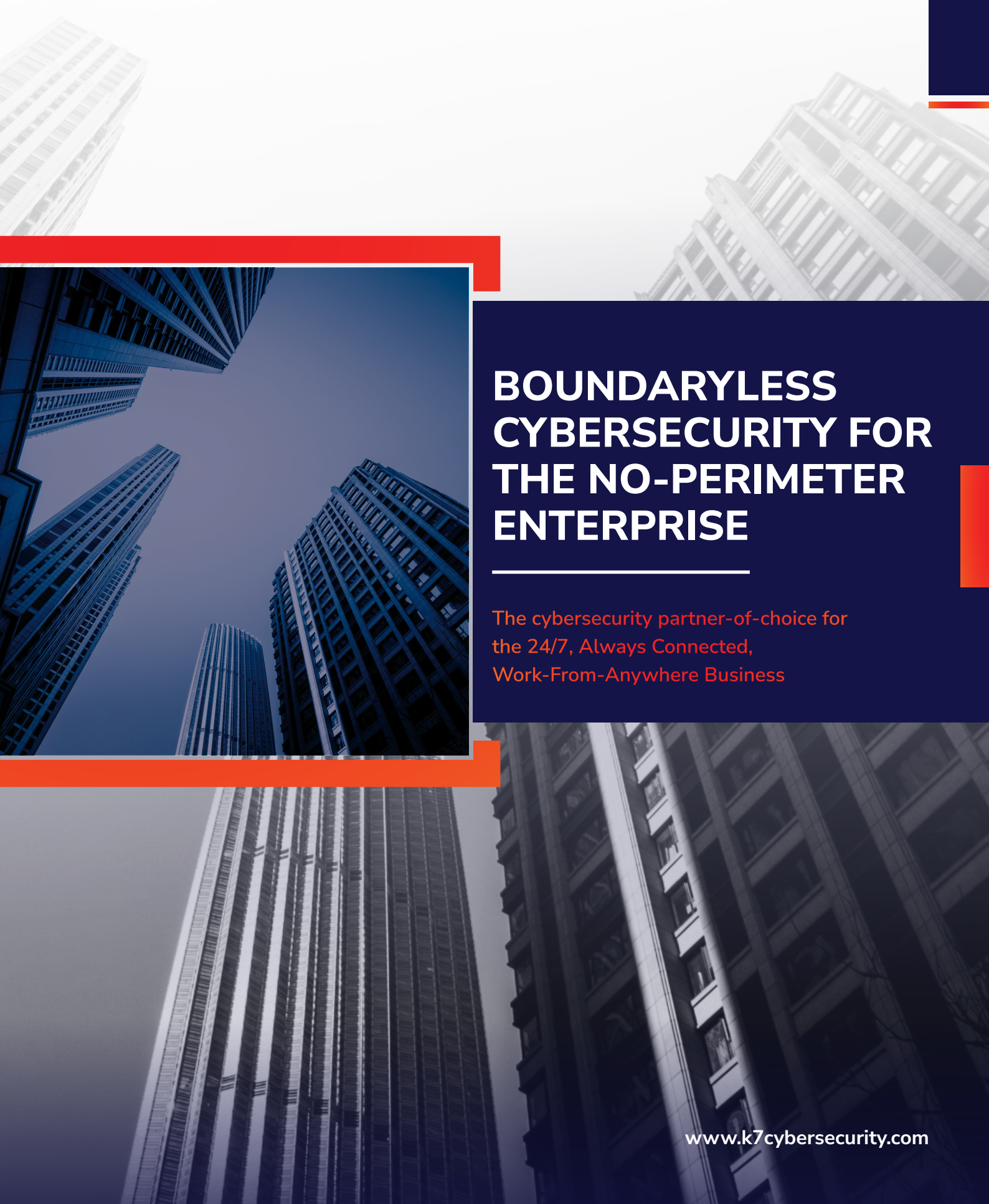




BOUNDARYLESS CYBERSECURITY FOR THE NO-PERIMETER ENTERPRISE

The cybersecurity partner-of-choice for
the 24/7, Always Connected,
Work-From-Anywhere Business

www.k7cybersecurity.com

MANAGED SECURITY PLATFORM, ENTERPRISE ENDPOINT SECURITY, NETWORK SECURITY, AND CYBERSECURITY CONSULTING SERVICES



Award
Winning



Cost
Effective



Easy to
Manage



AI-Enhanced
Multi-Layered
Protection



Multi-Jurisdictional
Compliance

The Attack Surface Increases as the Perimeter Dissolves

There's no such thing as a defined IT perimeter anymore. Pervasive computing allows businesses to operate without being restricted by place or time. 24/7 operations, digital customer touchpoints, work from home, Bring Your Own Device, the data-driven enterprise – they all contribute to providing both means and motive for cyberattacks as the attack surface and the value of enterprise data keeps increasing.

