Krypton
Endpoint Security

Endpoint Security (EPS) Enterprise

More Secure and More Advanced

Our Endpoint Security solution provides complete protection for all endpoints with advanced cybersecurity technology. It goes beyond traditional antivirus to detect, prevent, and respond to modern threats, ensuring business continuity with simple management and reliable performance.

Why is Krypton Endpoint Security Important?

The rapid growth of digital transformation, remote work, and internet usage has significantly expanded the cyber-attack surface. Traditional security methods are no longer sufficient to protect modern business environments from evolving cyber threats.

Every device connected to a corporate network—desktops, laptops, servers, or mobile devices—can become a potential entry point for cybercriminals. As the number of endpoints continues to grow, securing them has become one of the most critical challenges for organizations.

Krypton Endpoint Security protects this frontline by delivering centralized visibility, control, and advanced threat protection. Through a unified management console, administrators can easily monitor, manage, investigate, and respond to security incidents across the entire network.

Organizations can choose the deployment model that best fits their business needs:

On-premise

Localized control through an in-house management server.

Cloud

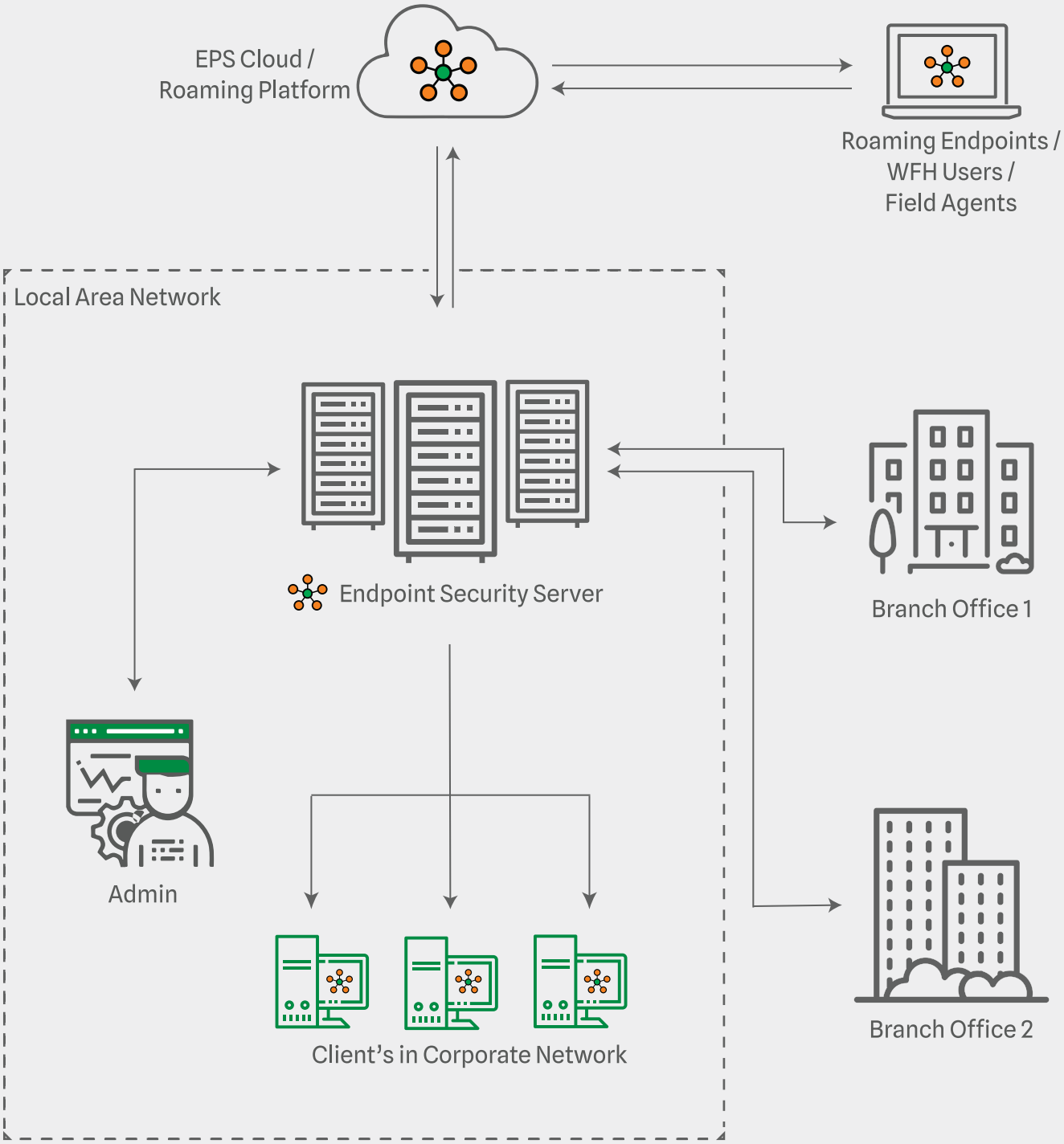
Secure, cloud-based management ideal for remote and mobile workforces.

