teams are concerned that solutions meant to secure work may also hamper work if they develop glitches that cannot be addressed easily through remote resolution methods, especially if the employee has limited/unreliable internet connectivity.

K7's Solution

K7 Cloud Endpoint Security

K7 Cloud Endpoint Security is designed to 'just work' and engineered to address IT teams' concerns:

- Endpoint installer is distributed easily to employees through an email with a download link
- Small installer size permits quick download even where connectivity is constrained
- Intuitive interface makes it easy for remote workers to install the solution by themselves
- The solution is pre-configured to suit most organisations, reducing post-installation tweaking
- User-specific cybersecurity measures, like group and policy assignment, can be included in the installer to avoid post-installation configuration
- Product is entirely developed by K7 and does not require integration with 3rd party code. This improves stability and avoids the need for difficult rollback of glitchy updates
- Endpoints reliably sync their policies when they come online, avoiding the need for IT to intervene and investigate failed policy updates on endpoints
- Does not identify genuine files as malware, saving IT effort in quarantining and investigating files over remote communication channels





Limited Cybersecurity Awareness

Employees who are beyond the perimeter of corporate IT are exposed to greater cyber risk. This risk is magnified by a lack of cybersecurity awareness because

- Lax cyber hygiene in an employee's personal life can open the doors to cyberthreats that affect their employer
- Threat actors launch phishing attacks which use social engineering to attack the user rather than the device. Technology solutions offer limited protection against phishing due to the variety of avenues that can be used to launch such attacks

K7's Solution

K7 Cloud Endpoint Security

K7 Endpoint Security provides protection against phishing attacks that eventually enter a user's device/include a malware component. This protection includes

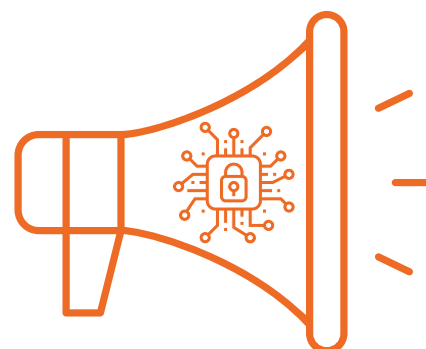
- Scanning and blocking of malicious attachments
- Blocking of links to phishing websites (websites designed to harvest user credentials or other critical information by copying the look and feel of legitimate websites)

K7 Academy

Not all cyberattacks involve malicious attachments, links, or other conventional forms of cyberthreat propagation. A phishing attack can originate on social media and may involve misleading the employee into disclosing confidential business information or authorising transfer of funds to the attacker. Such attacks do not involve malicious code in any form and the only defence is an alert employee who is aware of the techniques that threat actors use.

K7 Academy counters such threats by providing cybersecurity awareness and training that is customised to the needs of your organisation. Training includes

- Employee cybersecurity training which includes the fundamentals of cyber hygiene, awareness on phishing attacks and how to spot them, and securing home IT infrastructure. These programmes can be tailored based on employee seniority to suit the level of access enjoyed at different hierarchy levels and consequent risk
- IT staff cybersecurity training to ensure that the IT team have the knowledge and skills required to maintain organisational cybersecurity in a remote working environment





K7 Enterprise Cybersecurity – Robust, Tested, Trusted

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

Our solutions are internationally recognised 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).





Copyright © 2021 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com