Unbound Cybersecurity

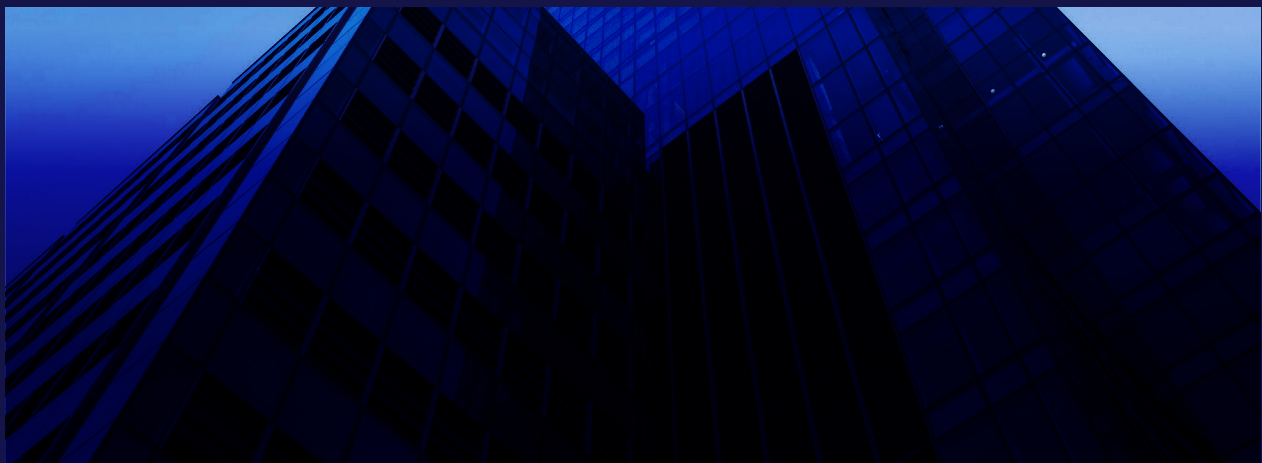
K7 Security's enterprise cybersecurity solutions are designed to provide 360° protection with assured compliance and threat defence for the digitally-enabled enterprise.

Our unified platform with EDR, MDR, and XDR delivers extended defence and single pane of glass cybersecurity with unparalleled security, observability, and compliance.

K7's comprehensive Endpoint Security for Desktops, Laptops, and Servers, and Network Security devices for enterprise networks put a complete stop to viruses, malware, ransomware, phishing, spam, hackers, and zero-day attacks. Our cybersecurity solutions protect all your devices, networks, and users, from the server in your head office to your most remote worker's laptop.

Our turnkey Cybersecurity Services deliver digital protection appropriate to each organisation's threat exposure and compliance obligations while helping businesses improve return on cybersecurity investment.

The global average cost of a data breach is \$4.88 million. Our enterprise cybersecurity solutions help you ensure continuity of operations, protect your brand, and keep you a step ahead of threat actors.



THE WINNING EDGE IN CYBERSECURITY



TECHNOLOGY

Cerebro Technology – Proprietary Machine Learning based engine (AI)

State-of-the-art K7 Labs

International Award Wins



DESIGN

Indigenously Developed Scan Engine

Easy to Install and Use

Low-impact Protection



TRUST

30 Years

27 Countries

Global Telemetry from Millions of Devices



USABILITY

Easy Report Generation

Quick Tech Support

Unobtrusive Scanning

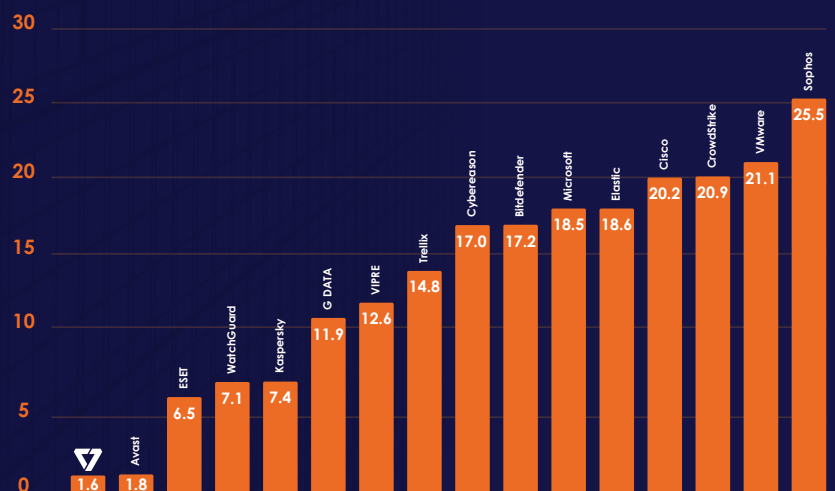
An Indian cybersecurity pioneer since the days of DOS, we have over 30 years' expertise in stopping cyberthreats, protecting millions of users across 27 countries. We design our products to be very easy to install and use, enabling efficient business operations.

We have further augmented our threat stopping prowess in the cloud century with a Threat Lab that analyses hundreds of thousands of threat samples every day and has won the Anti-Malware Testing Standards Organization's Real-Time Threat List Contributor Award, and enhanced our solutions with Artificial Intelligence to stop cyberthreats that no one is even aware of!

AWARDS & CERTIFICATIONS



WORLD #1 -
LEAST IMPACT
ON DEVICE
PERFORMANCE



AV-Comparatives Performance Test



THE K7 ENTERPRISE CYBERSECURITY SUITE

Available for any size of business, from fledgling startups to very large, multi-site conglomerates, K7 Enterprise Cybersecurity ensures that your business can be safe and grow safely in the face of escalating cyberthreats.

