



K7 SECURITY

K7 IMS

Integrated Managed Services ensure
Perpetual Cybersecurity Posture Improvement
to Combat Perpetual Threat Landscape Evolution

www.k7computing.com

Perpetual Digital Innovation is Accompanied by Potential Digital Destruction

The computing revolution has led to continuous disruptive innovation fuelled by digital-first, data-hungry business processes that create opportunities to unlock value through sophisticated data analysis. New products and services are arising from the new perspectives gained by analysing enterprise data, leading to more data gathering and further innovation.

The acceleration in digitisation has been accompanied by a surge in cyberattacks as threat actors adopt the same technologies, and even similar business models, that legitimate businesses use, to unleash large scale digital destruction on organisations and even nations. Threat actors and threat defenders are locked in a perpetually escalating arms race which is driving up cybersecurity costs.

K7 Integrated Managed Services

Perpetual Cybersecurity Posture Improvement

K7 Integrated Managed Services (K7 IMS) 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, delivering a perpetually improving enterprise cybersecurity posture that can stay ahead of the rapid and relentless evolution of the cyberthreat landscape.

All elements of enterprise digital infrastructure, including on-premises, cloud, remote functions, legacy equipment, and operational technology, benefit from dynamic, AI-enhanced, cyberthreat protection that leverages the MITRE ATT&CK framework and UEMBA to create a perpetually elevated cybersecurity posture.



Framework

Complete visibility into cyberthreats across the enterprise requires gathering data across all digital touchpoints. K7 IMS has been engineered to receive and process inputs from all constituents of the organisation's digital infrastructure, ensuring comprehensive security across all potential points of entry that may attract the attention of threat actors.

Raw Logs: OS, Applications, Services, Processes



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



User: Windows AD, DNS, DHCP, LDAP



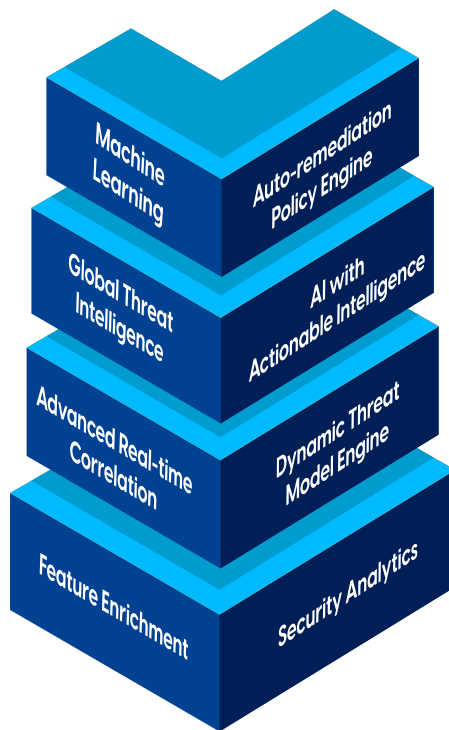
Cloud Logs: IaaS, PaaS, SaaS, Audit, VPC, Identity



