A PC Development Group AI product

AEGISVAULT AI MANAGED ENDPOINT PROTECTION

Protect Computers with AI Trend Building Guards.

AegisVault AI watches business computers for security, patch, health, and behavior trends, then turns the important signals into technician-approved actions before downtime gets expensive.

Request Onboarding | Download promo PDF

24/7
trend awareness across covered computers

AI
prioritized guards for technician review

Human
approval before sensitive changes

Guard status ACTIVE

Observe
endpoint health

Detect
trend shifts

Approve
safe action

Resolve
show evidence

DATA PRIVACY

Local AI protection without sending customer data to cloud LLMs.

AegisVault AI is powered by local large language models hosted inside PC Development Group's secure business network. Endpoint context stays within the protected environment and is not sent to public cloud AI services or used to train cloud language models.

Hosted locally

AI analysis runs inside PC Development Group's controlled network, not on public chatbot infrastructure.

Firewall protected

The AI environment is guarded by industry-leading firewall controls aligned with cybersecurity best practices.

Used on our own systems

PC Development Group's computers and servers are protected by AegisVault AI too, so the platform is operated under the same security expectations it delivers.

TREND BUILDING GUARDS

Designed to catch the pattern, not just the alert.

AegisVault AI groups endpoint signals into practical guardrails so technicians can see what changed, why it matters, and what action is ready for review.

01

Security posture

Surface antivirus gaps, risky states, missing evidence, and stale protection signals before they become customer-facing incidents.

02

Patch pressure

Track update drift and repeated patch failures with enough context to choose the right remediation path.

03

Computer health

Watch storage, check-ins, performance, and reliability signals that quietly build toward downtime.

04

Approval state

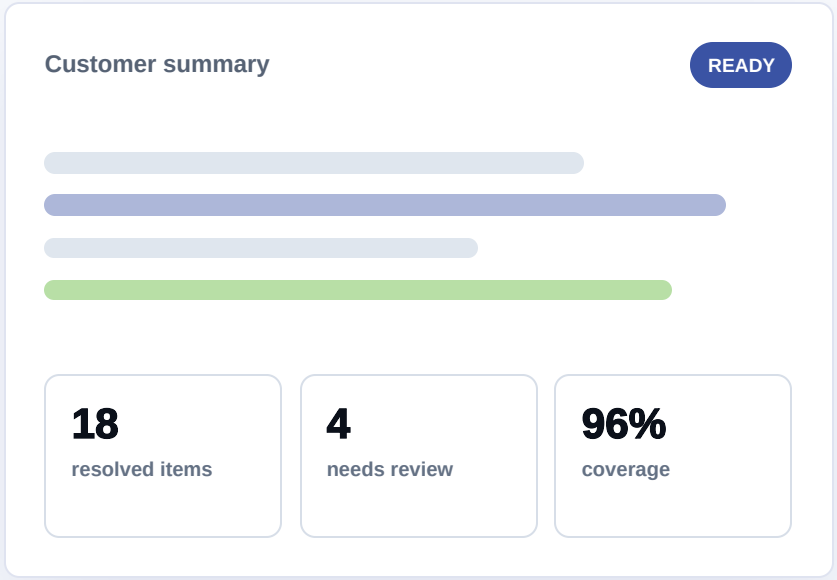
Keep sensitive changes behind a human decision while preserving a clean record of what was approved and why.

CONTROLLED REMEDIATION LOOP

AI narrows the work. Technicians keep the judgment.

The platform focuses attention on the devices and risks that need action, then moves each item through review, execution, verification, and customer-ready reporting.

Watch	Collect endpoint security, patch, and health signals.
Rank	Identify trend changes and prioritize by business risk.
Approve	Route sensitive recommendations for technician review.
Resolve	Run the selected action path and verify the result.
Report	Summarize coverage, fixes, and next steps clearly.



BOARDROOM-READY OUTPUT

Translate technical work into evidence customers can understand.

AegisVault AI keeps reports focused on covered computers, completed protection work, unresolved risks, and recommended next steps. The language stays customer-facing instead of exposing internal tooling details.

Open the promotional PDF

AEGISVAULT AI

Protect the computers your customers depend on.

Request Onboarding

Download PDF