MANAGED SECURITY PLATFORM

- EDR
- MDR
- XDR
- SIEM
- SOAR

ENDPOINT SECURITY

- On-Premises
- Cloud
- Operational Technology

NETWORK SECURITY

- K7 SD-WAN
- K7 Next Generation Firewall
- K7 VPN Concentrator
- K7 Connect 500
- K7 AAA
- K7 ToW

CYBERSECURITY SERVICES

- Cyber Defence Assessment
- Red Team Assessment
- Vulnerability Assessment and Penetration Testing (VAPT)
- Governance, Risk, and Compliance (GRC) Consulting
- Information Security Assurance Programme (ISAP)
- Integrated Managed Services (IMS)

K7 INFINISHIELD

An AI-enhanced unified platform delivering single pane of glass cybersecurity, K7 InfiniShield integrates enterprise security infrastructure, surfaces relevant threat signals, and delivers timely, contextual alerts to transform the effectiveness of enterprise cybersecurity and ensure compliance.



Fully Managed SIEM
Integrating Data from
Any Source



SOAR with Integration
across Endpoints,
Networks, and the Cloud



Proprietary EDR for
Enhanced Device
Protection



XDR for Integration of 3rd
Party Solutions



MDR for Perpetually
Improving Enterprise
Cybersecurity Posture



AI-enhanced, Real-time,
MITRE ATT&CK based
Threat Detection



Attack Surface
Management (ASM)
for Control Over Digital
Footprint



Anomalous Behaviour
Detection through UEBA



Comprehensive Log
Management with Analysis
of Real-time and Archived
Logs



Simplified Compliance
across Jurisdictions



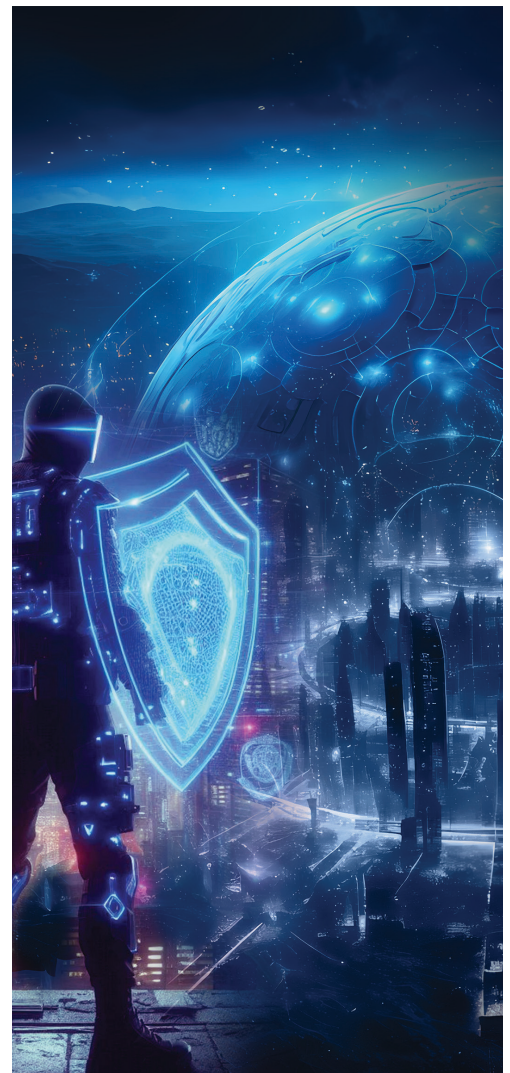
Vulnerability Management
to Prevent Attacks and
Harden Infrastructure



Event Capture without
Additional Hardware
Appliances

BENEFITS

- 24/7 threat monitoring, threat hunting, and analysis
- Increased SOC efficiency and productivity
- Quicker threat detection and response
- Improved threat hunting
- Reduced alert fatigue
- Automated incident response
- Elevated security posture
- Enhanced compliance and reporting
- Elimination of security blind spots
- Customised reports to track SLAs and KPIs



K7 ENDPOINT SECURITY

(K7 EPS)

Developed to suit the requirements of the modern enterprise, our Endpoint Security can scale to protect any size of business operations and supports rapid rollout with quick installation and hassle-free deployment.



Custom-built Web Server for Optimised Performance



No Need for Specialised Hardware/ Software



Console can be Installed on both Server as well as Client



Certified Least Impact on System Performance



Effective Protection Against Ransomware



Machine Learning Enhanced Web Categorisation Engine



Global Policy Override



Comprehensive Device Control



Customisable Client Installation Package



G Suite – Domain-specific Restriction

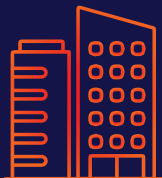


Control from Anywhere (Cloud)



No Dedicated Machine (Cloud)

DEPLOYMENT MODELS



ON-PREMISES



CLOUD

BENEFITS

- Advanced protection against Malware
- Enhanced with Artificial Intelligence
- Special Anti-Ransomware module with both signature- and behaviour-based detection, and protection against remote ransomware
- Antiphishing and Malicious Site Blocking for safe internet use
- Two-Way Firewall with Intrusion Detection & Prevention (IDS/IPS)
- Granular device control and management
- Web filter to block unauthorised/ inappropriate content
- Centralised control over installation of applications
- Optional cloud deployment for anytime, anywhere control

TESTIMONIAL

“

Every organisation in the healthcare sector has to worry about cyberattacks, especially ransomware. We were additionally concerned about the performance impact and manageability of cybersecurity solutions. K7 EPS has allayed both concerns. The behaviour-based ransomware protection has stopped every attack across our branches without slowing down any device. We are also very happy with the easy monitoring, responsive support, and flexible licensing.