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

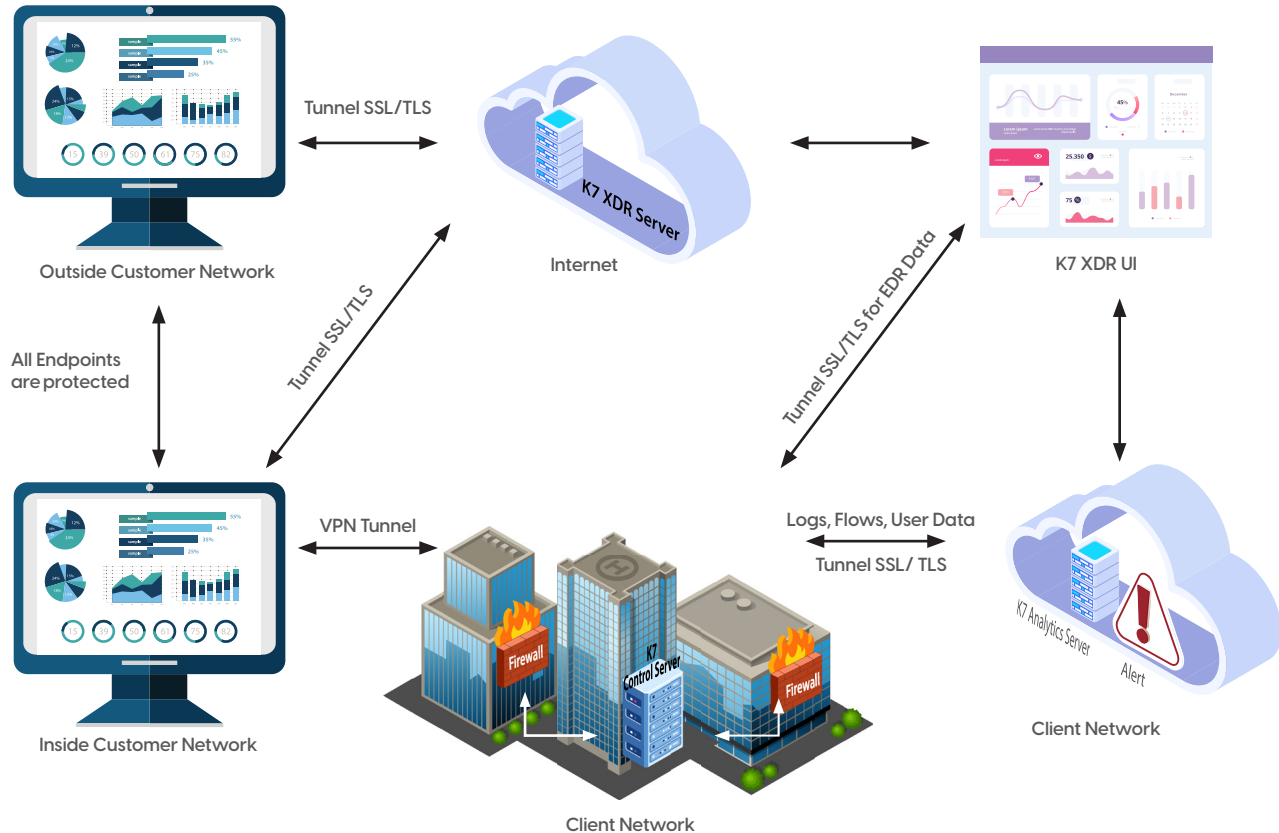
Assured SLA- and KPI-driven Information Security