Hybrid

A flexible combination of on-premise and cloud for maximum adaptability.

With Krypton Endpoint Security, businesses gain stronger protection, simplified management, and the confidence to operate securely in today's dynamic digital landscape.

Krypton Endpoint Security (EPS) Network Flow Diagram



Key Features of Krypton Endpoint Security (EPS)

Cloud Based Endpoint Security Console

Cloud-Based Endpoint Security Console enables administrators to securely manage and monitor all endpoints from anywhere. With reliable, device-independent access, IT teams can control security operations through any internet-enabled PC, laptop, tablet, or mobile device ensuring flexibility without compromising security.

Advanced Device Control

Advanced Device Control enables organizations to securely manage and monitor the use of workstations, USB devices, Bluetooth, and other removable media. With centralized policy enforcement, offline protection, and detailed activity tracking, businesses can prevent data leakage and maintain full control over endpoint device usage.

Centralized and Real-time Administration

Centralized and Real-Time Administration provides a web-based management console with a unified view of all endpoints. Through an intuitive dashboard, administrators can monitor security health, threat activity, vulnerabilities, and update status in real time enabling faster decisions and stronger security control.

Application Control

Application Control enables organizations to centrally manage and control applications across all endpoints. Administrators can allow, block, or terminate applications, deploy software and patches, and remove unauthorized third-party application ensuring a secure and compliant IT environment.

Multilayered Protection

Multilayered Protection delivers comprehensive defense against viruses, malware, ransomware, and emerging cyber threats. With dedicated shields for web threats, phishing, malicious websites, and adware, it ensures secure browsing while optimizing system performance and conserving bandwidth.

Data Backup

Data Backup ensures critical business data is securely backed up and centrally managed from the server. By protecting data from ransomware, corruption, and accidental loss, it helps organizations maintain business continuity and recover quickly from security incidents.

Anti-Phishing

Anti-Phishing protects users from fraudulent websites and deceptive links designed to steal credentials and sensitive information. By blocking fake login pages and malicious URLs in real time, it helps organizations prevent data breaches and financial fraud.

Easily Manage & Control Network Protection

Easily Manage & Control Network Protection allows administrators to monitor all protected and unprotected endpoints from a single console. Launch scans, deploy updates, and ensure comprehensive security across the network—simplifying management and strengthening overall pro

IDS/IPS

IDS/IPS (Intrusion Detection & Prevention System) actively monitors network traffic to detect and block malicious activities targeting application vulnerabilities. It provides real-time alerts for threats like port scanning and DDoS attacks, helping organizations safeguard their network and maintain business continuity.

Data Loss Prevention

Protect your organization's sensitive information with comprehensive Data Loss Prevention. Our solution continuously monitors confidential and user-defined data across removable media, network channels, and web applications. It captures real-time endpoint snapshots during potential data breach incidents, giving security teams clear visibility and actionable insights. This ensures stronger compliance, faster response, and reduced risk of data leakage across the enterprise.

Firewall

Firewall provides robust protection by monitoring inbound and outbound network traffic. Administrators can easily define and manage rules based on IP addresses, ports, applications, and more—ensuring secure and controlled network access.

System Tune-Up

System Tune-Up is a smart, user-friendly utility that keeps your computers running at peak performance. It optimizes speed, repairs registry issues, and frees valuable disk space by removing unnecessary files. With automated scheduling and monthly disk checks, it ensures reliable, hassle-free maintenance for professional environments.

Session Activity

This feature provides centralized visibility into user sessions across all managed endpoints. It records key events such as log-in, log-out, remote desktop access, system start, and shutdown activities. With simple configuration from the EPS admin console, organizations can strengthen security, improve compliance, and maintain full accountability of endpoint usage.

