K7 SECURITY

DATA SHEET

K7 Endpoint Security

for Operational Technology

Operational Technology and industrial computing assets are the backbone of manufacturing and other industries that rely on physical processes. Combining digital technology with mechanical and electrical systems delivers greater efficiency and enables superior control over the production process, but allows digital threats to impair physical systems.

Maintaining the integrity of production processes and the security of manufacturing data are essential for the long-term viability of production plants, but security systems must not impact production through excessive consumption of computing resources.

Enterprise-Grade Anti-Malware

K7 Endpoint Security for Operational Technology provides comprehensive real-time multi-layered protection against viruses, ransomware, phishing, zero-day attacks, and many other cyberthreats, backed by K7 Labs' analysis of hundreds of thousands of threat samples every day.

Multi-industry Cybersecurity Expertise

K7 Security's cybersecurity solutions have been successfully deployed across Manufacturing, Oil & Gas, Defence, Research, Healthcare, Communications, BFSI, and other security-sensitive must-run industries that form part of critical national infrastructure.

Performance Optimised Endpoint Security

K7 Security's solutions have been engineered to minimise resource consumption, and successfully protect SCADA systems running on 1 GHz processors, thin clients with less than 1 GB of RAM, and operations in remote locations with just 24 kbps connectivity.

Centralised Management

K7 Endpoint Security for Operational Technology supports centralised management with SIEM integration, empowering CISOs with control of IT and OT cybersecurity across multiple facilities and regions.

Multi-console Administration

Enterprises with multiple production facilities or those that utilise independent networks require autonomous cybersecurity management for each organisational subdivision. K7 Endpoint Security for Operational Technology supports multiple consoles, allowing multiple admins to independently and simultaneously manage and maintain cybersecurity in their subdivisions.

Add-on Servers

K7 Endpoint Security for Operational Technology supports deployment of add-on servers that act as secondary K7 web servers which link endpoints in branches to the primary K7 web server at headquarters, conserving bandwidth utilisation by avoiding the need for multiple endpoints to link directly with the primary server.

Legacy Device Protection

Operational Technology systems often rely on legacy computing devices that are particularly vulnerable to cyberattacks as they have reached end-of-support. K7 ensures protection of such legacy industrial assets with wide platform support extending to Windows XP.

Offline Updates

K7's offline update facility enables high-security isolated intranets to receive program enhancements and malware definitions using data storage devices, enabling air-gapped industrial systems to gain updated cyberthreat protection while avoiding the risks associated with internet connectivity.

Key Features

- Low-cost, high-performance protection for Operational Technology endpoints
- Detect and mitigate real-world threats such as viruses, spyware, ransomware, hacker intrusions, and phishing attacks in real time
- Granular Firewall with integrated HIDS to block targeted system-level attacks
- Device access protection against USB propagated malware threats
- Optimised performance and small memory footprint extends the useful life of older systems
- Create and enforce consistent endpoint security policy across desktops and servers
- Centralised control and granular enforcement of website access based on pre-defined categories, including gambling, adult-related content, hacking tools, and more
- Centralised application control policies block unwanted or harmful applications
- Detailed reports on applications, devices, and threats can be generated in Excel and PDF formats
- Enterprise Asset Management tracks all endpoint hardware assets on the network, generates reports, and sends notifications on changes
- Effortless migration process. K7 will uninstall any existing product and install itself automatically

Multi-layered Protection

K7 Sentry – On Access/On Demand Scans - On-access and on-demand scanning technology identifies and blocks both known and unknown malware objects before they impact computing devices

Heuristic Malware Detection Technology – Complementing traditional signature-based detection, heuristic detection uses behavioural analysis to proactively identify and block unknown malware in addition to zero-day exploits.

Ransomware Protection - Ransomware protection monitors the behaviour of potentially-suspicious processes, especially any process that writes to certain target file types and blocks attempts to change them.

K7 Firewall (HIDS/HIPS) – Proactively Block Threats - Host-based firewall with an integrated Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS) protects against direct application and system-level attacks.

K7 SafeSurf – Secure Online Browsing - Protects endpoints from internet-based malware infections and drive-by-download attacks by using heuristic URL analysis and cloud-based website reputation services

K7 Device Control – Eliminate USB and Storage Media Infection - Block access to unknown and unauthorised USB storage devices which may contain a malware payload. Set host level policies to enforce device password access, file execution, and on-demand or automatic device scanning configurations

K7 Application Control – Block Unauthorised Applications – Implement a centralised policy to control unwanted applications installed on endpoints. Instant messengers, BitTorrent clients, or other bandwidth intensive applications can be blocked from running or accessing the network, or denied internet access

K7 Web Filtering – Block Unauthorised Content – Centralised policy definition and enforcement of restrictions on access to unauthorised or inappropriate content. Web filtering covers thousands of predefined websites grouped by category and blocked continuously or at scheduled times

Key Security Platform Support

Endpoint
Both 32- & 64-bit architecture, except XP

- Microsoft Windows XP (SP2 or later)[32bit], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 (SP1 or later), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019

Server Console
Both 32- & 64-bit architecture

- Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019

Salient Features

- Protection augmented by Artificial Intelligence
- Smart Firewall with Integrated HIDS/HIPS
- Block Application Network/Internet Access
- Detect Viruses, Spyware, and Phishing Attacks
- Web Filtering (Website Blocking/Filtering by Category)
- Centralised Management
- Rootkit and Ransomware Detection
- USB Device Access Protection/USB Vaccination
- Multiple Daily Malware Definition Updates
- Vulnerability Scanning
- Block Devices based on Class ID/Device ID
- Security Information and Event Management (SIEM) Integration

About K7 Security

K7 Security develops endpoint and server anti-malware solutions for small, medium, and enterprise-class businesses, offering a broad range of features and capabilities to counter today's most destructive cyberattacks. K7's Endpoint Security for Operational Technology supports centralised management to simplify deployment, streamline IT operations, and meet both internal and external compliance requirements.

K7 Cyber Security FZCO M2 - Ali Saif Al Mansoori Business Center, M Floor,
Arzoo Building, Next to Al Twar Centre, Al Qusais 2, Dubai, UAE
Phone: + 971563672864 | www.k7cybersecurity.ae.

July 2023

© 2023 K7 Cyber Security FZCO, All Rights Reserved.