”

PAWAN KUMAR
Al Wifaq Medical Group

K7 SD-WAN

K7 SD-WAN manages the network demands of modern enterprises that combine distributed operations, utilising multiple data transport services, with access to SaaS services and applications hosted in on-premises data centres and public or private clouds. Intelligent network traffic direction and optimised routing reduce operational costs while improving application performance and business productivity.



Works with All
ISP Links



Seamless and Secure
Remote Access to CRM/ERP
software



100% Uptime
between HQ and
Branch



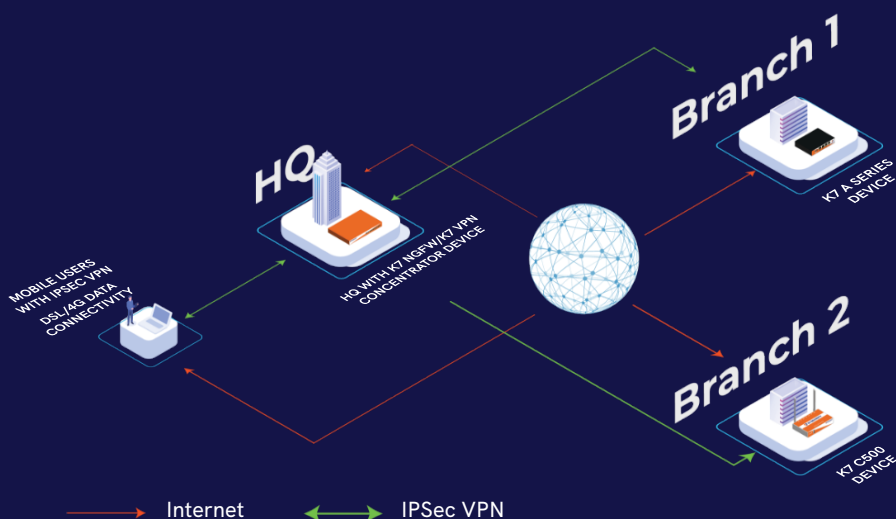
Remote
Manageability



Multiple Virtual
VPN Servers



SLA
Management



BENEFITS

- Easy Deployment
- Easy Management
- Centralised Monitoring and Control
- Simplified WAN Connectivity and Optimisation
- Multi-branch Connections
- Dynamic Path Selection
- Scalable Appliances (Future Proof)
- Cost Effective Solution
- Logs & Reporting

TESTIMONIAL

“

Providing efficient Nidhi services requires the reliable and secure flow of financial information across the organisation. We chose K7 SD-WAN to ensure dependable connectivity across our Head Office and 40 branches and we are delighted with the results. The team from K7 took just 10 days to deploy the SD-WAN solution across 40 branches. All our internal servers are now accessible with 100% uptime across all branches, and we have gained seamless load balancing and failover across 2 ISP lines. We are also very pleased with the quick and knowledgeable resolution of support requests.

”

K7 NEXT GENERATION FIREWALL (K7 NGFW)

K7 NGFW gateway security devices provide robust access control, user authentication, secure site-to-site communications, and network- and application-level attack protection.



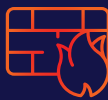
Integrated Routing



VPN (SSL/IPSec)



AAA User
Management



SPI Firewall with IDS/
IPS



Geo IP Filter



Traffic Analyser



Web Security



Content Filter



Email Security



Real-time Network Sniffer



Active Load
Balancing and
Failover



QoS Bandwidth
Management

BENEFITS

- Hardened platform for access control, user authentication, site-to-site communications, and network- and application-level attack protection
- AAA (triple-A) user management to enforce policies and audit usage
- Supports multi LAN/WAN connections with VPN failover for maximum uptime
- Anomalous traffic and protocol behaviour scanning for protection against DOS/DDOS attacks
- Application layer proxies look deep within packet content for inconsistencies, invalid or malicious commands, and executable programs

DEPLOYMENT MODELS



K7 A - SERIES
4 Ports | 30-200 Users



K7 S – SERIES
6 Ports | 60-350 Users



K7 M - SERIES
8 Ports | 100-550 Users

K7 VPN CONCENTRATOR

K7 VPN Concentrator devices enable simple, secure, and robust interconnection between headquarters and branch offices, and between offices and data centres or remote workers by creating and managing multiple VPN tunnels.



