About

Malware Protection Plus is a Next-gen Antivirus that neutralizes ransomware and prevents malware exploits and breaches with AI-powered scanning and real-time behaviour detection. It utilizes advanced memory scanning and autonomous malware disinfection to remediate zero-day threats and sophisticated threats.

State of the current threat landscape
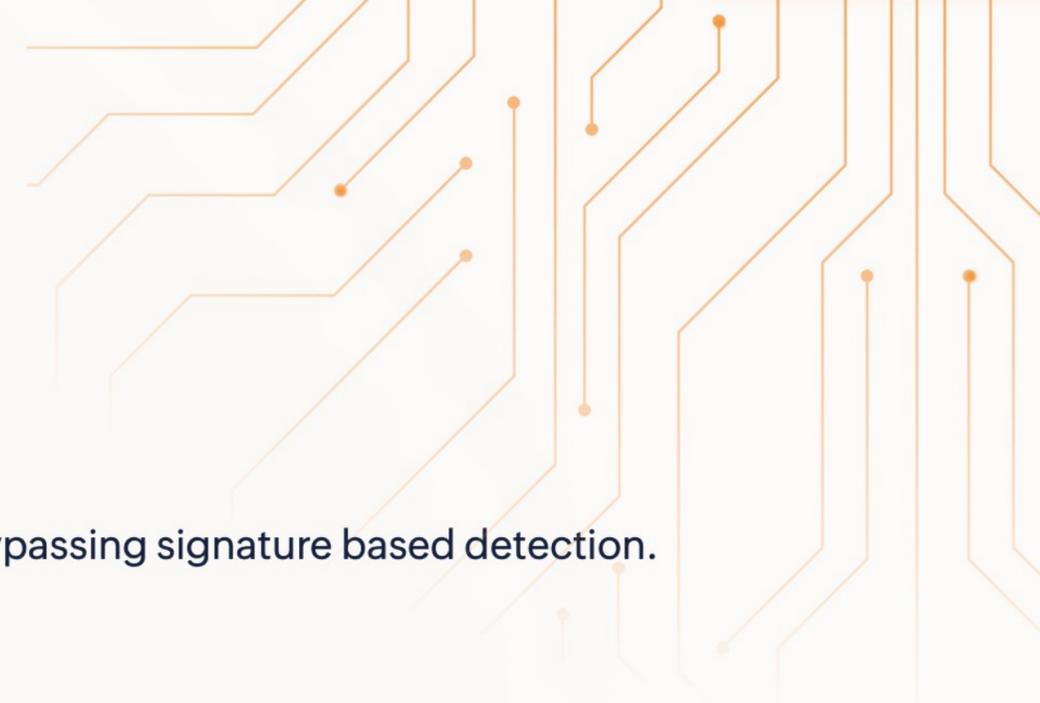
Increased vulnerability to advanced threats

Fileless, memory-based attacks, zero-day exploits, evasive malware can bypass legacy defenses bypassing signature based detection.

Lack of proactive detection and RCA

Without AI-driven detection or deep attack forensics, malware can dwell undetected for weeks or months, leading to massive breaches.

Compliance and Reputational risk

Failure to meet security standards and breaches can lead to damaged reputation, lawsuits and hefty fines.

Higher risk of ransomware attacks

Encryption of critical data and data loss can to business downtime and compliance fines.

Overall higher cost of cyber incidents

Beyond potential ransom payments, the absence of NGAV significantly increases the cost of attack recovery, including forensics and system restoration.

Problem with traditional Antivirus

Reliant only on known threat patterns

Signature-based miss sophisticated threats

Delayed response

Traditional AV depends on periodic updates for spotting new threats.

Ineffective against fileless attacks

No significant protection against in-memory or fileless attacks.

Over-reliance on back ups

Traditional AV lacks the mechanism to secure backups.

Limited offline protection

Traditional AV requires regular definition updates to work seamlessly.

Overview of Malware Protection Plus

AI-powered detection

Malware protection plus utilizes both deep learning and dynamic behaviour analysis to detect and block both seen and unseen malware threats.

Ransomware defense and recovery

Detect and neutralize ransomware attacks and roll back encrypted files to their pre-attack state.

Behaviour and signature based detection

Combine traditional signature-based detection with behavioural AI analysis to identify malicious activity and stop threats—even those without any known signatures.

Advanced memory scanning

Detect highly evasive fileless malware operating in memory that evades traditional disk based scanning.

Self-managed malware remediation

Quarantine and disinfect malware without any human intervention and restore modified files and registries.

Anti-exploit mechanism

Protect process integrity with memory hardening and anti-exploitation techniques ensuring vulnerabilities cannot be exploited by attackers.

Threat detection

Multilayered detection
Identifies and blocks both known and unknown malware threats.

Zero-day & ransomware detection
Detects encryption-based attacks and emerging threats.

Fileless & In-memory attack prevention
Stops advanced evasive malware.

