

K7 CYBER SECURITY

K7 InfiniShield

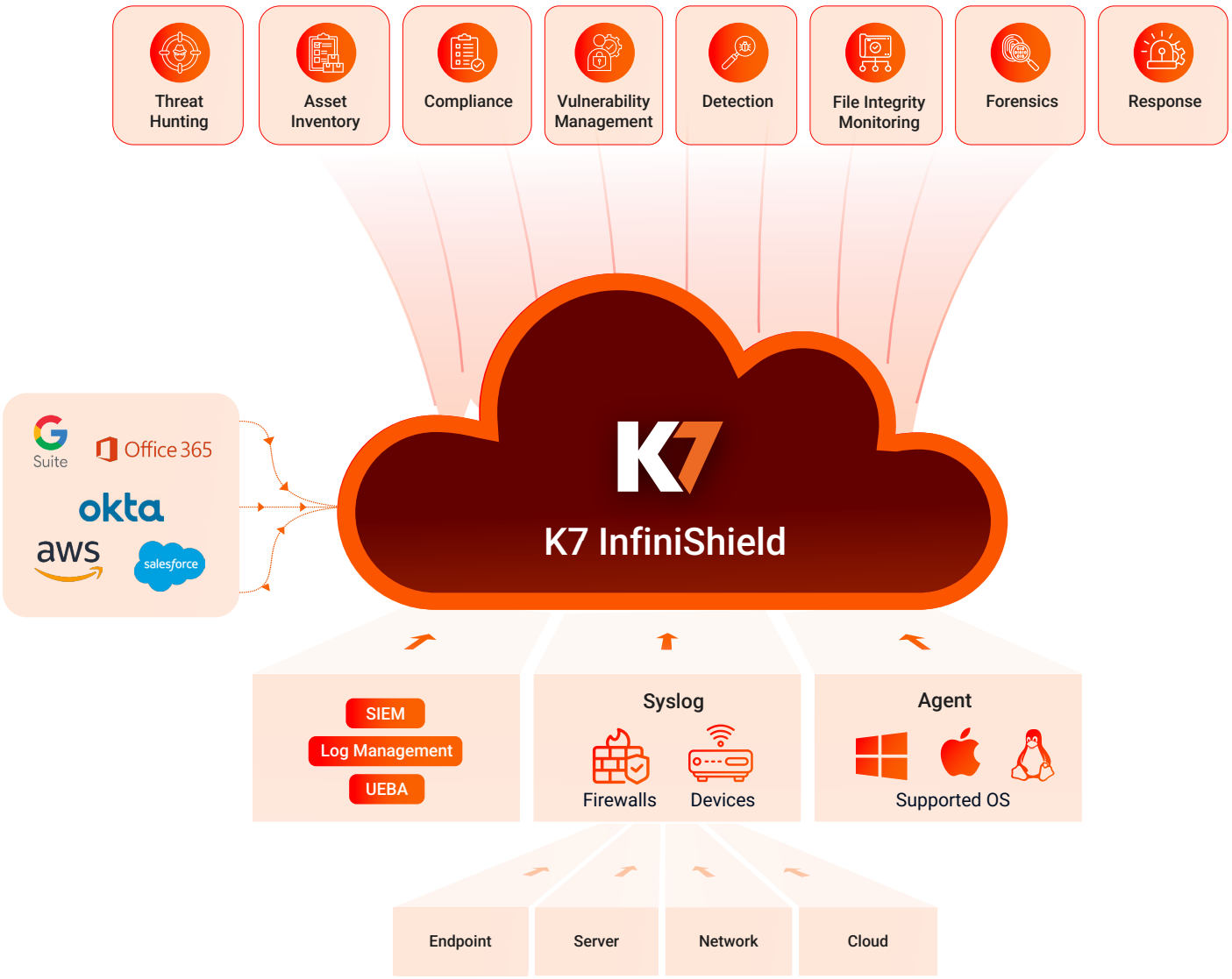
Unified Platform for Extended Defence with
Unparalleled Security, Observability, and Compliance

Enterprise cybersecurity is a patchwork of diverse solutions from multiple vendors that increases the cost and complexity of cybersecurity, resulting in gaps in cyber defences and stress on IT teams who struggle to weave together multiple reports and alerts to gain a holistic view of security across the organisation.



K7 InfiniShield – AI-enhanced Unified Platform for Single Pane of Glass Cybersecurity

K7 InfiniShield is a unified platform that integrates enterprise security infrastructure, surfaces relevant threat signals, and delivers timely, contextual alerts to transform the effectiveness of enterprise cybersecurity and ensure compliance.