Multiple Virtual
VPN Servers



2x Scalable
Appliance



Auto Failover of
VPN Tunnels



Intrusion Detection/
Prevention



Geo IP Filter



Perfect
Forward
Secrecy



Encryption: DES,
3DES-192, AES (128
& 256), Blowfish-128



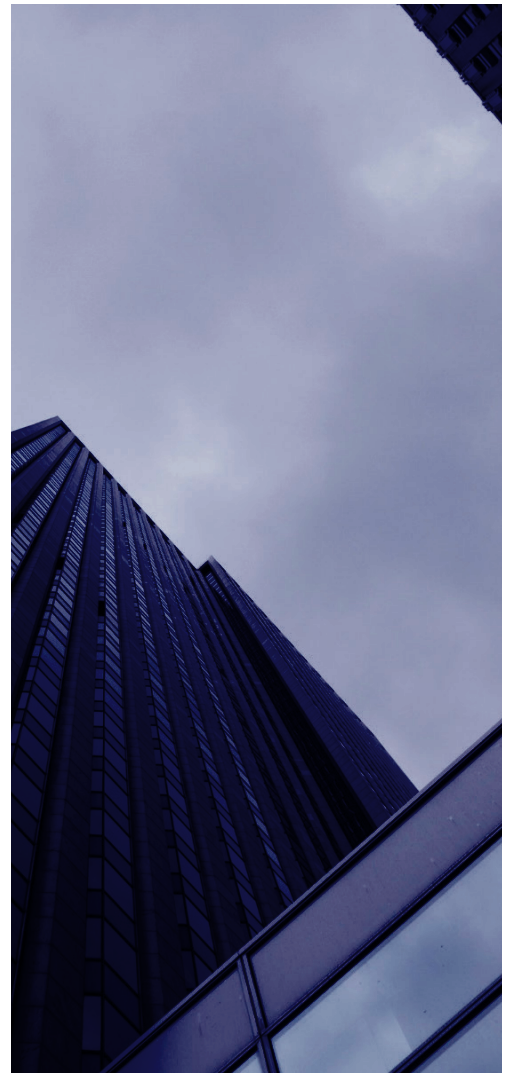
Message Integrity: MD-5
& SHA-1, SHA256,
SHA384, SHA512



Daily Scheduled
Reports

BENEFITS

- 100% uptime
- Works with all ISP links
- No static IP requirement
- Password-protected private key
- Monitoring of connected/disconnected VPN clients on a real-time basis
- Alerts on VPN client failure
- Remote Manageability
- SLA Monitoring



K7 CONNECT 500

The K7 Connect 500 range of Secure Branch Connectivity Devices overcomes the disadvantages of private WAN services for small satellite facilities. Working in tandem with the K7 Next Generation Firewall or K7 VPN Concentrator device in the head office, K7 Connect 500 devices provide reliable and cost-effective interconnection between a small facility or branch office and headquarters or a data centre or even the cloud.



Works with Local, Public IP and any ISP



Network Failover



Network Security



Active-Active Load Balancing and Automatic Failover between ISP/USB/SIM



Failover Between VPN and ISP



Content Filtering



Remote Management



Secure Remote Access



SNMP Enabled for SOC/SIEM Integration

BENEFITS

- No static IP requirement at branches
- Secure VPN access to head office
- Supports Wired and LTE/4G Dongle (ISP/Single SIM/Dual SIM) links for Bandwidth Aggregation, Active-Active Load Balancing, and Failover
- Supports MPLS, Leased Line, and Broadband for seamless Failover
- Block inappropriate website access
- Allow only what is required for productivity
- Domain Filter allows only specific domains on specific port numbers
- 24/7 uptime between branch and HQ, besides Time & Cost Savings
- Immediate incident response & resolution

DEPLOYMENT MODELS

CONNECT 500G

2X1GE RJ45 WAN Ports
3X1GE RJ45 WAN Ports
1X4G/LTE USB Port

CONNECT 500G S1

2X1GE RJ45 WAN Ports
3X1GE RJ45 WAN Ports
1X4G/LTE USB Port
1X4G SIM Interface (Single SIM)

CONNECT 500G S2

2X1GE RJ45 WAN Ports
3X1GE RJ45 WAN Ports
1X4G/LTE USB Port
2X4G SIM Interfaces (Dual SIM)

Enterprise-grade Authentication, Authorisation, and Accounting (AAA) framework provides secure and scalable user authentication for wired and wireless network access, with detailed logs and reports for regulatory compliance.



Works with Any
Firewall/Access Point



Works with Any
Device Supporting
Standard NAS
Protocol



Auto MAC Binding
(5 Devices/User)



Department-based
Authentication



FUP



1:1 Priority
Bandwidth



SMS/Payment
Gateway Integration



Self-registration
Portal



5K User Scalability



2K Device Scalability

BENEFITS

- Multiple ISP support with bandwidth aggregation on link priority
- PMS integration for hotels
- AD/LDAP/Google Oauth/SAML based login
- Social network/club membership based login
- Voucher/coupon coupled with SMS OTP login
- Automatic deletion of users on account expiry

DEPLOYMENT MODELS



ON-PREMISES



CLOUD

K7 TOW

K7 ToW (Tally on WAN) enables quick and secure connectivity with the Tally server for multiple users, allowing employees working from home to use residential internet to access Tally installed in the head office.



Works With
Any ISP



Multiple Virtual Work
From Home Servers



2x Scalable



Encryption: DES, 3DES
192, AES (128 & 256)



Message Integrity:
SHA-1, SHA256,
SHA 384, SHA512



Daily Digest
Reports



Geo IP Filter



High Availability

BENEFITS

- Avoid using Terminal Server, Remote Desktop Protocol, Virtual Desktop Interface, Client Access Licenses
- No plugins are required in the Tally server
- Remote employees can connect using ADSL, broadband, mobile internet, or a hotspot
- Only authorised users are permitted to access the Tally server
- Automatic load balancing & failover for multiple ISP links
- Monitoring of Work From Home clients with alerts



K7 CONSULTING SERVICES

K7 Consulting Services provides assured compliance and threat defence for enterprise customers. With over 912,500 man-hours of expertise in threat discovery, malware investigation, and attack remediation, K7's consultants have the tools, skills, and perspective required to fortify the cyber defences of enterprises that combine 24/7 operations, multi-platform infrastructure, and multi-jurisdiction compliance requirements.