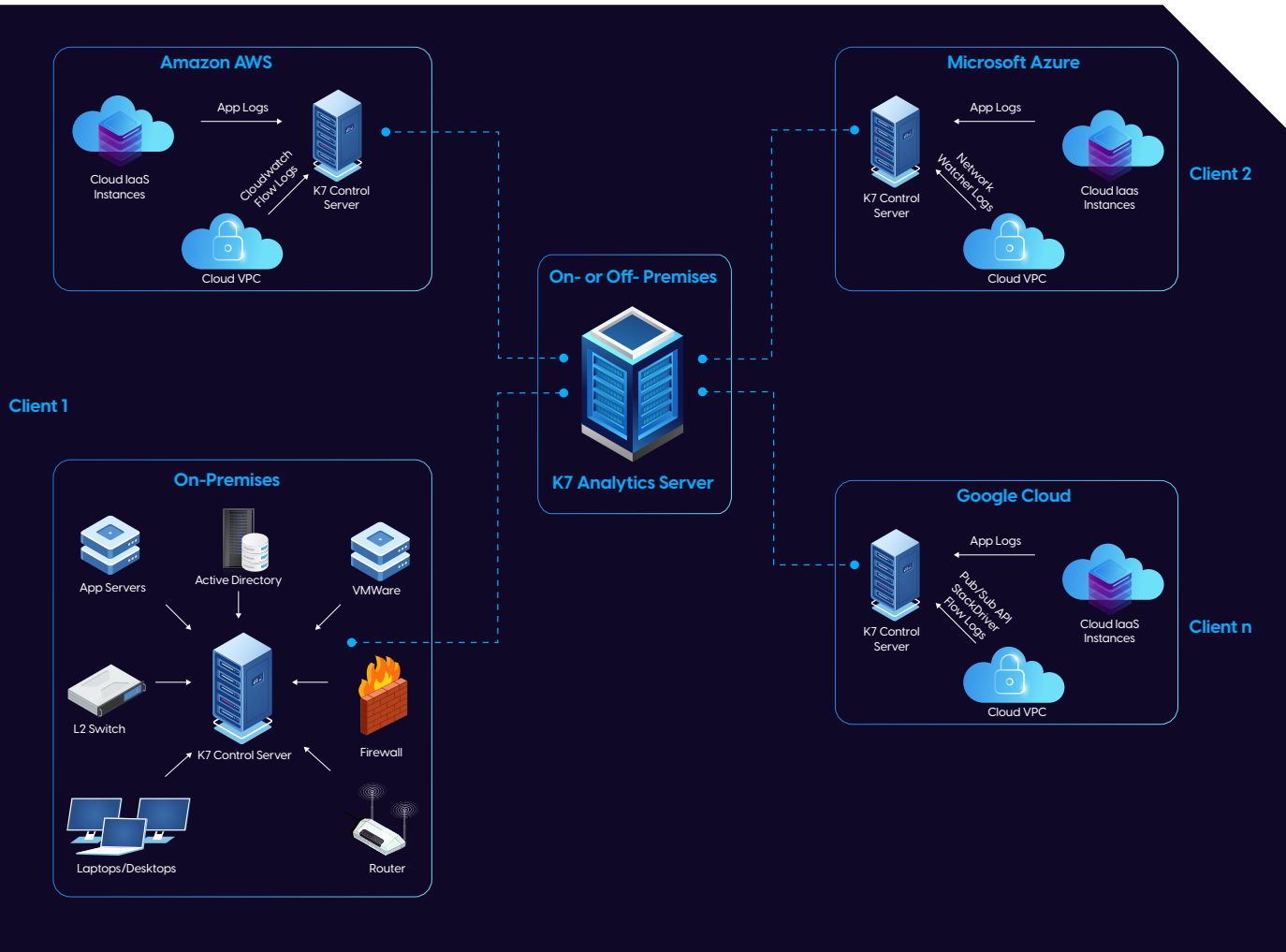
Architecture

K7 IMS has been designed to integrate all enterprise digital assets across on-premises, cloud, and remote workspaces, providing comprehensive cybersecurity for the 24/7, work-from-anywhere enterprise.

K7 IMS XDR Deployment Architecture



K7 IMS MSSP Deployment Architecture



Features

K7 IMS leverages K7's multi-decade expertise in cybersecurity to incorporate features that deliver comprehensive protection against current and future cyberattacks integrated with compliance, helping security teams secure business operations and avoid regulatory scrutiny.

Threat Protection

Cyber Crime

- Ransomware
- Malware
- Spyware
- APTs
- Potential infiltration
- Botnet detection
- Trojan activity

Vulnerability Exploits

- Unknown
- Known OS
- Apps
- Firmware
- Vulnerability assessment

Email Exploits

- Spam
- Business email compromise

Insider Threats

- Malicious insider
- Compromised credentials
- UEBA
- Privilege misuse
- Suspicious login

