



ENDPOINT PROTECTION PLATFORM

CatchPulse

If It's Not Trusted, It Doesn't Run.

Because prevention is better than cure.

Something is malicious. Ask whether it's allowed.

Endpoint protection built on a simple premise: stop asking whether



THE PROBLEM WITH DETECTION

Detection Has Always Been the Wrong Game

The Problem: From legacy AV to modern EDR, traditional security plays a losing game: identify the threat, then block it. This logic has a ceiling. Detection requires a threat to be known before it can be stopped.

The Vulnerability: Zero-day exploits carry no signatures, fileless attacks hide entirely in memory, and "living-off-the-land" techniques hijack your trusted system tools.

The Reality: The attack that bypasses your AV isn't more sophisticated. It's just newer.

Features	CatchPulse	Traditional AV
Security Model	Proactive: Zero Trust blocks all unknown files.	Reactive: Only stops known threats.
Zero-Day Defense	Instant protection against brand-new malware.	Vulnerable until an update is released.
Unknown Files	Blocked in Lockdown Mode until approved.	Permitted until threat detected.
Threat Detection	AI multi-engine cloud scanning.	Relies on a single antivirus engine.
IT Management	Simple workflow in SecureAge Central.	High overhead tracking complex blocklists.

BUT WHAT ABOUT EDR?

Different Layer. Different Question. Stronger Together.

EDR asks "is this behavior malicious?" and answers after execution. CatchPulse asks "is this file trusted?" and answers before. They protect different points on the attack timeline. The strongest endpoint posture uses both.

	CatchPulse	EDR	Together
Point in attack	Pre-execution	Post-execution	Full kill-chain coverage
Core question	Is it trusted?	Is it malicious?	Trusted to run, watched while running
Zero-days	Blocked by default	Detected if recognized	Most never execute; residual caught
AI-generated malware	Unknown = blocked	Must match a pattern	Prevention doesn't depend on recognition
Legacy / air-gapped	Full support	Often limited	Coverage where EDR can't run

Aligned to: NIST SP 800-167 | CIS Controls v8 Safeguard 2.5 | MAS TRM §9 | PCI-DSS 4.0

Architected Against AI-Assisted Attacks

CatchPulse's block-first architecture is threat-method agnostic. It does not matter whether an attack was written by a human or generated by AI - if it is not trusted, it does not execute.

Lateral movement: Any process - regardless of how intelligently crafted - is blocked the moment it falls outside trusted policy.

Zero-days: An AI-generated zero-day is still an unknown executable - and unknown means blocked.

THE CATCHPULSE APPROACH

Default-Deny. Not Default-Detect.

Instead of asking "is this file malicious?" CatchPulse asks: "is this file trusted?" If no, it doesn't run. Unknown doesn't mean "scan harder". Unknown means blocked.

CORE DIFFERENTIATOR

Application Control & Allowlisting

01

Take control of what runs in your environment with a zero-trust execution model. Only approved applications are allowed - everything else is stopped before it can pose a risk. Blocks unknown and unapproved executables, scripts, and files at the point of execution regardless of threat signature.

Untrusted - Blocked before execution

Trusted Apps - Run securely

Trusted Installers - Files inherit trust

INTELLIGENCE LAYER

AI-Powered Malware Scanner

02

Traditional scanners only catch what they already know. CatchPulse AI Scanner breaks this cycle by using machine learning to identify unseen malware and mutated ransomware variants from the very first day they are released. It doesn't just respond to threats - it anticipates them.

DETECTION BREADTH

Cloud AV - Multi-Engine

03

Aggregates multiple commercial-grade AV engines for a detection rate no single engine achieves. Runs in the cloud - no local overhead. Protected even when offline; notified of new threats the moment you boot up. Works alongside your existing local AV without conflicts.

RISK VISIBILITY

Vulnerability Assessment Scan

04

Eliminate hidden risks before they're exploited. Vulnerability Assessment automatically scans applications, detects weaknesses, and delivers clear remediation reports - keeping your environment compliant and secure.