K7 CYBER DEFENCE ASSESSMENT (K7 CDA)

K7 Cyber Defence Assessment delivers a start-from-scratch reimagination of enterprise cybersecurity, with a clear, actionable roadmap to progress from the current state to the desired end state by revamping three elements of cybersecurity.

GOVERNANCE

Tabletop Exercise

- ▶ Policies
- ▶ Procedures
- ▶ Protocols
- ▶ Standards

VULNERABILITY IDENTIFICATION

Hunt and Detect

- ▶ Assess
- ▶ Test
- ▶ Review

THREAT RESPONSE

Security Resilience Framework

- ▶ Evaluate
- ▶ Strategise
- ▶ Enhance

BENEFITS

- Continuous security posture improvement
- Derisk operations
- Improve compliance
- Improve cybersecurity ROI



K7 RED TEAM ASSESSMENT (K7 RTA)

The K7 Red Team Assessment simulates real-world cyberattacks to identify vulnerabilities in an organisation's internal and external cybersecurity posture and evaluate the organisation's ability to detect, respond to, and contain threats.

FRAMEWORK

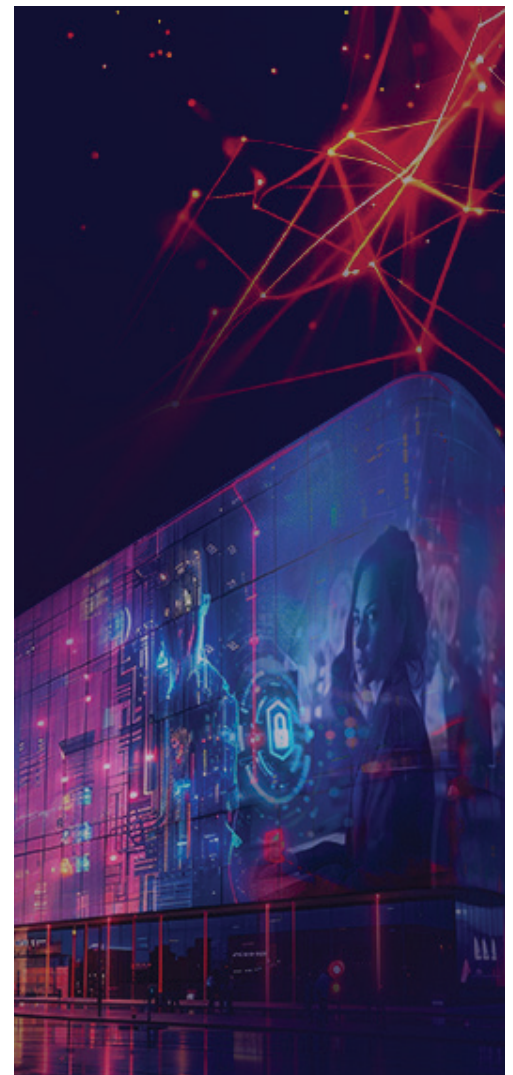
- External assessment
- Susceptibility simulation
- Internal assessment