Brute Force

- Password spraying
- Dictionary attack
- Credential surfing

DNS Attacks

- DNS tunnelling
- DNS fast fluxing

Denial of Service

- Volumetric
- Application layer
- Protocols
- ICMP
- Amplification
- SYN Attack

Web Exploits

- SQL injection
- Cross-site scripting
- Local file inclusion
- Directory traversal
- Remote file execution
- Cross-site request forgery

Other

- Data/IP exfiltration
- IoT/IIoT cybersecurity
- OT/ICS cybersecurity
- Detect IT mistakes
- Detect Shadow IT
- NBAD
- IDS/IPS

Platforms, Policies & Compliance

Policy Enforcement

- Limit access to critical assets
- Stop unwanted connectivity, applications
- Segment and segregate networks
- Proactively identify multi-stage, multi-vector malware/ ransomware

Platform Security

- IaaS
 - AWS, GCP, Azure
- SaaS
 - O365
 - Azure AD
- PaaS
- CASB
 - API-based

Compliance

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



COMPLIANCE

The background of the slide features a person in a dark suit and tie. Overlaid on this are several white icons: a scale of justice, a checklist, a document with a pencil, a hand holding a checkmark, a gear with a checkmark, a gear with an exclamation mark, a head with a question mark, and a stack of books. A large, rounded rectangular box with the word 'COMPLIANCE' in bold white capital letters is centered on the right side of the image.

The K7 Advantage

K7 IMS delivers significant simplification of enterprise cybersecurity management, with state-of-the-art technology that offers unparalleled real-time threat detection and response. Asset-based licensing offers cyber defence-in-depth with substantial cost-savings. Combined with capability that only K7 can offer, K7 IMS provides an unmatched value proposition to the enterprise seeking assured cyberthreat protection.

Cybersecurity Management Benefits

Effort Minimisation: Machine Learning enabled platform reduces human intervention

Single Dashboard: Threat detection and remediation in one solution

Relevant Notifications: Only reports threats that have been analysed and confirmed

Boundaryless Protection: Secures computing assets that are not connected to the enterprise network

Dual Scope: Single platform for both protection and compliance

Quick Deployment: Rapid rollout across the organisation

Complete Visibility: Transparency in all data flow and IT asset interaction within/ outside the network

UEBA: Flags and analyses outliers to help identify zero-day attacks

Technology Benefits

Easy Integration: Integrate all digital infrastructure with native connectors

Reduction in Human Error: Automated analytics provide quick and reliable threat assessment avoiding human fallibility

Data Archiving: Log data is securely archived for compliance and forensics, and can be retrieved without complex search queries

Real-time Threat Detection: Threat signals with high data volume and velocity are processed in real-time for proactive threat detection and mitigation

Smart Intervention: AI and ML based threat models analyse logs, threat intelligence, context, anomalies, and scan reports to provide optimum remedial action

Reduction in MTTI/MTTR: Proactive and automatic detection and response reduce Mean-Time-To-Identify (MTTI) and Mean-Time-To-Response (MTTR)

Financial Benefits

Capex Savings: Avoid investment in multiple siloed solutions, such as EDR, SIEM, DLP, etc., and integration of products that are not designed to be compatible

Opex Savings: Avoid expenditure on cybersecurity talent that is hard to find and difficult to retain