Vulnerability Scanner

Safeguard your business with a smart, user?friendly security solution that continuously scans every endpoint, server, and roaming device across your network. Our Vulnerability Scanner pinpoints weaknesses before they become risks, giving your IT team clear, actionable insights to strengthen defenses, maintain compliance, and protect sensitive data. Designed for corporate environments, it delivers enterprise?grade protection with simplicity and confidence.

Low disk space email alert

Stay ahead of storage issues with proactive low disk space alerts. Our solution notifies administrators instantly via email and WhatsApp, ensuring uninterrupted operations and minimizing downtime. Simple, reliable, and designed for enterprise efficiency.

File Sharing Activity

File Sharing & Activity Monitoring feature provides real-time visibility into file access across managed endpoints. It securely tracks and logs user activity, capturing details such as user identity, file name, and client IP address. This helps organizations protect sensitive data, ensure compliance, and quickly detect unauthorized or suspicious file access.

User Activity Monitor

Track user browsing and application activity in real time to enhance security, productivity, and compliance across your organization.

Patch Management

Simplify vulnerability management with centralized patching for Microsoft and third-party applications. Ensure systems stay secure, up to date, and compliant with minimal effort across your enterprise.

Printer Activity Monitor

Monitor and control printing activity across all managed endpoints with complete visibility into print jobs. Capture essential details such as document name, user, device, time, and copy count to improve security, reduce misuse, and support compliance.

Offline Updates - Weekly

Keep your security infrastructure up to date with weekly offline updates, even in isolated networks. Download updates once and seamlessly distribute them to all endpoints over the LAN—no internet access required—ideal for high-security and regulated environments.

Web Protection

Enhance productivity and security with smart web protection. Block harmful sites, streaming media, and unauthorized downloads—keeping your workforce safe, focused, and efficient

Traffic monitoring

Traffic Monitoring provides administrators with real-time visibility into internet and network traffic. Advanced graphical dashboards make it easy to track usage patterns, identify bottlenecks, and ensure optimal network performance.

Push Installer (Remote Install)

Deploy security agents remotely across your network with ease. Scan for protected and unprotected systems and push installations centrally, saving time and simplifying management for large enterprise environments.

Totally Offline Installation & activation of Server and all Clients

Install and activate the server and all clients completely offline. Ideal for secure or isolated environments, ensuring full protection without requiring internet access.

Remote Data Wiper

It deletes data in selected folders and repeatedly overwrites stored data to prevent recovery using recovery software or forensic image, meaning that it is no longer of any use to anyone. For securely shredding files and folders on the computer using multiple shredding algorithms up to 7 passes.

Disk Encryption

Secure your critical data with comprehensive encryption at the file, folder, volume, and full-disk levels. Even if a device is lost or stolen, encrypted data remains protected and accessible only to authorized users. Easy to manage and reliable, it safeguards corporate information against unauthorized access and data breaches.

Global Threat Intelligence

Stay ahead of cyber threats with Global Threat Intelligence—delivering real-time insights on advanced attacks and strategic guidance to protect your organization.

Advanced protection against file attachments

Protect your business from malicious files with multi-layered security that monitors email, web uploads, network shares, and USB devices in real time.

Advanced ML and AI interaction

Advanced ML and AI-driven protection detects, analyzes, and blocks evolving cyber threats in real time, keeping your business one step ahead.

Endpoint forensic

Endpoint Forensic delivers detailed device-level insights to detect breaches, support threat hunting, and enhance your organization's cybersecurity resilience.

SIEM Integration

SIEM integration centralizes security data from firewalls, antivirus systems, IDS/IPS, and logs into a single platform. This enables real-time monitoring, rapid threat detection, and streamlined incident response, giving your organization a clear, unified view of its security posture. Stay ahead of cyber threats with advanced analytics and actionable insights for proactive defense.

Update manager

Update Manager ensures seamless and reliable delivery of security updates and patches from multiple servers. This keeps your endpoints protected, minimizes downtime, and strengthens your overall security posture with efficient, automated update management.

Asset Management

Gain full visibility into your IT environment with our Asset Management. Effortlessly track hardware, software, and system activity across all endpoints. Monitor changes, optimize resources, and ensure accurate, real-time insights for smarter IT decisions and stronger operational control.