COMPONENTS



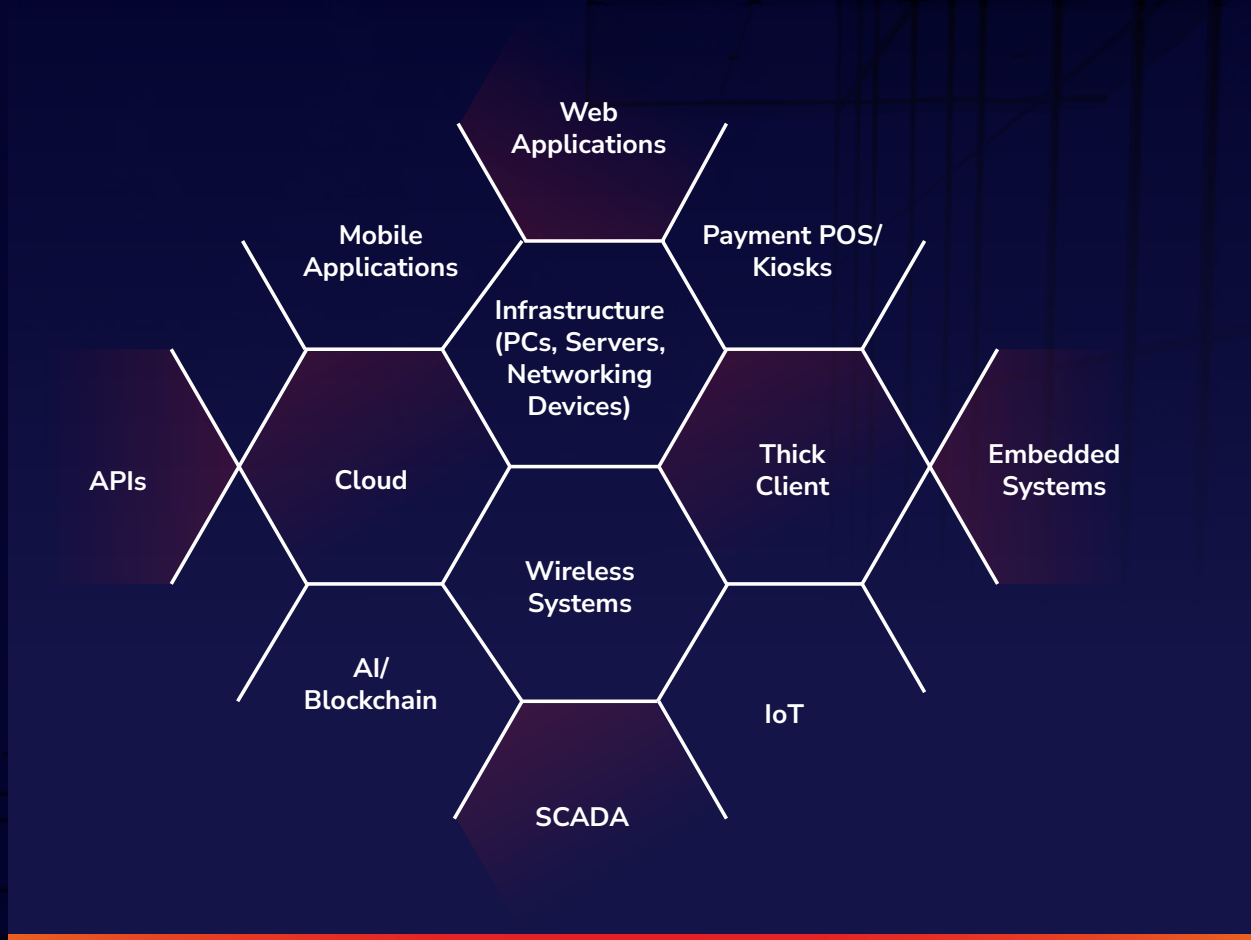
BENEFITS

- List of identified vulnerabilities with CVSS score, CWE ID, and OWASP category
- Elaboration of exploitation techniques with purpose, target system, and impact
- Recommendations to mitigate efficiencies and improve security posture
- Technical and executive debriefs that aid future security efforts
- Guardrails to ensure business continuity is maintained, with zero-risk/restoration assurance



K7 VULNERABILITY ASSESSMENT AND PENETRATION TESTING (K7 VAPT)

K7 VAPT provides forensic investigation of enterprise cyber defences utilising white hat hacker attacks on the various elements that comprise enterprise IT ecosystems.



K7 GOVERNANCE, RISK, AND COMPLIANCE CONSULTING (K7 GRC)

K7 GRC analyses an organisation's digital infrastructure, processes, and compliance through the twin lenses of meeting team- or function-specific requirements and achieving enterprise-wide strategic objectives.

INFRASTRUCTURE

- Information security audits
- VAPT
- Digital communication integrity verification
- Bring Your Own Device (BYOD) and Shadow IT risk assessment

PROCESS

- Industry best practices adherence
- Hardware and software lifecycle management
- Business continuity management

COMPLIANCE

- Finance – PCI DSS, SAMA, Central Bank Compliance
- Healthcare – ADHICS, NABIDH
- ISO – ISO 9001, ISO 22031, ISO 27001
- Data Protection – GDPR

BENEFITS

- ISO/IEC 27001 compliant reports
- Allows management to focus on core operations
- Increase in productivity from avoiding cyberattacks
- Reduction in fixed payroll costs
- Reduction in Mean Time To Remediation
- Reputational boost from avoiding data breaches
- C-suite guidance on improving cybersecurity posture
- Increased customer trust leading to greater wallet share

TESTIMONIAL

“

We pride ourselves on maintaining the highest standards in the transfer of funds as even a single mishap will destroy customer trust. In pursuit of this goal, we engaged K7 Cyber Security to audit our compliance with CBUAE's IT guidelines on Business Continuity Management and Information Security. We are extremely pleased with the approach, methodology, and professionalism demonstrated by the team from K7 and appreciate the comprehensive and well-structured audit report that was submitted.

”