Exclusive Capability

Superior Insight

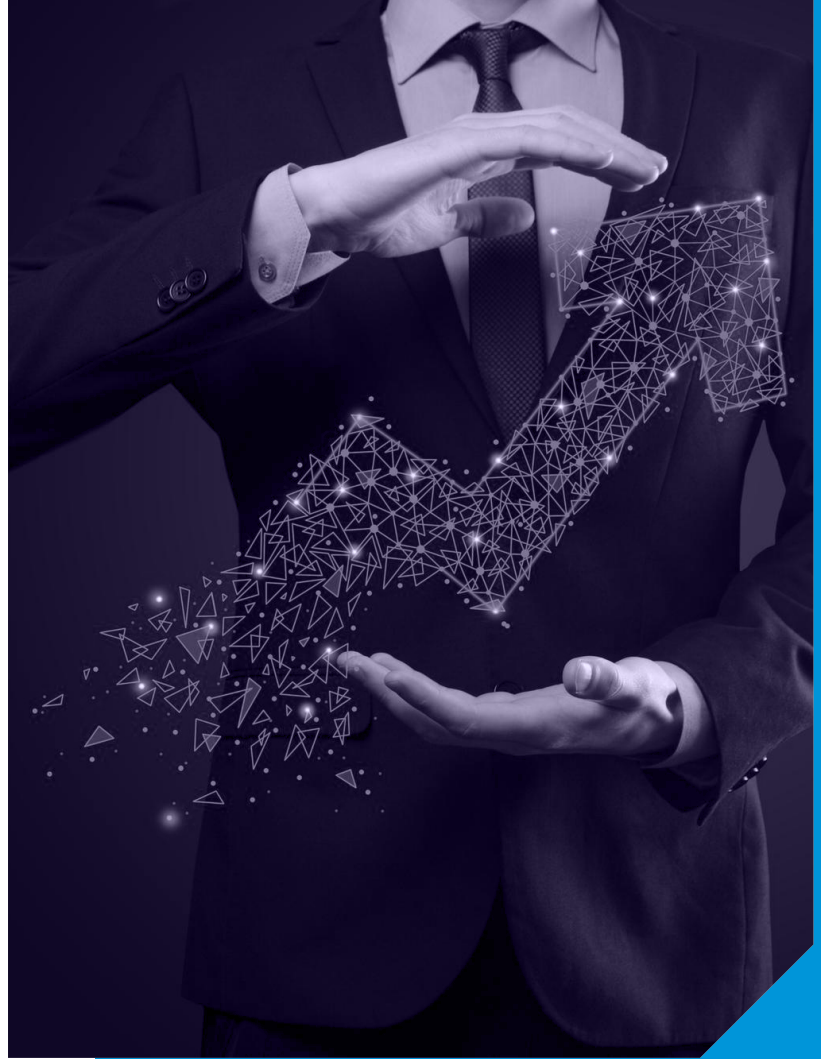
- Discover links between alerts
- Analyse across SIEM, UEBA, NBA
- Trace threat activity timeline
- Quickly understand alert context

ML-Enhanced

- No code implementation
- Prebuilt models
- Easy customisation
- Compatible with any input data

MITRE ATT&CK Framework

- Validate detection coverage
- Protect against APT Groups
- Trace progression of attack



Why K7?

30+ Years' Experience in Cybersecurity

K7 was founded in 1991 as a pure play cybersecurity provider. K7 now protects more than 25 million users across 27 countries and has the extensive breadth and depth of cybersecurity expertise required to evaluate and strengthen cyber defences across a wide spectrum of industries.

912,500 Manhours of Expertise

K7's expert team is comprised of cybersecurity specialists who represent 912,500 manhours of expertise in threat discovery, malware investigation, and attack remediation. K7's experts have the tools, skills, and perspective required to analyse enterprise IT as a cyberattacker would and quickly identify vulnerabilities, isolate anomalous events, and respond to threat activity.

Superior Methodology & Processes

The methodology and processes followed by K7's team have been honed across numerous cybersecurity assignments in organisations operating in a wide variety of industries and jurisdictions, and are designed to be insightful, incisive, and actionable, enabling businesses to rapidly improve their cybersecurity posture and satisfy their compliance requirements.

K7 Labs

K7 Labs is one of the world's leading antimalware research and threat intelligence centres. The lab analyses hundreds of thousands of malware samples every day, 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 Organization (AMTSO). K7 Labs' state-of-the-art research facility enables in-depth investigation of, and the development of countermeasures against, any cyberthreat the modern enterprise might face.





India | Singapore | UAE | USA

businessenquiry@k7computing.com

www.k7computing.com