LSASS Protection
Block credential theft attacks.

LOTL Detection
Stop misuse of system tools like PowerShell.

C2 Detection
Cut off malware's communication with attackers.

Threat scanning and investigation

Deep Memory Scanning
Uncover hidden threats in memory.

Predict & prevent attacks
Identify Indicators of Compromise early.
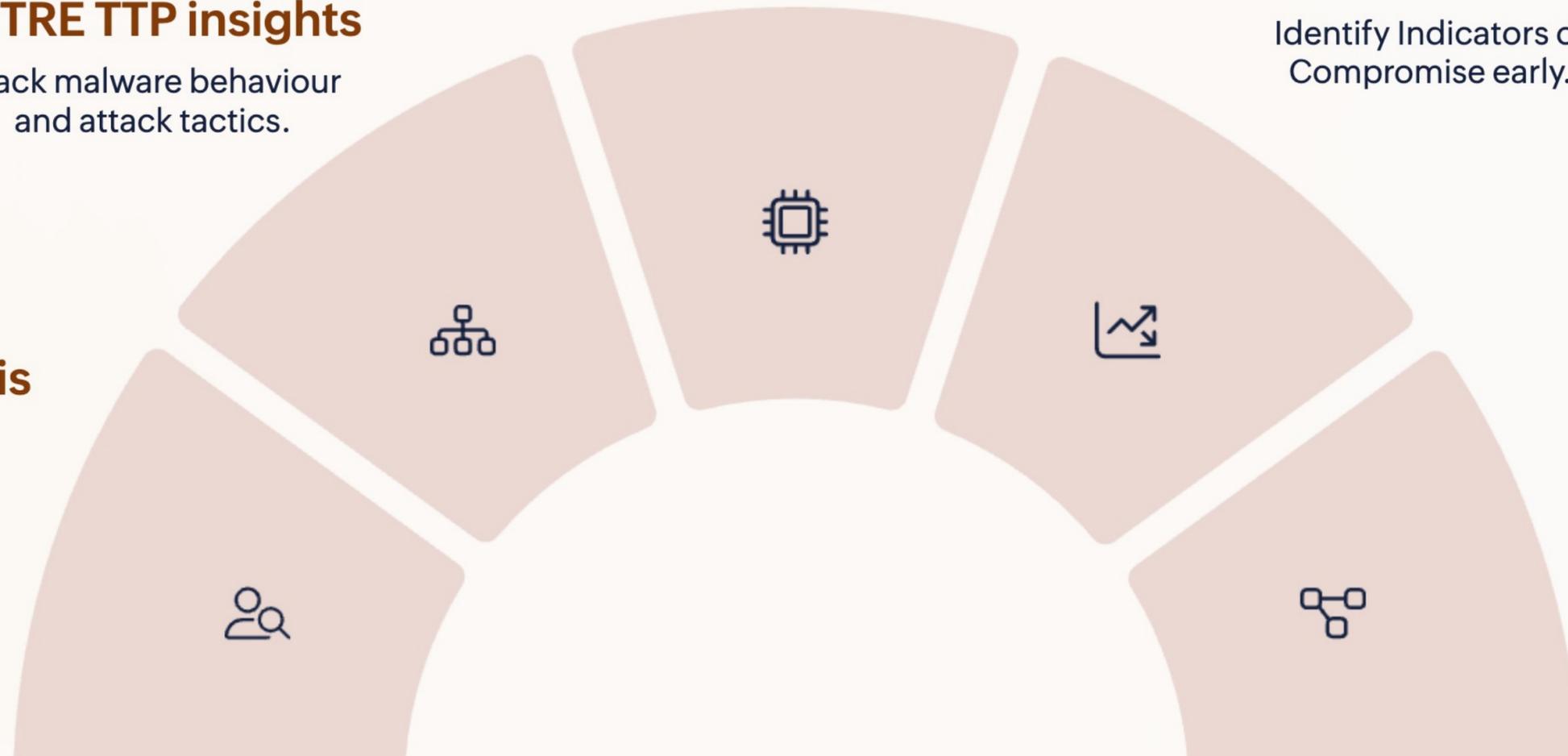
MITRE TTP insights
Track malware behaviour and attack tactics.

Root cause analysis
Uncover how threats infiltrate your system.

Incident correlation
Gain deeper visibility for faster response.

Threat Mitigation

Autonomous Disinfection

Automatically removes malware and restores system files.

Real-time process termination

Stops threats before they can execute.

Exploit protection

Prevents malware from exploiting vulnerabilities.

Ransomware defense

Blocks encryption attempts and ensures fast recovery.

Repeat-attack deterrence

Learns from past attacks to prevent recurrence.

Device isolation

Cuts off infected devices to stop the spread.