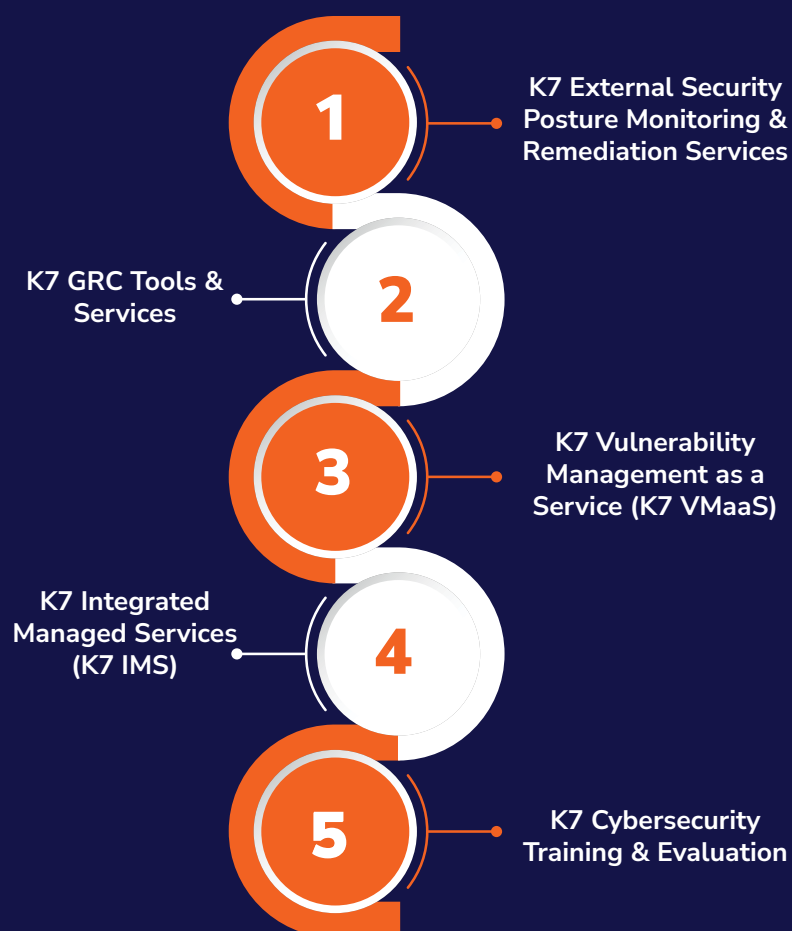
Arun Henry

Hadi Express Exchange

K7 INFORMATION SECURITY ASSURANCE PROGRAMME (K7 ISAP)

K7's Information Security Assurance Programme encompasses a framework of policies and procedures covering legal, physical, and technical controls to identify threats and mitigate vulnerabilities in real time by using specialised AI, automation, and gamification-based technology, to achieve a state-of-the-art cybersecurity posture.

COMPONENTS



BENEFITS

- Secure environment for business operations
- Relief from InfoSec operational concerns
- Periodic reports
- Compliance matrix with intuitive dashboard
- Contractually defined SLAs and KPIs



K7 INTEGRATED MANAGED SERVICES (K7 IMS)

K7's Integrated Managed Services provides a multi-tier, multi-tenant platform that overcomes the deficiencies of conventional static, or occasionally revamped, enterprise cybersecurity by providing continuous monitoring of the organisation's digital ecosystem, leveraging the MITRE ATT&CK framework and UEBA to create a perpetually elevated cybersecurity posture.

FRAMEWORK

Raw Logs: OS, Applications, Services, Processes



Router and Switch Flows: Netflow, IPFIX, sFlow and Raw Traffic



User: Windows AD, DNS, DHCP, LDAP



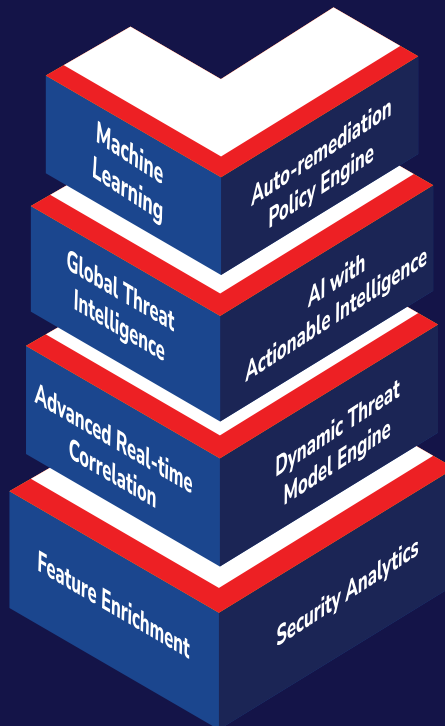
Cloud Logs: IaaS, PaaS, SaaS, Audit, VPC, Identity



Existing Security System: Events and Alerts



Endpoint Agents: Laptops and Mobile Devices



Comprehensive Visibility



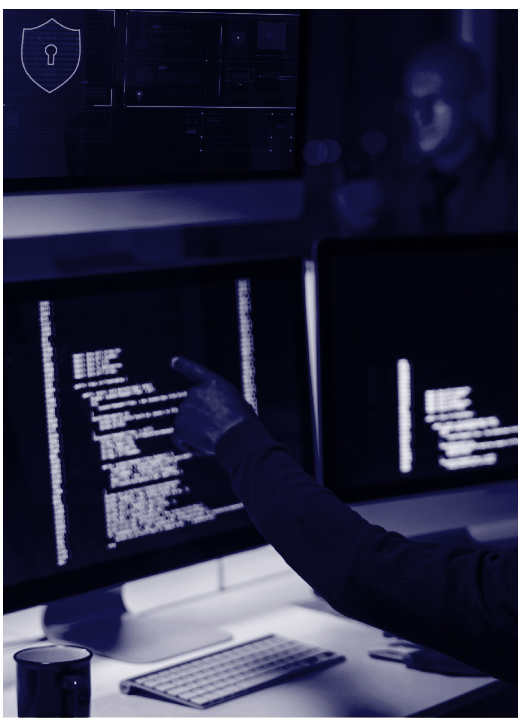
Proactive Threat Detection



Automatic Real-Time Threat Containment & Elimination



Continuous Compliance & Reporting



BENEFITS

- Easy integration
- Reduction in human error
- Complete visibility
- Reduction in Mean-Time-To-Identify (MTTI) and Mean-Time-To-Response (MTTR)
- Capex and opex savings



India | Singapore | UAE | USA

The Global Cybersecurity Pioneer