Unrivalled Fusion of Technology and Services

The 7 Constituents of K7 InfiniShield

K7 InfiniShield transforms cybersecurity by combining multiple cybersecurity components together and delivers

1. A **cloud hosted analytical SIEM** that correlates and enriches data and provides behavioural analytics as well as log management capabilities
2. An **endpoint solution** that captures and streams key events in real-time from devices to the cloud-hosted SIEM
3. **Stream detection and event correlation** to detect malware as well as malicious user and entity behaviour on endpoints as well as in the SIEM
4. An **aggregator** that captures data from network devices and cloud services
5. An **orchestration and operational platform** that can connect to device APIs or servers/workstations to execute jobs as necessary in response to a threat
6. A **browser-based management interface** that allows for sub-second searching and visualisation using an easily understood query language
7. An **operational platform** that allows for endpoint management

K7's Services

K7 InfiniShield includes Managed Detection and Response (MDR) that delivers a perpetually improving enterprise cybersecurity posture that can stay ahead of the rapid and relentless evolution of the cyberthreat landscape.

Cybersecurity specialists from K7 provide

- 24/7 threat monitoring, threat hunting, and analysis
- Incident response and remediation
- Security Information & Event Management (SIEM) integrating data from any source
- Anomalous behaviour detection through User and Entity Behaviour Analytics (UEBA)
- Attack Surface Management (ASM) for comprehensive visibility, monitoring, and control over an organisation's digital footprint
- Vulnerability management to prevent attacks and harden infrastructure
- Network/Cloud Services monitoring
- Customised reports to track SLAs and KPIs



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 to create a perpetually elevated cybersecurity posture.

Enterprise Cyber Defence – Without Equal!

Comprehensive Security, Seamless Protection

Cybersecurity should be exhaustive, not exhausting. K7 InfiniShield collects security event information from every element of enterprise digital infrastructure, and correlates across endpoints, network, cloud, Active Directory, logs, email, identity data, users, jobs, and dashboards to surface threats.

Security teams no longer need to sift through mountains of data and can focus their efforts on high-impact initiatives and preventive and remedial action.



Dashboards



Managed XDR



Cloud SIEM



AI Assistant



Incident Response



Threat Hunting



Log Management

Benefits

- Quick, easy deployment with no additional hardware/VM footprint
- Sensor-driven unified platform enables proactive identification and mitigation of security gaps across the attack surface
- Single dashboard view of, and search across, all cybersecurity assets
- Native forensic capabilities enable in-house analysis, with artefact collection across online and offline endpoints
- Reduction in Mean-Time-To-Identify (MTTI) and Mean-Time-To-Response (MTTR)

Highlights

- Fully managed SIEM with integration of proprietary EDR and third-party data from any source
- Comprehensive log management with analysis of real-time and archived logs
- AI-enhanced real-time threat detection
- AI Assistant providing context-based retrieval and accurate answers with relevant references
- Automated threat containment and mitigation
- Global threat intelligence feeds from K7 Labs
- MITRE ATT&CK based threat detection
- Cloudflare integration delivers automated detection of WAF blocks, bot activity, and DDoS attacks

Superior Visibility Delivers Superior Insight

Single-pane view of enterprise digital infrastructure including endpoints, networks, applications, devices, processes, APIs, cloud, file access, browsing history, and remote access ensures attack surface management with no dark zones and delivers quick identification of threats that would otherwise be invisible.



Alerts



Graph Explorer



Analytics



Asset Inventory



Continuous Monitoring



Behavioural Analytics



Infrastructure



Network



Application Logs



NVIDIA GPU Monitoring



Distributed Tracing



Cloud



User Activity



Cloud File Storage

Benefits

- Immediate notifications for critical issues enable rapid incident response
- Trend monitoring identifies patterns and supports resource requirement projections
- Customisable dashboards and visualisations help security teams monitor problematic areas without compromising their across-the-enterprise view
- Cloud Security Posture Management (CSPM) identifies and eliminates cloud misconfiguration

Highlights

- Customisable dashboards
- Comprehensive asset inventory
- Network monitoring
- Vulnerability monitoring with patch management
- Anomalous behaviour detection through User and Entity Behaviour Analytics (UEBA) and continuous behaviour profiling, with Mimecast integration to mitigate human risk
- Data lake with extensive cybersecurity event information storage facilitates incident analysis



Intelligent, Scalable Security Management

Intelligent automation and customisable playbooks help security teams orchestrate response and minimise human error at any scale of operations. Deploying cybersecurity and backing up data is simplified with endpoint discovery and integration.

Reports

Integration

Playbooks

Integrated Ticketing

SOAR

Infrastructure Management

Remote Access

Live View

Benefits

- Comprehensive SOAR capabilities with integration across endpoints, networks, and the cloud, and support for agentic AI, improve security team effectiveness and efficiency
- Extensible with APIs and scripting engine for deep customisation
- Marketplace for sensors facilitates integration of cybersecurity solutions from diverse vendors

Highlights

- Automatic location and execution of saved jobs, with explicit confirmation, based on user intent
- Customised reports with CSV, YAML, and JSON exports from within generated reports
- Authorised remote shell access from a browser
- Session sharing and collaboration without 3rd party tools
- Integrated ticketing for quick issue resolution



Enhanced Compliance, Zero Hassle

Avoid scrutiny and penalties with automated compliance against multiple regulations.