Advanced Memory Protection

Protect your endpoints with multilayered memory defense that detects and blocks ransomware and fileless attacks. Using advanced heuristic analysis, this feature safeguards against sophisticated threats, ensuring your organization stays secure and resilient.

Two Factor Authentication (2FA)

Elevate your security with Two-Factor Authentication. By adding an extra verification step, 2FA blocks unauthorized access, protects sensitive data, and gives your organization peace of mind with stronger, modern account protection.

Network Access Control

Protect your network by ensuring only authorized users and devices gain access. NAC enforces security policies, blocks unauthorized connections, and safeguards your organization from potential threats, keeping your network secure and compliant.

Live Chat and Remote Desktop Viewer

Enable seamless support and communication with one-click remote desktop access, instant live chat, and customizable notifications. Quickly assist users, share critical updates, and maintain smooth operations across your organization with ease and efficiency.

Mobile Device Management for Android

Effortlessly secure and manage all Android devices—mobiles, tablets, and interactive panels—from one intuitive platform. Enforce security policies, control apps, track locations, and remotely wipe data to protect against threats, ensure compliance, and boost organizational productivity.

Password Management

Secure, streamline, and control administrative passwords effortlessly. Remotely set, update, and track passwords across all endpoints with a single click, ensuring strong security, full visibility, and simplified IT management.

Krypton EPS - Product Edition & Feature Comparision

Krypton Endpoint Security Features	Advanced for Business	Total	Enterprise	EDR
Antivirus & Anti-Malware	✓	✓	✓	✓
Anti-Ransomware Shield	✓	✓	✓	✓
Anti-phishing	✓	✓	✓	✓
Email Protection - Spam Protection	✓	✓	✓	✓
Firewall Protection	✓	✓	✓	✓
IDS / IPS	✓	✓	✓	✓
Instant Messaging Protection	✓	✓	✓	✓
OS Vulnerability Scanner	✓	✓	✓	✓
Roaming Platform	✓	✓	✓	✓
Artificial Intelligence	✓	✓	✓	✓
Asset Management - Hardware & Software Change Report	✓	✓	✓	✓
Email/SMS Notification	✓	✓	✓	✓
Web & Browsing Protection	✓	✓	✓	✓
LAN Monitor	✓	✓	✓	✓
Advertise Blocker	✓	✓	✓	✓
Advanced Device Control	✓	✓	✓	✓
SIEM Integration	✓	✓	✓	✓
Data Backup	✓	✓	✓	✓
Application Control - Block List & Safe List		✓	✓	✓
System Tunner		✓	✓	✓
Patch Management		✓	✓	✓
File Activity Monitor		✓	✓	✓
Session Activity Monitor		✓	✓	✓
Web Filtering & Category Control		✓	✓	✓
Password Management		✓	✓	✓
Traffic Monitor			✓	✓
Printer Activity Monitor			✓	✓
Data Loss Prevention (DLP)			✓	✓
YouTube Access Manager			✓	✓
Google Login Management			✓	✓
Live Chat and Remote Desktop Viewer			✓	✓
Disk Encryption			✓	✓
IT Ticket System			✓	✓
Endpoint FastQueryX				✓
Realtime IoC Hash and URL Blocking				✓
Endpoint Threat Scan				✓
Pre-Attack Surface Reduction				✓
Network Service & Process Management				✓

System Requirements

EPS Server

Component	Minimum Requirement
Operating System	**Windows** : Windows Server 2022 / 2019 / 2016 /2012 / 2008 / 2003 **Linux** : Ubuntu 19 and later
Processor	~ 500Mhz or Faster
RAM	~ 4 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates
Additional Software	Dot Net Framework
Internet Connection	For EPS Server System only

EPS Client

Component	Minimum Requirement
Operating System	**Windows** : Windows 11/ 10 / 8.1 / 8 / 7, Vista, & XP **Mac** : macOS 10.12 and later **Linux** : Ubuntu 16.04 and later, RHEL 7.6 and later, Fedora 32 and later, Debian 9 and later, CentOS 7.8 and later, Suse 12.0 and later Boss 7 and later **Android** : Android version 9.0 to 15.0 Mobile Device Management for Android - MDM Mobile, Tablets & Interactive panels
Processor	~ 500Mhz or Faster
RAM	~ 2 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates

Certifications

For free demo visit: www.adminconsole.net

Net Protector AntiVirus
eps@npav.net | 9595306452 | sales@npav.net | 9272707050 | www.adminconsole.net