TRUST BOUNDARY CONTROL

Restricted Application Policies

05

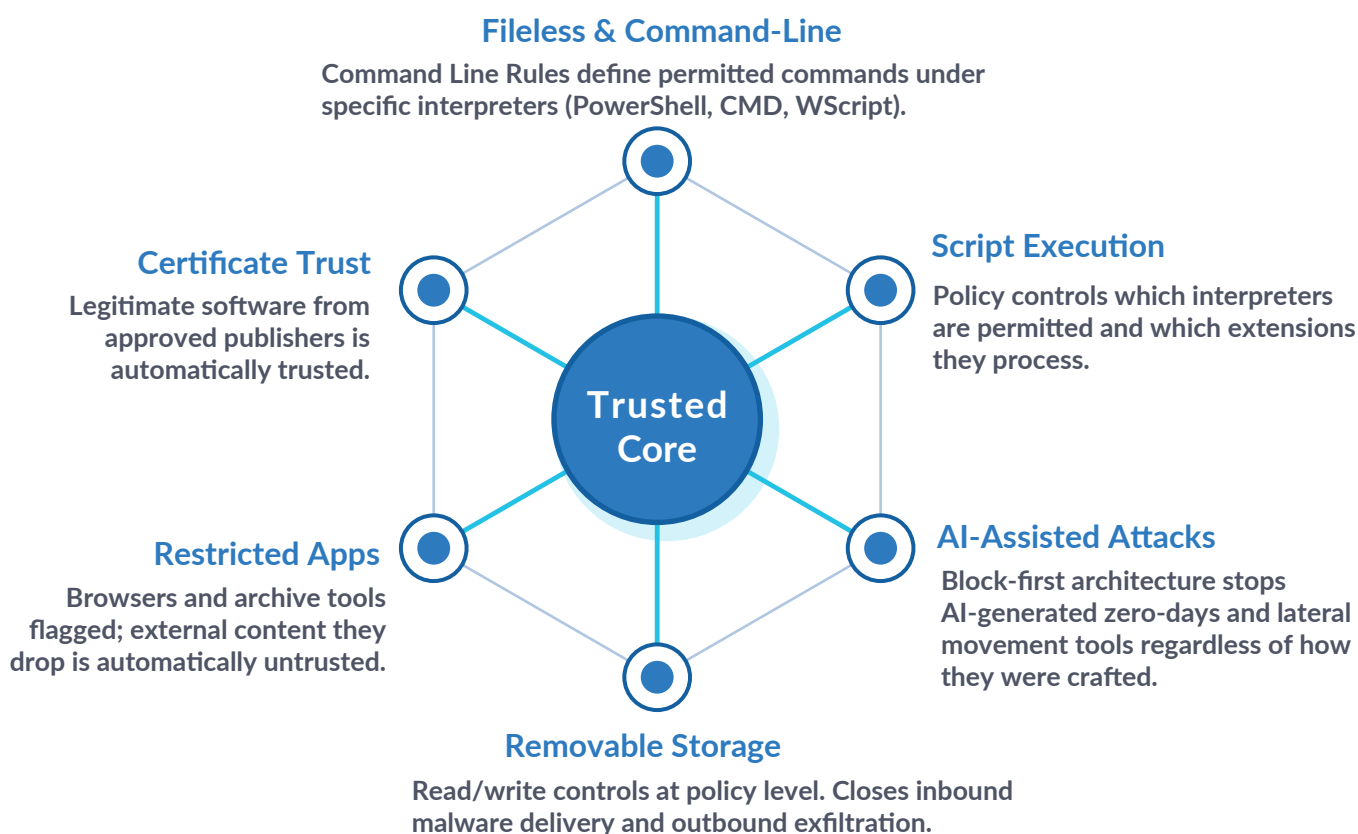
Applications that download external content - browsers, archive tools - can be flagged restricted. Any executable they create is automatically untrusted regardless of claimed identity. Your browser keeps working normally. It just can't vouch for what it brings in.

COVERAGE

The Attack Surface Traditional AV Can't See

Modern attacks don't rely on dropping malicious executables. CatchPulse is built to close the gaps that AV and EDR leave open.

Closing the attack surface traditional AV cannot see.



Built for IT Teams, Not Just Security Teams

SecureAge Central - Management Dashboard

SecureAge Central is the unified management server behind CatchPulse, giving administrators a single pane of glass across their entire endpoint estate. The dashboard surfaces real-time metrics on device health, vulnerability exposure, and malware categories like scripts or executables. This allows IT teams to instantly push policy changes without reboots, providing complete operational visibility without needing a separate management product.

Policy Management

Deploy policies across all endpoints without reboots.

Allowlists Management

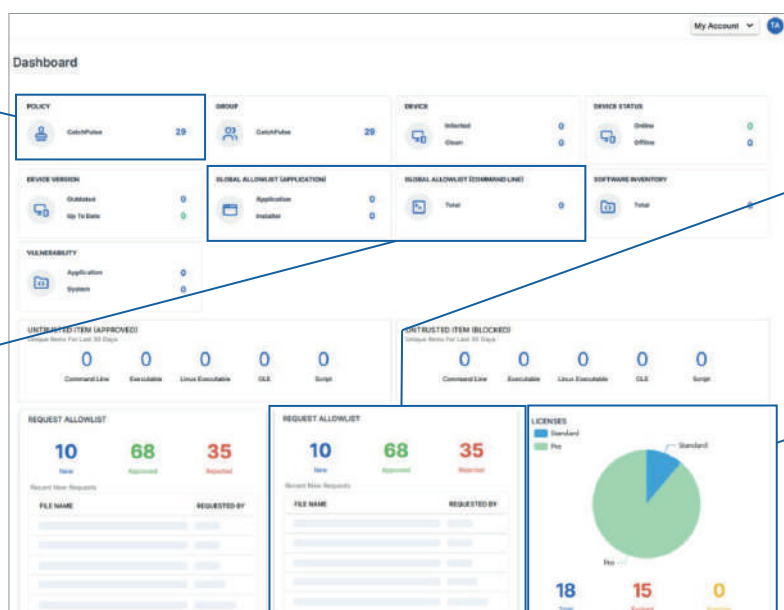
Track and manage allowlists for applications and command line.