File Integrity Monitoring

Compliance Tracking

Benefits

- Simplified compliance across jurisdictions
- Define organisation-specific regulatory criteria

Highlights

- Continuous file integrity monitoring
- Alerts when files are copied to drives, transferred, or renamed
- Inbuilt templates for major standards and regulations
- Recommendations to improve compliance automation

Unmatched Capabilities

K7 InfiniShield's host-based agents can also act as **collectors,** enabling event capture without additional hardware appliances.

AI Assistant ingests data from a wide variety of sources, enables context-based information retrieval, and understands user intent to automatically execute saved jobs.

Customers can select one or more of the agents as **log aggregators** and forward data (flows and logs) from their devices (routers, switches, etc.) to the aggregators to monitor the network.

K7 InfiniShield leverages **APIs** to integrate with an expanding number of cloud services and K7 works with customers to integrate any custom services and/or applications that provide APIs.

Logs, enriched on-premises, are sent to the K7 InfiniShield cloud (subject to transfer limits, expandable) over an an encrypted tunnel where they are further enriched and reside for 30 days and can be accessed via APIs or a rich user interface.

Analysts can access all of the data, including alerts and reports, in the K7 InfiniShield cloud using an **easy-to-use query language.** Visual widgets allow analysts to easily interact with the data, build and download reports, and create customised dashboards.

K7 InfiniShield's SIEM **ingests data in real-time** from a wide variety of sources, including host-based, network, and cloud services. Integration with Active Directory and DNS servers minimise false positives. A flexible pipeline allows ingestion of custom logs. Lookback assessment is enabled through analysis of 6 months of historical Microsoft Entra ID/365 logs.

The platform provides behavioural analysis via

- Behavioural Detection through instrumentation on the endpoint
- Behavioural Analytics using historic and real-time logs ingested into the K7 InfiniShield SIEM. This module is customised for each organisation after an initial baselining period

Sensor-based **Data Loss Prevention (DLP)** scans content for sensitive data via regex, tracks file access, and alerts security teams on access or transfer.

K7 InfiniShield leverages an operational platform to **automate responses** to high fidelity alerts. K7 works with the customer and their installed technologies/APIs to determine response playbooks.

K7 InfiniShield stores 30 days of logs (subject to log volume, expandable) for immediate results. A flexible query language allows for easy **searching, visualisation, and analytics.**

Powered by the World #1 in Performance

K7 InfiniShield is powered by K7's proprietary scan engine that performs AI-assisted threat evaluation and blocking at the endpoint, delivering attack protection at the edge and avoiding the delay in communicating with the cloud for routine security activity.

The K7 scan engine is renowned for its efficiency and is proven to protect without impacting device performance.

Why Choose K7 InfiniShield?

Increased SOC Efficiency & Productivity
Automates and optimises security processes to reduce manual effort.

Faster Threat Detection & Response
Correlates data across multiple layers for rapid, accurate attack identification.

Improved Threat Hunting
Delivers deeper visibility and advanced analytics for proactive threat mitigation.

Reduced Alert Fatigue
Consolidates and prioritises alerts to cut through noise and minimise false positives.

Automated Incident Response
Orchestrates and accelerates remediation actions to contain threats in real time.

Enhanced Security Posture
Unifies endpoint, network, cloud, and email security for end-to-end protection.

Better Compliance & Reporting
Centralises security insights to simplify audits and regulatory adherence.

Eliminates Security Blind Spots
Integrates and analyses data across the entire attack surface for complete visibility and observability.

Service-Level Agreement
Maintains availability of 99.9% each month, excluding scheduled maintenance.



Why Choose K7?

Unparalleled Expertise

K7's principals have responded to several of the largest incidents in the world, supported CERT-IN, and led investigations and remediation efforts in the GCC and India.

Wide Industry Exposure

K7's clients span several sectors, including finance, retail, telecom, media, technology services, maritime, university, legal, and government.

Superior Trust

K7 has helped harden the servers of Indian defence to prevent infiltration.

Superior Knowhow

K7 has been involved in various research and development efforts aimed at assuring compliance and automating threat detection.



About K7 CyberSecurity

Cybersecurity is built on trust, and we believe trust must be earned through accountability. We develop our own security technology, continuously strengthen our capabilities, respond when threats evolve, and stand behind the outcomes we deliver. K7 CyberSecurity functions as a single vendor who provides complete, intelligent, and customer-centric security that answers to you.



K7 CYBER SECURITY

Security That Answers To You

www.k7cybersecurity.com

© 2026 K7 Enterprise Security Private Limited. All Rights Reserved.

20261029l