Encrypted file recovery

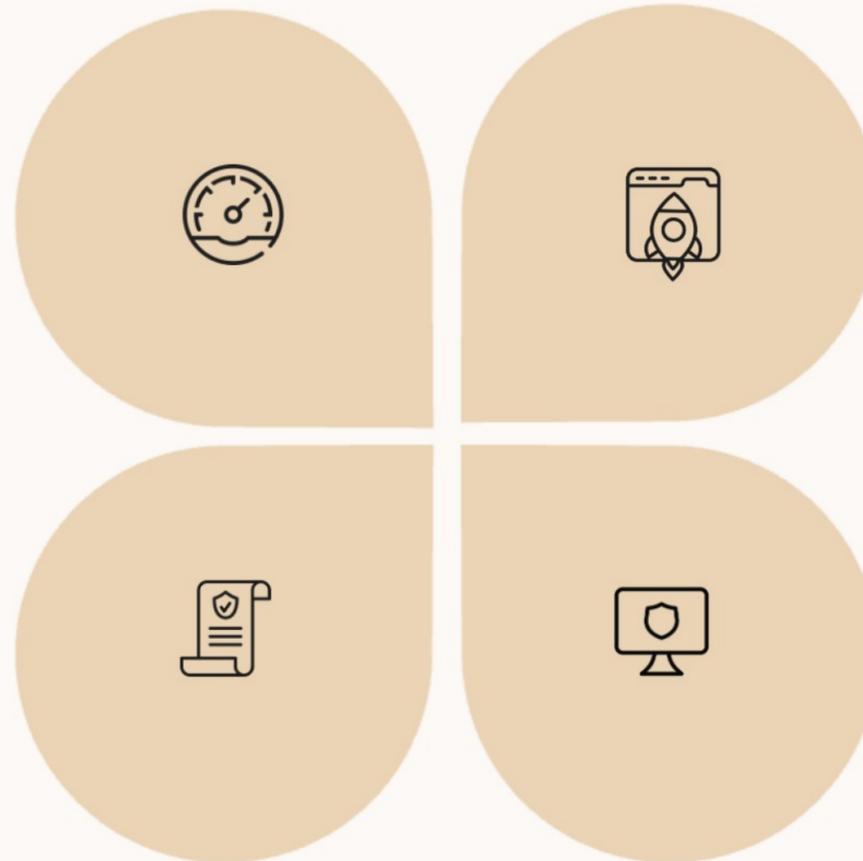Restores systems to their pre-attack state.

What sets Malware Protection Plus apart?

Lightweight agent

Operates invisibly without slowing users with zero performance lag, even during full-system scans.

Easy Deployment

Deploy enterprise-wide protection in minutes. No reboots, downtime, or complex setups are required.

Targeted Policies

Organize security by department for targeted strategies with custom group policies.

Offline Defense

Ensure continuous protection even offline using local intelligence and behavioral analysis.
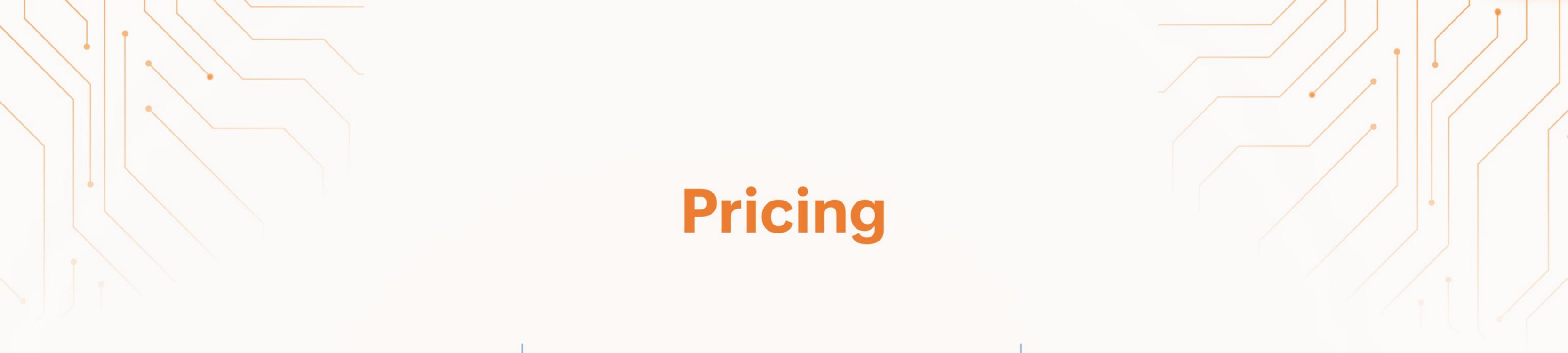
Pricing

$0

Free up to 25 endpoints

$14.99 per endpoint

Billed annually

On-premise

Deployment model

Learn and Explore

Home

Visit our website for detailed product information.

Free Trial

Experience the product with a free 30-day trial.

Get a Quote

Request a personalized price quote for your business.

Personalized Demo

Schedule a personalized demo with our product specialists.

Getting Started

Quick start guides for easy installation and setup.