End-user Application Requests

A clear dashboard to review requests in real time. Automatically updates local or global allowlists to keep workflows moving without compromising security.

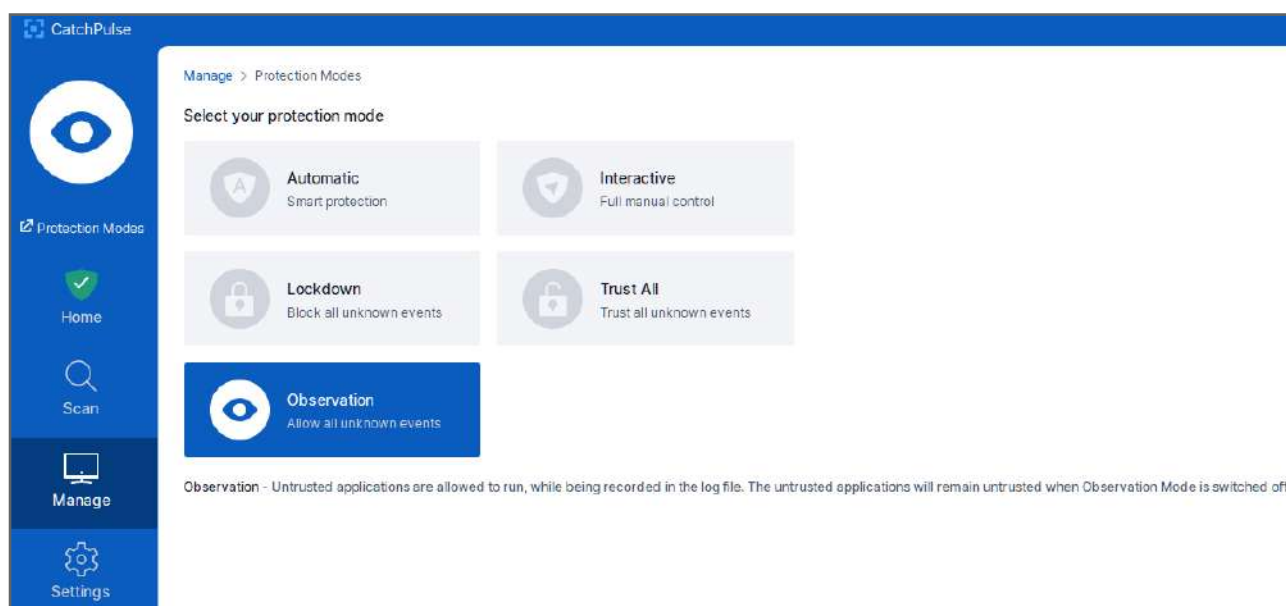
License Utilisation

To review active license counts, monitors expiration dates and deployment volumes to prevent over-purchasing and ensure continuous product compliance.



Exclusive feature: Observation Mode

New deployments don't go live at full enforcement on day one. Observation Mode silently logs and surfaces untrusted activity without blocking it —giving you a clear picture of your application landscape before tightening security controls.



Key Differences At A Glance

Features	Lite	Standard	Pro
AI Engine			
Scan Type	On-demand only	Real-time + Full Scan	Real-time + Full Scan
Application Control	—		
Multi-Device Management			
Dashboard	—		
Device Management	—		
Device Infection Status	—		
Untrusted Item Management	—	—	
Alerts & Activity			
Email Alerts	—		
Allow List Management			
Global Allow List	—		
Allow List Approval Request	—		
Vulnerability Assessment	—	—	
Reporting & Policy Management	—	—	
Trial Duration	—	30 Days	60 Days
Post-Trial	Always Lite	Reverts to Lite	Reverts to Lite

GET STARTED

See the Default-Deny Model in Action

We'll walk through a live demo built around your environment profile - trust levels, rollout sequencing, existing tool integration, and policy design for your specific context. No generic product tour.

3 Fusionpolis Way,
#05-21 Symbiosis,
Singapore 138633

+65 6873 3710
sa.sales@secureage.com

TECHNICAL SPECIFICATIONS HARDWARE REQUIREMENTS

- 2 GHz Pentium 4 or higher processor
- 1 GB RAM or as recommended by Windows OS
- 300 MB hard disk free space or more
- NTFS-formatted local hard disk
- Min. screen resolution: 1024x768 at 100% scale

SUPPORTED OPERATING SYSTEMS

- Windows 11 (64-bit)
- Windows 10 (32-bit & 64-bit)
- Windows Server 2025 (64-bit)
- Windows Server 2022 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2016 (64-bit)

LIMITED SUPPORT

- Windows 7 - Windows 8
- Windows Server 2008 - 2012

Stop Guessing.



CatchPulse

Start Securing.